GIUSTIZIA INSIEME

Costituzione e Carte dei diritti fondamentali" class="voce">

Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla data retention. I riflessi sulla disciplina interna

di Federica Resta

6 marzo 2021

Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla *data retention*. I riflessi sulla disciplina interna

La sentenza del 2 marzo scorso della Corte di giustizia, su rinvio pregiudiziale sollevato dalla Corte suprema estone, chiarisce due aspetti importanti della disciplina della data retention desumibile dall'art. 15, p.1, della direttiva 2002/58/CE, applicabile alla materia dopo la declaratoria di invalidità della direttiva 2006/24/CE sancita dalla stessa Corte nel 2014. La sentenza odierna chiarisce, da un lato, come la disciplina vigente esiga la limitazione dell'acquisibilità processuale dei dati di traffico ai soli procedimenti per gravi reati o per gravi minacce per la sicurezza pubblica e, dall'altro, che l'acquisizione dei dati è subordinata all'autorizzazione di un'autorità terza (giudice o autorità indipendente) rispetto all'autorità pubblica richiedente (nella specie era il pubblico ministero estone).

Sommario: - 1. La giurisprudenza della Corte di giustizia sulla *data retention* 2. La giurisprudenza italiana 3. La sentenza del 2 marzo della Cgue e i suoi riflessi sulla disciplina interna

1. La giurisprudenza della Corte di giustizia sulla data retention.

Con sentenza del 2 marzo, resa nella causa C-746/18, su rinvio del Riigikohus (Estonia), la Corte di giustizia europea – a soli cinque mesi da quella resa nel caso Privacy International – consolida ulteriormente quell'indirizzo innovativo che ha già caratterizzato il suo approccio al tema della data retention.

L'avvio a quest'indirizzo pretorio è stato fornito dalla sentenza Digital Rights dell'8 aprile 2014 (cause riunite C-293/12 e C-594/12), con cui Corte di giustizia ha dichiarato l'illegittimità della direttiva 2006/24/Ce per violazione del principio di proporzionalità nel bilanciamento tra protezione dati ed esigenze di pubblica sicurezza. La violazione del principio di proporzionalità era, in quel caso, ravvisata, in particolare: nella previsione di misure di conservazione dei dati applicabili in via indifferenziata e generalizzata "all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, in assenza di differenziazione, limitazione o eccezione in ragione dell'obiettivo del contrasto ai *serious crimes*; nell'omessa adozione di criteri oggettivi idonei a limitare l'accesso a tali dati per sole esigenze di accertamento di reati sufficientemente gravi da giustificare una simile ingerenza"; nell'omessa previsione dei parametri sostanziali e procedurali per l'accesso, da parte delle competenti autorità nazionali, ai dati in esame, in particolare non richiedendo in ogni caso il previo controllo dell'autorità giudiziaria o di un'autorità amministrativa indipendente; nell'omessa introduzione di parametri idonei a differenziare la durata della conservazione dei dati.

La Corte ha, in quella sede, precisato anche che il principio di stretta proporzionalità tra limitazioni dei diritti fondamentali ed esigenze di pubblica sicurezza esige una differenziazione specificamente modulata in base al tipo di delitto, alle esigenze investigative, al tipo di dato e di mezzo di comunicazione utilizzato. E questo, comunque nel rispetto di alcune garanzie essenziali, quali, in particolare, la subordinazione di tali limitazioni all'autorizzazione di un'autorità terza quale l'autorità giudiziaria o comunque un'autorità amministrativa indipendente.

Con la sentenza resa nel caso Tele2 Sverige (cause riunite C 203/15 e C 698/15) il 21 dicembre 2016, la Corte di giustizia ha dichiarato incompatibile con la direttiva 2002/58 (lette retroattivamente alla luce della Carta di Nizza e riespansa a seguito dell'invalidazione della 2006/24 ad opera della sentenza Digital Rights) ogni previsione interna che, per fini di contrasto dei reati: a) imponga la conservazione, generale e indiscriminata, di tutti i dati di traffico e relativi all'ubicazione degli utenti dei mezzi; b) 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.

Le discipline interne sulla data retention devono pertanto prevedere- osserva la Corte- **l**'accessibilità dei dati conservati solo da parte dell'autorità giudiziaria o di un'autorità amministrativa indipendente, in base a circostanze e procedure disciplinate dalla legge per esigenze di accertamento di gravi reati, notificando la misura all'interessato (come già affermato dalla Corte EDU nella sentenza Zakharov del 4.12.15), non appena le esigenze investigative lo consentano.

Ma l'aspetto maggiormente innovativo della pronuncia concerne l'esigenza di rendere selettiva e mirata la stessa conservazione dei tabulati, limitandola in ragione del tipo di dato, del mezzo di comunicazione considerato, della durata della ritenzione, delle persone coinvolte (che devono avere un collegamento almeno indiretto con la commissione di gravi reati), finanche di criteri geografici che limitino la conservazione ad aree caratterizzate da rischi specifici. Si tratta di criteri che finiscono con il mutare profondamente la natura stessa della data retention come misura preventiva e come tale applicabile massivamente, in vista di un'acquisizione, soltanto eventuale e retrospettiva, in sede giudiziaria.

2. **La giurisprudenza italiana**

I principi affermati dalla Corte hanno indotto il Garante per la protezione dei dati personali a invitare più volte il legislatore (con una segnalazione e i pareri resi sugli schemi di decreti legislativi di adeguamento al Gdpr e, rispettivamente, di recepimento della direttiva 2016/680) a riformare la disciplina interna sulla conservazione dei tabulati, che non limita (né limitava allora) l'acquisizione ai soli reati gravi, né subordina (né subordinava) tale acquisizione al vaglio del giudice.

La carenza di proporzionalità della disciplina interna è risultata poi aggravata dalla novella di cui alla l. 167/2017, che ha esteso a sei anni il termine massimo di conservazione dei tabulati, con acquisibilità dei dati, in questo caso, limitata tuttavia ai procedimenti per reati distrettuali o per i quali la durata delle indagini preliminari è ampliata a due anni. E naturalmente, benché l'acquisibilità dei dati raccolti oltre due anni prima (per i tabulati telefonici, un anno prima per i telematici e un mese per le chiamate senza risposta) sia limitata a tale categoria di reati particolarmente gravi, proprio la natura retrospettiva di questo strumento investigativo implica la conservazione generalizzata dei dati di traffico per sei anni, salvo poi limitarne l'utilizzabilità

processuale ai soli casi considerati. L'incidenza della misura sulla privacy dei cittadini è, dunque, particolarmente forte, a fronte di un'utilizzabilità processuale dei dati così massivamente raccolti, in fondo limitata, con implicazioni probabilmente poco coerenti con il principio di proporzionalità tra esigenze investigative e privacy.

Tuttavia, più volte la Corte di Cassazione (Cass., Sez. V, 24 aprile 2018, 273892 e Sez. III, 23 agosto 2019, n. 36380) ha ritenuto la disciplina interna compatibile con il canone di proporzionalità in quanto delimita temporalmente la durata della conservazione; demanda al pubblico ministero l'effettivo controllo della stretta necessità dell'acquisizione dei dati. Ad avviso della Corte, l'attribuzione di tale vaglio al pubblico ministero non contrasta con le indicazioni della Corte di giustizia relative al controllo rimesso al "giudice" o ad una autorità amministrativa indipendente, in quanto tale nozione dovrebbe, secondo la Cassazione, essere equiparata a quella di "autorità giudiziaria" idoneo a ricomprendere anche la magistratura requirente.

La sentenza 13 febbraio 2020, n. 5741 della Corte di Cassazione ha, inoltre, affermato che "non può ritenersi che la disciplina italiana di conservazione dei dati di traffico (c.d. *data retention*) sia in contrasto con le pronunce della Corte di giustizia datate 8 aprile 2014 e 21 dicembre 2016 poiché la suddetta normativa prevede la conservazione dei dati per un periodo limitato pari a 24 mesi, subordina la possibilità di acquisizione degli stessi soltanto per finalità di accertamento e repressione dei reati, prevede che l'utilizzazione degli stessi dati sia sottoposta al provvedimento di acquisizione emesso da parte del Pubblico Ministero e cioè di un organo giurisdizionale che procede nell'ambito di una attività di indagine preliminare. Ne deriva quindi affermare che la legislazione italiana non prevede la facoltà delle autorità pubbliche di accesso indiscriminato ai dati sensibili bensì la limita ai soli casi di indagini per fatti di reato svolte entro un determinato arco temporale di 24 mesi (elevati a 72 solo per fatti di reato di particolare allarme sociale) e la subordina alla autorizzazione proveniente da un organo giurisdizionale. [...] Va pertanto ribadita la legittimità della normativa nazionale di riferimento costituita dall'art. 132 Codice della privacy, poiché la deroga al diritto alla riservatezza delle comunicazioni è prevista per un periodo limitato, ha come esclusivo obiettivo l'accertamento e la repressione dei reati è subordinato alla emissione di un provvedimento da parte di un'autorità giurisdizionale".

Con la sentenza del 6 ottobre scorso resa nel caso Privacy International (C 623-17), la Corte di giustizia europea ha poi chiarito come alla conservazione dei dati di traffico funzionale al successivo utilizzo per fini di sicurezza nazionale si applichi comunque la disciplina di protezione dati e, quindi, anche il canone di proporzionalità. Si è trattata di un'affermazione importante, che ha escluso che l'esimente della funzionalità del trattamento a fini di sicurezza

nazionale possa “coprire” anche la conservazione dei dati ad esso finalizzata, sebbene comunque nel nostro ordinamento finanche i trattamenti per fini di sicurezza nazionale siano soggetti alla disciplina di protezione dati (art. 58 dlgs 196/2003).

3. **La sentenza del 2 marzo della Cgue e i suoi riflessi sulla disciplina interna**

Con la sentenza del 2 marzo, la Corte di giustizia ha invece chiarito due aspetti essenziali: da un lato la limitazione dell’acquisibilità processuale dei dati di traffico ai soli procedimenti per gravi reati o per gravi minacce per la sicurezza pubblica e, dall’altro, la subordinazione dell’acquisizione dei dati all’autorizzazione di un’autorità terza rispetto all’autorità pubblica richiedente (la Corte precisa che l’accesso delle autorità nazionali competenti ai dati conservati dev’essere “subordinato ad un controllo preventivo effettuato o da un giudice o da un’entità amministrativa indipendente e (…) la decisione di tale giudice o di tale entità [deve] interven[ire] a seguito di una richiesta motivata delle autorità suddette”) .

Più precisamente, sotto il primo profilo, la Corte precisa che “l’articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell’articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l’accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all’ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull’ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l’accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo” Sotto il secondo profilo, la Corte rileva come la disciplina europea osti “ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l’azione penale in un successivo procedimento, competente ad autorizzare l’accesso di un’autorità pubblica ai dati relativi al traffico e ai dati relativi all’ubicazione ai fini di un’istruttoria penale”.

Anche questa sentenza, come le altre, ha riflessi importanti sulla disciplina interna, che considera i gravi reati come criterio idoneo a modulare diversamente la profondità cronologica dell’acquisizione processuale, senza tuttavia limitarne in via generale l’ammissibilità. Inoltre,

merita qualche riflessione la compatibilità con la sentenza della procedura interna che legittima all'acquisizione il pubblico ministero – che vi provvede con decreto motivato – non esigendo, diversamente da quanto previsto per le intercettazioni, il vaglio del giudice (in disparte la disciplina del freezing di cui al comma 4-ter dell'art. 132 dlgs 196/2003, che a fortiori andrebbe ripensato)..

Tale diversità di regime e il conseguente diverso ruolo svolto dal giudice nell'ambito delle due discipline è stata ritenuta conforme dalla Corte costituzionale che, accogliendo la teoria tedesca delle "sfere" concentriche lungo le quali si articolerebbe, con diversa intensità, la tutela dei diritti fondamentali, già con la sentenza n. 81 del 1993, ha ravvisato nell'acquisizione dei tabulati un'incidenza solo marginale sul diritto alla libertà e segretezza delle comunicazioni di cui all'art. 15 Cost. Come sottolinea Carlotta Conti (Sicurezza e riservatezza, in Dir.pen.porc., 2019, n. 11, 1572), infatti, la natura emergente o periferica del diritto inciso è il parametro che induce la Corte a ritenere, secondo i principi di adeguatezza e proporzionalità, non indispensabile il rispetto della riserva di giurisdizione, considerando sufficiente un modello di tutela più tenue, costituito da un provvedimento del pubblico ministero adeguatamente motivato. La Corte allora delineava, dunque, parallelamente alle prove incostituzionali (e come tali inammissibili) perché, appunto, lesive di diritti costituzionalmente tutelati, la categoria delle prove (allora atipiche) "rafforzate" perché incisive su diritti di libertà, ammettendo per lesioni solo periferiche di tali diritti un bilanciamento "attenuato" che moduli le tutele in ragione dell'entità solo marginale della compressione del diritto.

Nella stessa prospettiva si muovono le sentenze su richiamate della Corte di cassazione del 2018, nonché quella del 23 agosto 2019, n. 36380, secondo cui "la soluzione italiana è coerente con il sistema di tipo accusatorio, nel quale, nel corso delle indagini preliminari, è il pubblico ministero l'autorità giudiziaria che procede, e con il sistema processuale che prevede, mediante le indagini difensive ed i poteri riconosciuti ai difensori anche in tema di acquisizione del dato, l'estensione, anche se parziale, del potere investigativo alla difesa. E ciò in una situazione in cui l'acquisizione del dato genera una compromissione decisamente inferiore rispetto a quella relativa alla captazione delle conversazioni, sia telefoniche che ambientali, la cui tutela è affidata invece al controllo del giudice per le indagini preliminari".

La ricostruzione della Corte costituzionale e quella, ad essa allineata, della stessa Corte di cassazione- pur condivisibile in quanto tesa a modulare le garanzie in misura proporzionale all'incidenza dello strumento investigativo sul diritto costituzionalmente tutelato- sembra tuttavia oggi distante dalla ricostruzione della Corte di giustizia. Essa, infatti, rimarca l'esigenza

di un vaglio da parte di un'autorità terza sulla richiesta di acquisizione: non tanto e non solo, dunque, "giudiziaria" (equiparandovi anche le autorità amministrative indipendenti), quanto piuttosto terza; dato, quest'ultimo, difficilmente compatibile con la figura del pubblico ministero come "parte pubblica"

E' probabilmente questa diversità di posizioni la ragione sottesa alla difficoltà che si registra, da noi, nell'adeguamento della disciplina della data retention ai principi sanciti dalla Corte di giustizia. Il giorno dopo la pubblicazione della sentenza Digital Rights il Sen. Casson presentò un'interrogazione relativa alle sue ricadute nel nostro ordinamento, in cui si chiedeva al Governo se intendesse proporre o comunque sostenere una rivisitazione della disciplina vigente in tema di *data retention*, tale da differenziare condizioni, limiti e termini di conservazione dei dati di traffico telefonico e telematico in ragione della particolare gravità del reato per cui si proceda e che eventualmente subordinasse anche (magari con la sola eccezione dei "delitti distrettuali" o comunque di criminalità organizzata per i quali può ammettersi la sola richiesta del pubblico ministero) la conservazione dei dati all'autorizzazione del gip, ferma restando, ovviamente, nei casi d'urgenza, la possibilità per il pubblico ministero di disporre la conservazione con proprio decreto, soggetto a convalida solo in fase successiva, sul modello dell'art. 267, c.2, cpp.

Forse questa potrebbe essere una prima base per riflettere su eventuali ipotesi di riforma della disciplina della data retention in linea con quanto richiesto dalla Cgue, anche considerando che il draft di regolamento europeo e-privacy, attualmente in discussione nelle sue fasi finali, non sembra introdurre sul punto (anche in ragione della tipologia di fonte normativa prescelta) nulla più che una deroga, per fini di giustizia, agli obblighi comuni in materia di conservazione dei dati di traffico.

F*ederica Resta, dirigente del Garante per la protezione dei dati personali (le opinioni qui espresse non impegnano in alcun modo l'Autorità di appartenenza)*