DATA RETENTION

NUOVA MODALITÀ DI ACQUISIZIONE DEI TABULATI DI TRAFFICO IN ITALIA: UN CAMBIAMENTO CHE HA PROFONDE RADICI NEL TEMPO

Decreto Legge del 30 settembre 2021, n. 132
Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP.

di Giovanni NAZZARO, *Lawful Interception Consultant, Security Manager, Auditor/Lead Auditor* ISO 27001, ingegnere, è un libero ed indipendente professionista che opera nell'*information technology* e nelle reti di telecomunicazioni da 20 anni, esperto in *security*, *legal* e *compliance* in tali ambiti. Esperto nella progettazione dei sistemi d'intercettazione e di *data retention* e nella definizione delle procedure organizzative ed operative per il loro utilizzo. Direttore di "*Sicurezza e Giustizia*" dal 2011 e della"*Lawful Interception Academy*" dal 2014, promotore della *LIA Certification* per la certificazione dei sistemi d'intercettazione. E' professore a contratto in Master Universitari di I e II livello.

La tendenza a considerare l'utilizzo delle nuove tecnologie come terreno fertile per individuare tracce utili alle moderne indagini ha condotto, nel tempo, il legislatore italiano alla ricerca di una disciplina che fosse al contempo regolatrice delle modalità di accesso alle informazioni e garantista del diritto di riservatezza dell'utente. Un difficile equilibrio che si è tradotto in continui e ripetuti interventi sulla relativa norma, in particolare sull'art. 132 del Codice privacy, e che ha mostrato l'attitudine ad esplorare diverse soluzioni che però, di fatto, non hanno mai soddisfatto tutte le parti coinvolte.

L'occasione di tale considerazione è fornita da ultimo dal decreto-legge del 30 settembre 2021 n. 132 che ha stabilito nuove modalità di accesso alle informazioni conservate dagli operatori di telecomunicazioni. Come nel passato, esattamente 17 anni fa, si è scelto nuovamente di intervenire con un atto normativo di carattere provvisorio, in quanto il Governo ha riscontrato un caso straordinario di "necessità e urgenza", parole che suscitano in noi non poche ansie dato il periodo più critico della pandemia appena superato e nel quale, effettivamente, sono stati utilizzati non meno di 10 decreti legge per regolare le attività e contenere il rischio di diffusione del virus.

Nelle premesse del testo e nel comunicato del Consiglio dei Ministri n. 38 si può riscontrare come la motivazione alla base della straordinaria necessità ed urgenza sia anche quella di mettere la legislazione italiana in linea col diritto comunitario e con la sentenza della Corte di Giustizia Ue del 2 marzo 2021, la quale ha stabilito che solo con decreto motivato del **giudice**, su richiesta del pubblico ministero o su istanza del difensore, si possono acquisire presso il fornitore i dati del traffico telefonico o telematico ai fini dell'accertamento del reato.

Per comprendere i reali motivi d'urgenza e di necessità ravveduti per il decreto legge in commento, tuttavia, **occorre ripercorrere interamente il periodo storico appena trascorso**, rilevare le tante e diverse azioni messe in campo dal legislatore nazionale ed europeo per i tragici eventi di terrorismo internazionale vissuti in Europa. Eventi caratterizzati da un lato dall'enfasi emotiva di quei momenti e dall'altro da una estrema necessità di fornire in breve tempo gli strumenti tecnici a chi svolge le indagini, che nei fatti hanno dato vita a indirizzi giurisprudenziali diversi con la pericolosità di generare esiti processuali altrettanto diversi.

1. Legge 26 febbraio 2004, n. 45

Il 7 gennaio 2004 veniva presentato alla Camera, di iniziativa governativa, il disegno di legge n. 4594 per rispondere alla "*volontà di fornire adeguate soluzioni ad alcuni dei problemi più urgenti che ostacolavano l'offerta del miglior servizio-giustizia ai cittadini*"[1]. Con gli articoli 3, 4 e 5 si è interveniva sull'articolo 132 del Codice privacy la cui formulazione originaria, secondo il legislatore stesso, poneva seri problemi in ordine alla tenuta del traffico, nonché alla conservazione dei dati relativi ad Internet. Il termine di conservazione di 30 mesi, originariamente previsto per tutti i reati, rischiava di non essere congruo allorquando le indagini avevano ad oggetto gravi fenomeni delittuosi. Il nuovo articolo 3, in particolare, prevedeva che i dati fossero conservati dal fornitore per il periodo ordinario di 24 mesi, termine suscettibile di proroga per ulteriori 24 mesi in presenza di indagini relative anche a reati di particolare gravità quali quelli indicati nell'articolo 407, comma 2, lettera a), del codice di procedura penale.

La Legge 45/2004[2] modificò la modalità di acquisizione dei dati presso il fornitore affinché fosse disposta dall'autorità giudiziaria, d'ufficio o su istanza del difensore dell'imputato, dell'indagato o delle altre parti private. Era fatta salva, comunque, la facoltà per il difensore della persona sottoposta ad indagini o dell'imputato di richiedere direttamente al fornitore i dati di traffico riguardanti il proprio assistito. Per quanto riguarda specificamente il pubblico ministero ed il difensore dell'imputato, si stabilì, una volta decorso il primo termine di 24 mesi, che gli stessi richiedessero al giudice, che decideva con decreto motivato, l'autorizzazione ad acquisire i dati.

Tale nuova disciplina fu contestata da un GIP del tribunale di Pavia che, con un'ordinanza del 12 marzo 2014, sollevò questioni di legittimità costituzionale in relazione alla nuova

1 XIV Legislatura - Scheda lavori preparatori - Atto parlamentare: 4594 (rif. https://leg14.camera.it/_dati/leg14/lavori/schedela/trovaschedacamera_wai.asp?Pdl=4594)

2 Legge 26 febbraio 2004, n. 45 "Conversione in legge, con modificazioni, del decreto-legge 24 dicembre 2003, n. 354, recante disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia" (rif. https://www.camera.it/parlam/leggi/04045l.htm#conve)

formulazione dell'art. 132: secondo il rimettente avrebbe pregiudicato il buon andamento dell'amministrazione della giustizia (art. 97 Cost.), specie se interpretato nel senso che al giudice spettasse non solo il compito di rilasciare l'autorizzazione, ma anche quello di provvedere alla materiale raccolta dei dati presso l'operatore di telefonia, quale semplice tramite per una successiva trasmissione dei dati stessi al pubblico ministero procedente. L'ingiustificata complicazione della procedura, d'altra parte, avrebbe implicato un contrasto con il principio di obbligatorietà di esercizio dell'azione penale (art. 112 Cost.). A questa ordinanza seguirono molte altre, due sempre del GIP del tribunale di Pavia, una del GIP del tribunale di Cuneo e del Gip del tribunale di Palmi ed una, infine, del GIP del tribunale di Roma il 23 dicembre 2004.
La Corte costituzionale ritenne non fondata, e quindi inammissibile, la questione di legittimità con la sentenza N. 372 del 2006[3].

2. Legge n. 155/2005 e Decreto Legislativo n. 109/2008

A Madrid, l'11 marzo 2004, una decina di bombe furono posizionate nelle stazioni ferroviarie di Atocha, El Pozo e Santa Eugenia: morirono 191 persone. A Londra, il 7 luglio 2005, sulla rete di trasporti pubblici quattro kamikaze si fecero esplodere nell'ora di punta in tre diverse stazioni e su un autobus a due piani: il bilancio fu di 56 morti e 700 feriti. Divenne chiaro a quel punto che la normativa a supporto delle indagini doveva evolvere, prevendendo l'esatto contenuto delle informazioni e le tipologie di comunicazioni da tracciare, tra cui anche i tentativi di chiamata (cd. squilli) che possono far esplodere una bomba a distanza.
In Italia, dopo appena 20 giorni dall'attentato a Londra, fu subito emanato il decreto legge n.144/2005 convertito in appena 4 giorni, il 31 luglio 2005, nella legge n.155. Il provvedimento introdusse nuove fattispecie penali al fine di offrire agli operatori più efficaci strumenti nel contrasto e nella repressione delle nuove forme di terrorismo, oltre ad intervenire sull'art. 132 del Codice privacy: accanto al traffico telefonico furono aggiunti anche i tentativi di chiamata; la conservazione dei dati relativi al traffico "telematico" fu prescritta in 6 mesi, più ulteriori 6 mesi per i reati di particolare gravità; per il primo periodo di conservazione l'acquisizione dei dati presso i fornitori fu sollevata dall'autorizzazione del giudice, quindi solo attraverso decreto del pubblico ministero o su istanza del difensore dell'imputato. Per il secondo periodo di conservazione rimase invece la previsione relativa all'acquisizione dei dati per mezzo dell'autorizzazione del giudice del decreto motivato. Per la prima volta venne introdotto il caso d'urgenza (art. 4-bis): "*il pubblico ministero dispone la acquisizione dei dati relativi al traffico telefonico con decreto motivato che è comunicato immediatamente e comunque non oltre ventiquattro ore al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. **Se il decreto del pubblico ministero non viene convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati***".
Nel 2005 il Regno Unito aveva la Presidenza del Consiglio dell'Unione europea e, a settembre dello stesso anno, si tenne una sessione plenaria sulla conservazione dei dati sulle telecomunicazioni presieduta dal Segretario di Stato inglese per gli Affari Interni. Tutti gli Stati raggiunsero un accordo poi ufficializzato dal Consiglio europeo durante il suo ritrovo del 1° e 2 dicembre. La direttiva 2006/24/CE del Parlamento europeo e del Consiglio, detta Data Retention Directive, è stata adottata nel marzo 2006 sotto la presidenza austriaca, ma è stata molto discussa e contestata. La direttiva conteneva disposizioni di dettaglio riguardo ai dati da conservare e l'indicazione del tempo minimo e di quello massimo che la legislazione degli Stati doveva stabilire per la conservazione (da sei mesi a due anni)[4].
In Italia la direttiva fu recepita dal decreto legislativo del 30 maggio 2008, n. 109, il cui art. 2 recava nuovamente importanti modifiche all'art. 132 del Codice privacy[5] rispetto all'impianto precedente, perché non conteneva più alcun criterio di selezione e accesso a seconda dell'obiettivo di lotta contro gravi reati e, soprattutto, l'accesso non era subordinato ad un previo controllo giudiziale o di una autorità amministrativa indipendente che garantisse "*l'uso strettamente necessario per raggiungere l'obiettivo perseguito*".
La Corte di giustizia europea, pronunciandosi l'8 aprile 2014 su due cause, in cui la stessa era adita in via pregiudiziale di una questione vertente sulla validità della direttiva 2006/24/CE, con la sentenza denominata appunto Digital Rights Ireland, ha invalidato di fatto la stessa. Grande soddisfazione è stata manifestata dalla Corte europea dei diritti dell'uomo che, ripetutamente in precedenza, aveva dichiarato che la memorizzazione da parte di un'autorità pubblica di dati attinenti alla vita privata di un individuo rappresenta, con le parole dell'avvocato generale, "*un'ingerenza di vasta portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale*". In realtà, non è solo questo il motivo per cui la direttiva è stata dichiarata invalida[6], ma ai fini del presente commento interessa sapere solo che il Decreto, che l'ha recepita in Italia, è ancora in vigore, in particolare l'art. 3 "Categorie di dati da conservare per gli operatori di telefonia e di comunicazione elettronica", a differenza di quanto invece è accaduto negli altri Stati europei.

3. Le sentenze della Corte di Giustizia Europea e le segnalazioni del Garante

Con la sentenza Digital Rights Ireland dell'8 aprile 2014[7], relativa alle cause riunite C-293/12 e C-594/12, la Corte di giustizia ha dichiarato l'illegittimità della direttiva 2006/24/Ce per violazione del principio di proporzionalità ravvisata soprattutto nella previsione di misure di conservazione dei dati applicabili in via indifferenziata e generalizzata a "*qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché [al]l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi*"; nell'omessa previsione dei parametri sostanziali e procedurali per l'accesso ai dati senza 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 anche in ragione della loro tipologia e, quindi, dell'utilità probatoria di ciascuna di essi.
Con la sentenza resa nel caso Tele2 Sverige del 21 dicembre 2016[8], relativa alle cause riunite C-203/15 e C-698/15, la Corte ha dichiarato incompatibile con l'articolo 15, paragrafo 1, della direttiva 2002/58 ogni previsione interna che, per fini di contrasto dei reati imponga la conservazione "*generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica*", nonché legittimi l'accesso "*delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione*".
Arriviamo infine all'ultima sentenza della Corte di giustizia dell'Unione europea del 2 marzo 2021, resa nella causa C-746/18[9], in cui si 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***

3 Sentenza 372/2006, Presidente: BILE - Redattore: SILVESTRI (rif. https://www.cortecostituzionale.it/actionSchedaPronuncia.do?param_ecli=ECLI:IT:COST:2006:372)

4 "Gli operatori telefonici non conservano i contenuti delle chiamate e degli SMS" di Marzia Minozzi su Sicurezza e Giustizia n. IV /MMXI (rif. https://www.asstel.it/wp-content/uploads/2012/01/SeG_IV_MMXI_ASSTEL.pdf)

5 Decreto Legislativo 30 maggio 2008, n. 109 "Attuazione della direttiva 2006/24/CE riguardante la conservazione dei 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" (rif. https://www.camera.it/parlam/leggi/deleghe/testi/08109dl.htm)

6 "EU's Data Retention Directive declared invalid" di Giovanni Nazzaro su Sicurezza e Giustizia n. II / MMXIV (rif. https://www.sicurezzaegiustizia.com/eu-s-data-retention-directive-declared-invalid/)

7 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62012CJ0293

8 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62015CJ0203

9 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:62018CJ0746

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*". Inoltre 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***".

Sulla base dei principi affermati dalla Corte, più volte il Garante privacy ha invitato il legislatore[10] (con i pareri resi sugli schemi di decreti legislativi di adeguamento al Regolamento Ue 2016/679, di recepimento della direttiva (UE) 2016/680 ed infine il 3 agosto 2021) a riformare la disciplina interna sulla conservazione dei tabulati, affinché limitasse l'acquisizione ai soli reati gravi e subordinasse tale acquisizione al vaglio del giudice.

Posizione diversa ha assunto invece la Corte di Cassazione (Cass., Sez. V, 24 aprile 2018, 273892, Sez. III, 23 agosto 2019, n. 36380 e Sez. II, 13 febbraio 2020, n. 5741) che ha ritenuto la disciplina interna compatibile con il canone di proporzionalità e conforme ai principi sanciti dalla Corte di giustizia perché delimita temporalmente la durata della conservazione, e demanda l'acquisizione dei dati al pubblico ministero e cioè ad un organo giurisdizionale che procede nell'ambito di una attività di indagine preliminare. Nell'ultima segnalazione il Garante ha evidenziato però che, a suo parere, la sentenza della CGUE del 2 marzo 2021 poneva in chiaro due aspetti che avrebbero reso non compatibile le sentenze della Corte di Cassazione: l'acquisibilità processuale dei dati di traffico va, da un lato, limitata ai soli procedimenti per gravi reati o per gravi minacce per la sicurezza pubblica e, dall'altro, va subordinata all'autorizzazione di un'autorità terza rispetto all'autorità pubblica richiedente. Parere tra l'altro recepito anche dal Tribunale di Roma sezione Gip-Gup, decr. 25 aprile 2021, secondo cui veniva superato "*anche l'indirizzo della giurisprudenza interna volto a ritenere il pubblico ministero autorità legittimamente deputata al vaglio acquisitivo dei tabulati in ragione della sua indipendenza, con "sopravvenuto contrasto tra l'art. 132, c.3, d.lgs. 196 del 2003 e la normativa dell'Unione europea, così interpretata dal giudice europeo, nella parte in cui attribuisce la competenza ad emettere il decreto motivato di acquisizione al pubblico ministero anziché al giudice*".

10 Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico (rif. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685978)

4. Decreto Legge del 30 settembre 2021, n. 132

Arrivando ai giorni nostri, nonostante la pronuncia resa dalla CGUE nella citata causa C-746/18, continuano a permanere decisioni di giudici di merito che applicano la norma vigente ritenendola del tutto conforme al diritto dell'Unione, a differenza di altri i quali, invece, accedono a soluzioni che disapplicano la normativa vigente. Oltre a questo si è aggiunto anche il rinvio pregiudiziale alla stessa Corte di giustizia, con ordinanza del tribunale di Rieti del 4 maggio 2021, diretto ad avere contezza dalla Corte, tra i vari aspetti, anche sull'idoneità del pubblico ministero italiano a rappresentare almeno un'autorità indipendente idonea a compiere le valutazioni pertinenti all'accesso ai dati, nonché sull'idoneità della pronuncia della Corte di giustizia a produrre "effetti retroattivi" rispetto a dati già acquisiti in precedenza che, in caso di giudizio positivo, produrrebbe effetti imprevedibili al momento sulle cause in tribunale.

Qui si è evidenziata la reale necessità ed urgenza dell'intervento del legislatore, che ha dato vita al decreto legge 132/2021, affinché fossero chiariti gli aspetti più controversi, ma soprattutto si evitasse di lasciare i singoli processi esposti alla variabilità dei vari indirizzi giurisprudenziali.

Si è tornati, quindi, oggi ad una disciplina nella quale **la legittimazione all'acquisizione dei dati** conservati appositamente per finalità di accertamento o di prevenzione di reati **è sempre attribuita al giudice** che procede, salva la possibilità di un intervento nei casi di urgenza da parte del pubblico ministero, con successiva convalida da parte del giudice [articolo 1, lettera a)]. Inoltre, benché la norma previgente richiedesse che il decreto del pubblico ministero fosse motivato, non era precisato il contenuto minimo richiesto per quella motivazione, il quale, invece, proprio in ragione del tenore dell'interpretazione che ne ha dato la Corte di giustizia, non può che essere agganciato ad una valutazione di sussistenza di un pregresso quadro indiziario di peso non minimale circa la sussistenza di un reato da accertare. Quanto alla scelta del presupposto, il legislatore ha ritenuto corretto individuarlo in un livello indiziario "almeno sufficiente", anche in relazione all'opportunità che il livello di accertamento richiesto debba essere di peso inferiore a quello richiesto per l'autorizzazione alle intercettazioni ("di gravità indiziaria"). Il nuovo testo riporta infatti "*ove rilevanti ai fini della prosecuzione delle indagini*" [articolo 1, lettera a)].

L'impianto del comma 4-bis dell'art. 132 del Codice privacy, così come era stato introdotto dalla Legge 155/2005, rimane confermato integralmente nel nuovo comma 3-bis [articolo 1, comma b)], prevedendo nei casi d'urgenza che il pubblico ministero disponga l'acquisizione dei dati con decreto motivato che è comunicato immediatamente. Il giudice decide sulla convalida entro 48 ore e nel caso i tabulati siano stati già acquisiti e la convalida sia negativa questi non potranno essere utilizzati.

L'altra importante novità è il riferimento edittale generale di gravità, individuato con riguardo alla misura della pena massima, indicata nella reclusione **non inferiore a tre anni**.

Accanto a questa previsione si è tenuto conto del fatto che vi sono specifici reati, la cui pena edittale è inferiore, ma per i quali la principale (se non unica) modalità di accertamento è da rinvenire esattamente nei tabulati telefonici: i reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono.

Infine, è stato introdotto l'ulteriore comma 3-ter dell'articolo 132 del Codice privacy, con il quale si chiarisce che l'esercizio dei diritti di cui agli articoli da 12 a 22 del regolamento (UE) 2016/679 resta possibile da parte dell'interessato tramite il Garante stesso.

Anche questo decreto-legge sarà convertito in legge nei successivi 60 giorni, probabilmente con le modifiche che saranno accolte durante il suo iter alla Camera, già iniziato con l'atto n. 3298. Nel frattempo è palese che dovranno essere superate le prime difficoltà di natura operativa, da un lato principalmente dal giudice, che è il "nuovo" attore della nuova procedura nonché garante dell'indipendenza della valutazione della richiesta di accesso ai dati, dall'altro lato dagli operatori di telecomunicazioni che, a parere di chi scrive, per assicurare la giusta continuità delle attività non potranno fare altro che applicare quelle stesse modalità utilizzate con la vecchia normativa. ©