DIRITTI COMPARATI
Comparare i diritti fondamentali in Europa

LA CGUE TORNA A PARLARE AGLI STATI MEMBRI IN MATERIA DI CONSERVAZIONE DEI METADATI E TUTELA DEI DIRITTI FONDAMENTALI: IN UN DIALOGO FRA SORDI, *REPETITA IUVANT*?

Posted on 8 Maggio 2023 by ***Giulia Formici***

La sentenza del 20 settembre 2022, pronunciata dalla Grande Sezione della CGUE nelle cause riunite *SpaceNet AG* (C-793/19) e *Telekom Deutschland GmbH* (C-794/19), è solo l'ultima tappa di quella *data retention saga* che ormai da tempo vede i giudici di Lussemburgo, le Corti degli Stati membri nonché i legislatori nazionali ed europei impegnati in un continuo e fitto confronto, che ha tuttavia spesso assunto i connotati di un dialogo fra sordi. Per comprendere appieno la portata di questa più recente decisione e cogliere la complessità che ancora caratterizza il dibattito sul tema pare necessario ricostruire per sommi capi il cammino giurisprudenziale – e normativo – sin qui percorso.

La CGUE, sin dalla nota sentenza *Digital Rights Ireland*, ha riconosciuto nella conservazione generalizzata e indiscriminata (c.d. *bulk data retention*) dei metadati derivanti dalle telecomunicazioni uno strumento capace di incidere profondamente sui diritti alla riservatezza e alla protezione dei dati (artt. 7 e 8, Carta di Nizza), ingenerando peraltro negli utenti la sensazione di essere sottoposti a costante sorveglianza. Partendo da tale

considerazione, i giudici europei hanno quindi promosso un'attenta lettura dei principi di necessità e proporzionalità, determinando rigidi requisiti quanto alla compatibilità con il diritto dell'UE di obblighi di conservazione imposti in capo agli operatori privati per finalità di prevenzione e repressione di reati gravi e/o minacce alla sicurezza nazionale. A partire dal 2014, in complesse e commentatissime decisioni – da *Tele2*, alle più recenti *Commissioner of An Garda Síochána*, *La Quadrature du Net* e *Privacy International*, passando per *Ministerio Fiscal* e *H.K. Prokuratuur* –, la *case-law* eurounitaria ha infatti fornito un'interpretazione sempre più puntuale dell'art. 15 Direttiva *e-Privacy*, cioè l'unica disposizione – peraltro estremamente vaga – che ad oggi consente agli Stati membri di adottare normative nazionali in materia di *data retention* per scopi securitari.

In estrema sintesi, in questa lunga saga giurisprudenziale è stato innanzitutto stabilito come non possa essere considerata limitata allo stretto necessario e giustificata in una società democratica una *bulk data retention* che coinvolga sistematicamente tutti gli utenti di servizi di telecomunicazione in maniera globale e comporti un obbligo di conservazione slegato da qualsiasi nesso, anche indiretto, tra ingerenza nella sfera privata e repressione di reati gravi. Unica forma di *retention* compatibile con il diritto dell'Unione diviene pertanto quella targettizzata (o mirata), ossia delimitata nel tempo o in una specifica area geografica o ad una cerchia di soggetti. Solo in un caso la CGUE ha affermato la proporzionalità di forme di conservazione generalizzata ed indiscriminata ovvero quando tali obblighi abbiano lo scopo di salvaguardare la sicurezza nazionale: se le minacce a quest'ultima risultano infatti maggiormente pericolose – si pensi alle attività di terrorismo – rispetto alla criminalità grave, esse non possono che consentire l'adozione di ingerenze più profonde e ampie nella vita privata e nel diritto alla protezione dei dati. Il ricorso a forme di *bulk data retention*, anche in tal caso, deve restare però di natura eccezionale, tanto che i giudici si spingono ad indicare – pur con termini che lasciano al legislatore nazionale un certo margine di discrezionalità – circostanze e garanzie stringenti, tra cui la sussistenza di una minaccia grave reale e attuale o prevedibile, la determinazione di una

durata circoscritta allo stretto necessario e la previsione di un controllo di legittimità da parte di un organo indipendente. La distinzione tra sicurezza nazionale, da un lato, e prevenzione, ricerca e perseguimento di reati gravi, dall'altro, conduce così ad un diverso vaglio di proporzionalità, che pure non giunge a giustificare un illimitato impiego di meccanismi insidiosi di sorveglianza generalizzata, che non possono in nessun caso assumere carattere sistematico.

Dinnanzi a quelli che, con una costante stratificazione di pronunce, sono divenuti punti saldi della *data retention saga*, le risposte delle Corti nazionali – e, conseguentemente, quelle dei legislatori degli Stati membri – non sono tuttavia risultate uniformi e hanno anzi disvelato le non poche criticità del dialogo multilivello in un ambito regolatorio, quello della tutela della sicurezza, da sempre gelosamente considerato di esclusiva pertinenza dagli Stati membri.

In alcuni casi le Corti interne hanno così dimostrato una certa ritrosia sia a pronunciarsi sulla conformità delle disposizioni interne in materia di *data retention* ai criteri delineati dalla CGUE, sia a promuovere rinvii pregiudiziali e dunque avviare un confronto con i giudici sovranazionali. Può essere letta in questi termini la posizione dell'ordinamento italiano, nel quale solo in tempi recenti si è provveduto ad introdurre modifiche in senso più garantista alla disciplina sulla conservazione dei metadati; tali interventi riformatori hanno, tuttavia, riguardato solo la disciplina sull'accesso e non anche quella della *retention* che è anzi, sorprendentemente, rimasta generalizzata ed indiscriminata nonché estesa per un periodo di tempo, altrettanto sorprendentemente, lungo. In altri Stati, come Regno Unito (prima, ovviamente, della Brexit) e Francia, le Corti sono invece intervenute – soprattutto a seguito di importanti rinvii pregiudiziali – confermando, nella sostanza, la compatibilità delle normative nazionali con l'interpretazione emersa dalla giurisprudenza europea, adottando letture spesso "restrittive" della portata di quest'ultima. In diversi casi, al contrario, i giudici interni, riprendendo quasi pedissequamente il *reasoning* dei giudici di Lussemburgo, hanno dichiarato l'incostituzionalità della normativa nazionale in materia di *data retention*, inducendo così un nuovo intervento del legislatore nazionale.

Anche in tali circostanze, realizzatesi ad esempio in Belgio e Portogallo, Governi e Parlamenti si sono però trovati di fronte alla difficoltà tanto di rinunciare *in toto* ad uno strumento considerato – anche dalle autorità di *law enforcement* e *Intelligence* – essenziale per il contrasto alla criminalità, quanto di disporre obblighi di *targeted data retention*, reputata inefficace e potenzialmente discriminatoria.
Una difficoltà, quella di conformarsi ai rigidi requisiti sanciti dalla CGUE, che ha caratterizzato anche il dibattito tedesco, dal quale ha origine la sentenza del settembre 2022: i rinvii pregiudiziali promossi dalla Corte amministrativa federale riguardano infatti le disposizioni in materia di *data retention* dettate dalla legge in materia di telecomunicazioni (TKG) e la loro compatibilità con il diritto dell'UE. Nonostante la normativa tedesca sulla *data retention* sia stata a lungo considerata una delle più stringenti e virtuose, sia sotto il profilo della limitazione nel tempo, della tipologia di dati da conservare e delle tutele previste, sia con riferimento alle misure volte alla protezione dei dati, alla regolamentazione dell'accesso e degli scopi per i quali è consentito l'impiego dei dati conservati (contrasto dei reati gravi o di prevenzione di un rischio concreto per la integrità fisica, la vita o la libertà di una persona o per l'esistenza di uno stato federale o di un Land), la TKG ha comunque determinato un obbligo generalizzato e indiscriminato di conservazione. Proprio valutando tale aspetto e ribadendo quanto già indicato nelle sue previe decisioni, la CGUE ha riaffermato nella sentenza in analisi che il diritto europeo osta a misure legislative nazionali che dispongano, a titolo preventivo e per finalità di lotta alla criminalità grave e a minacce gravi alla sicurezza pubblica, una *bulk data retention* dei dati relativi al traffico e all'ubicazione. Resta compatibile con il diritto dell'UE, invece, la disposizione di una conservazione generalizzata nei soli casi in cui essa venga – eccezionalmente e con specifiche salvaguardie – motivata da esigenze di tutela della sicurezza nazionale, nonché qualora la *retention* abbia ad oggetto unicamente dati che non consentono una invasione pervasiva della sfera privata, quali gli indirizzi IP attribuiti all'origine di una connessione o i dati relativi all'identità anagrafica degli utenti.
Nel ribadire la legittimità e proporzionalità della sola conservazione di tipo

mirato, i giudici, anche rispondendo alle critiche mosse dai governi di molti Stati membri intervenuti nel procedimento, hanno specificato che tali misure possono essere targettizzate, a titolo esemplificativo, nei confronti di persone sottoposte a indagine o iscritte nel casellario giudiziario, ove la condanna comporti rischio elevato di recidiva, o rispetto a luoghi specifici, identificati sulla base di elementi oggettivi – ma non necessariamente di indizi concreti –, quali il tasso medio di criminalità o le loro specifiche caratteristiche (luoghi sensibili o molto frequentati). Viene ammessa infine la c.d. conservazione rapida: qualora, dinnanzi a reati o attentati già accertati o la cui esistenza è ragionevolmente sospettata, l'analisi dei metadati venga considerata utile per scopi di indagine, ben può essere ordinato ai fornitori – mediante l'approvazione di un provvedimento sottoposto a controllo giurisdizionale effettivo – di non procedere alla cancellazione di specifici metadati (si pensi a quelli riguardanti le persone con cui la vittima di reato grave è stata in contatto).
Da tutti i profili evidenziati si può insomma comprendere come la ricca e dettagliata decisione della CGUE non introduca particolari innovazioni rispetto alla giurisprudenza precedente ma si inserisca semmai perfettamente nel solco già tracciato. La pronuncia si pone infatti come una sorta di utile "antologia" che sistematizza, precisa e rafforza le coordinate essenziali del bilanciamento operato dai giudici europei tra esigenze di sicurezza – nazionale o pubblica – e tutela dei diritti fondamentali. Si viene ad aggiungere così un ulteriore tassello a quel lento e ancora non del tutto effettivo percorso di "costituzionalizzazione" della *data retention*: essa non viene *in toto* compromessa e vietata dalla CGUE; piuttosto la sua compatibilità con il diritto dell'UE e la Carta di Nizza viene riportata entro confini "costituzionali" definiti dalla rigorosa lettura dei principi di necessità e proporzionalità che consentono entro certi limiti la compressione dei diritti (E. Celeste, G. Formici, *Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism and Legislative Inertia*, in corso di pubblicazione). Gli interventi dei giudici possono essere visti come il segnale di una graduale ma attento "contenimento" – soprattutto ad opera della giurisprudenza – delle istanze e tensioni pro-securitarie. Queste, lungi dal caratterizzare solo la gestione emergenziale

del terrorismo, mostrano di essere rafforzate dalle potenzialità inimmaginate dell'innovazione tecnologica: il progresso scientifico, l'avanzamento di tecniche di AI e di analisi dei Big Data disvelano nuovi minacciosi orizzonti di sorveglianza massiva – anche predittiva – in grado di mutare pericolosamente quella lettura del rapporto tra cittadini e sospettati, tra libertà e potere, tra diritti e autorità che è da sempre posta alla base degli ordinamenti democratici, dello stato di diritto e del costituzionalismo.

Il destino di un simile percorso di "costituzionalizzazione" e il suo possibile approdo ad un traguardo finale rimane senza dubbio ancora oggetto di discussione: certo l'intervento della CGUE, con diversi esiti, ha portato in numerosi Stati – come si è detto – ad avviare una seria discussione in materia di *data retention*, conducendo infine ad un innalzamento del livello di tutela dei diritti attraverso la predisposizione di limiti e salvaguardie prima assenti. Se ciò è senz'altro vero, il rispetto pieno dei requisiti indicati dalla giurisprudenza qui richiamata non pare ancora raggiunto: la "sordità selettiva" dimostrata sino ad ora da diversi legislatori nazionali dinnanzi alle parole dei giudici di Lussemburgo evidenzia la difficoltà di operare un bilanciamento da molti governi ritenuto troppo compromesso a favore dei diritti dalla giurisprudenza europea. Un dialogo fra sordi, quello che si è venuto a determinare, che si osserva anche nel dibattito normativo in seno all'UE quanto all'adozione di un nuovo Regolamento che aggiorni la ormai vetusta Direttiva *e-Privacy*. Pure su questo fronte, infatti, è emerso in tutta la sua problematicità il dibattito sull'inserimento di nuove disposizioni sulla *data retention* in grado di incontrare l'approvazione degli Stati membri e, al contempo, di conformarsi alla giurisprudenza europea. A livello nazionale, poi, la sentenza del settembre 2022 aprirà certamente ulteriori scenari e controversie: è quanto già accaduto in Germania, dove si è già avviato un acceso scontro politico sulla possibile nuova disciplina normativa in materia di conservazione dei metadati da adottare in attesa di una – altamente – probabile disapplicazione della TKG da parte dei giudici tedeschi.

Solo le scelte dei legislatori nazionali e sovranazionale nonché la reazione

delle Corti interne potranno dire se, nel prossimo futuro, questo "*repetita*" della CGUE dei principi e requisiti già affermati nella sua ricca e complessa *case-law* gioverà al dibattito sulla *data retention*. Questo reiterato e coerente intervento dei giudici di Lussemburgo, anche di fronte alle posizioni fortemente critiche espresse dagli Stati membri, produrrà infine l'esito di rendere efficacemente ascoltato un monito fino ad ora, in gran parte, disatteso?