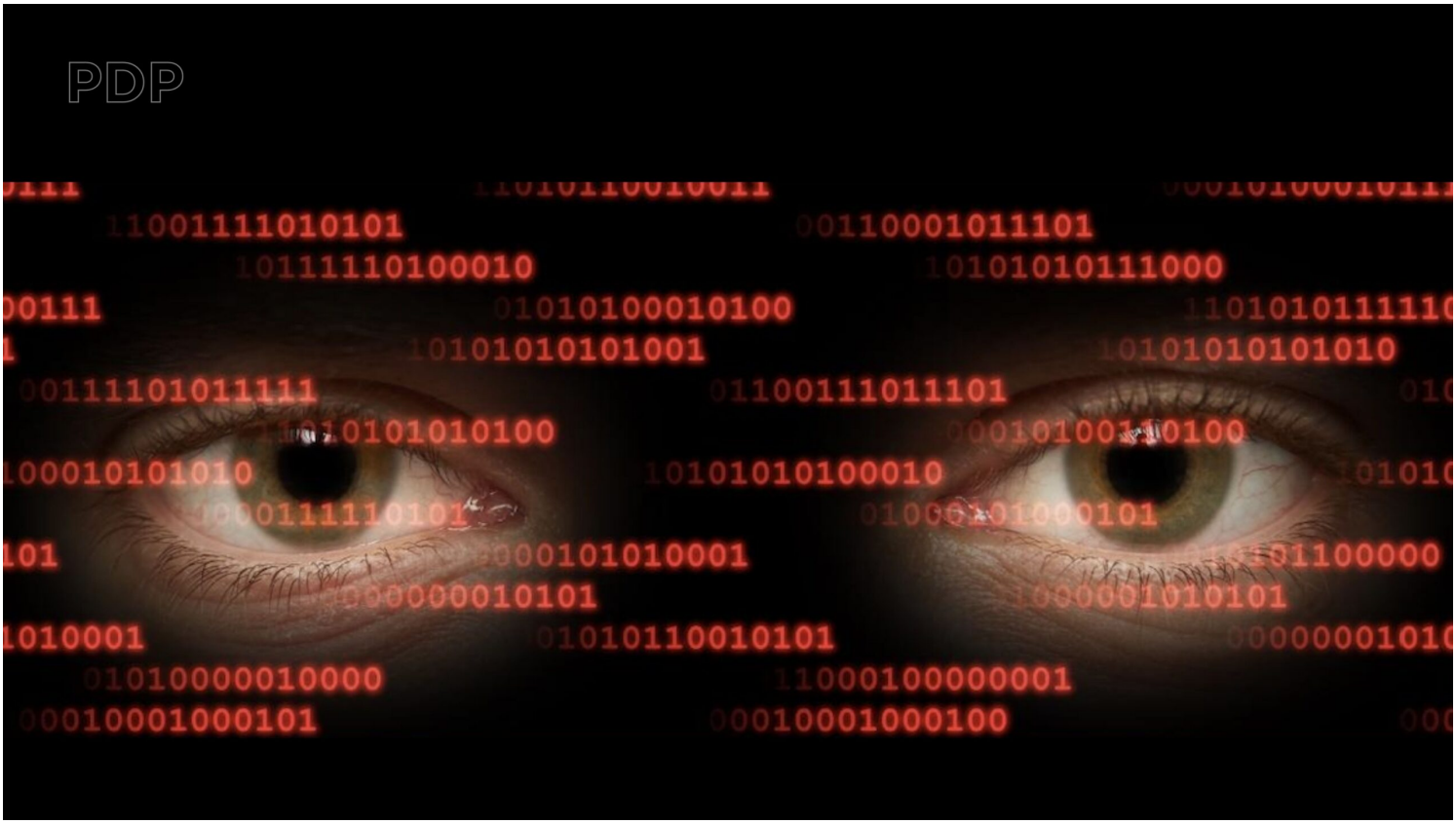
RISERVATEZZA E DATA RETENTION: UNA STORIA INFINITA

Leonardo Filippi



SOMMARIO: 1. Introduzione.- 2. I principi europei.- 3.Le deroghe europee.- 4.La giurisprudenza della Corte di giustizia U.E.- 5.La normativa italiana.- 6. L'art. 256 c.p.p.- 7. Il codice della *privacy*.- 8. La "conservazione generalizzata e indifferenziata" dei dati del traffico e di ubicazione.- 9. La legislazione dell'emergenza e la conservazione di tutti i dati per sei anni .- 10. La novella del 2021.- 11. La estesa legittimazione alla richiesta di acquisizione dei dati.- 12. Il decreto che autorizza o convalida l'acquisizione dei dati . - 13. Il decreto autorizzativo e la presunzione di innocenza.- 14. L'inutilizzabilità dei dati acquisiti *contra legem*.- 15. La necessaria ostensione al gestore del decreto che autorizza l'acquisizione dei dati.- 16. Il regime transitorio per i dati acquisiti prima del 30.9.2021.- 17. Questioni aperte .- a) I *files* di log; b) La richiesta di un indirizzo IP.- c) la richiesta .sulla titolarità di un'utenza.- d) la conservazione rapida dei dati (*quick freeze*).-18.

Conclusioni.

1.Introduzione.

La storia della disciplina italiana dei tabulati è lunga e travagliata, avendo subito plurimi interventi legislativi nel tentativo di bilanciare le esigenze della riservatezza con quelle investigative.

Per giunta si è verificata una progressiva e accresciuta capacità sia di raccolta dei dati (*data retention*), sia di affinamento delle tecniche di conservazione e di lettura dei dati stessi. È vero che i dati esteriori delle comunicazioni non contengono il contenuto dei messaggi e quindi provocano una lesione alla riservatezza minore rispetto all'intercettazione delle comunicazioni. Tuttavia, tali dati forniscono notizie molto rilevanti, come le utenze contattate, la frequenza delle chiamate, il tempo e la durata delle stesse, le persone frequentate ed anche la presenza all'interno di una determinata cella d'aggancio di un utente e quindi la sua ubicazione in tempo reale. Si tratta perciò talvolta anche di dati sensibili perché investono la personalità e la sfera privata del titolare dell'utenza telefonica o telematica, dando indicazioni sulla vita privata delle persone, come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tali persone e gli ambienti sociali da esse frequentati.

Le diverse modifiche legislative hanno riguardato non solo la durata di conservazione dei dati (che originariamente era di 30 mesi per i soli dati del traffico telefonico), ma anche l'altalenante legittimazione alla richiesta di acquisizione :prima del solo P.M., estesa per poco tempo al difensore, ma restituita a lungo al "monopolio" del solo P.M. e da ultimo estesa nuovamente al difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private.

Una tale incertezza è diffusa in un sistema come il nostro che va da un eccesso all'altro, in cui la tutela della riservatezza, prima sconosciuta ora forse, in certi casi, è tutelata persino troppo. Ma ormai facciamo parte dell'Unione europea, l'Italia ha aderito a diverse convenzioni internazionali (prime fra tutte la Conv. e.d.u. e la Carta dei diritti fondamentali) e l'art. 117 Cost. prescrive il rispetto, oltre che della Costituzione, anche dei «vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali».

2.I principi europei.-

In ossequio al principio del primato del diritto dell'Unione europea su quello nazionale, è necessario esaminare preliminarmente la normativa europea sulla vita privata e sulle comunicazioni elettroniche.

È tuttora vigente la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12.7.2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche).

Da notare che la direttiva 2006/24/CE (c.d. Direttiva Frattini) modificò la Direttiva 2002/58/CE, ma fu invalidata dalla pronuncia della Grande Camera della Corte giust. U.E. 8.4.2014, *Digital Rights*, per cui vi è stata la reviviscenza della precedente direttiva 2002/58/CE.

L'art. 5 § 1 della direttiva 2002/58 sancisce il principio di riservatezza sia delle comunicazioni elettroniche sia dei dati relativi al traffico a queste correlati e implica il divieto imposto, in linea di principio, a qualsiasi persona diversa dagli utenti di memorizzare senza il loro consenso tali comunicazioni e dati.

L'art. 6 della stessa direttiva 2002/58/CE, nonché i considerando 22 e 26, autorizzano il trattamento e la memorizzazione dei dati relativi al traffico da parte dei fornitori di servizi di comunicazione elettronica soltanto nella misura e per la durata necessaria per la commercializzazione dei servizi, per la fatturazione degli stessi e per la fornitura di servizi a valore aggiunto. Una volta terminato tale periodo, i dati che sono stati trattati e memorizzati devono essere cancellati o resi anonimi.

L'art. 9 § 1 della medesima direttiva disciplina i dati relativi all'ubicazione diversi dai dati relativi al traffico e stabilisce che tali dati possono essere trattati soltanto in presenza di determinate condizioni e dopo essere stati resi anonimi oppure con il consenso degli utenti o degli abbonati.

3. Le deroghe europee.-

È la stessa direttiva 2002/58 a consentire alcune deroghe alla disciplina ordinaria, ammettendo delle eccezioni ai principi generali e, in quanto eccezioni, esse non sono suscettibili quindi di interpretazioni estensive e tanto meno analogiche.

L'art. 15 § 1 della direttiva 2002/58 consente agli Stati membri di introdurre eccezioni all'obbligo di principio,

enunciato all'art. 5 §1, della stessa direttiva, di garantire la riservatezza dei dati personali nonché ai corrispondenti obblighi, menzionati in particolare, agli artt. 6 e 9 di detta direttiva, qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale, della difesa e 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 che prevedano la conservazione dei dati per un periodo di tempo limitato, qualora ciò sia giustificato da uno dei suddetti motivi.

4.La giurisprudenza della Corte di giustizia U.E.-

La Grande Camera della Corte di giustizia U.E. ha ripetutamente affermato il contrasto - rispetto all'art. 15, § 1, della menzionata Direttiva 2002/58/CE - della disciplina legislativa di diversi Stati europei che, come quella italiana, consente una conservazione generalizzata e indifferenziata dei dati relativi al traffico telefonico, informatico e dei dati relativi all'ubicazione, e non prevede l'autorizzazione di un giudice o di un'autorità amministrativa indipendente.

Le pronunce, che negli ultimi sette anni hanno riguardato le legislazioni di quasi tutta l'Europa occidentale, ribadiscono, peraltro, principi già perentoriamente affermati in passato dalla stessa Corte a tutela della riservatezza, della protezione dei dati di carattere personale, della libertà di espressione e d'informazione, nonché del principio di proporzionalità delle limitazioni a tali diritti e libertà. Si tratta delle seguenti sentenze: Corte giust. U.E., Grande Camera, 21.12.2016, *Tele2 Sverige e Watson* e altri/ Svezia e Regno unito; Corte giust. U.E., Grande Camera, 2.10.2018, *Ministerio Fiscal* /Spagna*;* Corte giust. U.E., Grande Camera, 6.10.2020, *Privacy International*/ Regno Unito; Corte giust. U.E. Grande Camera. 6.10.2020, *La Quadrature du Net* e altri/Francia e Belgio; Corte giust. U.E. Grande Camera, 2.3.2021, *H.K.* / Estonia; Corte giust. U.E. Grande Camera,5.4.2022, *G.D.*/Irlanda.

Si è così formata una giurisprudenza europea ormai consolidata su alcuni principi : a) divieto di «conservazione generalizzata e indifferenziata» dei dati relativi al traffico e all'ubicazione per finalità di prevenzione delle minacce gravi alla sicurezza pubblica e di repressione della criminalità grave; b) ammissibilità di una «conservazione mirata» dei dati relativi al traffico e dei dati relativi all'ubicazione per fini di prevenzione delle minacce gravi alla sicurezza pubblica e di repressione della criminalità grave; c) ammissibilità di una «conservazione generalizzata e indifferenziata» degli indirizzi IP; d) ammissibilità di una

«conservazione generalizzata e indifferenziata dei dati relativi all'identità civile» degli utenti; e) ingiunzione ai fornitori di servizi di comunicazione elettronica di procedere, «per un periodo determinato», alla «conservazione rapida» (*quick freeze*) dei dati relativi al traffico e dei dati relativi all'ubicazione; f) garanzie comuni a tutte le misure: rispetto delle condizioni e garanzie effettive contro il rischio di abusi.

5.La normativa italiana.-

La disciplina legislativa italiana è articolata su diverse disposizioni, che nel tempo si sono sovrapposte e sono state modificate in tempi diversi, ma sempre ignorando totalmente il rispetto della riservatezza su dati personali.

6. L'art. 256 c.p.p.-

In passato il pubblico ministero, così come il giudice, poteva acquisire i tabulati telefonici e telematici, come qualsiasi altro documento, in forza dell'art. 256 c.p.p.

Com'è noto, l'art. 256 c.p.p. fu introdotto dall'art. 8 l. 18 marzo 2008, n. 48, Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica. Esso impone un dovere di esibizione alle persone tenute al segreto professionale (art. 200 c.p.p.) e a quello di ufficio (art. 201 c.p.p.), che devono consegnare immediatamente all'autorità giudiziaria che ne faccia richiesta gli atti e i documenti e ogni altra cosa esistente presso di esse per ragione del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreti di Stato ovvero di segreto inerente al loro ufficio o professione. Il segreto è comunque escluso nei casi di cui all'art. 204 c.p.p., cioè per i fatti di eversione dell'ordinamento costituzionale ed altri ivi indicati.

7. Il codice della *privacy.*-

Il d. lgs. 30.6.2003, n. 196 (Codice in materia di protezione dei dati personali) entrò in vigore nel 2003 ed ha subito molteplici modifiche. Senza ripercorrere l'intero iter delle modifiche, ricordiamo che il più recente intervento si deve al d.-l. 30.9.2021, n. 132.

8. La "conservazione generalizzata e indifferenziata" dei dati del traffico e di ubicazione.-

L’art. 132, comma 1, c.p.p. stabilisce che i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione.

Il comma 1-bis prescrive, invece, che i dati relativi alle chiamate senza risposta sono conservati per trenta giorni.

In questo modo l’art. 132 codice *privacy* si limita a regolamentare la durata della conservazione, ma senza specificare quali dati debbano essere conservati: cioè disciplina una “conservazione generalizzata e indifferenziata” di tutti i dati, che la Corte di giustizia U.E. vieta, prescrivendo, invece, una “conservazione mirata” dei dati relativi al traffico e dei dati relativi all’ubicazione “per fini di prevenzione delle minacce gravi alla sicurezza pubblica e di repressione della criminalità grave”.

9. La legislazione dell’emergenza e la conservazione di tutti i dati per sei anni.-

L’art. 24 (Termini di conservazione dei dati di traffico telefonico e telematico) l. 20.11.2017, n. 167 (Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017), in attuazione dell'art. 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli artt. 51, comma 3-quater, e 407, comma 2, lettera a), c.p.p. il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'art. 4-bis, commi 1 e 2, d.l. 18 febbraio 2015, n. 7, conv., con mod., dalla l. 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'art. 132, commi 1 e 1-*bis*, del codice in materia di protezione dei dati personali, di cui al d. lgs. 30 giugno 2003, n. 196.

Poiché i gestori non possono certo prevedere per quali reati perverranno in futuro le richieste di

acquisizione dei dati e potrebbero pervenire richieste di acquisizione dei dati rilevanti in indagini sul terrorismo o su criminalità organizzata, sono costretti a conservare tutti i dati per sei anni. Di fatto, quindi, la conservazione di tutti i dati è per settantadue mesi, che è una durata veramente inaccettabile e contrastante con il principio di proporzionalità dell'ingerenza.

10. La novella del 2021.-

Il d.-l. n. 132/2021, conv. con mod. dalla l. n. 178/2021 ha modificato l'art. 132 Codice *privacy*, sostituendo il comma 3 e inserendovi i nuovi commi 3-*bis*, 3-*ter* e 3-*quater*.

Inoltre, ha aggiunto una disposizione transitoria nel comma 1-*bis* della legge di conversione n. 178/2021.

Infine, ha modificato l'art. 267, comma 1, c.p.p. esigendo l'indicazione di "specifiche" ragioni nella motivazione del decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile.

L'intervento legislativo del 2021 ha finalmente assicurato la riserva di legge (indicando i "casi", comprese anche le gravi molestie telefoniche, che è difficile ritenere trattarsi di "criminalità grave", oltre i "modi" dell' acquisizione) e di giurisdizione (autorizzazione del giudice che procede con decreto motivato sulla rilevanza dei dati per l'accertamento dei fatti).

Ma la Corte giust. U.E. prescrive l'indicazione sia della "categoria dei dati acquisibili", compresi quelli di ubicazione, sia della durata del "periodo per il quale viene richiesto l'accesso ai dati", che devono essere limitati a "quanto è strettamente necessario" ai fini dell'indagine in corso.

Invece, la novella del 2021 non ha minimamente inciso sull'oggetto della acquisizione dei dati, perché tutti i dati di traffico possono essere indifferentemente acquisiti e anche per l'intero periodo per cui sono stati conservati, consentendo così non solo una «conservazione generalizzata e indifferenziata» dei dati relativi al traffico, ma anche una "acquisizione generalizzata e indifferenziata", cioè proprio ciò che vieta la direttiva europea e la giurisprudenza della Corte del Lussemburgo.

La novella del 2021 non ha modificato nemmeno la durata della conservazione, che rimane di due anni (per

il traffico telefonico), di un anno (per il traffico telematico), 30 giorni (per le chiamate senza risposta), ma, come abbiamo visto, di fatto i gestori devono conservare tutti i dati per sei anni.

La Corte di giustizia U.E. richiede anche di individuare per legge i "soggetti" i cui dati possono essere acquisiti ed aveva ammonito che l'accesso a tali dati può, in linea di principio, essere consentito, in relazione con l'obiettivo della lotta contro la criminalità, soltanto per i dati di "persone sospettate di progettare, di commettere o di aver commesso un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere". Solo eccezionalmente, "in situazioni particolari, come quelle in cui interessi vitali della sicurezza nazionale, della difesa o della sicurezza pubblica siano minacciati da attività di terrorismo, l'accesso ai dati di altre persone potrebbe essere parimenti concesso qualora sussistano elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro attività di questo tipo".

Invece l'art. 132 codice *privacy* consente l'acquisizione dei dati anche dei di soggetti non raggiunti da sospetto di reato e quindi semplici persone informate sui fatti o testimoni.

11. La estesa legittimazione alla richiesta di acquisizione dei dati.-

Essendo esplicitamente legittimati alla richiesta non solo il P.M., il difensore dell'imputato, della persona sottoposta alle indagini e della persona offesa, ma anche quello delle «altre parti private», si consente pure al difensore della parte civile, del responsabile civile e del civilmente obbligato per la pena pecuniaria di presentare istanza di acquisizione dei dati direttamente al G.I.P. o al giudice che procede.

È esclusa invece una acquisizione d'ufficio da parte del giudice, essendo la richiesta di parte presupposto dell'autorizzazione.

12. Il decreto che autorizza o convalida l'acquisizione dei dati.-

Nonostante non sia disciplinato dal codice di rito penale, il decreto del giudice che autorizza o convalida l'acquisizione dei dati presso il gestore del servizio di telecomunicazioni, previsto dall'art. 132, comma 3,

codice *privacy*, è assimilabile al decreto del G.I.P. che autorizza o convalida l'intercettazione di comunicazioni. Anche il decreto che convalida l'acquisizione disposta d'urgenza dal pubblico ministero ricorda quello di convalida dell'intercettazione.

Si tratta di acquisizione che, come l'intercettazione, è atto a sorpresa, nel senso che il P.M. o la parte privata richiedente non sono tenuti a informare le altre parti dell'avvenuta acquisizione.

L'acquisizione dei dati è quindi atto diverso dal sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni, disciplinato dall'art. 254-bis c.p.p. La disposizione indica le modalità acquisitive dei dati, cioè mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.

Relativamente alla motivazione del decreto di acquisizione dei dati, il decreto-legge privilegiava il P.M. nell'acquisizione dei tabulati telefonici, telematici e di ubicazione, durante le indagini preliminari tanto che essi potevano essere acquisiti solo se rilevanti per la "**prosecuzione delle indagini".** Invece, la legge di conversione consente l'acquisizione a tutte le parti anche in momenti successivi (ad es. in sede dibattimentale). Infatti, il testo definitivo richiede che l'acquisizione dei tabulati sia rilevante «**per l'accertamento dei fatti**» e non solo ai fini della «prosecuzione delle indagini». In questo modo l'acquisizione dei dati può essere autorizzata, dal giudice che procede, anche dopo la chiusura delle indagini preliminari e per tutto il corso del processo, sempre che ovviamente i dati siano ancora conservati.

13. Il decreto autorizzativo e la presunzione di innocenza.-

Anche la disciplina dei tabulati risente della direttiva europea (UE) 2016/343 sulla presunzione di innocenza, di recente recepita in Italia con il d. lgs. 8.11.2021, n. 188, per cui anche nelle richieste e nei decreti di autorizzazione all'acquisizione dei dati, così come nei decreti in tema di intercettazioni, trova applicazione la nuova disposizione dell'art. 115-*bis* c.p.p. Si tratta infatti di provvedimenti che hanno come presupposto indizi di reato (e non di reità) e quindi da annoverare tra quelli «diversi da quelli volti alla decisione in merito alla responsabilità penale dell'imputato», per cui «la persona sottoposta a indagini o l'imputato non possono essere indicati come colpevoli fino a quando la colpevolezza non è stata accertata con sentenza o decreto

penale di condanna irrevocabili» e l'autorità giudiziaria deve limitare i riferimenti alla colpevolezza della persona sottoposta alle indagini o dell'imputato alle «sole indicazioni necessarie a soddisfare i presupposti, i requisiti e le altre condizioni richieste dalla legge per l'adozione del provvedimento"[1]. Si noti infine che il decreto che autorizza l'acquisizione dei dati, come quello in materia di intercettazioni, non hanno la garanzia di alcuna impugnazione.

14. L'inutilizzabilità dei dati acquisiti *contra legem*.-

L'art. 132, comma 3-*quater*, stabilisce che «I dati acquisiti in violazione delle disposizioni dei commi 3 e 3-*bis* non possono essere utilizzati».

In questo modo, il legislatore ha finalmente disciplinato, sotto il profilo sanzionatorio, tutte le ipotesi di acquisizione patologica dei dati. In realtà, le S.U. Gallieri già in passato avevano affermato che il divieto di utilizzazione previsto dall'art. 271 c.p.p. è riferibile anche all'acquisizione dei tabulati telefonici tutte le volte che avvenga in violazione dell'art. 267 c.p.p., cioè in assenza del prescritto decreto motivato[2].

Comporta quindi l'inutilizzabilità dei dati a carico dell'imputato il fatto che essi siano stati acquisiti oltre il termine di conservazione stabilito dalla legge; o la circostanza che l'autorizzazione sia stata data per un reato che non consente l'acquisizione dei dati; la mancanza di un decreto del G.I.P. o del giudice che procede o l'assenza in esso di una motivazione specifica sulla qualificazione giuridica, sui "sufficienti indizi di reato" o sulla loro rilevanza "per l'accertamento dei fatti".

Inoltre, anche i dati acquisiti d'urgenza dal P.M. sono inutilizzabili non solo in caso di mancata o tardiva convalida del G.I.P., ma pure se il decreto motivato del P.M. è stato emesso in assenza di «ragioni d'urgenza» o del «fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini».

Invece, l'utilizzabilità *in bonam partem*, cioè a favore dell'imputato, è invece sempre possibile, perché la Costituzione pone la tutela dei diritti inviolabili dell'uomo ad obiettivo fondamentale dell'ordinamento, per cui, nel processo penale l'innocenza e comunque la minore responsabilità dell'imputato devono poter sempre essere accertate. D'altra parte, le prove conferenti all'assoluzione o alla minore responsabilità sottostanno ai soli sindacati di esistenza e di attendibilità, non anche a quello di conformità al modello legislativo, e quindi non possono mai essere dichiarate inutilizzabili.

Anche le Sezioni Unite Carpanelli del 1997 avevano chiarito che le dichiarazioni favorevoli al soggetto che le ha rese e ai terzi restano al di fuori della sanzione di inutilizzabilità sancita dall'art. 63, co. 2, c.p.p., alla stregua della *ratio* della disposizione, ispirata al diritto di difesa[3].

15. L**a necessaria ostensione al gestore del decreto che autorizza l'acquisizione dei dati**.-

Il testo del decreto-legge stabiliva che «i dati sono acquisiti presso il fornitore con decreto motivato del giudice», mentre la legge di conversione richiede che «i dati sono acquisiti **previa autorizzazione rilasciata dal giudice con decreto motivato**», per cui si è dubitato se tale decreto debba essere presentato ai gestori.

Ma il dubbio sembra agevolmente superabile con la considerazione che, quando si intacca un valore fondamentale, se ne deve dare giustificazione al detentore di esso mediante esibizione del titolo che legittima l'intrusione (così, ad esempio, in occasione di perquisizione o sequestro, deve essere esibito il relativo decreto al detentore del bene). Pertanto, non si dovrebbe dubitare che il P.M., la parte o il soggetto privato che chiede l'acquisizione dei tabulati debba esibire al gestore del servizio di telecomunicazioni il decreto di autorizzazione emesso dal G.I.P.[4] Né è possibile vedere analogie con l'art. 267 c.p.p. e quindi ritenere che, come il P.M., dopo l'autorizzazione del G.I.P., non deve ostendere il decreto autorizzativo dell'intercettazione al gestore, così dovrebbe fare anche per i tabulati. Il confronto non è pertinente perché in tema di intercettazioni esiste una disposizione specifica, l'art. 267, comma 3, c.p.p., che prevede l'emissione di uno specifico decreto con cui il P.M. dà esecuzione all'intercettazione, mentre una disposizione analoga non esiste per i tabulati.

Pertanto, la modifica del testo originario in quello definitivo, di carattere meramente formale, non consente di omettere l'esibizione al gestore del provvedimento autorizzativo.

16. Il regime transitorio per i dati acquisiti prima del 30.9.2021.-

Il regime transitorio per i dati acquisiti prima del 30 settembre 2021 è disciplinato dall'art. 1, comma 1-*bis*, d. l. 30.9.2021, n. 132, conv. con mod. dalla l. 23.11.2021, n. 178 . Esso stabilisce che i dati relativi al traffico telefonico, al traffico telematico e alle chiamate senza risposta, acquisiti nei procedimenti penali in data precedente alla data di entrata in vigore del presente decreto, possono essere utilizzati a carico dell'imputato solo unitamente

ad altri elementi di prova ed esclusivamente per l'accertamento dei reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e dei reati di minaccia e di molestia o disturbo alle persone con il mezzo del telefono, quando la minaccia, la molestia o il disturbo sono gravi.

Tale disposizione transitoria può ovviamente rispettare soltanto la "riserva di legge", indicando, per i tabulati acquisiti prima del 30 settembre 2021, i "casi" (reati puniti con la pena dell'ergastolo o della reclusione **non inferiore nel massimo a tre anni e reati di gravi minacce, molestie o disturbo alle persone con il mezzo del telefono) e i "modi" dell'ingerenza** sulla vita privata conseguente all'accesso ai dati di traffico (che sono indicati nella disposizione generale di cui all'art. 132 codice *privacy*). Ma, non potendo rispettare la "riserva di giurisdizione", giacchè i dati, prima del d.l. n. 132/2021, erano legittimamente acquisibili con decreto del P.M., compensa il *deficit* di giurisdizionalità esigendo in via transitoria ciò che l'art. 132 codice *privacy* non richiede in via generale e cioè che l'utilizzabilità **a carico dell'imputato (dovendo ritenersi l'utilizzabilità *in bonam partem* sempre ammessa)** dei tabulati **è legittima solo unitamente ad altri elementi di prova che fungano da "riscontro" ad essi.**

Secondo la disposizione transitoria, è ora prevista una duplice condizione per l'utilizzazione a carico dell'imputato dei dati già acquisiti nei procedimenti penali in data precedente alla data di entrata in vigore del decreto-legge. Infatti, essi possono essere utilizzati «solo unitamente ad altri elementi di prova» ed esclusivamente per l'accertamento degli stessi reati per i quali ora art. 132 d.lgs. n. 196/2003 consente la loro acquisizione

E non può non destare meraviglia che il regime transitorio sia più garantista di quello ordinario, tanto che tale discrasia potrebbe suscitare anche qualche problema di costituzionalità.

La Corte di cassazione ha affermato che la disciplina transitoria introdotta dall'art. 1, comma 1-bis, l. 23.11.

2021, n. 178, di conversione del d.l. 30.9.2021, n. 132, che ha consentito l'utilizzazione dei dati relativi al traffico telefonico, al traffico telematico e alle chiamate senza risposta acquisiti nei procedimenti penali in data antecedente all'entrata in vigore del d.l. citato è compatibile con l'art. 15, par. 1, della Direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni, modificata dalla Direttiva 2009/136/CE, in quanto, in un'ottica di ragionevole ed equilibrato contemperamento di interessi diversi, persegue la finalità di non disperdere dati già acquisiti, subordinandone la utilizzazione alla significativa illiceità penale di predeterminate ipotesi per cui è consentita l'acquisizione a regime e alla sussistenza di "altri elementi di prova", quale requisito di compensazione della mancanza di un provvedimento giudiziale di autorizzazione all'acquisizione stessa[5].

17. Questioni aperte.-

La materia dei dati di traffico telefonico, telematico e di ubicazione è piuttosto intricata e suscita diverse questioni su alcuni casi pratici.

a. **I *files* di *log*.-**

Si discute se siano sottoposti alla disciplina dei tabulati anche i *files* di *log*, che sono dei registri che documentano tempi e orari della connessione al sistema dei diversi IP: volendo fare un paragone con il traffico automobilistico, sarebbe come il registro del casellante che annota tutte le targhe dei veicoli che entrano in autostrada.

I *files* di *log*, in particolare, sono costituiti dalla registrazione sequenziale e cronologica da parte del sistema informatico delle operazioni effettuate da un utente o da un amministratore ovvero anche dalla registrazione delle operazioni compiute in automatico da un sistema e costituisce una sorta di "registro degli eventi".

L'analisi dei *files* di *log* consente di ottenere una serie di informazioni, utili nel procedimento penale e relative al "traffico di dati telematici" come se un determinato utente in un particolare giorno ed ora si è collegato alla rete tramite un provider; la data ed ora della sessione di navigazione; quale indirizzo *IP* temporaneo ha avuto in assegnazione per la durata della connessione; l'indirizzo *IP* utilizzato per la sessione di navigazione; quali informazioni (strutturate in "pacchetti") ha inviato o ricevuto per mezzo dell'indirizzo IP assegnato (accessi ai

siti, scaricamento di pagine *web* o di specifici *files*, conversazioni in *chat*, partecipazioni a *newsgroup*, trasmissione o ricezione di posta elettronica); l'anagrafica dell'intestatario di un contratto di utenza internet.

Si è affermato in dottrina che tali *files* di *log* non conterrebbero dati di traffico, ma solo di individuazione degli *IP*, per cui sarebbero esclusi dalla disciplina dettata dall'art. 132 d.lgs. n. 196/2003 per l' acquisizione dei tabulati.

In realtà sono proprio e soltanto i c.d. *log files* che contengono dati relativi al traffico telematico, nel senso che non esistono altri dati sul traffico telematico. Tanto è vero che i *files* di *log* devono essere conservati dai gestori di telecomunicazione per dodici mesi. E, poiché l'art. 132 Codice *privacy* menziona la conservazione e l'acquisizione dei dati telematici, alla pari dei dati telefonici, ne consegue che anche per l'acquisizione dei *files* di *log* occorra la previa autorizzazione del giudice.

- **La richiesta di un indirizzo IP .-**

La Grande Camera ammette una "conservazione generalizzata e indifferenziata" degli indirizzi IP (dall'inglese *Internet Protocol address*), che sono un'etichetta numerica che identifica univocamente un dispositivo (detto *host*) collegato a una rete informatica che utilizza l'*Internet Protocol* come protocollo di rete: continuando nel confronto con il traffico automobilistico, l'indirizzo IP sarebbe la targa di ogni veicolo che entra in autostrada.

- **La richiesta sulla titolarità di un'utenza.-**

La richiesta al gestore di un servizio di telecomunicazioni di conoscere l'intestatario di un'utenza telefonica o telematica non è un dato relativo al traffico. Anche la Grande Camera ammette una "conservazione generalizzata e indifferenziata dei dati relativi all'identità civile" degli utenti.

In effetti l'art. 132 codice *privacy* disciplina la conservazione e l'acquisizione dei soli "dati di traffico" telefonico e telematico e la mera identificazione dell'utente al quale è intestata una determinata utenza non può essere considerata acquisizione di un dato di traffico, alla pari dell'accertamento del luogo di residenza di un

soggetto o della intestazione di un numero di targa di un veicolo o del numero di matricola di un'imbarcazione o di un aeromobile[6].

d) La "conservazione rapida" dei dati (*quick freeze*).-

La giurisprudenza della Corte giust. U.E. viene incontro alle esigenze investigative perchè ammette che si possa rivolgere una ingiunzione ai fornitori di servizi di comunicazione elettronica di procedere, ma solo "per un periodo determinato", alla "conservazione rapida" dei dati relativi al traffico e all'ubicazione. Tale tecnica è particolarmente importante e utile per individuare tutti i dispositivi che si trovano, ad esempio, sul luogo e all'ora del delitto.

18. Conclusioni.-

Dovendo esprimere un giudizio sulla novella legislativa, questo può essere positivo, nonostante non siano state rispettate appieno le indicazioni della giurisprudenza della Corte di giustizia U.E. e anche se sarebbe stato preferibile realizzare una "riserva di codice" e inserire le nuove disposizioni subito dopo gli artt. 266-271 c.p.p.

La Corte giust. U.E. ha infatti affermato che il principio di proporzionalità dell'ingerenza impone una conservazione "mirata" dei dati, mentre in Italia continua una conservazione "generalizzata e indifferenziata" di essi.

La giurisprudenza europea prescrive anche la determinazione sia della "categoria dei dati acquisibili", compresi quelli di ubicazione, sia della durata del "periodo per il quale viene richiesto l'accesso ai dati", che devono essere limitati a "quanto è strettamente necessario" ai fini dell'indagine in corso. Invece, si è omessa una disciplinata della categoria dei dati di ubicazione, è rimasta indeterminata la durata del periodo per il quale è richiesto l'accesso (che può riguardare l'intero periodo di conservazione) ed è immutata anche l'irragionevole durata della conservazione dei dati per 72 mesi (6 anni)

L'art. 132 Codice *privacy* consente tuttora l'acquisizione di tutti i dati conservati e anche nei confronti di soggetti non raggiunti da sospetto di reato e quindi semplici persone informate sui fatti o testimoni, in contrasto con i principi giurisprudenziali europei.

Pertanto, su tutti tali punti rimasti pretermessi e contrastanti con il diritto U.E., sarà inevitabile sollevare questione di legittimità costituzionale in rapporto all'art. 117 Cost., che, com'è noto, vincola la potestà legislativa dello Stato al rispetto, tra l'altro, dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali.

Biasimevole è anche non aver prescritto una motivazione "rafforzata" sui presupposti dell'acquisizione, in modo da evitare le consuete formule di stile, ma vuote di contenuto, che finora la giurisprudenza ha ammesso nel campo delle intercettazioni.

Ciononostante, l'intervento legislativo in materia di tabulati telefonici, e telematici è riuscito ad adempiere almeno alle principali indicazioni europee. Ne è risultata una disciplina dell'acquisizione dei dati per lo più conforme alla Costituzione, alle Convenzioni sovranazionali e alle indicazioni della Corte di giustizia U.E., anche se qualche aggiustamento in futuro sarà indispensabile, almeno sui punti evidenziati.

Purtroppo, è stata persa l'occasione per disciplinare con legge alcuni strumenti di indagine, attualmente in uso nella prassi investigativa, come le riprese visive, l'agente segreto attrezzato per il suono, le *body-cam*, le intercettazioni mediante droni e il "*code catcher*", che è in grado di registrare le informazioni provenienti da tutti i cellulari che si trovano in una certa area.

---

[1] Secondo P. FERRUA, *La direttiva europea sulla presunzione di innocenza e i provvedimenti cautelari,* ne *Il Penalista*, 27.10.2021, il rispetto della "presunzione di innocenza" stabilita dalla Convenzione europea e della "non presunzione di colpevolezza" contemplata dalla Costituzione esige che nei provvedimenti cautelari oggetto di prova sia la "probabile colpevolezza", anziché la "colpevolezza", fermo restando lo standard probatorio dell'"oltre ogni ragionevole dubbio".

[2] Cass., Sez.un.,24.9.1998, Gallieri, in *Cass. pen.*,1999,465.

[3] Cass., Sez. un., 13.2.1997, Carpanelli, in *Dir. pen.e proc.,* 1997, p. 602.

[4] In senso contrario, affermando che si tratta di una formulazione che non lascia dubbi sul fatto che l'acquisizione, una volta autorizzata, è demandata alle parti - pubbliche e private- che hanno richiesto

l'autorizzazione e che - pertanto- il provvedimento di autorizzazione non dovrebbe essere oggetto di ostensione, C. PARODI, *Convertito il decreto in tema di tabulati: (quasi) tutto chiaro,* ne *Il Penalista*, 19.11.2021.

[5] Cass., sez. III, 31.1.2022 (dep. 1.4.2022), n. 11991.

[6] Nel senso che "la gravità dell'ingerenza sulla vita privata conseguente all'accesso ai dati di traffico va esclusa - alla stregua di quanto affermato dalla sentenza CGUE del 2 marzo 2021, H.K., nella causa C-746/18 - ove l'acquisizione sia finalizzata al solo scopo di identificare l'utente interessato", v. Cass., sez. I, 20.4.2022 (dep.20.5.2022), B., n. 19890).