GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico

Illustre
Sen. Maria Elisabetta Alberti Casellati
Presidente del Senato della Repubblica

Illustre
On. Roberto Fico
Presidente della Camera dei deputati

Illustre
Prof. Giuseppe Conte
Presidente del Consiglio dei ministri

Illustre
Alfonso Bonafede
Ministro della giustizia

Le scrivo in relazione a possibili modifiche della disciplina delle intercettazioni tra presenti realizzate, in particolare, mediante captatore informatico.

Recenti avvenimenti, descritti anche dagli organi di informazione, hanno infatti dimostrato i rischi suscettibili di derivare dal ricorso, a fini investigativi, da parte delle società incaricate, a determinati software le cui peculiari caratteristiche meriterebbero, a nostro avviso, una disciplina specifica. Ci si riferisce, in particolare, a programmi informatici connessi ad app, non direttamente inoculati, quindi, 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 di trasformarsi in pericolosi strumenti di sorveglianza massiva.

Appare, dunque, opportuna una riflessione in ordine ai limiti di utilizzo di questi software a fini intercettativi, valutando anche la possibilità di un divieto o, in subordine, dell'adozione di ulteriori, specifiche cautele.

L'esame di tale questione è utile, anche, per una più ampia riflessione su alcuni possibili miglioramenti della disciplina delle intercettazioni, che sottoponiamo all'attenzione del Governo e del Parlamento.

Nell'allegarLe il testo che espone, più diffusamente, la problematica qui soltanto accennata, tanto Le segnalo ai sensi degli articoli 37 del decreto legislativo 18 maggio 2018, n. 51 e 23, comma 1, lettera a) del decreto legislativo 10 agosto 2018, n. 101, grato, anche a nome del Collegio del Garante, per l'attenzione che vorrà riservare alle suesposte considerazioni e confermandoLe sin d'ora la più ampia disponibilità dell'Autorità ad ogni collaborazione che dovesse essere ritenuta utile.

Antonello Soro

Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico

L’utilizzo a fini intercettativi in sede giudiziaria, dei captatori informatici è una misura indubbiamente utile alla luce dell’evoluzione delle tecnologie disponibili.

Esso consente, infatti, di prescindere dall’installazione fisica dei dispositivi di captazione per realizzare intercettazioni di comunicazioni e conversazioni tra presenti, inoculando direttamente nel dispositivo-ospite il software-spia.

Tuttavia, le caratteristiche innovative proprie di questi software - e, più in generale, dell’attività intercettativa telematica su terminali mobili di tipo smartphone o su dispositivi informatici assimilabili - sono tali da determinare un sostanziale, rilevantissimo mutamento negli effetti e nelle potenzialità di un mezzo di ricerca della prova, quale quello intercettativo, pensato e normato con riferimento a ben altre realtà.

Alcuni agenti intrusori sarebbero, infatti, in grado non solo di "concentrare", in un unico atto, una pluralità di strumenti investigativi (perquisizioni del contenuto del pc, pedinamenti con il sistema satellitare, intercettazioni di ogni tipo, acquisizioni di tabulati) ma anche, in talune ipotesi, di eliminare le tracce delle operazioni effettuate, a volte anche alterando i dati acquisiti.

Le garanzie stabilite dal codice di rito penale, a tutela dell’indagato (dal riscontro effettivo del giudice sugli atti compiuti dagli inquirenti e sul rispetto delle condizioni stabilite dalla legge per ciascun atto, al contraddittorio sulla prova) risulterebbero, così, fortemente depotenziate dal ricorso, non adeguatamente circoscritto, a tali metodologie di indagine, in ragione delle peculiari caratteristiche che le rendono difficilmente inquadrabili nelle categorie gius-processuali tradizionali.

Questa difficoltà di qualificazione dogmatica è, del resto, alla base del contrasto interpretativo composto, nell’aprile 2016, dalle Sezioni Unite della Corte di Cassazione, che hanno precisato le condizioni di utilizzo dei captatori informatici per realizzare intercettazioni di conversazioni e comunicazioni tra presenti, anche in ambito domiciliare.

Le particolari caratteristiche di queste metodologie di indagine rendono, infatti, l’intercettazione ambientale "itinerante" in quanto disposta su un dispositivo mobile e, per ciò solo, ontologicamente incompatibile con l’indicazione del luogo e le particolari tutele accordate alla riservatezza delle conversazioni svolte in ambito domiciliare.

Cogliendo molte delle indicazioni delle Sezioni Unite, il legislatore ha recentemente disciplinato il ricorso ai captatori informatici, ammettendolo in particolare per le sole intercettazioni tra presenti e demandando a un successivo decreto ministeriale la definizione dei requisiti tecnici dei programmi informatici funzionali all’esecuzione di tali operazioni investigative.

In sede di parere sia sullo schema di decreto legislativo di riforma della disciplina delle intercettazioni, sia sullo schema di decreto ministeriale attuativo, il Garante ha fornito al Governo alcune proposte di integrazione del testo, utili a circondare di maggiori garanzie l’utilizzo dei captatori informatici a fini investigativi.

In sede di parere sullo schema di decreto legislativo, in particolare, si invitava a valutare l’opportunità di includere nel decreto autorizzativo -anche per i delitti di competenza delle Procure distrettuali- l’indicazione dei luoghi e del tempo della captazione al fine di rafforzare, anche in questo ambito, le garanzie connesse ad un più incisivo controllo del giudice sull´attività investigativa. Si rappresentava, peraltro, come tale modifica avrebbe contribuito a sviluppare in tutta la sua portata il criterio di delega di cui all´articolo 1, comma 84, lett. e), della legge 103 del 2017, laddove prescrive di scindere la fase dell´inserimento del captatore da quella della effettiva attivazione del microfono, al fine di circoscrivere per quanto possibile l´invasività di tale mezzo di ricerca della prova e di garantire la dovuta corrispondenza delle operazioni intercettative all´oggetto del decreto autorizzativo.

Inoltre, il Garante invitava il Governo a precisare alcune parti del decreto legislativo che rischiavano di legittimare, in via interpretativa, l´acquisizione (sia pur senza possibilità di utilizzazione in giudizio) di dati personali anche al di fuori dei limiti temporali e spaziali stabiliti dal decreto autorizzativo del gip.

Infine, si ravvisava l’opportunità di introdurre un espresso divieto (con la relativa sanzione in caso di inosservanza) di conoscibilità, divulgabilità e pubblicabilità di intercettazioni realizzate mediante captatori, inerenti soggetti estranei ai fatti per cui si proceda, peraltro in conformità ai criteri di delega.

In sede di parere sullo schema di decreto ministeriale, invece, il Garante aveva sottolineato l’esigenza di specificare con maggiore dettaglio i moduli software suscettibili di utilizzo, tra quelli che, comunemente, compongono un sistema di intercettazione mediante captatore informatico (es. il software che, installato sui dispositivi target, opera l’acquisizione delle informazioni; il sistema di

inoculazione; il sistema di gestione; ecc.).

Si rilevava, inoltre, la necessità di indicare in modo puntuale le misure tecniche da adottare al fine di garantire la riservatezza dei dati sui sistemi funzionali all'esecuzione delle intercettazioni mediante captatore informatico, specificando ad esempio le modalità di accesso ai sistemi da parte degli operatori autorizzati, le funzionalità di registrazione delle operazioni ivi svolte, le modalità di trasmissione dei dati acquisiti mediante captatore.

Infine, si suggeriva di escludere il ricorso a captatori il cui funzionamento abbassasse il livello di sicurezza del dispositivo-ospite per impedirne la compromissione da parte di terzi, con eventuali riflessi negativi sulla protezione dei dati personali ivi contenuti, nonché sulla stessa riservatezza dell'attività investigativa.

La maggior parte di tali indicazioni non sono state recepite dai testi definitivamente approvati. In essi manca, soprattutto, la previsione di garanzie adeguate per impedire che, in ragione delle loro straordinarie potenzialità intrusive, questi strumenti investigativi, da preziosi ausiliari degli organi 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 diffuse dagli organi di stampa, in relazione alle particolari modalità di realizzazione delle captazioni mediante malware, da parte delle società incaricate ex art. 348, comma quarto, c.p.p.

Le indagini giudiziarie in corso, di cui ha dato notizia la stampa, hanno infatti dimostrato i rischi connessi all'utilizzo di captatori informatici in assenza delle necessarie garanzie e, soprattutto, con il ricorso, da parte delle società incaricate, a tecniche particolari, meritevoli di cautele ulteriori, in ragione delle loro peculiari caratteristiche e specifiche potenzialità.

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, estremamente 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.

A tal fine, si potrebbe ricorrere all'integrazione del decreto ministeriale del 20 aprile 2018, ovvero si potrebbe novellare il decreto legislativo n. 216 del 2017, la cui efficacia in parte qua è comunque differita ai provvedimenti autorizzativi emessi dopo il 31 luglio prossimo.

In subordine, ove non si ritenesse di sancire un divieto espresso di ricorso a tali tecniche, si potrebbe prevedere - anche in tal caso, preferibilmente con norma primaria - 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 introdurre - in sede legislativa o anche soltanto novellando il citato decreto ministeriale - un espresso divieto di ricorso a captatori idonei a cancellare le tracce delle operazioni svolte sul dispositivo ospite. Ai fini della corretta ricostruzione probatoria e della completezza e veridicità del materiale investigativo raccolto 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 "integrità, sicurezza e autenticità dei dati captati" che, ai sensi dell'art.4, comma 1, del decreto ministeriale, i software utilizzati devono assicurare, garantendo così effettivamente la completezza della

“catena di custodia della prova informatica”.

Più in generale, sul piano applicativo, se non attraverso una specifica integrazione del decreto ministeriale stesso, si potrebbe anche 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, per la realizzazione delle attività di manutenzione. 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.

Tanto si segnala ai sensi degli articoli 37 del decreto legislativo 18 maggio 2018, n. 51 e 23, comma 1, lettera a) del decreto legislativo 10 agosto 2018, n. 101, ai fini dell’adozione dei provvedimenti ritenuti opportuni, confermando la piena disponibilità dell’Autorità per la collaborazione che dovesse essere ritenuta utile.