QUESITI

STEFANO ATERNO

L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nella privacy

L'art. 2 L. 17 aprile 2015, n. 43 (c.d. "decreto antiterrorismo") ha introdotto nel codice di procedura penale l'art. 234-*bis* c.p.p., recante Acquisizione di documenti e dati informatici, con il quale si disciplina l'acquisizione di documenti e dati informatici conservati all'estero («1. È sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare»).

Questa disposizione normativa si inserisce in un quadro repressivo tipico della lotta al terrorismo nel quale con strumenti legislativi eccezionali e di prevenzione si risponde, o meglio, si tenta di rispondere, all'utilizzo di sistemi tecnologici e informatici sempre più potenti e avanzati in grado di criptare ogni tipo di comunicazione e nascondere ogni traccia di attività delittuose, vanificando gli sforzi delle forze di polizia e delle intelligence più efficienti.

L'art. 234-*bis* c.p.p. in primo luogo, indirettamente, conferma una tecnica investigativa consolidata basata sull'acquisizione di dati e documenti informatici conservati sulla rete. Quando i dati informatici (informazioni, documenti, foto, *post* e messaggi in chiaro dei social *network,* spesso presenti su piattaforme informatiche all'estero) sono disponibili e fruibili grazie ad una semplice navigazione in rete, la loro acquisizione per finalità di indagine può avvenire anche senza che qualcuno presti il consenso.

In particolare, rientrano in questa categoria ad esempio i dati relativi ai profili pubblici sui *social network*, il contenuto di un sito *web* o di un *blog,* le fotografie pubblicate su piattaforme di condivisione a livello mondiale, i messaggi lasciati *on line* nei gruppi di discussione pubblici e altri dati simili.

La caratteristica che hanno tutte queste informazioni è che per scelta consapevole (o a volte inconsapevole) dell'interessato o del proprietario del dato stesso, essi sono condivisi con una sfera indeterminata di soggetti.

Per acquisire tali dati con modalità forensi e per finalità di indagine (anche difensiva) esistono sistemi *software,* anche *open source*, che garantiscono in modo sufficiente e spesso ripetibile, l'integrità e la genuinità del dato informatico acquisito da remoto, operando quindi nel rispetto delle norme codicistiche introdotte dalla L. 18 marzo 2008, n. 48 (art. 247, 248, 352 e 354 c.p.p.).

Ma l'art. 234-*bis* c.p.p. in realtà attribuisce un potere molto più ampio. Consente, sempre e a chiunque, di acquisire documenti e dati informatici conservati all'estero non disponibili al pubblico grazie al semplice consenso prestato da un non meglio specificato "legittimo titolare".
Dal punto di vista soggettivo tale potere di acquisizione sembra esercitabile anche dalla polizia giudiziaria non delegata dal pubblico ministero nonché dal legale che svolge le indagini difensive sempre che vi sia il consenso di qualcuno che li detiene o di un soggetto che esercita su di essi un diritto soggettivo.
Preliminarmente affronteremo questa seconda tipologia di dati "non pubblici" soffermandoci più avanti e diffusamente sul controverso significato di "legittimo titolare". Non disponibili al pubblico sono tutti quei dati informatici che un soggetto non ha voluto condividere pubblicamente con una pluralità di individui, non ha voluto diffondere nella rete, che ha voluto mantenere riservati, protetti, conservati nel *cyberspazio* in apposite aree accessibili *on line* con l'utilizzo di credenziali di autenticazione o con tecniche di cifratura. Certamente in questa categoria rientrano anche tutti quei dati e quelle informazioni che il soggetto ha voluto condividere solo con una ristretta cerchia di utenti (esempio i messaggi "privati" presenti su molti *social network*). Nella maggior parte dei casi si tratta di dati memorizzati e "residenti" su piattaforme informatiche caratterizzati da una gestione su *cloud computing* e spesso difficilmente collocabili geograficamente sul territorio. Tra i dati di cui all'art. 234-*bis* c.p.p. vi potrebbero essere anche dati oggetto di comunicazione e di corrispondenza (pensiamo solo ai flussi di dati tipici delle *chat*) oppure alle caselle di posta elettronica. È noto infatti che le società che gestiscono applicazioni per telefoni cellulari o sistemi in *cloud*, sui quali vengono veicolate comunicazioni tra due o più soggetti, non garantiscono e non assicurano la distruzione o l'assenza di memorizzazione delle comunicazioni finanche dopo l'avvenuta cancellazione della conversazione sul dispositivo degli utenti.
Rientrano in questa seconda ipotesi anche tutti i cd. metadati ovvero quelle informazioni, utili a fini investigativi (anche difensivi), relative alla struttura tecnica di un *file*, alla sua creazione, modifica, scambio, cancellazione, diffusione oppure anche quei dati relativi alle connessioni, all'accesso, alla durata e all'attività di un utente su una piattaforma informatica. I metadati (per loro natura non sono pubblici) sono presenti e memorizzati nei server delle società che forniscono ogni tipo di servizio informatico per conto dei loro clienti (*account email, app*, gioco *on line*, *chat*, *social network, storage* dei dati tipo *dropbox* o *google drive, amazon*).
Ad un anno dall'ingresso nel codice di procedura penale dell'art. 234-*bis* c.p.p. non si ha notizia dell'applicazione e dell'uso investigativo di questo

strumento ma forse è presto per fare analisi statistiche soprattutto se la sua introduzione è stata determinata da esigenze antiterrorismo.
Alcune delle perplessità che circondano questa norma derivano dalla possibilità per le forze di polizia e per la magistratura di chiedere alla società situata all'estero i dati e le informazioni oggetto di comunicazione o di corrispondenza scambiate in tempo reale tra due o più soggetti sotto indagine in Italia ma non necessariamente presenti entrambi sul suolo italiano. L'acquisizione di tali dati costituirebbe una intercettazione telematica che non può essere effettuata ai sensi dell'art. 234-*bis* c.p.p. in quanto sarebbe in violazione delle norme sulle intercettazioni e sulle rogatorie internazionali avvenendo l'acquisizione spesso in tempo reale e non sempre su dati statici, bensì su *server* stranieri (che li "rimbalzano" su *server* italiani o sui *server* delle forze di polizia) costituendo una vera e propria captazione da remoto (ovvero dall'Italia) di un dato informatico che contiene una comunicazione tra due soggetti memorizzata su un *server* all'estero.
La norma in commento trae spunto dall'art. 32 della Convenzione di Budapest del 2001 sui crimini informatici e le indagini telematiche (ratificata dall'Italia con la legge n. 48 del 2008)[1] che ha ispirato il Legislatore italiano nella formulazione dell'art. 234-*bis* c.p.p. soprattutto nel punto in cui prevede che il richiedente può ottenere i dati informatici se : "..ottiene il consenso lecito e volontario del soggetto legalmente autorizzato a trasmettere tali dati attraverso detto sistema informatico".
Differentemente da quanto accade per le norme della Convenzione di Budapest del 2001, che sono applicabili solo in materia di *cybercrime,* l'art. 234-*bis* c.p.p. si può applicare in occasione di qualunque ipotesi delittuosa. ...

[1] «*A party may, without the authorisation of another Party: a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b) access of receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the party through that computer system*» in *www.conventions.coe.int* (STCE n. 185). Il richiamo è presente in BERRUTI, *Commento al d.l. 7/2015, art. 2,* Cyber terrorism*: esigenze di tutela preventiva e nuovi strumenti di contrasto*, in *www.lalegislazionepenale.eu.*