Senato della Repubblica XIX LEGISLATURA

Giunte e Commissioni

RESOCONTO STENOGRAFICO n. 10

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

25ª seduta: giovedì 2 marzo 2023

Presidenza del vice presidente SISLER

INDICE

Audizione di un professore associato di diritto penale

Audizione del direttore amministrativo di RPC SpA

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 professor Roberto Borgogno, professore associato di diritto penale, e, in videoconferenza, il dottor Raffaele Andreozzi, direttore amministrativo di RPC SpA.

I lavori hanno inizio alle ore 9,15.

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.

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

PROCEDURE INFORMATIVE

Audizione di un professore associato di diritto penale

PRESIDENTE. L'ordine del giorno reca il seguito dell'indagine conoscitiva sul tema delle intercettazioni, sospesa lo scorso 28 febbraio.

Sono oggi in programma due audizioni, che saranno svolte separatamente: quella del professor Roberto Borgogno, professore associato di diritto penale, e quella, in videoconferenza, del dottor Raffaele Andreozzi, direttore amministrativo di RPC SpA.

Professor Borgogno, nel darle il benvenuto e ringraziarla per la sua presenza, le ricordo che, a causa dei nostri tempi contingentati, ha circa dieci minuti per un'illustrazione generale cui seguiranno le domande dei commissari alle quali potrà rispondere completando eventualmente il suo intervento.

BORGOGNO. Signor Presidente, onorevoli senatrici e senatori, nel ringraziarvi per questo invito, di cui sono molto onorato, faccio presente che, in qualità di docente all'Università la Sapienza, oggi vorrei trattare qui con voi un argomento che ritengo di stretta attualità, connesso al se-

questro di dispositivi elettronici digitali, come *smartphone* o memorie di *computer*, nei quali siano conservati, come ormai sempre più spesso accade, non solo dati sensibili o ultrasensibili dei proprietari, ma anche tracce e contenuti di comunicazioni fissati su *chat* o *e-mail* conservati in tali dispositivi.

Qui c'è un punto fondamentale sul quale la giurisprudenza di legittimità si è più volte pronunciata, dicendo che in realtà le conversazioni conservate su tali dispositivi non possono essere equiparate a intercettazioni telefoniche, quindi, una volta sequestrate, devono essere trattate come documenti e pertanto possono essere acquisite in qualsiasi procedimento penale sostanzialmente senza limiti.

Un'altra corrente giurisprudenziale afferma che queste conversazioni non possono essere considerate neanche come corrispondenza, quindi non godono nemmeno delle garanzie ad essa riservate. Si dice che le intercettazioni riguardano un contenuto in atto e per la corrispondenza vale esattamente lo stesso, cioè si può intendere per corrispondenza solo la comunicazione nel momento in cui viene inviata ad un certo destinatario e non è ancora pervenuta.

Questa posizione giurisprudenziale, com'è evidente, crea problemi molto rilevanti, perché è chiaro che, attraverso il sequestro di un dispositivo digitale, si può arrivare a conoscere tutta la vita di una persona, quindi si possono acquisire non soltanto dati molto delicati, ma soprattutto conversazioni che risalgono molto indietro nel tempo. Al contrario di quello che accade per le intercettazioni, in cui l'autorizzazione è concessa per un tempo determinato, con il mero sequestro dei suddetti dispositivi, che non è ovviamente circondato da tutte le garanzie previste per le intercettazioni o il sequestro di corrispondenza, il pubblico ministero può prendere conoscenza di una mole enorme di dati e di informazioni.

Qual è, a questo punto, il problema da valutare? La giurisprudenza ultimamente si è confrontata con questi temi, partendo però da un assunto fondamentale, e cioè che il nostro codice di procedura penale, con riferimento al sequestro di tali dispositivi, contiene certamente alcune garanzie, quando il sequestro avviene su iniziativa della Polizia giudiziaria, perché dalla combinata lettura degli articoli 352 e 354 del codice di procedura penale emerge che la Polizia giudiziaria, quando agisce d'iniziativa, deve limitare il sequestro soltanto ai dati effettivamente rilevanti per il procedimento penale in corso, per l'ipotesi di reato che si sta profilando. Si possono sequestrare e assicurare con le procedure previste per la copia forense del dispositivo soltanto i dati pertinenti all'indagine.

Questo però non è previsto – ed è un grosso limite della legislazione attuale – quando invece agisce il pubblico ministero, ovviamente con un decreto motivato, che però può riguardare l'intero dispositivo. In questo caso, a leggere le attuali disposizioni del codice di procedura penale, in particolare gli articoli 254-*bis* e 260, si ricava che il pubblico ministero, attraverso la copia forense, può assicurare al processo l'intero contenuto del dispositivo digitale, con la relativa enorme mole di dati,

che possono riguardare l'intera vita di una persona sottoposta ad indagine.

In realtà, i limiti a quest'attività del pubblico ministero derivano esclusivamente dalla giurisprudenza di legittimità: un suo orientamento più recente si è preoccupato di questa carenza legislativa e, con diverse pronunce, ha cercato di porre dei limiti, dicendo innanzitutto che il sequestro dei contenuti del dispositivo dev'essere ovviamente limitato a quanto è pertinente e proporzionato alle necessità d'indagine, altrimenti il sequestro assumerebbe una finalità puramente esplorativa, cosa ovviamente impossibile, perché vietata dai principi di adeguatezza e di proporzionalità che governano il tema delle misure cautelari reali.

Rimane però un grosso problema, quello dei limiti, dettati dalla giurisprudenza, soprattutto perché attualmente non c'è modo per l'indagato di controllare che vengano effettivamente rispettati. C'è stato un caso molto recente, quello di un'indagine che ha riguardato anche esponenti politici e per il quale tra l'altro recentemente è stato sollevato un conflitto di attribuzione proprio tra il Senato della Repubblica e la procura di Firenze. Il Pubblico ministero ha realizzato il sequestro di dispositivi digitali sostanzialmente senza l'adozione di cautele e limiti opportuni. Tra l'altro, in tale conflitto di attribuzione si propone proprio questo problema, ossia se il sequestro delle conversazioni conservate su dispositivi digitali possa ormai essere effettivamente equiparato a tutti gli effetti a una corrispondenza e quindi debba godere delle stesse garanzie.

Un'importante sentenza della Corte di cassazione del 2020, che si è espressa proprio in relazione a quest'indagine, ha fissato importanti princìpi, che forse meritano di essere ricordati qui: il pubblico ministero, quando esegue la copia dei dispositivi digitali, deve utilizzarla non come copia fine (normalmente si esegue la copia digitale del dispositivo, che così viene restituito all'indagato e il pubblico ministero ne conserva tutto il contenuto, con tutte le opportune garanzie di genuinità e di stabilizzazione dei dati); in realtà, non è così: la copia che il pubblico ministero acquisisce in questo modo è soltanto una copia mezzo, che cioè servirà a stabilire cosa all'interno del dispositivo è effettivamente pertinente all'indagine e deve quindi essere oggetto di sequestro. Questo dovrebbe quindi svolgersi nelle seguenti tre fasi: si sequestra il dispositivo; se ne esegue la copia informatica (la copia mezzo); si eseguono poi una ricerca di elementi utili ed effettivamente pertinenti all'indagine e poi anche la copia mezzo deve essere restituita all'interessato, altrimenti c'è il rischio che questi dati rimangano nella disponibilità del pubblico ministero e diano luogo, se esaminati dalla Polizia giudiziaria o dallo stesso pubblico ministero, ad ulteriori indagini, pertanto il sequestro avrebbe un contenuto meramente esplorativo.

Questo principio molto importante, che è di garanzia, finora è stato espresso soltanto a livello giurisprudenziale con questa sentenza che per il momento non è stata seguita da altre negli stessi termini. Credo quindi che qui sarebbe importante un intervento legislativo per colmare tale lacuna. Come potrebbe essere realizzato questo intervento legislativo? Se-

condo l'opinione espressa in dottrina, che mi pare corretta, probabilmente lo strumento potrebbe essere il contraddittorio già in fase d'indagine fra indagato e pubblico ministero sotto il controllo del giudice, per esempio attraverso l'inclusione di questa fase processuale nell'ambito degli accertamenti irripetibili. Normalmente, si dice che gli accertamenti sui dispositivi digitali possono essere condotti in qualsiasi momento, perché, una volta fatta la copia forense, quello che succede dopo è un accertamento comunque ripetibile; qui invece probabilmente l'esigenza sarebbe quella di dire che, quando si effettua la copia forense di un dispositivo digitale, bisogna che immediatamente si avvii questa fase di contraddittorio, sotto il controllo del giudice, fra indagato e pubblico ministero, perché soltanto i dati pertinenti all'indagine siano acquisiti effettivamente nel fascicolo processuale e tutto il resto sia immediatamente restituito all'indagato, in tempi ovviamente molto ridotti, proprio per mantenere tutte le possibili garanzie.

Attualmente, il codice di procedura penale non prevede che questa fase e questo controllo siano eseguiti in tempi prefissati. Il pubblico ministero in realtà attualmente può quindi trattenere questa copia forense anche per un tempo illimitato, con tutti i rischi connessi alla possibilità che tali dati confluiscano nel processo e siano utilizzati per ulteriori indagini.

La mia idea è che questo sia effettivamente un punto importante e una lacuna da colmare all'interno del codice di procedura penale e probabilmente una linea d'intervento potrebbe essere quella di cui ho parlato. Credo di poter concludere qui questo intervento, precisando che mi riservo di fornire un appunto scritto, anche alla luce del dibattito che si svolgerà.

BAZOLI *(PD-IDP)*. Signor Presidente, desidero innanzitutto ringraziare il professor Borgogno per la sua utile relazione, che tocca un punto che molti auditi hanno sollevato: quello dell'acquisizione dei dati degli *smartphone* e dei telefonini.

Vorrei farle due domande in merito, professore, perché gli spunti che ci ha dato sono molto utili. La prima questione è se ritiene che debbano essere messi anche limiti rispetto alla possibilità di sequestro degli *smartphone* e dei cellulari. Come saprà, nella scorsa legislatura, anche sulla scorta della giurisprudenza delle Corti europee, abbiamo introdotto alcuni limiti per esempio per l'acquisizione dei tabulati telefonici, che non c'erano nel nostro ordinamento. Mi chiedo se, dal suo punto di vista, sarebbe opportuno rivedere la disciplina che riguarda il sequestro di questi strumenti che hanno potenzialmente una grande invasività nella *privacy* degli indagati.

La seconda domanda è se ritiene che si debba applicare anche ai contenuti degli *smartphone* sequestrati la disciplina che obbliga a riversare le conversazioni intercettate nell'archivio digitale elettronico, per evitare la fuga di notizie che riguarda anche la documentazione in essi contenuta.

Siccome altri auditi ci hanno indirizzato verso una riflessione su questo tema, vorrei conoscere la sua opinione.

SCARPINATO *(M5S)*. Signor Presidente, concordo pienamente con le osservazioni del professor Borgogno, che ha toccato un punto che senza dubbio richiede una nuova disciplina legislativa.

Intanto, professor Borgogno, vorrei chiedere preliminarmente se ci può fornire gli estremi esatti della sentenza della Cassazione che ha citato, che è molto interessante.

Per quanto riguarda la disciplina – e qui mi riaggancio all'osservazione del senatore Bazoli – piuttosto che un contraddittorio immediato con la difesa, ritiene possibile replicare, adattandola, la stessa disciplina attualmente prevista per l'archivio digitale delle intercettazioni?

Sulla base dell'esperienza, infatti, le dico che possono esservi dati che sul momento non sembrano rilevanti e che invece, a seguito dell'approfondimento delle indagini, risultano esserlo. Per esempio, una rubrica telefonica può contenere 300 numeri: posso concentrarmi su dieci di essi, ma poi lo sviluppo successivo delle indagini mi fa capire che il trecentesimo numero è essenziale per chiudere il cerchio.

In un primo momento quindi effettivamente non sempre è possibile circoscrivere esattamente gli elementi rilevanti: alcuni è chiaro che non lo sono (come le foto private), ma per altri è difficile. Incamerare quindi nell'archivio digitale dati potenzialmente rilevanti, procedere a una selezione di quelli che poi si rivelano processualmente rilevanti e avere a quel punto un contraddittorio con la difesa, che dalla sua parte può dire quali altri elementi ritenga rilevanti o meno, sotto il profilo processuale, consentirebbe una dialettica più approfondita e più puntuale su cosa è processualmente rilevante o no.

Immagina possibile per le intercettazioni telefoniche ambientali una replica adattativa della stessa disciplina prevista per l'archivio digitale?

RASTRELLI *(FdI)*. Signor Presidente, ringrazio anch'io il professor Borgogno per la presenza, anche perché le sue indicazioni hanno consentito di focalizzare la nostra attenzione sul tema del sequestro dei dispositivi digitali. Noi ci stavamo occupando anche dei captatori informatici ed è di tutta evidenza che ormai una messe impressionante di informazioni confluisce nei dispositivi digitali.

Lei ha immaginato anche *de iure condendo* la possibilità della formula dell'accertamento irripetibile come garanzia dal punto di vista processuale. Sotto il profilo sostanziale, a suo avviso, per questa specifica tipologia di sequestri non andrebbe parallelamente immaginato anche un catalogo di reati che consenta un accesso così invasivo? È chiaro infatti che non si sequestra il dispositivo in quanto *hardware*, ma si consente comunque l'accesso a informazioni che vanno dai *file* digitali contenuti nel dispositivo alle localizzazioni, addirittura alle ricerche attraverso i motori di ricerca informatici; si può scandagliare cioè senza alcun limite a ritroso l'intera esistenza di un soggetto.

PRESIDENTE. Professor Borgogno, anche io avrei un quesito da aggiungere alle domande che le hanno già rivolto e che non ripeterò.

Anzitutto, la ringrazio per aver posto in evidenza una lacuna del nostro corpo normativo ormai abbastanza importante, perché è ovvio che i telefonini e gli *smartphone* fanno parte della vita di tutti noi, quindi credo che la materia vada disciplinata compiutamente e non ci si possa limitare a una sentenza della Cassazione.

La domanda che vorrei farle è la seguente: nel telefonino, come ha detto, c'è la vita di tutti noi, ma anche di chi interagisce con noi e magari non ha nulla a che fare con le indagini, né direttamente, né indirettamente. Secondo lei, merita una tutela anche chi vede la propria vita e la propria *privacy* violate? Non mi riferisco al soggetto oggetto del sequestro, ma a chi ha interagito con lui e i cui dati e la cui vita vengono a questo punto messi nelle mani di altri soggetti, anche aziende private.

BORGOGNO. Signor Presidente, ringrazio tutti gli intervenuti per le interessanti domande, alle quali cerco di rispondere in maniera ordinata, replicando ad alcuni argomenti ormai comuni.

Innanzitutto direi che il tema fondamentale è inserire ulteriori limiti, sostanzialmente analoghi a quelli delle intercettazioni telefoniche (ad esempio, introdurre un catalogo di reati ai quali possono riferirsi questi tipi di sequestro). Sarei del seguente avviso: a me non convince questa distinzione che la giurisprudenza fa fra sequestro di dispositivo digitale e intercettazione telefonica. Capisco che ci può essere un fondamento, perché è chiaro che l'intercettazione di una conversazione nel momento in cui avviene è un atto molto invasivo da parte dell'autorità giudiziaria, perché non si conosce il momento in cui viene effettuato, quindi certamente una differenza c'è.

È anche vero però che, come sentivo sottolineare prima, quando viene acquisito un dispositivo digitale, possono essere acquisiti dal pubblico ministero dati di una serie enorme di conversazioni, che possono riguardare correttamente anche terzi del tutto estranei al procedimento penale e oltretutto – perdonatemi la battuta – questo materiale viene acquisito già in forma scritta, quindi non è nemmeno necessario trascriverlo, come si fa con le trascrizioni telefoniche. Quello che il pubblico ministero acquisisce è in realtà il contenuto esatto delle conversazioni informatiche intercorse fra l'indagato e una serie enorme di terzi estranei.

A mio modo di vedere, quindi, gli interessi in gioco sono ovviamente gli stessi (la libertà, la segretezza della corrispondenza e di ogni altra forma di comunicazione). Credo che sia corretto porsi il problema d'introdurre limiti analoghi a quelli previsti per le intercettazioni telefoniche. Poi naturalmente bisogna vedere se si tratta esattamente degli stessi limiti, però credo che il tema sia molto corretto e che sia opportuno porlo, anche perché ormai, per esempio a livello di giurisprudenza convenzionale, in Corte europea queste comunicazioni sono equiparate sostanzialmente alla corrispondenza. Il tema della tutela di interessi costituzionalmente tutelati è quindi sicuramente centrale.

Il senatore Scarpinato mi ha chiesto se non si potesse introdurre un meccanismo analogo a quello previsto per l'archivio digitale, quindi un contraddittorio successivo all'acquisizione dei dati. Su questo avrei alcuni dubbi, nel senso che il problema posto dalla sentenza che citavo prima (che, poiché me n'è stata fatta richiesta, ricordo essere della Sezione VI, n. 34265, del 2020), la quale fa proprio riferimento al caso *Open* oggetto anche del conflitto di attribuzioni di cui parlavo poc'anzi, sottolinea proprio l'esigenza cioè di evitare, fin dal momento in cui viene acquisito, un utilizzo incontrollato del dispositivo digitale, magari anche per l'avvio di nuove indagini o magari da parte della Polizia giudiziaria che effettua la selezione dei dati, quindi che trasforma naturalmente questo in un sequestro puramente esplorativo.

Se dobbiamo stare ai principi indicati da questa sentenza, che a me sembrano molto importanti e sui quali è necessario riflettere molto, credo che il contraddittorio per forza di cose in questo caso debba essere anticipato, nel senso che ci vuole un controllo nel momento in cui il dispositivo viene acquisito e il materiale viene selezionato. Altrimenti, come sottolinea anche questa sentenza, c'è un rischio di acquisizione incontrollata di notizie e di dati che possono riguardare tutta la vita di un individuo, ma anche di terze persone coinvolte.

D'altra parte, il conflitto di attribuzione nasce proprio da questo elemento, perché il senatore Renzi, che poi ha proposto al Senato di sollevare il conflitto, è stato attinto proprio dal sequestro effettuato a carico di terze persone, che era finalizzato a reperire informazioni a carico di esponenti politici che potevano avere avuto rapporti con questi terzi estranei al processo, che però erano stati oggetto del sequestro di dispositivi informatici.

A me sembra quindi che il tema sia molto delicato e, tra le alternative che ho sentito proporre qui, a vedermi maggiormente favorevole è quella di cercare di equiparare la disciplina in tema di acquisizioni di dispositivi a quella delle intercettazioni telefoniche anziché introdurre strumenti come il contraddittorio differito con la difesa dell'indagato, che capisco possono avere delle ragioni, ma non credo siano così tutelanti per gli interessi costituzionali che qui bisogna salvaguardare.

Questa è la mia la mia idea e mi pare di aver risposto.

PRESIDENTE. Ringraziandola per la chiarezza dell'esposizione, le ricordo che, se lo desidera, può lasciare agli atti della Commissione sia gli estremi della sentenza di cui ha parlato sia una sua nota scritta.

BORGOGNO. Nel rinnovare il mio ringraziamento a lei e a tutta la Commissione per l'attenzione, faccio presente che mi riservo senz'altro di produrre la documentazione richiesta.

Audizione del direttore amministrativo di RPC SpA

PRESIDENTE. È ora in programma l'audizione in videoconferenza del dottor Raffaele Andreozzi, direttore amministrativo di RPC SpA, a

cui do il benvenuto e a cui lascio la parola, ricordandogli che ha a disposizione circa dieci minuti per il suo intervento introduttivo, prima di ascoltare le domande dei senatori, a cui potrà infine replicare.

ANDREOZZI. Signor Presidente, onorevoli senatori, sono Raffaele Andreozzi, responsabile amministrativo dell'azienda RPC Servizi Tecnologici SpA, e vi ringrazio veramente di cuore per questa prima e preziosa possibilità che date alla nostra azienda di esprimere la nostra opinione sul delicatissimo e difficilissimo lavoro che svolgiamo quotidianamente nell'ambito investigativo delle intercettazioni legali per le procure della Repubblica. Si tratta di un'attività che rappresenta un fiore all'occhiello del nostro Paese, grazie all'eccellenza delle risorse che impieghiamo quotidianamente e agli importanti investimenti che facciamo per questo particolare settore strategico di nicchia.

Sono infatti onorato dell'attenzione che oggi ci dedicate per fare una breve descrizione dell'attività svolta dalle nostre aziende, che oggi sembra focalizzarsi purtroppo solo sul discorso dei *trojan*, ma vi assicuro che i cosiddetti captatori informatici oggi rappresentano veramente tra il 3 e il 5 per cento al massimo dell'intera filiera investigativa che mettiamo in campo quotidianamente.

La nostra azienda, l'RPC SpA, fa parte tra l'altro di un'associazione di categoria, la I.L.I.I.A (*Italian Lawful Interception Intelligence & Association*), con la quale tra l'altro recentemente abbiamo iniziato un processo di certificazione dei nostri sistemi. Quest'associazione racchiude circa venti aziende del settore, che attualmente rappresentano circa il 50 per cento della spesa complessiva annua del Ministero della giustizia che appunto investe sulla parte delle intercettazioni.

Siamo un'azienda nata nell'anno 2000, operiamo in via esclusiva – e questo tengo a precisarlo – per le Forze di polizia e la procura della Repubblica, quindi non lavoriamo assolutamente per aziende private, e offriamo una tecnologia investigativa a 360 gradi. L'azienda nasce e si sviluppa grazie al *know-how* di personale tecnico specializzato che ha vissuto in prima linea le problematiche delle investigazioni in territori ad alta concentrazione criminale. Attualmente siamo operativi in varie regioni italiane e lavoriamo costantemente su attività d'indagine per i reparti investigativi principali dei Carabinieri, della Polizia, della Guardia di finanza e dei reparti speciali, instaurando con loro rapporti di fiducia e reciproca stima, cercando di contrastare il fenomeno della criminalità organizzata e proponendo servizi innovativi – ve lo assicuro – con personale superspecializzato e con livelli qualitativi di eccellenza.

Considerate che impieghiamo il nostro personale notte e giorno, ventiquattr'ore su ventiquattro, trecentosessantacinque giorni all'anno. Siamo sempre al fianco della Polizia giudiziaria anche in particolarissime e delicatissime attività di installazioni che, ve lo assicuro, a volte si svolgono anche in condizioni assolutamente proibitive.

Ho voluto fare questa piccola sottolineatura per farvi capire che non noleggiamo solamente i *device* (dispositivi ambientali, microspie, *global*

positioning system o GPS), né svolgiamo solamente intercettazioni, ma siamo veramente al fianco delle Forze dell'ordine anche nell'installazione di tali dispositivi.

La nostra azienda è una società per azioni, che dispiega un'articolata struttura operativa su quasi tutto il territorio nazionale, soprattutto nelle regioni più calde – permettetemi di usare questo termine – come la Campania, la Calabria, la Basilicata, la Puglia, la Sicilia o il Lazio.

Abbiamo praticamente organizzato sedi operative proprio su questi territori per contrastare la criminalità organizzata, che ci permettono di offrire e garantire, come spesso viene richiesto nelle gare d'appalto di alcune procure, l'erogazione dei servizi in tempi rapidissimi. Questo ci aiuta in quanto il personale che selezioniamo conosce bene il territorio in cui si opera, quindi la vicinanza fisica ci aiuta sicuramente a lavorare meglio e a installare adeguatamente i dispositivi sui *target* o nei luoghi particolari in cui dobbiamo intervenire.

Grazie alla nostra organizzazione aziendale, ormai da qualche anno, stiamo cercando di innalzare sempre di più i livelli e gli *standard* di sicurezza. Già da tempo, anche grazie alle richieste del Garante della *privacy*, abbiamo iniziato questo percorso procedendo al riconoscimento delle certificazioni ISO 9000 o ISO 27001, che riguardano soprattutto la parte della sicurezza dei dati, ai nostri sistemi. Queste certificazioni riguardano proprio le attività di progettazione, sviluppo e fornitura degli apparati a noleggio.

L'adeguamento tecnologico della nostra azienda e tutte le competenze che abbiamo acquisito negli anni ci hanno permesso di produrre in completa autonomia anche i cosiddetti *device*, quindi le famose microspie, i localizzatori satellitari e sistemi video o audiovideo sincronizzati. Cerchiamo così di coprire l'intera filiera delle intercettazioni, senza alcuna contaminazione esterna. Questa è un elemento molto importante, perché riusciamo a controllare tutto il processo, dall'acquisizione del dato fino alla sua memorizzazione, sicurezza e conservazione. Questi prodotti vengono ingegnerizzati in base a specifiche tecniche provenienti da chi opera sul campo, che conosce bene ciò di cui hanno bisogno le Forze di Polizia, e a cui può quindi fornire le indicazioni necessarie anche a miniaturizzare i dispositivi che utilizziamo per svolgere tali attività.

La nostra azienda si è cimentata con successo nello sviluppo di queste soluzioni tattiche. In particolar modo, abbiamo creato negli anni un sistema di acquisizione dati: nel nostro caso, sono orgoglioso di citare il nome di un sistema che si chiama « Ombra » ed è una centrale operativa che viene installata presso le procure della Repubblica permettendo di acquisire tutti i dati intercettati, da tutte le diverse tipologie d'intercettazione (ambientali, GPS, telefoniche o telematiche). Addirittura sono una nostra prerogativa anche le attività che svolgiamo presso le case circondariali, dove pure ci occupiamo dell'intercettazione di alcuni colloqui.

Non da ultimo, va citato anche l'impegno costante del nostro gruppo di sviluppo *information technology* (IT) per l'adeguamento dei nostri sistemi alle nuove stringenti normative imposte dal Garante della *privacy*.

Devo confermare che negli ultimi anni il livello di sicurezza imposto da queste nuove normative è aumentato notevolmente, infatti il Garante della *privacy* ha introdotto misure particolari, come l'inserimento di registri inalterabili, quindi oggi riusciamo a tracciare esattamente tutto ciò che avviene all'interno dei nostri *server* (qualsiasi accesso o situazione comandati dall'esterno vengono tracciati da questi registri inalterabili, come pure l'accesso ai sistemi stessi). Come sapete, la Polizia giudiziaria opera da remoto e per accedere al *client* di riascolto (che quindi permette l'ascolto e l'elaborazione dei dati) deve effettuare gli accessi non più con semplici *login* e *password*, ma con una *strong authentication*, che prevede un *token* di sessione a tempo limitato. Lo preciso per sottolineare che la sicurezza dei nostri sistemi nel tempo è aumentata sempre di più.

L'attività della nostra azienda non si limita quindi alla sola fornitura di prodotti e servizi elettronici, ma va considerata in un'ottica veramente più ampia, di supporto investigativo, con tecnologie e soluzioni sempre più avanzate e innovative, che tengono conto ogni giorno di moltissime variabili a cui dobbiamo rispondere in tempi brevissimi, in un contesto che muta giorno per giorno.

PRESIDENTE. Abbiamo compreso la difficoltà in cui vi muovete, ma purtroppo mi vedo costretto a interromperla a causa del contingentamento dei tempi dei nostri lavori, per lasciare la parola ai senatori che vogliano porle dei quesiti, non prima però di averla ringraziata per il suo contributo.

BAZOLI *(PD-IDP)*. Signor Presidente, vorrei fare una domanda al dottor Andreozzi, che ha detto che ci sono alcune regole, imposte dal Garante della *privacy*, che garantiscono la tracciabilità delle operazioni eseguite.

Nel corso delle altre audizioni, però, diversi auditi, anche provenienti dal mondo dell'informatica o di società specializzate, ci hanno segnalato che probabilmente ad oggi c'è una carenza sul piano regolamentare sia per garantire meglio la tracciabilità di tutte le operazioni d'intercettazione che vengono effettuate, quindi anche la loro ricostruzione *ex post*, sia sotto il profilo della verifica e del controllo per impedire sostanzialmente che i dati che vengono acquisiti possano essere manipolati. Occorre quindi una regolamentazione più puntuale che garantisca e assicuri che non si verifichi quello che potrebbe accadere in teoria, ma che poi non si è mai verificato nella pratica, anche se sappiamo che la tecnologia è in continua evoluzione, quindi servono un regolamento e una normativa che impediscano la manipolazione dei dati acquisiti, garantendone l'impossibilità.

Siccome queste sollecitazioni ci sono state fatte da più parti, anche da soggetti auditi che, lo ripeto, appartengono al mondo dell'informatica, vorrei capire se, dal suo punto di vista, l'attuale assetto normativo è sufficiente oppure in realtà occorrerebbe qualcosa in più.

ANDREOZZI. Signor Presidente, tutti i processi di acquisizione e di fruizione dei dati possono essere sicuramente migliorati. La sicurezza dei sistemi può essere migliorata, ma ricordo che purtroppo abbiamo a che fare con persone e uomini, quindi certifichiamo l'accesso ai nostri sistemi con procedure di sicurezza, vietando l'accesso abusivo da parte anche del nostro stesso personale. Ai nostri sistemi possono infatti accedere solo ed esclusivamente persone con specifica autorizzazione, che vengono tracciate e monitorate: non possono far altro che visionare le eventuali problematiche segnalate e risolverle, ma di sicuro non possono effettuare altre manipolazioni dei dati.

La manipolazione ovviamente in astratto è possibile (lo stesso vale anche per la Polizia giudiziaria che potrebbe attuare operazioni dolose), ma ovviamente ognuno si assume le proprie responsabilità. Abbiamo comunque il tracciamento di questi accessi per cui tutte le operazioni – lo ribadisco – vengono tracciate su registri inalterabili. Come saprete, inoltre, è in programma un sistema ministeriale che si chiama *StarSupport* Bomgar, che dovrebbe registrare addirittura gli accessi fisici, cioè registrare veri e propri filmati dell'accesso dei nostri sistemisti sui nostri sistemi.

Penso quindi che le misure di sicurezza adottate per adesso siano più che esaustive.

PRESIDENTE. Ringrazio il dottor Andreozzi per il suo contributo.

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

I lavori terminano alle ore 10.

€ 1,00