GIURISPRUDENZA PENALE

Il sistema del *Data Retention* come strumento investigativo.

di ***Alessandra Cardone***

Sommario. 1. Introduzione – **2.** Il concetto di Data Retention – **3.** L'attività investigativa nell'era tecnologica – **4.** L'orientamento della Corte di Giustizia europea – **5.** Considerazioni finali

1. Introduzione

Attraverso l'utilizzo, smisurato, di internet e dei dispositivi informatici vengono realizzate un numero illimitato di attività quotidiane che talvolta sfociano nell'illecito.

Di qui la necessità di confrontarsi con gli strumenti volti ad accertare e reprimere ogni forma di attività criminosa realizzata in rete andando oltre il sistema delle intercettazioni, già preso in considerazione dal legislatore e dagli organi requirenti, verso un campo più ostico che oscilla tra l'esigenza di prevenire e comprimere la realizzazione di reati e la tutela di diritti personalissimi: il problema relativo al Data Retention.

2. Il concetto di Data Retention

Per Data Retention si intende il **periodo di conservazione dei dati** telefonici e relativi al traffico telematico.

Un sistema che realizza la possibilità di rintracciare ed identificare la fonte e la destinazione di una comunicazione, determinandone tutte le coordinate: la data, l'ora e la durata, il tipo di connessione, le attrezzature utilizzate dagli utenti per comunicare e la loro ubicazione.

I limiti posti attualmente per l'espletamento di questa attività sono chiari e garantisti: nessun dato di cui sia facilmente individuabile e conoscibile il contenuto può essere conservato ed estrapolato se non dalle autorità nazionali competenti ed autorizzate e per fini tassativamente individuati dalla normativa comunitaria e dalla giurisprudenza di legittimità.

Attualmente, in Italia, il tempo di conservazione di tali informazioni è di *un anno per i dati relativi al traffico telematico, due anni per i dati relativi al traffico telefonico e trenta giorni per quelli attinenti le chiamate senza risposta* (**art. 132 del Codice della *privacy***).

Una tempistica *à la page* dato che nella società del XXI secolo le comunicazioni telematiche contano un numero di gran lunga maggiore rispetto quelle telefoniche. L'intervento della legge europea n. 167 del 2017, che ha introdotto all'art. 24 *l'obbligo di conservazione per sei anni dei dati necessari all'accertamento e della repressione dei reati di cui agli artt. 51 co.*

3-quater e 407 co. 2, lettera a) c.p.p., ha ampliato le problematiche già esistenti sui tempi di conservazione dei dati esterni alle comunicazioni.
La norma svilisce, di fatto, la portata dell'art. 132 del Codice della *privacy*, perché in questo modo l'esigenza investigativa sarà sostenuta dalla legge europea del 2017 senza considerare che i gestori dei servizi di connettività, quando raccolgono i dati, ignorano i reati per il cui accertamento tali informazioni potranno essere richieste dall'autorità giudiziaria.
Tuttavia, va osservato che l'autorità giudiziaria, indipendentemente dalla prassi fino ad ora verificata, deve rispettare le scadenze riconducibili dalla normativa prevista per ogni tipologia di dato preso in considerazione e per ogni reato per il quale le informazioni vengono richieste.
Dunque, per le fattispecie non riconducibili alla competenza della Legge europea n. 16 del 2017, la richiesta di esibizione dei metadati dovrà rispettare le scadenze di : trenta giorni per le chiamate senza risposta; un anno per i dati relativi al traffico telematico; due anni per le informazioni circa il traffico telefonico, pena l'impossibilità di procedere o, eventualmente, l'inutilizzabilità dei dati esibiti.
Il Data Retention, nonostante la sua natura innovativa e poco conosciuta, si poggia su un contesto normativo già esistente: la **direttiva 2006/24/CE**[1] tesa a regolamentare la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione; **la direttiva 2002/58/CE** del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.
Tuttavia, è altresì fondamentale il riferimento al Regolamento Generale sulla Protezione dei dati personali per meglio inquadrarne l'ambito applicativo.
L'art. 5 del GDPR, nello specifico al comma 1 lettera e), richiede che i dati personali siano "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione*

[1] La direttiva europea 2006/24/CE del Parlamento europeo e del Consiglio regolamenta la conservazione (compreso i tempi) di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. Adottata in seguito agli attentati di Londra e Madrid del 2004 e 2005, armonizzava le disposizioni degli Stati membri dell'UE sulla conservazione dei dati delle conversazioni telefoniche e del traffico telematico, garantendone, quindi, la disponibilità a fini di indagine e di perseguimento di gravi reati.
Cfr. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32006L0024&from=de

nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («*limitazione della conservazione*»)".
L'articolo 13 comma 2, lettera a) del GDPR prevede che *il titolare del trattamento debba informare gli interessati circa il periodo di conservazione dei dati personali, oppure, se ciò non è possibile, almeno dei "criteri utilizzati per determinare tale periodo"*.
È chiaro che un tempo di conservazione infinito non è ammissibile, deve essere sempre limitato e deve essere necessariamente proporzionato alla finalità medesima. Alla scadenza del termine di conservazione il dato va cancellato (ovviamente da tutti i supporti, compreso i backup), oppure in alternativa anonimizzato.
La cancellazione del dato una volta perseguite e raggiunte le finalità predefinite è idoneo ad assicurare la protezione dei dati di carattere personale (art. 8 Carta di Nizza), la tutela della libertà di espressione e di informazione (art. 11 Carta di Nizza) e della vita privata e della vita familiare (art. 7 Carta di Nizza).

3. L'attività investigativa nell'era tecnologica
Così la conservazione dei dati di traffico telefonico e telematico faciliterebbe l'attività investigativa degli inquirenti, essendo essa propedeutica a delineare il profiler del soggetto agente.
Su questa base si cerca di capire se, ed in che modo, il sistema del Data Retention sia idoneo ad adempiere agli obiettivi di ricerca della prova alla pari delle intercettazioni. Sul punto si è espressa la Corte di Giustizia europea che, con sentenza, ha limitato l'utilizzo e la conservazione del dato per i soli fini investigativi in conformità del diritto comunitario.
Il punto di partenza ricade sul sistema investigativo. In un tempo precedente all'insediarsi della tecnologia probabilmente l'attività degli organi requirenti e della polizia giudiziaria avrebbe seguito il metodo dell'investigatore belga H. Poirot ma ad oggi le cose stanno diversamente.
Alla stregua dell'evoluzione tecnologica, attualmente, l'intercettazione sembra essere il mezzo di ricerca della prova più utilizzato per lo svolgimento delle operazioni di captazione occulta durante la fase delle indagini preliminari.
Attorno al tema delle intercettazioni ruotano principi di rango costituzionale: l'esigenza processuale di ricerca della prova come altresì il rispetto dei diritti fondamentali dell'uomo. Dunque, è giocoforza ritenere che tali aspetti devono confrontarsi con il diritto alla riservatezza delle comunicazioni (art. 15 Cost.); con il diritto al rispetto della vita privata e della vita familiare (art. 7 Carta dei Diritti

Fondamentali dell'Uomo); libertà di espressione e di informazione (art. 11 Carta dei Diritti Fondamentali dell'Uomo); rispetto della dignità dei soggetti coinvolti.
La riforma del 2019 (D.L. 161/19) ha permesso l'utilizzo del Trojan che consiste nell'inserimento di un captatore informatico su un dispositivo elettronico portatile per il perseguimento di reati contro la Pubblica Amministrazione ovvero di reati posti in essere da pubblici ufficiali.
Dunque, il campo applicativo nell'uso dell'intercettazione è circoscritto ai delitti inseriti nel Titolo II del Libro II codice penale.

4. L'orientamento della Corte di Giustizia europea

L'art. 24 della Legge n. 167 del 29 novembre 2017, dispone che gli operatori telefonici sono tenuti a conservare i dati del traffico telefonico e telematico, nonché i dati relativi alle chiamate senza risposta, acquisiti a decorrere dal 21 aprile 2015, per il termine di 72 mesi.
Tuttavia, la Corte di Giustizia europea aveva già invalidato la Direttiva 2006/24/CE del 15 marzo 2006 del Parlamento europeo e del Consiglio, inerente la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, che imponeva un termine di conservazione dei dati da un minimo di 6 mesi sino a massimo di 24 mesi.
Per la Corte, il legislatore europeo, con l'adozione della direttiva sulla conservazione dei dati, ha **ecceduto i limiti imposti dal rispetto del principio di proporzionalità.**
Inoltre, più di recente la stessa Corte (sentenza dell'8 aprile 2014, cause riunite, C-293/12 e C-594/12), ha dichiarato l'illegittimità della direttiva "Frattini" (2006/24/CE) per incompatibilità con il principio di proporzionalità tra esigenze investigative e misure limitative della privacy.
Di qui la necessità di riformare la disciplina interna tale da garantire un equo bilanciamento di interessi in gioco, circoscrivendo i limiti di ammissibilità della misura in questione data l'eccessiva invasione nel diritto alla riservatezza.
Nel 2016, la Corte di Giustizia europea con la sentenza Tele2 Sverige (cause riunite C 203/15 e C 698/15) ha dichiarato incompatibile con la direttiva 2002/58 ogni previsione interna che, per contrastare reati *imponga la conservazione, generale e indiscriminata, di tutti i dati di traffico e relativi all'ubicazione degli utenti dei mezzi*; *legittimi l'accesso delle autorità nazionali competenti ai dati conservati per finalità ulteriori rispetto a quelle di contrasto dei "serious crimes"*, in assenza di un previo vaglio giurisdizionale o comunque di un'autorità amministrativa indipendente e di garanzie relative alla conservazione dei dati nella Ue.

Non osservando quanto rilevato dalla giurisprudenza comunitaria, la legge n. 167/2017 ha esteso a sei anni il termine massimo di conservazione dei tabulati, con la possibilità di acquisire dati limitatamente ai procedimenti per reati distrettuali o per i quali la durata delle indagini preliminari è estesa a due anni.

Orientamento della Suprema Corte[2], sostiene che la disciplina in riferimento sarebbe compatibile con il principio di proporzionalità poiché in sostanza circoscrive in un tempo limitato la conservazione del dato oltre a demandare al pubblico ministero l'effettivo controllo dell'acquisizione dei dati. Dunque, la Cassazione sostiene la pronuncia della Corte di Giustizia che rimette il controllo al giudice o ad una autorità amministrativa indipendente. Secondo l'interpretazione della Corte alla qualità di autorità amministrativa indipendente e di giudice dovrebbe essere equiparata quella di "autorità giudiziaria", ricomprendendo in questo modo anche la magistratura requirente.

Tuttavia, questa ricostruzione rischia di non essere più compatibile con i principi affermati dalla Corte di giustizia con la sentenza del 2 marzo 2021 (C-746/18) su rinvio pregiudiziale della Corte suprema estone, con particolare riferimento alla limitazione dell'acquisizione processuale dei dati di traffico ai soli procedimenti per gravi reati o per gravi minacce per la sicurezza pubblica e, dall'altro, alla subordinazione dell'acquisizione dei dati all'autorizzazione di un'autorità terza rispetto all'autorità pubblica richiedente (nella specie, il pubblico ministero).

Nella recente pronuncia, la Corte stabilisce che il diritto comunitario si oppone ad una normativa nazionale che *impone a un fornitore di servizi di comunicazione elettronica, a fini di lotta contro le infrazioni in generale o di salvaguardia della sicurezza nazionale, la trasmissione o la conservazione generalizzata e indifferenziata di dati relativi al traffico e alla localizzazione*".

Ogni regola vuole però le sue eccezioni e la Corte nella sentenza sopra riportata, ne indica le relative deroghe.

È ammesso l'accesso e l'utilizzo per fini investigativi ad una serie di dati di comunicazioni elettroniche dai quali si possa trarre informazioni sulla vita privata di un soggetto, solo in presenza di due condizioni: ove occorra accertare, perseguire, contrastare gravi forme di criminalità, ovvero prevenire gravi minacce alla sicurezza pubblica.

Se così fosse, nulla impedirebbe all'Autorità giudiziaria nazionale e al pubblico ministero di avvalersi di questo strumento per condurre l'attività investigativa.

Inoltre, lo Stato membro può derogare all'obbligo di garantire la riservatezza dei dati telefonici e telematici qualora la conservazione generale e indiscriminata di tali dati avvenga per un periodo limitato (eventualmente prorogabile nel caso in cui la minaccia persistesse) e se strettamente

[2] Cass., Sez. V 24 aprile 2018 n. 273892 e Sez. III 23 agosto 2019 n. 36380

necessario (è il caso di minaccia presente e prevedibile alla sicurezza nazionale).
Allo stato attuale, l'ordinamento interno va adeguato ai principi emersi dalla giurisprudenza nazionale ed europea prevedendo che l'accesso del pubblico ministero ai tabulati sia subordinato all'autorizzazione del giudice ovvero, in caso di urgenza, alla realizzazione cui fa seguito la convalida.

5. Considerazioni finali

L'Italia sembra essere il solo paese ad aver adottato una disciplina interna che prevede la conservazione del dato fino a 6 anni.
In Russia la Data Retention è fino a 6 mesi e circoscritta a particolari ragioni di sicurezza nazionale.
La Francia ha fissato per la conservazione dei dati un termine non superiore a 12 mesi. In Germania vengono conservati per 10 settimane, quanto a traffico telefonico e navigazione in internet, mentre i dati sulla geolocalizzazione sono cancellati dopo 4 settimane.
In Belgio le tempistiche variano dai 6 ai 9 mesi, in base alla gravità dei reati riscontrabili. Stesso criterio in Spagna, dove la norma fissa la conservazione dati a 12 mesi, che possono essere ridotti a 6 mesi o estesi a 2 anni, a seconda delle fattispecie. In Australia si conservano i dati di traffico telefonico e internet per 2 anni. Il caso americano è a sé: la conservazione del dato è di 1 anno.
Questo risulta essere un campo ancora aperto che abbisogna di essere analizzato e chiarito nella sua interezza. Ci vorrà ancora del tempo affinché il bilanciamento[3] tra esigenza di reprimere ogni forma di attività delittuosa con qualsiasi mezzo e interesse a tutelare la sfera del dato personale, sia avvalorato e sostenuto da una disciplina normativa puntuale e dettagliata.

[3] Art. 52 c.1 della Carta dei Diritti Fondamentali dell'Unione Europea, secondo cui è richiesta una riserva di legge per giustificare l'ingerenza pubblica nella sfera privata, la quale deve in ogni caso rispettare il nucleo essenziale dei diritti coinvolti e deve comunque essere proporzionata all'obiettivo da raggiungere, che deve corrispondere all'attuazione di finalità di interesse generale riconosciute dall'Unione Europea o all'esigenza di proteggere diritti e libertà altrui