Senato della Repubblica XIX LEGISLATURA

Giunte e Commissioni

RESOCONTO STENOGRAFICO n. 7

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

21ª seduta: giovedì 16 febbraio 2023

Presidenza del presidente BONGIORNO

INDICE

Audizioni del procuratore presso il tribunale di Brescia

Audizione del *managing director* di RCS 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 dottor Francesco Prete, procuratore della Repubblica presso il tribunale di Brescia, e il dottor Alberto Nobili, managing director *di RCS 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, è stata richiesta l'attivazione dell'impianto audiovisivo a circuito chiuso, nonché la trasmissione televisiva sui canali *web* e satellitare del Senato della Repubblica, e che la Presidenza del Senato ha fatto preventivamente conoscere il proprio assenso. Poiché non vi sono osservazioni, tale forma di pubblicità è adottata per il prosieguo dei lavori.

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

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

PROCEDURE INFORMATIVE

Audizione del procuratore della Repubblica presso il tribunale di Brescia

PRESIDENTE. L'ordine del giorno reca il seguito dell'indagine conoscitiva sul tema delle intercettazioni, sospesa nella seduta del 2 febbraio.

Sono oggi previste le audizioni del procuratore della Repubblica presso il tribunale di Brescia, dottor Francesco Prete, e del *managing director* di RCS Spa, dottor Alberto Nobili, che ringrazio per aver accettato il nostro invito.

Avverto che le audizioni si svolgeranno separatamente.

Ad intervenire per primo sarà il dottor Francesco Prete, che potrà svolgere una relazione introduttiva, cui seguiranno eventuali richieste di chiarimento da parte dei componenti della Commissione, alcuni dei quali stanno seguendo i lavori da remoto.

Cedo dunque la parola al dottor Prete, che ha tra l'altro già inviato alla Commissione un documento scritto, che è in distribuzione.

Prego, signor procuratore.

PRETE. Signor Presidente, ringrazio lei e la Commissione tutta per l'invito.

Inizio con un'osservazione, sottolineando che in relazione al tema delle intercettazioni e, nello specifico, se vogliamo focalizzarne un aspetto, a quello delle cosiddette fughe di notizie, mi pare che la magistratura italiana sia parte del problema, ma al contempo anche della sua soluzione.

Visto che il tempo non è molto, ricordo brevemente che, dopo gli anni di « Mani pulite » e prima del 2017, l'anno che in qualche misura ha segnato uno spartiacque tra il prima e il dopo, i procuratori della Repubblica avevano avvertito il problema, in maniera tale da raccomandare con forza alla Polizia giudiziaria di attenersi a quella che poi più avanti è stata definita la sobrietà contenutistica nella redazione degli atti. A tali direttive seguì la proposta dei procuratori della Repubblica di istituire un archivio riservato delle intercettazioni, ove segregare gli atti che dovevano rimanere segreti proprio a garanzia e a tutela della dignità e della riservatezza delle persone.

Il Consiglio superiore della magistratura ha fatto la sua parte con una delibera del 2016; il legislatore è intervenuto, soprattutto con il decreto legislativo n. 216 del 2017 e da questo punto possiamo ripartire.

L'intervento legislativo ha introdotto, tra le altre cose, l'archivio riservato delle intercettazioni su cui si gioca gran parte della partita.

Saltando una serie di passaggi per ragioni di sintesi, il punto è capire se l'archivio riservato ha oggi un'attuazione soddisfacente nelle prassi lavorative delle procure della Repubblica. Mi pare di poter dire – e in questo senso faccio esercizio di ottimismo – che, dopo le direttive dei procuratori, dopo la circolare del Consiglio superiore della magistratura e dopo gli interventi legislativi, in particolare quello del 2017, il problema della fuga di notizie si è ridimensionato. I casi eclatanti forse si contano sulle dita di una mano e potrei dire che, grazie a un *self-restraint* che tutti hanno dimostrato, oggi la situazione è migliorata, anche se non tantissimo e vengo al tema.

La Polizia giudiziaria, probabilmente per una sorta di abitudine lavorativa e di prassi tramandate – se vogliamo, forse, anche per una certa pigrizia – continua a inserire nelle informative brani di conversazioni che, non solo probabilmente sono poco rilevanti – ma questo è un giudizio di merito – ma non coincidono con quelle che poi alla fine dell'indagine vengono inserite nell'elenco che poi conterrà quelle che supereranno la fase della pubblicità ed entreranno come fonti di prova nel procedimento. Tuttavia, il fatto di averle incorporate nel testo delle informative nella fase genetica e nello sviluppo delle indagini comporta come conseguenza l'impossibilità di espungerle successivamente, sicché restano nel fascicolo del pubblico ministero e questo è un aspetto su cui riflettere e in relazione al quale introdurre correzioni.

La procura della Repubblica di Brescia – cito l'esempio del mio ufficio – ha introdotto una direttiva che ha provato tra l'altro a spiegare con una certa determinazione alla Polizia giudiziaria che gli atti che via via vengono composti nel corso delle indagini preliminari devono contenere nel testo base i passaggi essenziali: questo è quanto dice la legge.

La trascrizione, che può servire un domani – e sottolineo il carattere potenziale della rilevanza – deve essere inserita in allegato. Gli allegati devono costituire materiale fino al momento in cui non si arriva alla selezione, che può avvenire nella fase di cui all'articolo 415-*bis* del codice di procedura penale, ma anche nella fase di richiesta di misura cautelare. In quel momento bisogna decidere quali allegati entrano nel fascicolo e quali no.

Con il sistema degli allegati si riesce facilmente a espungere le conversazioni che in un primo momento sono apparse rilevanti, ma che ad un giudizio più approfondito *a posteriori* hanno perso tale carattere. Ciò potrebbe anche aiutare a risolvere il problema delle conversazioni parzialmente rilevanti, quelle cioè che contengono al loro interno passaggi di utilità processuale e passaggi che ne sono del tutto privi. In questo modo si potrebbe fare una selezione più comodamente e quindi fare entrare nel fascicolo quello che al giudizio finale merita di essere acquisito come fonte di prova, tenendo segregato il resto nell'archivio.

Il secondo passaggio che mi sono permesso di evidenziare in termini di possibile prospettiva pratica di attuazione della riforma riguarda l'uso estensivo dell'archivio riservato delle intercettazioni. L'archivio è stato congegnato e architettato per « ospitare », quindi per ricevere e custodire le conversazioni telefoniche, ambientali e le comunicazioni, anche telematiche, quindi tutto ciò che attiene all'istituto delle intercettazioni. In realtà, però, nell'ambito delle indagini penali si prevedono possibilità diverse di acquisizione di dati altrettanto sensibili e, tuttavia, esulanti dal perimetro delle intercettazioni. Ipotizziamo che venga sequestrato lo *smartphone* di una persona: al suo interno si troverà una massa più o meno estesa di dati, anche sensibili. Tali dati vengono acquisiti attraverso lo strumento del sequestro e quindi al di fuori dall'ambito delle intercettazioni in senso proprio. È successo proprio nella mia procura: chi vi parla ha deciso di tenere custodito il telefono cellulare di una persona imputata perché al suo interno vi erano molti dati, anche eccentrici rispetto alle indagini, certamente sensibili e tuttavia acquisiti non con lo strumento delle intercettazioni, ma con quello del sequestro.

Mi viene allora da pensare che l'archivio dovrebbe essere utilizzato anche tutte le volte in cui l'autorità acquisisca dati sensibili, non già con lo strumento delle intercettazioni, ma tramite altri strumenti: si pensi ai sistemi di videosorveglianza, che captano immagini che – è considerazione di senso comune – in certi casi possono essere molto più lesive della sfera di riservatezza della persona rispetto alle parole, che spesso richiedono uno sforzo interpretativo di cui le immagini invece non necessitano.

Abbiamo dunque immaginato – ripeto – e soprattutto già attuato precauzioni per custodire nell'archivio delle intercettazioni il materiale acquisito con strumenti diversi rispetto alle intercettazioni.

Questo è il presente, rispetto al quale chi vi parla non ha difficoltà a ipotizzare aperture anche nel senso di un incremento degli istituti a garanzia dei diritti dell'indagato. Lo dico scandendo le parole perché, pur

avendo per ruolo istituzionale la posizione di chi avrebbe più comodità con un maggiore margine di manovra, mi rendo conto tuttavia che ci sono strumenti acquisitivi di dati che non rientrano nella disciplina delle intercettazioni, che sono in qualche misura sguarniti di garanzie e che ben potrebbero essere invece assistiti da forme di tutela della riservatezza e della dignità delle persone con una serie di accorgimenti. Perché, ad esempio, quando si sequestra un telefonino, deve essere il solo pubblico ministero arbitro di decidere che cosa far confluire nel fascicolo del dibattimento e che cosa no? Perché non immaginare un intervento del difensore sulla falsariga di quanto previsto dall'articolo 268 del codice di procedura penale, vale a dire un intervento del difensore che nel contraddittorio del giudice, sia pure successivo, contribuisca all'individuazione del materiale da acquisire e quindi, per converso, a quello da scartare?

Credo che il pubblico ministero italiano non sia alieno dal poter recepire queste misure a garanzia dell'indagato, purché – e devo sottolinearlo con molta forza – non si impoverisca lo strumento. Il senso finale del mio ragionamento è quello di prevedere forme che accompagnino l'acquisizione del dato, la sua selezione e la formazione della prova, ma non privino l'autorità inquirente dello strumento.

A tale proposito, nella mia breve relazione troverete un piccolo paragrafo dedicato ai prossimi scenari, che ci vedono molto indietro rispetto ad altri Paesi europei, come vi potranno spiegare i tecnici delle intercettazioni. Da parte mia, mi limito a dire che Paesi come la Francia, il Belgio e la Germania, soprattutto a seguito di fatti di terrorismo di enorme gravità, hanno introdotto delle norme che consentono al pubblico ministero di violare le piattaforme criptate, cioè dei *server* utilizzati dalla criminalità organizzata o dalle frange del terrorismo per scambiarsi comunicazioni. È chiaro che in quei *server* ci sono anche dati penalmente irrilevanti o riguardanti persone che nulla hanno a che fare, né con il crimine organizzato, né con il terrorismo.

La domanda è se sia possibile aggredire una piattaforma che contenga una massa di dati, parte dei quali potrebbe essere utile alle indagini. Mi viene da pensare a quanto all'epoca del terrorismo fu introdotto dalla legge Reale nell'ordinamento con le perquisizioni per blocchi di edifici: era chiaro che si sacrificava qualcosa, ma era altrettanto chiaro lo scopo.

La perforazione, la violazione di piattaforme criptate in Italia non è possibile. Abbiamo vissuto con una certa umiliazione il fatto che le Polizie giudiziarie francesi, che oltretutto possono contare su sistemi coperti dal segreto di Stato, hanno violato piattaforme criptate all'interno delle quali hanno trovato una massa di comunicazioni intercorse tra esponenti della criminalità organizzata italiana: ci hanno allora benevolmente concesso – è qui l'umiliazione – di utilizzare questi dati captati e intercettati da loro, senza tuttavia coinvolgerci nell'indagine.

C'è poi un secondo aspetto. Semmai un *server* di questo tipo fosse allocato in Italia, non saremmo in condizione di bucarlo, perché nel nostro ordinamento non esiste una norma che legittimi un intervento di que-

sto tipo, neppure per fatti di terrorismo che, mi sento di dire, per certi aspetti sono ancora più gravi di quelli di criminalità organizzata. È solo un esempio, signor Presidente, signori senatori, per dire che la normativa italiana sconta dei ritardi che si ripercuotono sull'efficacia investigativa e – in prospettiva – repressiva del nostro ordinamento e del nostro Stato. Ben venga, dunque, l'apertura verso nuove forme di garanzia, ma – lo dico quasi come una preghiera – bisognerebbe non toccare l'attuale e aprire nuove possibilità investigative.

PRESIDENTE. La ringrazio, signor procuratore.

La Commissione è particolarmente attenta al tema, infatti sta approfondendo la materia, recependo una serie di suggerimenti che stanno arrivando, secondo me utilissimi.

BAZOLI *(PD-IDP)*. Signor Presidente, innanzitutto saluto e ringrazio il dottor Prete per la sua relazione, nel corso della quale ci ha offerto alcuni spunti di riflessione molto utili, peraltro in linea con quanto emerso in occasione di altre audizioni in cui ci sono state segnalate diverse esigenze, tra cui, per esempio, quella di coprire con una disciplina più garantista il sequestro degli *smartphone.* Ricordo, ad esempio, quanto riferitoci dal dottor Melillo circa la necessità di utilizzare nuovi strumenti (come l'hackeraggio di piattaforme) per combattere in maniera adeguata la criminalità internazionale.

Si tratta di profili molto interessanti. Nessuno ci aveva parlato – ed è un elemento che trovo altrettanto interessante – della necessità di istruire la Polizia giudiziaria nella fase delle indagini preliminari sul fatto di tenere separate le trascrizioni di intercettazioni potenzialmente lesive della *privacy*, che sono destinate a non finire all'interno del fascicolo delle indagini in modo da garantire la riservatezza.

Vorrei rivolgerle una domanda, dottor Prete. In particolare, vorrei sapere da lei se, rispetto all'utilizzo dei *trojan*, cioè dei captatori informatici – uno degli strumenti più invasivi oggi a disposizione degli inquirenti – l'attuale disciplina codicistica è adeguata oppure se andrebbero introdotti dei presupposti o dei criteri per l'accesso a questi strumenti così invasivi della *privacy*, per cui si renda necessario qualche aggiornamento della disciplina generale.

Le faccio questa domanda anche in relazione alla circostanza che ci è stata riferita dal professor Gatta, che abbiamo ascoltato nel corso della nostra indagine, il quale ci ha detto che in realtà l'uso del *trojan* nell'ambito delle intercettazioni è abbastanza limitato, visto che solo il 3 per cento di tutte le intercettazioni avviene tramite captatore informatico. Ci è stato però anche segnalato che presso la procura di Brescia si registra un dato un po' disallineato rispetto a questa percentuale: si parla del 9,5 per cento per quanto concerne l'uso del captatore informatico sul totale delle intercettazioni rispetto al 3 per cento della media italiana.

Vorrei capire se può fornirci qualche elemento e qualche informazione al riguardo.

PRESIDENTE. Senatore Bazoli, mi pare che il professor Gatta abbia riportato dati non propri, ma recuperati dal sito del Ministero.

ZANETTIN *(FI-BP-PPE)*. Signor Presidente, la prima domanda che intendo fare coincide in verità con quella posta dal collega Bazoli. Siamo rimasti tutti un po' sorpresi dai dati, soprattutto con riguardo all'utilizzo del *trojan* fatto dalla procura di Brescia, che pare sia di gran lunga maggiore rispetto a quello di altre procure della Repubblica, specialmente del Nord. L'altro aspetto che il professor Gatta aveva sottolineato, infatti, è che tendenzialmente il *trojan* viene utilizzato in procure di frontiera, in cui magari la criminalità organizzata o il terrorismo sono più diffusi, soprattutto al Sud, per cui la procura di Brescia sembrava un po' una mosca bianca e ciò ci ha sicuramente incuriosito.

Quanto poi al riferimento da lei fatto ai *server* criptati, le posso dire che forse io sono uno dei più attenti e più garantisti, per così dire, sul tema delle intercettazioni. Tuttavia, voglio rassicurarla sul fatto che, per quanto riguarda i reati di terrorismo e di mafia, anche la parte politica più sensibile ai temi della tutela della riservatezza dei cittadini non vuole fare sconti. Da questo punto di vista deve essere dunque ben chiaro che le procure devono essere dotate di tutti gli strumenti investigativi più sofisticati e più moderni perché, di fronte a questo genere di crimini, non ci possono essere esitazioni.

Torno infine ad un passaggio della sua relazione che reputo molto interessante, dottor Prete, che mi consente di fare un riferimento al tema del sequestro dello *smartphone*. Quello che come avvocati abbiamo studiato sui libri di procedura penale e abbiamo poi visto negli anni di pratica in tema di sequestro è completamente diverso dal sequestro di uno *smartphone*: il sequestro secondo il codice di procedura penale è tradizionalmente un sequestro di cose pertinenti al reato, di elementi probatori. Quando oggi invece parliamo di *smartphone*, facciamo riferimento a qualcosa che ha una valenza a 360 gradi.

Le chiedo dunque, dottor Prete, se non reputi – come peraltro reputo io – che forse proprio con riguardo al sequestro dello *smartphone*, al di là della presenza dell'avvocato nell'acquisizione dei dati, sia necessario inserire delle cautele che fino ad oggi ci sono sfuggite. Giustamente abbiamo pensato al *trojan*, che è uno strumento molto invasivo, ma anche il sequestro dello *smartphone*, sulla base di un istituto giuridico straconsolidato e strautilizzato nella nostra pratica giudiziaria, con i dati presenti al suo interno in realtà allarga a dismisura l'applicazione in concreto dell'istituto. Probabilmente quindi qualche riflessione sul tema e qualche cautela in più da parte del legislatore sarebbero opportune.

PRESIDENTE. Vorrei fare anch'io qualche riflessione, signor procuratore, in merito a quanto lei ha detto sulle informative di Polizia giudiziaria, che spesso contengono brandelli di conversazioni telefoniche.

Lei ha chiarito che il problema sarebbe stato eliminato da una vostra direttiva. Io personalmente sono contraria alle direttive, che possono es-

sere a macchia di leopardo, perché magari un'altra procura non le adotta, con la conseguenza che, come dico sempre, il trattamento dell'imputato dipende dalla procura nella quale va a finire. Le chiedo se non sarebbe più utile un intervento normativo, anche al fine di uniformare il trattamento e la gestione dell'informativa.

Quanto al *trojan*, visto che le sono state rivolte varie domande, lei ritiene che al riguardo sia necessario colmare una lacuna legislativa, considerate le peculiari caratteristiche del captatore informatico dal punto di vista dell'invasività? Ci è stato detto che si tratta di strumenti di eccezionale portata; trattandosi di un *software*, in astratto ci potrebbero essere ovviamente delle manipolazioni. Ha qualche proposta al riguardo? Ci è stato riferito che c'è una lacuna, ma ancora non abbiamo indicazioni chiare da un punto di vista propositivo e a noi piacerebbe anche ricevere delle proposte da parte degli auditi.

C'è infine un ultimo punto che non è stato toccato. La Commissione nelle prossime settimane si occuperà anche dell'archivio riservato europeo. Vorrei sapere come gestite i dati dell'archivio riservato nei vostri rapporti con altri organismi, non solo nazionali, ma anche sovranazionali e con le procure europee. C'è uno scambio? Chi li tiene?

PRETE. Inizio a rispondere partendo dalle domande del senatore Bazoli, che ringrazio.

Ho allegato alla mia prima nota – che è stata in parte modificata dalla successiva che ho lasciato comunque alla Commissione – un prospetto per quanto riguarda l'uso del *trojan* nella mia procura, dal quale si evince che nel 2022 sono state disposte 38 informative con captatori attivi per i reati comuni e 156 per la DDA. Già questo dà la misura di come lo strumento venga utilizzato prevalentemente per i reati di criminalità organizzata. C'è soprattutto un dato che va letto nel secondo prospetto e cioè che quelli effettivamente attivati sono – purtroppo – zero per i reati comuni e 44 per la DDA. Come voi sapete, infatti, disporre un'intercettazione con *trojan* non vuol dire affatto che poi si riesca ad inocularlo. Quindi, se noi ragioniamo sui decreti autorizzativi, abbiamo dei numeri; quando però poi si passa a considerare a cascata l'attuazione e l'effettiva operatività dei decreti, spesso la Polizia giudiziaria non riesce a inoculare il *trojan* per le più svariate ragioni tecniche, per cui i numeri non sono sempre univocamente leggibili.

In ogni caso, indipendentemente da tutto, resta il fatto che la grandissima parte delle operazioni condotte attraverso i *trojan* riguarda la criminalità organizzata che, purtroppo per noi, senatore Bazoli – lei lo sa, essendo bresciano – non manca neppure nel nostro territorio.

Il senatore Zanettin ha toccato il medesimo punto e mi pare di capire che abbia posto l'accento su due passaggi. Innanzitutto, ha sottolineato che non c'è alcuna intenzione di indebolire lo strumento per la lotta ai fenomeni criminali più gravi e questo naturalmente ci fa enorme piacere. In secondo luogo, si ritiene giusto, opportuno e anche urgente introdurre delle norme a garanzia delle persone, in relazione ai sequestri

degli *smartphone*: sono d'accordo perché, al di là del mezzo di ricerca della prova – si chiami esso intercettazione telefonica o sequestro – il risultato finale è che vengono incamerati dati sensibili e non c'è motivo per gestirli in maniera differente, a seconda del mezzo di ricerca della prova utilizzato. Il risultato finale è il medesimo e credo quindi che identico debba essere il trattamento. È dunque auspicabile un intervento riformatore, rispetto al quale c'è da parte nostra massima apertura, così da consentire al difensore di intervenire nella fase di selezione del materiale, prevedendone la custodia nell'archivio, in attesa della procedura di selezione.

Il Presidente ha posto l'accento sulla redazione delle informative e, in particolare, sullo strumento delle direttive, che effettivamente può determinare il problema di una situazione a macchia di leopardo.

Ritengo certamente auspicabile un intervento normativo. Nel 2017 il legislatore ha introdotto questo strumento che, voglio ricordarlo con piacere, fu proposto dai procuratori della Repubblica. È chiaro che, con il passare degli anni, strada facendo si corregge il tiro. Accade – lo dico per esperienza – che la Polizia giudiziaria, non tanto per pigrizia, ma per rendere più chiaro e completo il quadro indiziario, tenda a inserire nelle informative tutto ciò che serve ad una più facile lettura; serve a noi, quando la scriviamo, e serve a voi quando la leggete. Non si pongono abbastanza il problema della ricaduta, vale a dire di quello che succede, perché poi accade che quel materiale resta nel fascicolo del pubblico ministero. Probabilmente bisogna « imporlo » alla Polizia giudiziaria, che in buonissima fede si comporta come ho descritto, per cui una previsione normativa di questo genere, a mio avviso, non sarebbe sbagliata, anche perché poi si tratta di tecniche di redazione degli atti e, quindi, di nulla di stravolgente.

Quanto al tema della necessità di una qualche modifica dell'attuale disciplina in materia di *trojan* e manipolazione, nella mia nota ho ricordato un aspetto, vale a dire che già oggi la legislazione prevede un trattamento differenziato, a seconda che il *trojan* venga usato per reati comuni oppure per reati contro la pubblica amministrazione o di criminalità organizzata.

Per i reati comuni la normativa è stringente, al punto che si richiede che il giudice nel proprio decreto individui il tempo e i luoghi in cui la captazione avviene attraverso l'accensione del microfono, che va spento allorquando la persona entri in un luogo di domicilio privato. Mi verrebbe da dire che è già nell'architettura normativa la possibilità di accendere e spegnere il microfono. So bene che la Commissione si è occupata anche di casi di cronaca, di microfoni accesi chissà perché e chissà come, però l'attuale normativa prevede già, almeno per i reati comuni, la possibilità di accendere o spegnere il microfono, a seconda del tempo e del luogo indicati dal giudice e, soprattutto, nel domicilio privato che va riservato.

Con riguardo inoltre all'archivio riservato europeo, devo dire che, al di là delle buone intenzioni, si registra una discreta collaborazione fra la

Polizie giudiziarie dei vari Paesi, che diventa più faticosa a livello più alto, quando bisogna procedere con gli ordini di indagine europei: la procura li chiede e il collega del Paese straniero li attua, secondo quello che ritiene di fare e per come ritiene di fare. Tutto sommato, dunque, non registriamo una grande convergenza e compattezza: vi è una sorta di gelosia – che purtroppo pare sia un tarlo, non solo di pubblici ministeri italiani – che porta a non condividere i risultati ed eventualmente i successi di un'indagine. Così, quando sono state perforate le piattaforme criptate di telefonini Sky-ECC o EncroChat, non ci hanno consentito di fare parte della squadra investigativa comune; ci hanno graziosamente messo a disposizione alcune cose, richieste con forza da noi e più o meno volentieri concesse, però non c'è stata una grande collaborazione.

PRESIDENTE. Ringrazio il procuratore Francesco Prete per il suo contributo; siamo andati oltre i tempi, però il suo punto di vista e le sue osservazioni erano particolarmente interessanti.

Ricordo a tutti che la nuova memoria, che è stata trasmessa dal procuratore, è in distribuzione e si distingue dalla precedente per la presenza di allegati.

Audizione del *managing director* di RCS Spa

PRESIDENTE. I nostri lavori proseguono con l'audizione del dottor Nobili, *managing director* di RCS Spa, che saluto e al quale do il benvenuto.

Nell'ambito dell'indagine sul tema delle intercettazioni che la Commissione sta svolgendo, ci interessa ascoltare da lei un'esposizione il più possibile idonea a renderci edotti delle sue conoscenze, se possibile, con termini accessibili a tutti.

Ringrazio il dottor Nobili, che ha già provveduto ad inviare alla Commissione una memoria, che è in distribuzione. A lui cedo subito la parola per un intervento introduttivo, cui seguiranno eventuali quesiti da parte dei colleghi. Prego, dottor Nobili.

NOBILI. Signor Presidente, onorevoli senatori, innanzitutto vi ringrazio per avermi dato l'opportunità di essere qui oggi e per l'occasione di confronto e approfondimento sul tema delle intercettazioni.

Nel tempo a mia disposizione intendo fornirvi un resoconto ragionato della storia di RCS Spa e descrivervi le linee evolutive delle tecnologie, nell'ottica di dare evidenza degli attuali processi di acquisizione e conservazione delle informazioni e dei relativi meccanismi a garanzia dell'integrità delle stesse.

Questa, peraltro, è un'occasione gradita per fornire su un tema sensibile e delicato come quello che la Commissione sta affrontando un seppur minimo contributo di pensiero, che speriamo possa esservi utile.

RCS Spa è storicamente un'azienda *leader* nel settore delle intercettazioni in Italia. Collabora da almeno trent'anni, cioè dagli inizi degli

anni Novanta, con le forze dell'ordine e con l'autorità giudiziaria e lo fa offrendo tecnologie evolute di acquisizione di elementi di prova mediante lo strumento delle intercettazioni.

In particolare, RCS Spa progetta, sviluppa e industrializza delle avanzate piattaforme di intercettazione e realizza tutto questo con l'impiego di circa 300 dipendenti operanti sul territorio nazionale ed erogando servizi mediante *server* centralizzati ubicati all'interno dei locali tecnici di almeno 60 procure della Repubblica e 19 Direzioni distrettuali antimafia su 26.

L'offerta di RCS Spa copre di fatto la catena del valore delle attività di *lawful interception*, fornendo servizi che vanno dall'installazione delle cosiddette periferiche tattiche (vale a dire microtecnologie audio-video e di localizzazione), fino a piattaforme tecnologiche abilitanti le intercettazioni telefoniche e i più complessi e moderni strumenti informatici che permettono lo svolgimento di attività telematiche passive e attive, nonché strumenti di analisi e correlazione in tempo reale di ingenti flussi di informazioni che possono provenire da periferiche e da sensori che operano su un medesimo bersaglio o *target* al fine di agevolare l'attività della Polizia giudiziaria.

Da poco più di un anno RCS Spa è entrata a far parte del gruppo Cy4gate, una realtà italiana nata nel 2014 con l'intento strategico di assicurare risposta a una crescente esigenza di difesa cibernetica da parte delle istituzioni e delle aziende. Da giugno 2020 Cy4gate è quotata in borsa nel segmento Euronext Growth di Milano e, quale soggetto quotato in borsa, offre le più ampie garanzie di trasparenza e di solidità finanziaria e gestionale, in quanto soggetta ovviamente a restrittivi requisiti normativi e a verifiche.

A seguito di questa importante operazione societaria, RCS Spa negli ultimi mesi ha intrapreso un percorso di trasformazione, di consolidamento e riorganizzazione della *governance* aziendale e dei propri processi e ciò nella prospettiva di un rafforzamento e di un efficientamento tendenti ad innalzare il livello qualitativo dei servizi erogati, con particolare attenzione alla sicurezza delle informazioni.

La storia di RCS Spa, quindi, è quella di un'azienda che nell'arco di trent'anni ha costruito al suo interno un notevole valore basato sul *know-how*, sull'*expertise*, sul sapere tecnologico, che ha permesso di costruire importanti piattaforme e prodotti di intercettazione.

I nostri prodotti, quindi, sono stati progressivamente costruiti nel tempo e hanno seguito le normali evoluzioni della normativa e della tecnologia, soprattutto nel comparto delle telecomunicazioni; sono anche frutto del costante allineamento e dello scambio di esperienze e di conoscenze con i settori più operativi della Polizia giudiziaria e della magistratura, in particolare quella operante nel territorio.

Il nostro intento è sempre stato ed è quello di fornire soluzioni tecnologiche per quanto più possibile rispondenti alle esigenze reali e attuali della Polizia giudiziaria, ovviamente seguendo quelle che sono sempre

state le indicazioni provenienti dal Garante della *privacy* e dai vari decreti ministeriali o circolari che si sono succeduti nel tempo.

Per garantire un'adeguata soluzione e un aggiornamento tecnologico, che è fondamentale per dare continuità a un servizio pubblico essenziale, aziende come la nostra hanno dovuto e devono affrontare investimenti molto importanti e dotarsi di piani industriali pluriennali. Gli investimenti, in particolare, sono mirati ad attrarre e mantenere pregiate risorse di elevatissime competenze tecniche tali da poterci permettere di sviluppare prodotti proprietari.

PRESIDENTE. La ringrazio per questa relazione introduttiva, dottor Nobili.

Lascio ora la parola ai colleghi per le domande, che consentiranno di evidenziare alcune tematiche di interesse.

ZANETTIN *(FI-BP-PPE)*. Dottor Nobili, sono stato io a richiedere la sua audizione presso questa Commissione, considerato che RCS Spa è stato forse l'operatore che più ha incuriosito noi esperti – anche se fino a un certo punto – del tema del *trojan*. Mi riferisco a quanto è accaduto anche nella pratica quotidiana, con le inchieste che hanno visto la vostra società protagonista di intercettazioni importanti, che hanno influito molto sul dibattito politico del Paese, oltre che sull'esito di alcuni giudizi.

In una precedente audizione l'ingegner Della Pietra ci ha riferito che, se in generale è vero che, nel rispetto della legge, i *server* vengono installati nelle procure da società come la vostra, è anche vero che poi il personale di tali società opera da remoto sui *server* con i privilegi di amministratore: questo dato ci induce ad alcune riflessioni. Innanzitutto, le chiedo se conferma quanto riferitoci dall'ingegner Della Pietra la scorsa settimana.

C'è poi la questione, emersa in particolare nel corso delle indagini di Perugia, di un *server* installato all'interno della procura di Napoli, almeno in apparenza senza rispettare il dettato normativo, nel quale in realtà transitavano tutte le intercettazioni di Italia. Alla mia domanda il dottor Melillo ha risposto che ciò avveniva a sua insaputa; nonostante a suo giudizio la cosa non abbia portato ad alterazioni o messo in dubbio la genuinità dei dati acquisiti, vorrei capire perché è successo e se c'è qualche vuoto normativo che magari potremmo colmare. Le chiedo se è d'accordo su questo o se contesta la questione in fatto e in radice.

SCARPINATO *(M5S)*. Dottor Nobili, le pongo una domanda semplice e diretta: avete la possibilità di leggere i dati contenuti nei *server* delle procure oppure no?

In secondo luogo, ove esista per voi questa possibilità, potete creare programmi criptati che impediscano alla società di gestione di leggere i dati contenuti nei *server*?

RASTRELLI *(FdI)*. Dottor Nobili, in raccordo a quanto chiesto dal senatore Scarpinato, al di là della fornitura di tutte le apparecchiature *sof-*

tware e *hardware*, immagino che voi curiate anche la manutenzione degli strumenti di deposito del dato intercettato. Vorrei sapere come viene garantita la manutenzione rispetto all'integrità del dato contenuto nei *server*.

PRESIDENTE. Prego, dottor Nobili, a lei la parola per le risposte.

NOBILI. Vi ringrazio per le domande. Comincio con il dire che, non essendo un ingegnere, le mie saranno necessariamente risposte non troppo tecniche.

Ovviamente ci sono ancora dei procedimenti in corso quindi, se mi si chiede se posso smentire punto per punto l'autorevole opinione di un consulente tecnico di parte, quello che posso dire è che recentemente, il 17 dicembre 2022, la sezione penale del tribunale di Perugia ha di fatto respinto le eccezioni sollevate dai consulenti tecnici di parte, confermando che i processi al tempo posti in essere erano genuini e hanno consentito l'acquisizione di fonti di prova nel rispetto della normativa. Come azienda stiamo guardando ovviamente con grande interesse a tutto questo. Abbiamo colleghi (tra questi anche ex colleghi) ancora sottoposti a procedimento.

Ripeto, rispetto l'opinione di persone dalla grande conoscenza tecnica, però mi attengo ai fatti e leggo quella che è comunque la pronuncia della sezione di un tribunale, peraltro supportata dall'attività degli ispettori del CNAIPIC della Polizia postale. So che ci sono ancora altre attività in corso, per cui non voglio assolutamente entrare nel merito. Rispettiamo l'attività e i commenti dell'autorità giudiziaria: per noi è fondamentale anche imparare dalle critiche che eventualmente possono esserci rivolte. Sicuramente non lavoriamo in un settore facile da governare perché, come dicevo nel mio intervento introduttivo, operiamo con tempistiche veramente molto brevi in un settore in cui l'obsolescenza tecnologica si misura in mesi e non in anni e questa è sicuramente la grande sfida di queste aziende.

Non so, senatore Zanettin, se ho risposto almeno in parte alla sua domanda. Questo è quanto mi sento di dire come direttore generale della società che rappresento.

Quanto alla possibilità di vedere i dati, un amministratore di sistema ha sicuramente dei privilegi: ricordo che alla fine stiamo parlando di *software*, quindi di sistemi informatici in cui è sempre previsto e ciò avviene su tutte le piattaforme tecnologiche, da quelle bancarie a quelle militari. È però altrettanto vero che ci sono dei sistemi di tracciamento in atto e una combinazione di misure tecniche e organizzative – anche se un'operazione fosse compiuta contro la legge da un operatore abilitato e autorizzato a fare questo – che permettono di ricostruire e riattribuire ad una determinata persona le attività che ha svolto, eventualmente di accesso o – se mai fosse questo il caso – anche di alterazione.

Questi privilegi di amministratore non sono diffusi e distribuiti tra molte persone: sicuramente chi svolge assistenza e manutenzione deve avere la possibilità di operare sul sistema, ma ci sono delle procedure

ben precise, per cui devono essere richiesti. Le operazioni sono tracciate, nel senso che vengono registrati i comandi di riga e, se parliamo di interfaccia grafica, ci sono sistemi che effettuano delle vere e proprie videoriprese – so che qualche consulente ne ha parlato – per rivedere esattamente sullo schermo i singoli *step*.

I *file* perimetrali di sistema e applicativi sono mantenuti all'interno di *server* e sono a disposizione per eventuali verifiche e attività investigative che l'autorità giudiziaria giustamente può mettere in atto in qualsiasi momento.

Questo è quanto posso dire. Ovviamente i fatti cui faceva riferimento il senatore Zanettin risalgono al 2019 e vi assicuro che dal 2019 al 2023 sono intervenute altre indicazioni, norme e circolari e, soprattutto a livello tecnologico, quattro anni sono veramente un abisso, è un'epoca diversa.

Non nego che si possa migliorare e si possano dare certamente ulteriori garanzie, ma ritengo in ogni caso che oggi ci sia una sufficiente combinazione di misure tecniche, organizzative e procedurali per garantire adeguata certezza dell'operato almeno di quanti lavorano nella società che rappresento.

Il senatore Rastrelli parlava di manutenzione e in effetti possiamo essere chiamati: c'è un servizio di assistenza di primo livello perché, ripeto, sono sistemi informativi e come tali possono presentare dei malfunzionamenti durante le attività, per cui spesso accade che la Polizia giudiziaria ci chiami per chiedere chiarimenti sul perché magari un captatore informatico non stia funzionando, sul perché si è interrotta la captazione, come accade per qualsiasi strumento informatico e in tal caso c'è necessità di un supporto in tempo reale. Come dicevo, però, ci sono delle procedure; quindi, laddove anche ci siano degli abusi, ci sono meccanismi che intervengono, a volte non semplici. Gli stessi consulenti e analisti stanno prendendo tempo effettivamente, perché non parliamo comunque di aspetti tecnici semplici: è richiesta sicuramente una verifica incrociata delle evidenze che emergono dai *log* di sistema e applicativi, cioè da quello che ha fatto un operatore rispetto a quello che ha registrato il *software* (magari è stato dato un certo *input*, che poi è venuto meno e così via). In alcuni casi può capitare che l'analisi richieda parecchio tempo, perché giustamente i periti prima devono capire come funziona il captatore informatico, non trattandosi del resto di un prodotto *standard*, per cui si trovano istruzioni su fonti: parliamo di strumenti che rispettano anche un segreto industriale che fa ovviamente la differenza con altri prodotti che si possono trovare sul mercato.

PRESIDENTE. Ringrazio il dottor Nobili per il contributo offerto ai nostri lavori e per il testo della sua relazione che ha voluto mettere a disposizione della Commissione.

Dichiaro così concluse le odierne audizioni.

Rinvio il seguito dell'indagine conoscitiva ad altra seduta.

I lavori terminano alle ore 10,15.

€ 1,00