GARANTE DELLA PROTEZIONE DEI DATI PERSONALI

AS 1659

Ringrazio la Commissione per aver inteso affrontare l'esame del decreto-legge anche da un punto di vista spesso omesso rispetto al tema complesso delle intercettazioni, ma sempre più importante: quello, appunto, della protezione dei dati personali.
Guardare al tema delle intercettazioni anche da questo punto di vista consente, invece, di valutare compiutamente l'impatto che questo mezzo di ricerca della prova ha sulla persona, modulando conseguentemente il bilanciamento tra esigenze investigative, diritto di difesa e, appunto, privacy.

La necessità di una rimodulazione di questo rapporto è stata da noi sottolineata più volte e, in particolare, in una nota inviata al Presidente del Consiglio nel 2015, sullo schema di ddl delega sul processo penale. Si rappresentava, in particolare, l'esigenza di "una più puntuale selezione del materiale investigativo assicurando, nel doveroso rispetto dei diritti della difesa, che negli atti processuali non siano riportati interi spaccati di vita privata (delle parti ma soprattutto dei terzi), del tutto estranei al tema di prova". Auspicavamo che venissero valorizzati il principio di proporzionalità tra privacy e mezzi investigativi su cui la Corte di giustizia ha fondato la sua più lungimirante giurisprudenza, nonché le indicazioni rese dalla CEDU, in particolare rispetto all'utilizzo di intercettazioni irrilevanti (*vds. la sentenza Craxi del 2003*).

Condivisibile ci appariva l'obiettivo, sancito nella legge-delega, di rafforzare la garanzia della riservatezza anticipando l'udienza stralcio nella cui sede eliminare le intercettazioni irrilevanti e omissando, nei brogliacci, le parti in conferenti, pur nel pieno rispetto del contraddittorio per (e sulla) prova. Positivo, poi, appariva il canone di sobrietà contenutistica previsto in sede cautelare, con l'imposizione al pubblico ministero di un'adeguata selezione delle intercettazioni da inviare a sostegno della richiesta, non ricomprendendovi quelle irrilevanti, da destinare all'archivio riservato con il relativo regime di segretezza.

Le misure volte a limitare la circolazione endoprocessuale delle intercettazioni eccedenti le reali esigenze investigative hanno dunque rappresentato, dal nostro punto di vista, un'importante innovazione della riforma del 2017, che sul punto recepiva un'esigenza di garanzia condivisa anche dalla stessa magistratura, come dimostrano le direttive emanate da alcune Procure nel 2016, nonché le buone prassi indicate dall'organo di governo autonomo nel luglio dello stesso anno.

E' determinante, dunque, che il decreto in conversione confermi quest'esigenza, pur modulando diversamente gli oneri di p.g. e p.m. circa le regole da osservare in fase di trascrizione e, quindi, rendendo quello che era un divieto, per la stessa p.g., di trascrizione di dati irrilevanti un dovere di vigilanza del PM circa l'assenza, nei verbali, di dati irrilevanti.

La modifica impone due considerazioni essenziali: in primo luogo è opportuno che, all'art. 268, c.2-bis, la sottrazione dal verbale riguardi tutti i dati personali irrilevanti e non soltanto quelli che siano anche sensibili (*dizione che va aggiornata a quella dell'art. 9 del Regolamento 2016/679, ovvero appartenenti a categorie "particolari", come pure al comma 6 si dic*e), ovvero inferiti da espressioni lesive della reputazione. La circolazione endoprocessuale di dati irrilevanti a fini investigativi è, infatti, illegittima sotto il profilo della proporzionalità, indipendentemente dalla natura sensibile del dato o dal suo carattere lesivo.
E che il canone di proporzionalità debba osservarsi, unitamente peraltro a quello di minimizzazione, anche in ambito processuale, è ormai definitivamente chiarito dall'art. 3 d.lgs. 51,

di recepimento della direttiva 2016/680 che introduce appunto una disciplina organica della protezione dati in ambito giudiziario penale e di polizia.
In secondo luogo, proprio la derubricazione del divieto di trascrizione in dovere di vigilanza del p.m. impone, per non vanificare la portata innovativa della riforma, un vaglio attento da parte dell'organo requirente, circa l'effettivo rispetto di questo canone di minimizzazione.

Per altro verso, il ripristino della disciplina codicistica della procedura di stralcio affievolisce la garanzia di riservatezza che la riforma Orlando perseguiva con una precisa scansione procedimentale di tale fase *e con la previsione del dovere del p.m. di impartire specifiche prescrizioni per la tutela del segreto sul materiale non trasmesso, in particolare nell' ipotesi di differimento del deposito per particolare complessità delle indagi*ni. Il ripristino, disposto dal decreto, del regime originario, unitamente alla rinuncia al regime di particolare segretezza prima previsto per le intercettazioni da sottoporre a stralcio rischia, insomma, di ripresentare le note criticità sul versante dell'indebita divulgazione degli atti d'indagine, attenuando non poco il potenziale innovativo della riforma.

Un analogo affievolimento delle garanzie di riservatezza deriva *dal ripristino della disciplina originaria del deposito di tutti gli atti a sostegno dopo l'esecuzione della misura*, *nonchè della* dalla soppressione dell'onere, per il p.m., di selezione preventiva, già in sede cautelare, delle sole intercettazioni rilevanti ai fini della richiesta misura cautelare, , che avrebbe consentito di contenere, almeno in parte, il rischio di esfiltrazione di dati, particolarmente ricorrente in questa fase.

Un' ulteriore attenuazione delle misure a tutela della privacy deriva, poi, dalla prevista soppressione della possibilità di procedere a porte chiuse in caso di rinnovazione, in sede dibattimentale, di richieste di acquisizione di intercettazioni contenute in archivio.

Ove tali scelte venissero confermate in conversione, si renderebbe dunque necessario rafforzare le garanzie di riservatezza (almeno) degli atti non acquisiti perché, in particolare, irrilevanti o inutilizzabili, contenuti nell'apposito archivio.
Sotto tale aspetto, il Garante potrà fornire il proprio contributo in sede di parere sul d.M. di disciplina dei criteri di accesso e consultazione dell'archivio, il cui oggetto potrebbe tuttavia essere esteso alla previsione delle particolari misure di sicurezza di cui dotare l'archivio stesso. La sua sicurezza e impermeabilità è, infatti, il presupposto essenziale della riservatezza degli atti lì conservati e, quindi, della privacy degli interessati ma anche dell'efficacia e segretezza dell'azione investigativa.
Analogamente, il distinto decreto (su cui sarebbe opportuno sentire il Garante) sul deposito telematico delle intercettazioni dovrà prevedere misure di protezione adeguate alla particolare rilevanza di questi flussi informativi, che non devono presentare alcuna permeabilità o vulnerabilità, come abbiamo voluto sottolineare già con il provvedimento del luglio 2013 sulle misure di sicurezza nell'ambito delle attività di intercettazione.

Inoltre, se non altro a fini di deterrenza, sarà necessario chiarire le conseguenze sanzionatorie della diffusione del contenuto delle intercettazioni non acquisite, ora oggetto di un generico divieto non presidiato, tuttavia, da specifiche sanzioni.
Da un lato, infatti, il segreto che *ai sensi dell'art.89-bis disp.att.*copre gli atti contenuti nell'archivio indurrebbe a ritenere configurabile, in caso di diffusione di tali atti, il delitto di rivelazione di segreti di cui all'art. 326 c.p. . Dall'altro lato, tuttavia, si dovrebbero ben chiarire i termini di applicabilità, a tale fattispecie, dell'illecito contravvenzionale di pubblicazione arbitraria di cui all'art. 684 c.p., la cui tenue comminatoria edittale sarebbe peraltro inadeguata ad esprimere la particolare offensività di tale condotta .

Sarà poi opportuno coordinare la previsione, di cui all'art. 269, c.2, del diritto degli interessati di chiedere al giudice la distruzione della documentazione non necessaria, a tutela della riservatezza, con l'innovativa procedura introdotta dall'art. 14 dlgs 51/2018. Tale norma legittima infatti "chiunque vi abbia interesse" (non, dunque, solo le parti processuali, al pari dell'art. 269, c.2,) a richiedere al giudice la rettifica, cancellazione o la limitazione dei dati che lo riguardano, anche durante il procedimento penale. Si tratta di una norma dalle notevoli potenzialità, che combinandosi con la procedura di distruzione di cui all'art. 269 potrebbe contribuire a rafforzare sensibilmente le garanzie di riservatezza soprattutto dei terzi, le cui conversazioni siano state indirettamente captate.

.Per quanto invece concerne le intercettazioni mediante captatori, sarebbe stato opportuno *cogliere quest'occasione per colmare le lacune normative che il Garante aveva rilevato in sede di parere sugli schemi di d.lgs. e di decreto attuativo, ma anche nell'ambito della segnalazione rivolta al Parlamento e al Governo lo scorso aprile.* Le straordinarie potenzialità intrusive di tali strumenti impongono, infatti, garanzie adeguate per impedire che essi, da preziosi ausiliari degli inquirenti, degenerino invece in mezzi di sorveglianza massiva o, per converso, in fattori di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio, rendendolo estremamente permeabile se allocato in server non sicuri o, peggio, delocalizzati anche al di fuori dei confini nazionali.

La necessità di tali garanzie sembra, peraltro, asseverata dalle notizie di cronaca (si pensi al caso Exodus), relative alle particolari modalità di realizzazione delle captazioni mediante malware, *da parte delle società incaricate ex art. 348, comma quarto, c.*p.p. Esse evidenziano (*salvo smentita da parte del Procuratore di Napoli, che conduce le indagini*) i rischi connessi all'utilizzo di captatori informatici con il ricorso, da parte delle società incaricate, a tecniche di infiltrazione prive della necessaria selettività.
Ci si riferisce, in particolare, all'utilizzo, ai fini intercettativi, di software connessi ad app, che quindi non sono direttamente inoculati nel solo dispositivo dell'indagato, ma posti su piattaforme (come Google play store) accessibili a tutti. Ove rese disponibili sul mercato, anche solo per errore in assenza dei filtri necessari a limitarne l'acquisizione da parte dei terzi - come parrebbe avvenuto *nei casi noti alle cronache* – queste app-spia rischierebbero, infatti, di trasformarsi in pericolosi strumenti di sorveglianza massiva..

Inoltre, pericoloso è l'utilizzo – che, pure, parrebbe essere stato fatto nei casi all'esame degli inquirenti – di sistemi cloud per l'archiviazione, addirittura in Stati extraeuropei, dei dati captati. La delocalizzazione dei server in territori non soggetti alla giurisdizione nazionale costituisce, infatti, un evidente vulnus non soltanto per la tutela dei diritti degli interessati, ma anche per la stessa efficacia e segretezza dell'azione investigativa.
Il ricorso a tali due tipologie di sistemi (*app o comunque software che non siano inoculati direttamente sul dispositivo-ospite, ma scaricati da piattaforme liberamente accessibili a tutti e, per altro verso, archiviazione mediante sistemi cloud in server posti fuori dal territorio nazionale*) dovrebbe, dunque, essere oggetto di un apposito divieto.

In subordine, si potrebbe prevedere che l'effettiva installazione nel dispositivo elettronico portatile e le conseguenti funzionalità acquisitive del captatore informatico, possano compiutamente realizzarsi solo dopo aver verificato l'univoca associazione tra il dispositivo interessato dal software e quello considerato nel provvedimento giudiziale autorizzativo..
In ogni caso, anche in ragione della rapida evoluzione delle caratteristiche e delle funzionalità dei software disponibili a fini intercettativi, sarebbe opportuno vietare il ricorso a captatori idonei a cancellare le tracce delle operazioni svolte sul dispositivo ospite. Ai fini della corretta ricostruzione probatoria e della garanzia del diritto di difesa è, infatti, indispensabile disporre di software idonei a

ricostruire nel dettaglio ogni attività svolta sul sistema ospite e sui dati ivi presenti, senza alterarne il contenuto.
Si potrebbe esplicitare, in questo senso, il requisito della "affidabilità, sicurezza ed efficacia" dei software utilizzabili a fini captativi- che dovrà essere declinato nel dettaglio dal dM di cui all'art. 2, c.3, su cui per tali ragioni è auspicabile sia acquisito il nostro parere- garantendo così effettivamente la completezza della "catena di custodia della prova informatica". Quest'esigenza è tanto più indispensabile rispetto ad operazioni investigative, quali quelle in esame, ad alto tasso di esternalizzazione e che come tali presentano maggiori vulnerabilità, essendo in larga parte affidate a privati che devono, quindi, essere adeguatamente responsabilizzati rispetto agli obblighi di sicurezza da garantire.

Sarà peraltro opportuno chiarire, all'art. 89, c.2, le conseguenze (in termini di inutilizzabilità dei contenuti captati) del ricorso a programmi informatici non conformi ai requisiti di sicurezza previsti con il dM.

Più in generale, sul piano applicativo, anche nei decreti attuativi si potrebbe prevedere l'adozione di un unico protocollo di trasmissione e gestione dei dati destinati a confluire sui server installati nelle sale intercettazioni delle Procure della Repubblica per la loro conservazione, evitando possibili disomogeneità nei livelli di sicurezza.

Si potrebbe inoltre valutare l'opportunità di rendere disponibili software gestionali idonei a consentire l'analisi dei dati inerenti le caratteristiche dell'accesso ai server utilizzati per l'attività intercettativa da parte dei fornitori privati, anche per la realizzazione delle attività di manutenzione (si pensi al procedimento penale nei confronti della società "Area"). Si eviterebbe, in tal modo, di rendere accessibili, alle aziende stesse, i sistemi di conservazione dei log di accesso alla strumentazione mediante cui è svolta l'attività captativa, rafforzando le garanzie di segretezza della documentazione investigativa.

Sarebbe, peraltro, opportuno definire i criteri di gestione, da parte di ciascun Procuratore della Repubblica, delle intercettazioni eseguite da altri uffici giudiziari e relative a procedimenti gli atti dei quali siano stati successivamente trasmessi per competenza ovvero comunque acquisiti per l'utilizzazione in procedimenti diversi ex art. 270, c.3, c.p.p.

Ferma restando l'opportunità dell'introduzione delle su descritte cautele, la particolare invasività dei software-spia e la loro attitudine a degenerare, sia pure in ipotesi patologiche, in strumenti di sorveglianza massiva, meriterebbe un supplemento di riflessione del Parlamento in ordine alla progressiva estensione dell'ambito applicativo di tale strumento investigativo, che dovrebbe invece restare eccezionale.

E' significativo che la Corte costituzionale tedesca, con sentenze del 27.2.2008 e 20.4.2016, abbia censurato la disciplina delle intercettazioni (sia pur preventive) mediante trojan, per violazione non solo della riserva di giurisdizione ma anche del principio di proporzionalità, che imporrebbe la limitazione di mezzi di prova così invasivi, dal ricorso dunque eccezionale, ai soli casi nei quali siano effettivamente indispensabili per la tutela di beni giuridici primari quali la vita o l'incolumità, con l'adozione di misure tali da circoscriverne l'impatto anche sui terzi.
Nell'escludere l'applicabilità analogica della disciplina delle intercettazioni tradizionali a questi nuovi strumenti investigativi, la Corte ne sottolinea l'intrinseca diversità, propria della loro capacità invasiva e dell'attitudine a esercitare un controllo ubiquitario sull'indagato ma anche sui terzi che gli siano vicini.

Considerazioni, queste, affini a quelle svolte dalla sentenza Musumeci della nostra Cassazione, oltre che dalle SSUU, anche in rapporto ai riflessi che la difficile predeterminazione dello sviluppo delle captazioni, dovuta alla natura itinerante e ubiquitaria del mezzo, ha sulla riserva di giurisdizione. La scarsa prevedibilità dello sviluppo delle captazioni rischia, infatti, di affievolire la funzione di garanzia propria del vaglio autorizzativo del gip, svuotandolo di senso. Per questo, abbiamo più volte sottolineato l'esigenza di compensare tale indebolimento del vaglio ex ante con un maggiore dettaglio della verbalizzazione delle operazioni compiute, così da rafforzare almeno il controllo ex post sulla legittimità dell'attività svolta.

Controllo su cui insiste, a ragione, anche la Corte costituzionale tedesca, esigendo però nel complesso un più rigoroso rispetto del principio di proporzionalità, a tutela del "generale diritto alla libertà del cittadino nei confronti dello Stato".

Questo dev'essere, anche per noi, il parametro essenziale da osservare nella disciplina di strumenti investigativi che devono poter garantire tanto la sicurezza quanto la libertà, secondo la sinergia che richiedono la normativa costituzionale e sovranazionale.