Audizione del Presidente del Garante per la protezione dei dati personali, Prof. Pasquale Stanzione - Audizioni sul disegno di legge n. 808 (Modifiche al codice penale, al codice di procedura penale, all'ordinamento giudiziario e al codice dell'ordinamento militare)

Audizione del Presidente del Garante per la protezione dei dati personali, Prof. Pasquale Stanzione - Audizioni sul disegno di legge n. 808 (Modifiche al codice penale, al codice di procedura penale, all'ordinamento giudiziario e al codice dell'ordinamento militare)

Senato della Repubblica - 2a Commissione Giustizia

(6 settembre 2023)

- IL VIDEO DELL'AUDIZIONE

Ringrazio la Commissione per aver inteso acquisire il punto di vista del Garante rispetto a un provvedimento che interessa la protezione dei dati soprattutto per disposizioni introdotte dall'articolo 2, in materia di intercettazioni e informazione di garanzia. Sul testo il Garante ha espresso un parere, favorevole con raccomandazioni, il 3 agosto, di cui riprenderò il contenuto, pur con gli aggiornamenti necessari a seguito dell'introduzione delle norme sulla centralizzazione dei data center per le intercettazioni, disposta dall'art.2 d.l. 105 del 2023.

Va preliminarmente rilevato come il disegno di legge introduca misure rilevanti per rafforzare le garanzie di riservatezza dei colloqui e delle conversazioni oggetto di captazione; in particolare di quelle che coinvolgano soggetti terzi rispetto alle parti processuali.

In primo luogo, infatti, si estende il divieto di pubblicazione (oggi limitato alle intercettazioni stralciate perché inutilizzabili o irrilevanti) ai contenuti captati che non siano stati riprodotti dal giudice nella motivazione di un provvedimento o utilizzati nel corso del dibattimento. Si introduce, conseguentemente, un corrispondente divieto di rilascio di copie avanzato da soggetti diversi dalle parti e dai loro difensori, in assenza dell'esigenza di utilizzazione dei risultati delle captazioni, in altro procedimento specificamente indicato.

Si limita, in altri termini, la possibilità di circolazione dei contenuti captati ai soli effettivamente utilizzati in sede processuale, di motivazione di un atto del giudice o in ambito dibattimentale.

In secondo luogo, si ricomprendono nella categoria delle espressioni da espungere dalle trascrizioni quelle riguardanti dati relativi a soggetti diversi dalle parti, limitando dunque la circolazione (già) endoprocedimentale dei dati dei terzi.

Le due principali modifiche proposte contribuiscono dunque, in maniera sinergica, a rafforzare le garanzie di riservatezza dei terzi e, per altro verso, a circoscrivere l'ambito circolatorio (endo- ed extra-procedimentale) dei contenuti captati, in virtù di un bilanciamento con il diritto di (e all') informazione, la cui definizione è riservata alla discrezionalità del legislatore.

In questa prospettiva può, tuttavia, valutarsi l'opportunità di introdurre alcune, puntuali modifiche ad altre disposizioni processuali (in materia di archivio delle intercettazioni e di caducazione del segreto), utili a garantirne un migliore coordinamento con le innovazioni proposte. In tal senso, all'articolo 89-bis, c.2, primo periodo, disp. att. c.p.p., si potrebbero aggiungere, in fine, le seguenti parole: "o, comunque, dati personali relativi a soggetti diversi dalle parti". Tale modifica è necessaria per allineare il novero delle intercettazioni da includere nell'archivio digitale con quello relativo alle intercettazioni oggetto di stralcio (art. 268, c.6, c.p.p.).

Per altro verso, la disciplina del segreto di cui all'articolo 269, c.1, secondo periodo, andrebbe coordinata con le innovazioni introdotte, in particolare ancorandone la caducazione all'inserimento nel fascicolo non già del pubblico ministero (art. 373, c.5) ma del giudice (art. 431), riferendolo peraltro non ai contenuti comunque utilizzati nel corso delle indagini preliminari, ma a quelli utilizzati dal pubblico ministero o dal giudice, nei rispettivi provvedimenti.

Tali modifiche contribuirebbero a realizzare un più organico coordinamento delle varie disposizioni processuali considerate con le innovazioni, opportunamente introdotte dal disegno di legge, in ordine alla limitazione del regime circolatorio dei contenuti captati.

Quali indicazioni più sostanziali, si potrebbe in primo luogo circoscrivere ulteriormente il rischio di un'indebita circolazione dei dati oggetto di stralcio - perché inutilizzabili o irrilevanti – bilanciando, tuttavia, tale interesse con l'esigenza di non disperdere del tutto, almeno durante il corso del giudizio nei suoi vari gradi, possibili fonti di prova inizialmente ritenute irrilevanti.

A tal fine, si potrebbero adottare alcuni accorgimenti per rendere effettiva la scansione temporale oggi prevista per la procedura di distruzione del materiale conservato nell'archivio digitale, agevolando l'individuazione dei contenuti da eliminare.

In tal senso si potrebbe, in particolare, valutare di disporre in sentenza, sul modello dell'articolo 262 c.p.p., la distruzione provvisoria- da effettuarsi tuttavia solo dopo che la pronuncia sia divenuta inoppugnabile: art. 269, c.2, c.p.p. - dei verbali e delle registrazioni conservati nell'archivio digitale, con indicazione del numero RIT (registro intercettazioni telefoniche). Tale accorgimento potrebbe agevolare la procedura di distruzione senza alternarne la scansione temporale, così garantendo tanto la riservatezza individuale quanto l'esigenza di non dispersione, fino al giudicato, di fonti di prova suscettibili di rilevare, eventualmente, in un secondo momento.

Ciò imporrebbe, peraltro, la garanzia dell'effettiva sicurezza delle condizioni di conservazione del materiale contenuto nell'archivio digitale.

La particolare delicatezza dei dati lì conservati, eccedenti le esigenze investigative attuali, impone in particolare, l'adozione di regole di sicurezza adeguate e conformi a quelle indicate dal Garante dapprima con provvedimento n. 356 del 18 luglio 2013 e, quindi, in sede di parere sul d.M. 20 aprile 2018.

La reale innovatività della riforma (come, del resto, delle precedenti che hanno previsto la devoluzione all'archivio delle intercettazioni non acquisite) dipende infatti, molto, da come verrà garantita l'effettiva impermeabilità dell'archivio, tramite misure di sicurezza sulla cui adeguatezza il Garante potrà offrire, in una prospettiva anzitutto collaborativa, la propria valutazione.

In tale contesto, è anche auspicabile consolidare il percorso di "razionalizzazione tecnica ed organizzativa dei sistemi di intercettazione, avente quale obiettivo finale la realizzazione dei cinque data center nazionali", cui allude il d.M. 6 ottobre 2022. Il d.l. 105 (sui cui decreti attuativi il Garante si pronuncerà), nel disporre l'istituzione delle infrastrutture digitali interdistrettuali e la migrazione dei dati dalle singole Procure, si muove certamente nella giusta direzione.

Per altro verso, al fine di garantire l'effettivo rispetto del divieto di circolazione endoprocessuale

dei dati captati dei terzi che risultino irrilevanti, si potrebbero agevolare i presupposti di azionabilità della tutela speciale accordata, anche ai terzi e con forme innovative, dall'articolo 14 del d.lgs. 51 del 2018.

Tale norma legittima, infatti, "chiunque vi abbia interesse" (non, dunque, solo le parti processuali, al pari dell'articolo 269, c.2, c.p.p.) a richiedere al giudice, sussistendone i presupposti, 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'articolo 269, potrebbe contribuire a rafforzare sensibilmente le garanzie di riservatezza soprattutto dei terzi, le cui conversazioni siano state indirettamente captate. L'avvio di tale procedura potrebbe, inoltre, garantire di espungere dati di terzi che siano erroneamente presenti negli atti processuali, in assenza dei presupposti ora previsti.

Naturalmente, l'effettività della norma sarebbe rafforzata con un sistema analogo a quello previsto dall'art. 10 AS 1512, nella XV legislatura, per evitare che il soggetto apprenda dell'esistenza, in atti processuali, di proprie conversazioni, direttamente dalla stampa, quando ormai l'intervento ablativo sarebbe tardivo.

Per garantire l'efficacia della tutela remediale senza, tuttavia, gravare il pubblico ministero di un onere informativo eccessivo quale potrebbe apparire quello ipotizzato dall'AS 1512, si potrebbe anche legittimare il terzo, previa conferma dell'esistenza di intercettazioni che lo coinvolgano, al loro ascolto ai fini dell'attivazione della procedura di distruzione di cui all'articolo 269, c.2, c.p.p, secondo periodo o dell' esercizio dei propri diritti alla limitazione o, eventualmente, rettifica dei dati ai sensi dell'articolo 14 d.lgs 51 del 2018.

In tal modo, tramite la connessione procedimentale tra il diritto di cui all'articolo 14 d.lgs. 51, l'istituto della distruzione di cui all'articolo 269 c.p.p. e i proposti limiti alla circolazione endoprocedimentale dei dati dei terzi, potrebbe essere accordata una tutela realmente effettiva alla riservatezza.

L'esame parlamentare del disegno di legge potrebbe rappresentare, peraltro, l'occasione per introdurre maggiori garanzie rispetto alle intercettazioni mediante captatori. Le potenzialità intrusive di tali strumenti impongono garanzie adeguate per impedirne la degenerazione in mezzi di sorveglianza eccessivamente ampia o, per converso, in fattori di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio, rendendolo permeabile se allocato in server non sicuri o, comunque, delocalizzati anche al di fuori dei confini nazionali.

La necessità di tali garanzie sembra, peraltro, asseverata da alcune vicende (si pensi al caso Exodus del 2019), relative a particolari modalità di realizzazione delle captazioni mediante malware, da parte delle società incaricate ai sensi dell'articolo 348, comma quarto, c.p.p. Esse evidenziano i rischi connessi all'utilizzo di captatori informatici con il ricorso, da parte delle società incaricate, a tecniche di infiltrazione prive della necessaria selettività.

Ci si riferisce, in particolare, all'utilizzo, ai fini intercettativi, di software connessi ad app, che quindi non sono direttamente inoculati nel solo dispositivo dell'indagato, ma posti su piattaforme accessibili a chiunque. 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.

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) potrebbe, 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 modificare il contenuto del dispositivo ospite e a cancellare le tracce delle operazioni svolte, come pure rilevato nell'ambito dell'indagine conoscitiva condotta, in materia, da questa Commissione. Ai fini della corretta ricostruzione probatoria, della garanzia del diritto di difesa come anche della privacy 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, corrispondentemente valorizzando l'esigenza di una verbalizzazione analitica delle operazioni compiute.

Si potrebbe esplicitare, in questo senso, il requisito, di cui all'articolo 89, c.4, disp. att. c.p.p., della "affidabilità, sicurezza ed efficacia" dei software utilizzabili a fini captativi (che devono appunto limitarsi alle sole operazioni autorizzate), 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'articolo 89, c.2, disp. att. c.p.p., le conseguenze del ricorso a programmi informatici non conformi ai requisiti di sicurezza previsti con il d.M.

Ferma restando l'opportunità dell'introduzione delle su descritte cautele, la particolare invasività dei software-spia merita certamente una riflessione del legislatore in ordine al reale ambito applicativo di questo mezzo di ricerca della prova. Certamente positiva è la previsione della necessità d'indicazione, nel decreto autorizzativo, delle ragioni di indispensabilità dell'utilizzo del trojan (introdotta dal d.l. 132 del 2021, convertito, con modificazioni, dalla legge n. 178 del 2021) e, per i delitti diversi da quelli di competenza delle Procure distrettuali o dai più gravi contro la p.a., dei luoghi e dei tempi di attivazione del microfono. In tal modo, infatti, si può, almeno in parte, circoscrivere la potenziale ubiquitarietà del mezzo e la difficile predeterminazione dello sviluppo delle captazioni.

Tuttavia, laddove il legislatore ritenesse di ripensare il perimetro di ammissibilità di questo tipo di captazione, utili spunti possono derivare dalla lettura forte dello scrutinio di proporzionalità tra esigenze investigative e riservatezza (nella declinazione dell'intangibilità della vita digitale) offerta, a proposito anche dei trojan, dalla Corte costituzionale tedesca, con sentenze del 27 febbraio 2008 (BVerfG, NJW 2008, 822, sulla online durchsuchung) e del 20 aprile 2016 (BVerfG, I, 20 aprile 2016 - 1 BVR 966/09, 1 BVR 1140/09). Particolarmente rilevante è la considerazione di come il canone di proporzionalità imponga una modulazione delle garanzie che tenga conto delle potenzialità del mezzo investigativo concretamente utilizzato e della sua capacità d'incidenza sul nucleo intangibile della vita privata del soggetto.

Vi ringrazio