filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Sicurezza pubblica e principio di proporzionalità: quando e come le agenzie di intelligence possono acquisire e ritenere i dati raccolti dal provider

12 Ottobre 2020
Roberto Louhichi

Indice:

1. Il caso Privacy International

Il 6 ottobre 2020, la **Corte di Giustizia dell'Unione Europea** si è pronunciata sul caso Privacy International (Case C.623/17) e sulle controversie ad esso riunite. Sulla scorta della precedente giurisprudenza, il giudice europeo statuisce circa l'**incombatibilità** rispetto al diritto dell'Unione delle norme nazionali che impongano alle società di servizi di comunicazioni elettroniche di effettuare **operazioni generali ed indiscriminate di trasmissione e ritenzione dei dati** di traffico e di geolocalizzazione per **finalità generali di salvaguardia della sicurezza pubblica o di prevenzione del crimine**.

La massima ha origine dalla soluzione di **due questioni pregiudiziali**, sollevate dall'Investigatory Powers Tribunal di Londra, giudice nazionale inglese competente a decidere sul ricorso avanzato dalla Privacy International, organizzazione non governativa per la difesa dei diritti umani, contro le agenzie di sicurezza e di Intelligence del Regno Unito ("SIA"), in cui la ricorrente lamentava che **l'acquisizione e l'utilizzo dei dati di comunicazione di massa** (chi utilizza il telefono/computer; ubicazione dei telefoni cellulari e di rete fissa interessati da chiamate in entrata o in uscita; ubicazione dei computer utilizzati per l'accesso ad Internet) **da parte delle SIA era contrario sia all'articolo 8 della Convenzione Europea dei Diritti dell'Uomo che alla normativa europea di settore**.

Le autorità resistenti replicavano circa la legittimità del trattamento in quanto essenziale alla tutela della sicurezza nazionale, sottolineando altresì come, una volta entrate in possesso dei dati, le SIA conservassero i medesimi in maniera sicura, utilizzando tecniche non orientate a obiettivi specifici e noti (cd. tecniche non mirate), ritenute essenziali per l'esercizio dei compiti delle autorità stesse, consistenti nella **prevenzione e repressione delle gravi minacce alla pubblica sicurezza**, con particolare riferimento al terrorismo, allo spionaggio ed alla proliferazione delle armi nucleari.

In quest'ottica, secondo le resistenti, l'acquisizione e l'utilizzo dei dati trasmessi dagli operatori di servizio di comunicazioni elettroniche deve ritenersi escluso dall'ambito di applicazione della direttiva e, in ogni caso, legittimo, in quanto fondamentale per la tutela della sicurezza nazionale del Regno Unito.
Fatte queste brevi premesse, si può passare all'analisi delle due questioni pregiudiziali

2. La prima questione pregiudiziale
La prima questione affrontata dal giudice europeo riguardava **l'applicabilità della direttiva 2002/58 (cd. Direttiva e-privacy) e l'esclusione dal suo campo di applicazione della sicurezza nazionale**.

> **In altre parole, il giudice del rinvio domandava se la prescrizione contenuta in un ordine rivolto da un ministro a un gestore di reti di comunicazione elettronica di fornire dati di comunicazione in massa alle agenzie di sicurezza e di intelligence di uno Stato membro rientri nell'ambito di applicazione del diritto dell'Unione e della suddetta direttiva.**

Sposando le conclusioni dell'Avvocato Generale, la Corte dà una risposta affermativa al quesito, concentrandosi sull'analisi delle disposizioni fondamentali della direttiva, ovverosia gli articoli 1, 3 e 15, i quali rispettivamente prevedono che:

- "*La presente direttiva non si applica alle* ***attività che esulano dal campo di applicazione*** *del trattato che istituisce la Comunità europea, [...] né, comunque, alle attività riguardanti la* ***sicurezza pubblica, la difesa, la sicurezza dello Stato*** *(compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale* " (articolo 1 comma 3);
- "*La presente direttiva si* ***applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica*** *accessibili al pubblico su reti pubbliche di comunicazione nella Comunità* " (Articolo 3 comma 1);
- "*Gli Stati membri possono* ***adottare disposizioni legislative volte a limitare i diritti e gli obblighi*** [...] *della presente direttiva, qualora tale restrizione costituisca,* [...], *una* ***misura necessaria, opportuna e proporzionata*** *all´interno di una società democratica per la* ***salvaguardia della sicurezza nazionale*** *(cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell´uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare* ***misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo*** ". (Articolo 15)

Nell'affermare l'applicabilità della direttiva al caso di specie, **non ritenendo dunque escluso dal campo di applicazione della fonte normativa l'esercizio di attività a tutela della pubblica sicurezza**, il giudice europeo argomenta come segue.

Le tre disposizioni sopra riportate devono essere interpretate in via sistematica, alla luce dello scopo di "**tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche**" perseguito dal legislatore europeo (articolo 1 comma 1).

> **Così, l'articolo 1 comma 1 va interpretato nel senso che restano escluse dall'ambito di applicazione della direttiva le attività dello Stato, nei settori specificatamente indicati, e non già le attività delle società di comunicazione elettronica che si interfaccino a quelle dello stesso. Vale a dire, la direttiva non deve applicarsi per le attività di sicurezza degli Stati membri ma vale invece diversamente per le attività di trattamento (quali la trasmissione alle agenzie governative) delle società di comunicazioni elettroniche che siano correlate alle prime.**

Depone a favore di questa conclusione il combinato disposto degli articoli 3 e 15, nella misura in cui:

- L'articolo 3 prevede l'applicazione della direttiva per i trattamenti personali ***connessi*** alla fornitura di servizi di comunicazione elettronica, focalizzandosi dunque sulla regolamentazione delle attività del provider di tali servizi;
- L'articolo 15, riconoscendo agli Stati membri il potere di adottare le suddette misure legislative limitative dei diritti degli interessati, presuppone necessariamente che tali disposizioni nazionali rientrino nell'ambito di applicazione della direttiva, la quale, oltre a dettare il rispetto delle **condizioni di necessarietà, opportunità e proporzionalità**, cita espressamente il fine di salvaguardia della sicurezza nazionale.

Dalla lettura composta delle due disposizioni, chiude sul punto la Corte, deve ritenersi che la direttiva si applichi anche alle disposizioni legislative che, come nel caso di specie, prevedono un obbligo del provider di trasmissione dei dati alle autorità di intelligence interne, poiché tale comunicazione costituisce un trattamento di dati da parte delle società di comunicazione, essendo dunque qualificabile come attività di queste ultime e non degli Stati (articolo 3 della direttiva), ed essendo esse riconducibili alle misure di cui all'articolo 15.

3. La seconda questione pregiudiziale

La seconda questione, subordinata a risposta favorevole alla prima, concerneva la **compatibilità delle misure legislative interne** (nello specifico Inglesi) **con i principi della Convenzione Europea dei Diritti dell'Uomo e della giurisprudenza dell'Unione Europea**.

A riguardo, lungi dall'analizzare puntualmente i rilievi specifici che il giudice fa alla normativa inglese, sono di fondamentale importanza le massime giuridiche che esso pronuncia.

In primo luogo, la Corte sottolinea come le **misure legislative** di cui all'articolo 15 devono essere **interpretate come eccezione al generale principio di salvaguardia dei diritti e delle libertà degli interessati**.

> **Tradotto, la direttiva 2002/58 non autorizza gli Stati membri ad adottare, sulla base delle necessità di salvaguardia nazionale, disposizioni interne limitative dei diritti e degli obblighi da essa riconosciuti ed imposti (con specifico riferimento al diritto di riservatezza delle comunicazioni), a meno che tali misure non siano compatibili con i principi generali del diritto dell'Unione, inclusi il principio di proporzionalità ed i diritti fondamentali della Convenzione.**

Chiarito il principio generale, il giudice passa a declinarlo alla luce dei casi concreti riuniti. Così, vengono espressamente dichiarate incompatibili con la direttiva, per violazione del principio di proporzionalità:

- le misure legislative nazionali che impongono al provider una **generale ed indiscriminata trasmissione dei dati** di geolocalizzazione e traffico alle agenzie di intelligence **per fini di generale salvaguardia della sicurezza pubblica**;
- le misure legislative nazionali che impongono al provider **una generale ed indiscriminata ritenzione dei dati** di geolocalizzazione e traffico **per generali finalità di prevenzione**;

Ammonisce la Corte come tali disposizioni costituiscano una ingerenza molto significativa nei diritti fondamentali riconosciuti dalla Convenzione e dal diritto dell'Unione, poiché esse **non richiedono alcun collegamento tra gli interessati, i cui dati sono oggetto dei trattamenti di cui ai due punti sopra, e le finalità generali di prevenzione e salvaguardia della sicurezza pubblica**.

> **In altre parole, il giudice europeo ammette limitazioni ai diritti degli interessati solo se basate su fattori oggettivi e non discriminatori che valgano a provare che la trasmissione e ritenzione di dati di un determinato soggetto sia dettata da una specifica esigenza di salvaguardia della sicurezza a lui correlata . Tali condotte sono dunque compatibili col diritto dell'Unione solo se portate avanti con tecniche mirate, ovverosia tecniche specifiche di acquisizione e ritenzione di dati di obiettivi specifici e noti.**

L'unica apertura che la Corte fa invece al ricorso a tecniche non mirate, consistenti nella raccolta e ritenzione di dati non già sulla base di obiettivi precisi e noti bensì di salvaguardia generale, è alle situazioni in cui uno Stato membro si trovi ad affrontare una seria minaccia, sia essa attuale o prevista, alla propria sicurezza nazionale.

Solo in questi casi limite l'applicazione del principio di proporzionalità della direttiva non preclude il ricorso ad ordini governativi di **trasmissione generale ed indiscriminata dei dati di traffico e geolocalizzazione**, a patto che il provvedimento sia successivamente **oggetto di una verifica della sussistenza di tali condizioni da parte di un organo giudiziario o un'autorità amministrativa indipendente**.

In tutti i casi, chiosa il giudice europeo, **la portata e la ritenzione dei dati non devono eccedere la quantità ed il tempo strettamente necessari** per il perseguimento delle finalità di sicurezza pubblica, siano esse specifiche o generali.

4. Conclusioni

La pronuncia sul caso Privacy International, nonché a quelli riuniti, rappresenta sicuramente una **giurisprudenza fondamentale per la materia e-privacy**, venendo a fissare una serie di punti che vale qui la pena, a beneficio del lettore, rapidamente scorrere:

- applicabilità della direttiva 2002/58 alla raccolta di dati, da parte di un provider, tramessi poi alle autorità di uno Stato membro per fini di salvaguardia nazionale;
- illegittimità delle disposizioni interne di uno Stato membro che riconoscano il potere di quest'ultimo a pretendere la trasmissione, in via generale ed indiscriminata (quindi mediante **tecniche non mirate**), di dati raccolti dal provider, se ciò è giustificato solo sulla base di una **generale esigenza di prevenzione e sicurezza pubblica**. L'ordine di trasmissione, generale ed indiscriminata, è invece legittimo se sorretto da esigenze di prevenzione correlate ad una **seria minaccia, sia essa attuale o prevista, alla prevenzione e sicurezza nazionale di uno Stato membro**;
- legittimità delle misure interne di uno Stato membro, purché disciplinanti **condizioni obiettive e non discriminatorie**, che riconoscano il potere di quest'ultimo a pretendere la trasmissione, in via specifica (quindi mediante **tecniche mirate**), di dati raccolti dal provider e relativi ad un obiettivo noto, se ciò è giustificato sulla base di una **concreta e specifica esigenza di prevenzione e sicurezza pubblica correlata all'interessato**;
- illegittimità delle misure interne che permettano allo Stato di acquisire dal provider e ritenere i **dati in misura superiore rispetto a quanto si rende necessario per il perseguimento delle finalità di prevenzione e salvaguardia nazionale**, integrando ciò una violazione del **principio di necessarietà** (articolo 15 della direttiva).

Resta da vedere che effetti questa giurisprudenza avrà sia sull'attività di intelligence degli Stati membri che sulla loro attività processuale, ricordando che, guardando al nostro ordinamento, l'art. 191 del Codice di Procedura Penale sanziona con l'**inutilizzabilità le prove** raccolte in violazione dei divieti stabiliti dalla legge e quindi, di conseguenza, anche dalla direttiva e-privacy, in quanto recepita dal Decreto Legislativo 196 del 2003 (Codice Privacy).

TAG: *privacy, intelligence, e-privacy*