GIUSTIZIA INSIEME

Processo Penale

La riforma della disciplina delle intercettazioni preventive dei Servizi di informazione per la sicurezza nella legge di bilancio

di Federica Resta

22 dicembre 2022

Federica Resta è dirigente del Garante per la protezione dei dati personali.
Le opinioni contenute nel presente contributo sono espresse a titolo esclusivamente personale e non impegnano in alcun modo l'Autorità

Tra gli emendamenti governativi al disegno di legge di bilancio, approvati in Commissione alla Camera dei deputati, il 123.01.000 introduce disposizioni rilevanti in materia di intercettazioni preventive da parte dei Servizi d'informazione per la sicurezza della Repubblica.

L'inserimento della disposizione nel disegno di legge di bilancio (che non può contenere norme a carattere ordinamentale: art. 15, c.2, l. 243 del 2012) è motivata essenzialmente in ragione dell'esigenza di modificare l'imputazione dei fondi destinati a coprire queste operazioni,

spostandola dal relativo capitolo all'interno dello stato di previsione del Ministero della giustizia allo specifico programma di spesa (il 5.2), contenuto all'interno dello stato di previsione del Ministero dell'economia e delle finanze. In questo modo, "*si consente anche di evitare la circolazione al di fuori del Comparto intelligence di documentazione contabile contenente elementi di natura sensibile, come numeri telefonici e autorità giudiziaria autorizzante, che rende riconducibile la relativa attività ai Servizi di informazione, determinando un evidente vulnus alle esigenze di riservatezza che caratterizzano le suddette operazioni".*

Tuttavia, l'emendamento non si limita alla modifica dell'imputazione contabile ma incide anche sulla disciplina dell'istituto, con innovazioni significative e una sua complessiva "sistematizzazione"(così definita dalla Relazione illustrativa).

In particolare, l'emendamento mira ad autonomizzare la disciplina delle intercettazioni del Comparto intelligence rispetto a quella delle intercettazioni volte alla prevenzione di gravi reati (art. 226 disp.att.c.p.p.) cui, invece, l'art. 4 d.l. 144 del 2005, convertito, con modificazioni, dalla l. 155 del 2005, nel suo testo attuale rinvia integralmente.

L'esigenza di una disciplina autonoma è comprensibile, in ragione delle caratteristiche che connotano le operazioni captative di competenza dei Servizi d'informazione per la sicurezza della Repubblica, finalizzate alla tutela di un interesse giuridico, quale la sicurezza nazionale, dallo statuto normativo del tutto peculiare. Così come comprensibile appare l'esigenza di sistematizzazione della disciplina, sinora caratterizzatesi per stratificazioni successive e rinvii normativi incrociati meritevoli, certamente, di un *drafting* migliore. L'emendamento, a tal fine, introduce, nel corpo del d.l. 144 del 2005, un apposito articolo, il 4-bis, recante appunto "Disposizioni in materia di intercettazioni preventive dei servizi di informazione per la sicurezza".

In estrema sintesi, le innovazioni principali della disciplina concernono i presupposti autorizzatori delle operazioni captative (non solo di natura intercettativa), i termini per il deposito dei verbali, gli adempimenti successivi alle comunicazioni al Copasir e le possibilità di utilizzo degli elementi acquisiti mediante le operazioni.

Con riferimento alla diversa disciplina dei presupposti legittimanti le operazioni, va anzitutto segnalata la soppressione del riferimento- che resta invece, nell'art. 226 disp.att.c.p.p. per le intercettazioni preventive "di polizia"- al contenuto dell'obbligo motivazionale del provvedimento autorizzatorio del Procuratore della Repubblica, relativo alla sussistenza di elementi investigativi che giustifichino l'attività di prevenzione e alla ritenuta (da parte dell'a.g.)

necessità del compimento dell'atto. La norma proposta prevede ora che le intercettazioni siano autorizzate "*quando risultano sussistenti le condizioni*" che le giustificano, ossia quando siano *ritenute* indispensabili per l'espletamento delle attività rimesse alle Agenzie (Aise e Aisi). Si esclude, dunque, la necessità che l'istanza sia sorretta da "*elementi investigativi*" giustificanti la captazione.

Tale, almeno apparente, alleggerimento dell'onere motivazionale della richiesta, è tuttavia compensato dall'oggetto della valutazione rimessa al Procuratore generale presso la Corte d'appello di Roma, che con decreto (motivato, conformemente al requisito richiesto dall'art. 15 Cost.) dovrà accertare la sussistenza della (ritenuta) indispensabilità delle attività intercettative (anche ambientali, come del resto già prevede la disciplina vigente) per l'espletamento delle attività demandate alle Agenzie. Tale indispensabilità costituisce, infatti, il requisito legittimante le captazioni ai sensi del nuovo art. 4-bis, c.1, d.l. 144 del 2005. Resta, peraltro, fermo, rispetto al testo vigente, l'onere motivazionale relativo alla sussistenza di ragioni che rendano necessaria la proroga (eventuale) dell'intercettazione.

Innovazioni rilevanti caratterizzano anche la disciplina del deposito, presso il Procuratore generale, dei verbali delle operazioni di ascolto svolte e dei contenuti intercettati, oltre che dei contenuti captati e dei supporti mobili eventualmente utilizzati. In particolare, il termine per il deposito viene esteso da cinque (prorogabili a dieci in caso di traduzione) a trenta giorni. Il termine del deposito- che può avvenire anche "con modalità informatiche" da individuarsi con dPCM- può peraltro essere prorogato ad un massimo di sei mesi, su autorizzazione del Procuratore generale, in presenza di richiesta motivata che comprovi "particolari esigenze di natura tecnica e operativa".

La norma, inoltre, onera espressamente il Procuratore generale della distruzione (in questo caso non qualificata dal requisito dell'immediatezza prescritto, invece, per il materiale depositato e le copie, anche informatiche, totali o parziali, dei contenuti) della documentazione da lui stesso detenuta, ad eccezione dei decreti autorizzatorii, una volta decorso il termine per l'adempimento, da parte del Presidente del Consiglio dei Ministri, degli obblighi di comunicazione al Copasir.

In ordine alla disciplina dell'utilizzo successivo degli elementi acquisiti attraverso le operazioni captative, la *data retention* e il tracciamento delle comunicazioni "per lo sviluppo della ricerca informativa", il generale divieto di utilizzo nel procedimento penale è confermato e anzi rafforzato. Il comma 5 del nuovo art. 4 bis sopprime, infatti, il riferimento (presente invece al comma 5 dell'art. 226 disp. att.c.p.p.) alla possibilità di utilizzo, ai soli fini investigativi, dei

risultati delle intercettazioni (e delle altre operazioni descritte).

Tale differenza si spiega con la strutturale diversità dell'attività d'intelligence rispetto a quella disciplinata dall'art. 226 disp.att., che mira pur sempre alla prevenzione di delitti. Per la prima ben si giustifica, dunque, un'ancor più radicale separazione rispetto al procedimento penale. Essa è, peraltro, temperata pur sempre dal dovere, sancito dall'art. 23, c.7, della l. 124 del 2007 in capo agli Organismi (*recte*: ai loro direttori) di comunicare *"informazioni ed elementi di prova relativamente a fatti configurabili come reati, di cui sia stata acquisita conoscenza nell'ambito delle strutture che da essi rispettivamente dipendono*" alla polizia giudiziaria. L'adempimento dell'obbligo può essere peraltro ritardato, su autorizzazione del Presidente del Consiglio dei ministri, "*quando ciò sia strettamente necessario al perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza*".

Significative sono, inoltre, le innovazioni che caratterizzano i presupposti legittimanti l'acquisizione dei tabulati e il tracciamento delle comunicazioni, ai sensi dell'art. 4-bis, c.4. Per tali operazioni, infatti, non è più previsto il requisito (sancito dall'art. 226 disp.att.) della necessità investigativa né il deposito di elementi a supporto, ma la mera finalizzazione di tali operazioni all'espletamento delle attività (genericamente indicate) demandate ai Servizi (non solo, a rigore, alle Agenzie, come invece dispone, per le intercettazioni, il comma 1 del'art. 4-bis). In tal senso depone, infatti, il riferimento operato dal comma 4 del citato articolo 4-bis, introdotto dall'emendamento, alle sole "modalità" di svolgimento delle operazioni di cui al comma 1 dell'articolo 4 del d.l. 144 del 2005 (ovvero previa richiesta di autorizzazione avanzata, anche dai direttori dei Servizi, su delega del Presidente del Consiglio dei Ministri).

Circa la "profondità cronologica" dell'acquisizione, ovvero la risalenza dei tabulati (tema oggetto di una copiosa giurisprudenza della Cgue), la norma continua, come per le operazioni di cui all'art. 226 disp.att.c.p.p., a far mero riferimento ai dati in possesso degli operatori (dunque, per i tabulati, con estensione del termine massimo di settantadue mesi tuttora in vigore ai sensi dell'art. 24 l. 167 del 2017). I tabulati, come già previsto dall'art. 226 disp.att., vanno distrutti entro sei mesi (termine prorogabile nel massimo a ventiquattro su autorizzazione del Procuratore generale, ma senza più la previsione del requisito, sancito invece dall'art. 226 disp.att., della indispensabilità per la prosecuzione dell'attività di prevenzione).

Tale nuova disciplina, pur sancendo presupposti meno stringenti dell'attuale rispetto alla *data retentio*n, sembra comunque compatibile con la giurisprudenza della Corte di giustizia europea, che in materia ha avuto modo di rilevare come:

- la direttiva 2002/58 si applichi a ogni tipo di conservazione dei dati di traffico, seppur finalizzata ad un'eventuale acquisizione per fini di sicurezza nazionale. L'argomento sotteso a tale assunto è che il fine perseguito non muta l'attività di conservazione, ritenuta in quanto tale lesiva della riservatezza già prima di ogni acquisizione: cfr., in particolare, CGUE, sent. 6 ottobre 2020, C 623-17, Privacy international,, ove al punto 49 si afferma che "*l'articolo 1, paragrafo 3, l'articolo 3 e l'articolo 15, paragrafo 1, della direttiva 2002/58, letti alla luce dell'articolo 4, paragrafo 2, TUE, devono essere interpretati nel senso che rientra nell'ambito di applicazione di tale direttiva una normativa nazionale che consente a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica di trasmettere ai servizi di sicurezza e di intelligence dati relativi al traffico e dati relativi all'ubicazione ai fini della salvaguardia della sicurezza nazionale*";
- il fine di sicurezza nazionale legittimi, tuttavia, la deroga ai limiti stringenti previsti per la *data retention* "giudiziale" tali da consentire la conservazione preventiva (che invece con le sentenze di aprile e settembre 2021 la Corte esclude, salvo presupposti limitati, per la *data retention* giudiziale). Significativa, in tal senso, la sentenza del 20 settembre 2022, Space Net, cause riunite C-793 e 794/19 che, ai fini della disciplina dei tabulati, traccia una distinzione (rilevante anche in termini di "gerarchia assiologica") tra "*criminalità particolarmente grave*" e minacce "*per la sicurezza nazionale*", la cui importanza "*è maggiore rispetto a quella degli altri obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58*" (punto 72) . In replica a un'eccezione della Commissione europea tesa ad equiparare i due presupposti, la Corte ha infatti ribadito (punti 92-94) che la salvaguardia della sicurezza nazionale corrisponde "*all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società, mediante la prevenzione e la repressione delle attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare da minacciare direttamente la società, la popolazione o lo Stato in quanto tale, quali le attività di terrorismo*". La Corte nota inoltre come, diversamente dalla criminalità, anche particolarmente grave, una minaccia per la sicurezza nazionale debba caratterizzarsi per requisiti di concretezza ed attualità o, quantomeno, prevedibilità, desumibili dalla ricorrenza di "*circostanze sufficientemente concrete da poter giustificare una misura di conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione, per un periodo limitato*". Tali diversità inducono la Corte a rigettare la tesi della Commissione volta ad equiparare la criminalità particolarmente grave alle minacce per la sicurezza nazionale, così introducendo, ad avviso dei giudici, una categoria intermedia tra la sicurezza nazionale e la pubblica sicurezza, applicando alla seconda i requisiti inerenti alla prima;
- le deroghe ammissibili per ragioni di sicurezza nazionale incontrino, tuttavia, il limite della proporzionalità, in quanto l'acquisizione non deve essere massiva. Come chiarisce la sentenza Privacy International ai punti 81 e 82, infatti, "*una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di procedere alla comunicazione mediante trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati*

> *relativi all'ubicazione ai servizi di sicurezza e di intelligence eccede i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica, così come richiesto dall'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta [...]; l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, dev'essere interpretato nel senso che osta ad una normativa nazionale che consente a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica, ai fini della salvaguardia della sicurezza nazionale, la trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence".*

Tanto la disciplina vigente quanto quella proposta dall'emendamento sembrano, dunque, conformarsi al canone di proporzionalità indicato come dirimente nel *reasoning* della Corte e applicabile, appunto, anche alle operazioni limitative della riservatezza (quali, appunto, la conservazione dei tabulati) funzionali ad esigenze di sicurezza nazionale.

Ma il controllo sull'osservanza, in concreto, di questo principio fondativo risiede, principalmente, nel vaglio rimesso al Procuratore generale presso la Corte d'appello di Roma sulla sussistenza dei requisiti legittimanti le operazioni. Un presidio importante, cui è affidato, in ultima analisi, il delicato equilibrio tra esigenze di salvaguardia della sicurezza nazionale e riservatezza individuale.