GIURISPRUDENZA PENALE

Data retention e procedimento penale. Gli effetti della sentenza della Corte di giustizia nel caso H.K. sul regime di acquisizione dei tabulati telefonici e telematici: urge l'intervento del legislatore.

di ***Federica Rinaldini***

Sommario. 1. I principi affermati dalla Corte di giustizia. – **2.** Il caso esaminato dalla Corte di giustizia. – **3.** I precedenti della Corte di giustizia e la giurisprudenza italiana. – **4.** Gli effetti della pronuncia della Corte di giustizia nel nostro ordinamento.

1. I principi affermati dalla Corte di giustizia.

La disciplina della "*data retention*", cioè della conservazione e acquisizione di dati "esterni" generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica, è da anni oggetto di attenzione da parte della legislazione e della giurisprudenza dell'Unione, che si è sempre sforzata di trovare un ragionevole punto di equilibrio tra le fondamentali esigenze di tutela del diritto dell'individuo alla riservatezza e dell'interesse pubblico all'accertamento dei reati.

Su tale delicata materia è intervenuta recentemente la Corte di giustizia dell'Unione Europea, Grande Sezione, con sentenza del 2 marzo 2021 (causa C-746/18) nel caso H.K., enunciando principi innovativi che necessariamente dispiegheranno effetti "rivoluzionari" nell'ordinamento giuridico italiano ed in particolare nel regime dell'acquisizione e dell'utilizzazione dei tabulati telefonici e telematici nel procedimento penale.

In relazione agli effetti delle sentenze della Corte di giustizia all'interno del nostro ordinamento, vige, come noto, il principio del "primato del diritto dell'Unione", legittimato dall'art. 11 Cost., secondo cui l'Italia "*consente… alle limitazioni di sovranità necessarie ad un ordinamento che assicuri la pace e la giustizia fra le Nazioni*". La Corte Costituzionale ha affermato con continuità che "*le statuizioni della Corte di giustizia delle Comunità europee hanno, al pari delle norme comunitarie direttamente applicabili cui ineriscono, operatività immediata negli ordinamenti interni*"[1]. Tale efficacia è stata riconosciuta dalla Consulta a tutte le sentenze della Corte di giustizia, sia a quelle pregiudiziali (come quella in esame) ai sensi dell'art. 267 TFUE, sia a

[1] Corte Cost., 13 luglio 2007, n. 284, in *Diritto e Giustizia on line*, 2007.

quelle che sono state emesse in sede di procedura d'infrazione ai sensi dell'art. 258 TFUE[2].
La pronuncia nel caso H.K. ha quindi carattere vincolante non solo per il giudice che ha sollevato la questione, ma anche riguardo a tutti i casi aventi per oggetto le norme interpretate dalla Corte.
In particolare, la sentenza in esame ha stabilito che l'art. 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002[3] - relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, come modificata dalla direttiva 2009/136/CE del Parlamento e del Consiglio del 25 novembre 2009 – letto alla luce degli artt. 7, 8 e 11, nonché dell'art. 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea[4] "*deve essere interpretato nel senso*

[2] Corte Cost., 23 aprile 1985, n. 113, in *Riv dir. agr.*, 1987, II, p. 330; Corte Cost., 11 luglio 1989, n. 389, in *Cass. pen.*, 1990, I, p. 565 e Corte. Cost., 24 giugno 2010, n. 227, in *Giur. Cost*, 2010, 3, p. 2598, secondo cui "*le sentenze della Corte di giustizia vincolano il giudice nazionale all'interpretazione da essa fornita, sia in sede di rinvio pregiudiziale, che in sede di procedura d'infrazione*".

[3] L'art. 15, comma 1, della direttiva stabilisce che "*Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli artt. 5 e 6, all'art. 8, paragrafi da 1 a 4 e all'art. 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'art. 13, paragrafo 1, della direttiva [95/46], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati. Ovvero l'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto [dell'Unione], compresi quelli di cui all'art. 6, paragrafi 1 e 2, del Trattato sull'Unione europea"*.

[4] Come noto, l'art. 7 della Carta dei diritti fondamentali dell'Unione Europea stabilisce che "*ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*". L'art. 8 prevede che "*ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. I dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*". L'art. 11, comma 1, enuncia che "*ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera*". Infine, l'art. 52, comma 1, prevede che laddove è stabilito che "*eventuali limitazioni dei diritti e delle libertà riconosciuti dalla Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate*

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 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"[5].
Parimenti lo stesso art. 15, paragrafo 1, della direttiva 2002/58/CE (modificato dalla direttiva 2009/136/CE), secondo la Corte di giustizia, "*osta ad una normativa nazionale, la quale renda il Pubblico Ministero, il cui compito è 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 dell'istruttoria penale*"[6].
In ossequio al "*principio di proporzionalità*" cristallizzato nell'art. 52 della Carta, la Corte di giustizia ha, quindi, delimitato l'ambito di acquisizione dei dati esterni alle comunicazioni (es. data, ora, luogo, numero del chiamante e del ricevente, ubicazione dell'intestatario dell'utenza etc.), circoscrivendolo al perseguimento di gravi forme di criminalità o di minacce alla sicurezza pubblica.
Inoltre, il titolare dell'acquisizione dei dati presso i gestori non potrà più essere il Pubblico Ministero, in quanto non considerato soggetto terzo rispetto al procedimento penale da lui stesso istruito. Necessaria è stata ritenuta la valutazione da parte di un Giudice o di un'autorità amministrativa indipendente, che verifichi la legittimità della richiesta di acquisizione.
Ma vi è di più: al fine di recepire i principi della Corte di giustizia, tale valutazione dovrà avvenire in via preventiva per evitare che venga autorizzato un accesso ai dati eccedente i limiti dello stretto necessario.

2. Il caso esaminato dalla Corte di giustizia.
Il caso rinviato alla Corte di giustizia riguarda una vicenda estone: l'imputata H.K. era stata condannata alla pena detentiva di due anni per una serie di furti di beni e di somme di denaro, nonché per aver utilizzato una carta

limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".
[5] Corte di giustizia, Grande Sezione, 2 marzo 2021, C-746/18.
[6] Corte di giustizia, Grande Sezione, 2 marzo 2021, C-746/18.

bancaria appartenente ad altro soggetto e per aver compiuto atti di violenza nei confronti di persone partecipanti ad un processo a suo carico.
La condanna era fondata, tra l'altro, sull'acquisizione dei verbali contenenti i dati relativi alle comunicazioni, che l'autorità incaricata dell'indagine aveva acquisito presso il gestore di servizi di telecomunicazioni[7].
Respinto l'appello avverso la sentenza di condanna di primo grado, H.K. proponeva ricorso in Cassazione, eccependo altresì l'inammissibilità dell'acquisizione dei processi verbali dei dati di telefonia per contrasto della normativa interna con l'art. 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni, letto alla luce degli artt. 7, 8 e 11, nonché dell'art. 52, paragrafo 1, della Carta.
La Corte di Cassazione estone ha, quindi, rinviato alla Corte di giustizia tre questioni pregiudiziali.
Con la prima si chiedeva se l'art. 15, paragrafo 1, della direttiva 2002/58/CE dovesse essere interpretato nel senso di dover limitare la normativa nazionale in materia di acquisizione dei dati esterni alle comunicazioni ai soli casi di lotta contro gravi forme di criminalità, in quanto trattasi di attività che costituisce un'ingerenza nei diritti fondamentali *ex* artt. 7, 8, 11 e 52, par. 1, dalla Carta.
Con la seconda questione, si è chiesto alla Corte se il suddetto art. 15, paragrafo 1, della direttiva 2002/58/CE, dovesse essere interpretato sulla scorta del principio di proporzionalità, in base al quale la limitazione dei diritti fondamentali, inevitabilmente causata dall'attività di acquisizione dei dati esterni di comunicazione, potrà avvenire solo nel caso in cui la quantità di dati da acquisire non sia grande, misura valutabile in riferimento al tipo dei dati raccolti ed alla loro estensione temporale.
Infine, alla Corte è stata rimessa la questione relativa alla possibilità di considerare il Pubblico Ministero, che dirige l'attività istruttoria e conseguentemente dispone l'acquisizione dei dati esterni alle comunicazioni, quale soggetto indipendente, così come già previsto dalla sentenza della Corte di giustizia del 21 dicembre 2016, nel caso *Tele 2*, secondo la quale – come di seguito illustrato - l'accesso ai dati da parte delle autorità nazionali deve essere sottoposto al controllo preventivo di un Giudice o di un'autorità amministrativa indipendente[8].

[7] Si precisa che questi dati afferivano in particolare a vari numeri telefonici utilizzati da H.K. e a diversi codici internazionali di identificazione di apparecchiatura telefonica mobile, riferiti a vari periodi fra il 2015 e il 2016.
[8] Corte di giustizia, Grande sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15 (cosiddetta sentenza *Tele 2*), in *Diritto dell'Informazione e dell'Informatica*, II, 2016, 6, p. 984.

La Corte di giustizia si è quindi espressa limitando l'acquisizione dei dati esterni alle comunicazioni e di quelli relativi all'ubicazione ai soli casi di reati gravi, contro la criminalità o posti a tutela della sicurezza pubblica, nonché ritenendo il Pubblico Ministero non competente ad autorizzare siffatta acquisizione, come sopra meglio enunciato.

3. I precedenti della Corte di giustizia e la giurisprudenza italiana.

La Corte di giustizia si era già precedentemente pronunciata in tema di *data retention,* per circoscriverne l'ambito di applicazione mediante un'interpretazione volta a dare maggiore rilievo ai diritti fondamentali dei singoli individui, rispetto alle esigenze di pubblica sicurezza[9].

Ed infatti, con la sentenza *Digital Rights - Ireland LTD* e *Kantner Landesregierung*[10] dell'8 aprile 2014 la Corte di giustizia, Grande Sezione, aveva dichiarato l'invalidità della direttiva 2006/24/CE[11] per violazione degli artt. 7, 8 e 52, paragrafo 1, della Carta, in quanto non stabiliva che l'interferenza dello Stato nella riservatezza del singolo individuo doveva essere minima. La Corte di giustizia aveva, difatti, ritenuto che, nonostante l'interesse della lotta alla criminalità fosse sicuramente avvantaggiato dall'utilizzo delle moderne tecnologie, la direttiva 2006/24/CE non rispettava il principio di proporzionalità, nella parte in cui non poneva precise regole oggettive, sia di carattere sostanziale che processuale, in tema di *data retention*.

La Corte di giustizia nel caso *Digital Rights* ha, quindi, ritenuto che la suddetta direttiva fosse da censurarsi nella misura in cui questa non operava alcuna limitazione alla conservazione dei dati, basata sull'obiettivo di perseguire reati gravi. In altri termini, si è osservato che l'ambito di applicazione della misura della conservazione dei dati ivi previsto, era così ampio da permettere

[9] Per un'attenta disamina della tematica si veda L. LUPARIA, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Diritto di Internet*, 2019, 4, p. 757 ss.; I. NERONI REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema* di data retention*,* in *Sistema penale*, Fascicolo 5/2020, p. 183 ss.

[10] Corte di giustizia, Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12 (cosiddetta sentenza *Digital Rights*), in *Giur. Cost.*, 2014, 3, p. 2948. La Corte di giustizia, Grande Sezione, interpellata in via pregiudiziale dall'Alta Corte irlandese e dalla Corte Costituzionale austriaca, ha dichiarato invalida l'intera direttiva 2006/24/CE in materia di conservazione dei dati.

[11] La direttiva 2006/24/CE, adottata dal Parlamento europeo e dal Consiglio UE, aveva ad oggetto la conservazione di dati generati trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. La stessa veniva quindi a modificare la precedente direttiva del 2002/58/CE.

il suo utilizzo anche in relazione a fattispecie penali non sufficientemente gravi da consentire la compressione di un diritto fondamentale.
Secondo la Corte, inoltre, l'accesso doveva essere oggetto di preventivo vaglio da parte di un Giudice o di un'autorità amministrativa indipendente, in modo da poter limitare l'uso di tali informazioni a quanto strettamente necessario ai fini della tutela della collettività.
È stato inoltre ritenuto che la direttiva 2006/24/CE non prevedeva criteri oggettivi in relazione alla durata della conservazione dei dati, tali da garantire la sua limitazione allo stretto necessario. Tale normativa è stata, quindi, ritenuta priva di garanzie sufficienti ad assicurare una tutela contro rischi di abuso o di utilizzo illecito.
Successivamente, la Corte di giustizia con la sentenza del 21 dicembre 2016, Grande Sezione, nel caso *Tele 2*[12], ha meglio delineato l'ambito di applicazione del principio di proporzionalità, sotteso alla normativa della *data retention*.
Con tale pronuncia, la Corte ha essenzialmente limitato la possibilità di accedere ai dati personali degli individui ai soli reati gravi. La legge nazionale che ammettesse, quindi, la conservazione indiscriminata dei dati di traffico ed il conseguente accesso da parte dell'autorità, sarebbe in contrasto con la normativa europea.
Le sentenze nei casi *Digital Rights* e *Tele 2* dimostrano il rigore con cui la Corte di giustizia ha interpretato la normativa sulla *data retention*, fornendo alla materia un elevato livello di protezione anche rispetto al contrapposto interesse statuale all'accertamento dei reati.
In una successiva pronuncia del 2 ottobre 2018, nel caso *Ministerio Fiscal*[13], la Corte ha fatto un piccolo passo indietro, riconoscendo la possibilità della *data retention* anche per reati non gravi. Anche in relazione a questi ultimi è stata ritenuta possibile la conservazione dei dati esterni delle comunicazioni telematiche e telefoniche, allorché le ingerenze nella riservatezza del singolo individuo da parte dell'autorità non siano da considerarsi gravi. A tale proposito, la Corte ha quindi specificato che l'acquisizione di dati idonei ad identificare il titolare di carte SIM, attivate con codice IMEI, di un telefono cellulare rubato, fosse possibile a prescindere dalla prospettazione di un reato grave, in quanto la ricerca dei soli dati anagrafici non sarebbe di per sé sola idonea a ledere i diritti dell'individuo, in quanto non particolarmente penetrante. Non occorrerebbe pertanto una soglia di rilevante gravità dei

[12] Corte di giustizia, Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15. Tale sentenza ha per oggetto la direttiva 2002/58/CE, cioè la normativa applicabile in materia a seguito della dichiarazione di invalidità della Direttiva 2006/24/CE da parte della sentenza nel caso *Digital Rights*
[13] Corte di giustizia, Grande Sezione, 2 ottobre 2018, C-207/16 (cosiddetta sentenza *Ministerio Fiscal*), in *Diritto dell'informazione e dell'informatica*, II, 2018, 6, p. 905.

reati. Circostanza quest'ultima invece assolutamente necessaria nel caso in cui i dati esterni alle comunicazioni permettano di formulare valutazioni in ordine alla vita privata dell'individuo (ubicazione del chiamante, data, ora e soggetti nei cui confronti intercorrono le comunicazioni, luoghi frequentati dal titolare dell'apparecchio elettronico etc.). In questo caso, quindi, si è addivenuti ad una distinzione: per i reati gravi la conservazione dei dati esterni di una comunicazione è ammessa, mentre per i reati comuni è consentita solo se l'ingerenza nella sfera privata del singolo non sia da considerarsi grave.

Sullo sfondo di questo panorama europeo, la giurisprudenza italiana, pur ribadendo formalmente i principi sanciti dalla Corte di giustizia, ha di fatto completamente disatteso il contenuto di queste pronunce, fornendo un'interpretazione volta a salvaguardare la normativa interna in tema di *privacy* e di acquisizione dei tabulati telefonici e telematici.

All'interno del nostro ordinamento, la materia è disciplinata dall'art. 132 del Codice della Privacy (d.lgs. 30.6.2003, n. 196), secondo cui i dati relativi al traffico telefonico e telematico sono acquisiti "*con decreto motivato del pubblico ministero*", "*per finalità di accertamento e repressione dei reati*", quindi senza alcun controllo preventivo effettuato da un Giudice o da un'autorità amministrativa indipendente e senza alcuna limitazione in ordine alla gravità dei reati.

La Corte di Cassazione, in più occasioni, ha ritenuto che "*la disciplina prevista dall'art.132 d.lgs. n. 196 del 2003 è compatibile con il diritto sovranazionale in tema di tutela della privacy (direttive 2002/58/CE e 2006/24/CE), così come interpretato dalla Corte di Giustizia dell'Unione Europea"*[14].

Le motivazioni della giurisprudenza di legittimità, volte a salvaguardare la normativa interna in tema di *data retention,* si basano, in estrema sintesi, sulle seguenti argomentazioni:

- la sussistenza di una normativa interna in tema di regolamentazione dell'accesso e della conservazione dei dati (alcune pronunce della Corte di giustizia riguardavano Stati privi di siffatta normativa);
- l'espressa enunciazione normativa della finalità di repressione dei reati;
- la delimitazione temporale dell'attività di memorizzazione;
- l'intervento preventivo dell'autorità giudiziaria, funzionale all'effettivo controllo della stretta necessità dell'accesso ai dati.

Gli elementi sopra indicati, presenti nella legislazione italiana, consentirebbero, pertanto, a parere dei Giudici di legittimità, di considerare

[14] Da ultimo Cass. pen., Sez. III, 19 aprile 2019, n. 36380, in *Diritto di Internet*, 2019, 4, p. 753. Sulla compatibilità della normativa nazionale in tema di acquisizione dei dati contenuti nei tabulati con quella europea, si vedano altresì: Cass. pen., Sez. III, 25 dicembre 2019, n. 48737 in *CED Cass. pen.*, 2020; Cass. pen., Sez. II, 10 dicembre 2019, n. 5741.

rispettato in concreto il principio di proporzionalità, sancito dalla giurisprudenza europea.
Non si può tuttavia sottacere come la normativa interna non operi alcun effettivo bilanciamento fra i diritti fondamentali dell'individuo e l'esigenza di accertamento e repressione di gravi reati mediante l'acquisizione di dati e informazioni presso i gestori di telefonia[15].
Non è difatti ravvisabile alcuna individuazione dei reati–presupposto particolarmente gravi legittimanti l'intrusione dell'autorità nella vita privata degli individui, non è previsto che un soggetto terzo e indipendente sia garante di siffatta legittimità, mediante una seria valutazione dei provvedimenti autorizzativi, che non possono più basarsi su motivazioni scarne o meramente formali.

4. Gli effetti della pronuncia della Corte di giustizia nel nostro ordinamento.

Come sopra evidenziato, i principi sanciti dalla Corte di giustizia dispiegano un effetto vincolante immediato *ultra partes* nel nostro ordinamento.
Quanto deciso in Lussemburgo è difficilmente compatibile con la disciplina prevista in Italia dall'art. 132 del Cod. *Privacy*, che non prevede nessuno dei limiti garantisti individuati nel caso H.K: accesso ai dati circoscritto a reati gravi e controllo preventivo da parte di un giudice o di una autorità amministrativa indipendente.
È inevitabile quindi che la giurisprudenza domestica si trovi in grande difficoltà ad affrontare le ricadute di tale rivoluzionaria sentenza all'interno del nostro ordinamento.
Allo stato, sono noti due provvedimenti, di due diversi uffici del G.I.P. presso il Tribunale di Roma, che hanno delineato effetti completamente differenti della sentenza della Corte di giustizia.
In un primo provvedimento in data 25.4.2021, il G.I.P. presso il Tribunale di Roma, chiamato a pronunciarsi sulla richiesta fatta del Pubblico Ministero per ottenere l'autorizzazione a disporre l'acquisizione dei dati relativi al traffico telefonico, pur disapplicando la norma interna (l'art. 132 d.lgs. n. 196/2003), ha ritenuto di disporre l'acquisizione dei tabulati[16].

[15] Come è stato ben osservato, la normativa interna dovrebbe essere sottoposta al vaglio rigoroso di una sua valutazione in termini di proporzionalità fra diritti lesi ed esigenze della collettività, in quanto materia afferente ai diritti fondamentali, in tal senso si veda I. NERONI REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, *op. cit.*, p. 185.
[16] G.i.p. presso il Tribunale di Roma, decreto 25.4.2021, in *Sistema Penale*, 29.4.2021, con commento di J. DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della grande camera della corte di giustizia ue: la svolta garantista in un primo provvedimento del g.i.p. di Roma*.

Il Giudice romano, partendo da condivisibili premesse, cioè ritenendo la sentenza comunitaria direttamente applicabile, confermato il sopravvenuto contrasto dell'art. 132 Cod. *Privacy* con la normativa dell'Unione Europea, con conseguente inapplicabilità della norma interna e applicazione dei principi sanciti dalla Corte lussemburghese, giunge però a conclusioni opinabili, laddove afferma che "*la categoria della "forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica" indicata dalla Corte di giustizia quale indispensabile condizione per rendere proporzionata (giustificata) l'acquisizione dei dati, è facilmente individuabile con il rinvio integrale ai reati previsti nel catalogo dettato dagli articoli 266 c.p.p. e 266 bis c.p.p.: è chiaro che l'acquisizione dei dati relativi al traffico telefonico potrà senz'altro consentirsi negli stessi casi in cui la ben più invasiva attività di intercettazione è ammessa dall'ordinamento processuale. In conclusione, disapplicata la norma interna (art. 132 d.lgs. n. 196/2003) e ritenuta la sussistenza dei presupposti delineati dalla normativa dell'Unione Europea ("la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica" sia, in concreto, per la gravità delle ipotesi delittuose sia in forza della riconducibilità, nel caso di specie, dei reati per i quali si procede agli articoli 266 c.p.p. e 266 bis c.p.p.) nonché l'evidente indispensabilità per l'immediata prosecuzione delle indagini, deve autorizzarsi quanto richiesto dal Pubblico Ministero"*.

In tale decreto, per salvare la possibilità di avvalersi dell'importante ed efficace strumento investigativo costituito dai tabulati telefonici, viene percorsa una strada che presenta però possibili ostacoli, sia in relazione ai dettami della sentenza H.K. della Corte di giustizia, sia per quanto previsto nella nostra Costituzione.

L'auspicata applicazione in via analogica della normativa sulle intercettazioni a quella dell'acquisizione dei "dati esterni" delle comunicazioni, pone innanzitutto il problema che la stessa normativa sulle intercettazioni di cui all'art. 266 c.p.p. dovrà fare i conti con la pronuncia della Corte di giustizia, in quanto i principi ivi espressi attengono ai limiti del diritto alla riservatezza, che concerne anche le intercettazioni. Non è così scontato che tutte le fattispecie penali previste dall'art. 266 c.p.p. possano ritenersi "*forme gravi di criminalità"* oppure *"gravi minacce alla sicurezza pubblica*", si pensi a quelle previste dall'art. 266 lett. e), f), f *ter*) (tra cui vi sono i reati di minaccia, usura, abusiva attività finanziaria, contraffazione di marchi e brevetti, introduzione nello Stato e commercio con segni falsi, frode nel commercio, vendita di prodotti con segni mendaci, etc.).

Inoltre, l'art. 15 della Costituzione, nell'annoverare la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione tra i diritti inviolabili dell'individuo, sancisce inderogabilmente che "*la loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge*". Ne consegue che ogni limitazione in tale

materia soggiace alla riserva assoluta di legge, oltre che di giurisdizione motivata.
Nessun dubbio che la tutela sancita da tale norma costituzionale si estenda anche ai tabulati telefonici e telematici, in quanto la Corte Costituzionale ha confermato "*l'ampiezza della tutela accordata dall'art. 15 della Costituzione alla libertà e alla segretezza della comunicazione, la quale é sicuramente tale da ricomprendere fra i propri oggetti anche i dati esteriori di individuazione di una determinata conversazione telefonica*"[17].
La giurisprudenza di legittimità in più occasioni ha posto l'accento sulla portata dei riflessi dell'art. 15 Cost. all'interno del nostro ordinamento, con decisioni che sono utili anche ad esaminare la questione attinente ai limiti dell'acquisizione dei tabulati telefonici e telematici.
Le Sezioni Unite della Suprema Corte, richiamando il *dictat* della Corte Costituzionale[18] hanno evidenziato che "*in base all'art. 15 Cost., lo stesso diritto è inviolabile nel senso che il suo contenuto di valore non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia che la disciplina prevista risponda ai requisiti propri della riserva assoluta di legge e la misura limitativa sia disposta con atto motivato dell'autorità giudiziaria*"[19].
Ne consegue che anche l'acquisizione dei dati esterni delle conversazioni deve essere regolamentata attraverso un'apposita disposizione di legge e disposta con atto motivato dell'autorità giudiziaria.
La soluzione della questione attraverso l'applicazione in via analogica della normativa sulle intercettazioni all'acquisizione dei tabulati, invocata nel provvedimento romano, stride quindi con il dettato costituzionale.
Non può non rilevarsi come le disposizioni di cui agli artt. 266 e ss. c.p.p. in tema di "intercettazioni di conversazioni o comunicazioni" siano norme di carattere "eccezionale" rispetto al principio di portata costituzionale forgiato nell'art. 15 Cost. La stessa Corte Costituzionale ha riconosciuto la *"natura indubbiamente eccezionale dei limiti apponibili a un diritto personale di carattere inviolabile, quale la libertà e la segretezza delle comunicazioni (art. 15 della Costituzione)*"[20].
Tali norme, pertanto, non sono suscettibili di applicazione analogica, come disciplinato dall'art. 14 delle Preleggi, secondo cui *"le leggi penali e quelle che*

[17] Corte Cost., 11 marzo 1993, n. 81.
[18] Corte Cost., 23 luglio 1991, n. 366.
[19] Cass. pen., Sez. VI, 13 febbraio 2019, n. 11160, in *Diritto & Giustizia*, 2019, (nota).
[20] Corte Cost., 23 luglio 1991, n. 366. Si veda altresì Cass. pen., Sez. V, 20 luglio 2020, n. 23438 e Cass. pen., Sez. II, 11 marzo 2021, n. 13809.

fanno eccezione a regole generali o ad altre leggi non si applicano oltre i casi e i tempi in esse considerati". Secondo un orientamento ormai consolidato ci si trova di fronte a norme "eccezionali" tutte le volte in cui viene introdotta una disciplina che deroga, rispetto a particolari casi, all'efficacia generale di una o più disposizioni[21].

Va infine considerato che la giurisprudenza sia costituzionale che di legittimità, anche a Sezioni Unite, si è più volte espressa nel senso di escludere l'applicabilità della normativa sulle intercettazioni telefoniche di cui agli artt. 266 e ss. c.p.p. all'acquisizione del tabulati telefonici e telematici, ritenendo che la disciplina di acquisizione di tale mezzo di ricerca della prova vada rinvenuta nell'art. 256 c.p.p.[22], norma che impone un generale dovere di esibizione a carico dei soggetti indicati negli artt. 200 e 201 c.p.p. tra cui possono essere fatti anche rientrare gli incaricati del servizio telefonico e telematico. Sulla base di tale orientamento, la giurisprudenza ha quindi fino ad oggi ritenuto che, per l'acquisizione dei tabulati telefonici e telematici, fosse sufficiente il decreto motivato del Pubblico Ministero, come del resto previsto anche dall'art. 132 Cod. *Privacy*.

Ebbene, dopo pronuncia della Corte di giustizia nel caso H.K., la normativa contraria ai principi ivi delineati, cioè l'art. 132 Cod. *Privacy,* deve essere disapplicata e al vuoto di disciplina che si viene a creare non si può supplire con applicazioni analogiche di norme eccezionali, ma deve necessariamente intervenire il legislatore italiano.

L'urgenza della necessità di tale intervento è dimostrata dalla contraddittorietà delle soluzioni che stanno fornendo gli uffici dei Giudici delle indagini preliminari a cui i Pubblici Ministero stanno ora chiedendo le autorizzazioni per l'acquisizione dei tabulati.

In un secondo provvedimento di un diverso ufficio del G.I.P. presso il Tribunale di Roma[23], si è giunti a conclusioni radicalmente difformi rispetto al primo decreto sopra analizzato.

Il Giudice ha dichiarato "*non luogo a provvedere*" sulla richiesta di autorizzazione del Pubblico Ministero a disporre l'acquisizione dei tabulati, ritenendo ancora applicabile, in attesa di un auspicabile intervento del legislatore, l'art. 132 d.lgs. n. 196/2003, che prevede appunto sia lo stesso Pubblico Ministero a poter procedere.

---

[21] Per tutti FIANDACA-MUSCO, *Diritto Penale. Parte Generale*, Bologna, 2014, p. 122.

[22] Si vedano Corte Cost., 17 luglio 1998, n. 281, in *Cass. pen.*, 1999, p. 27; Cass. pen., S.U., 23 febbraio 2000, n. 6, in *Cass. pen.*, 2000, p. 2595; Cass. pen., Sez. VI, 21 luglio 2000, n. 8458, in *Arch. Nuova proc. pen.*, 2001, p. 558.

[23] G.I.P. presso il Tribunale di Roma, in *Sistema Penale*, 5.5.2021, con commento di A. MALACARNE, *Ancora sulle ricadute interne della sentenza della Corte di Giustizia in materia di acquisizione di tabulati telefonici: il G.i.p. di Roma dichiara il "non luogo a provvedere" sulla richiesta del p.m.*

In tale provvedimento, pur ravvisando un sopravvenuto quadro di contrasto giurisprudenziale tra Corte di Cassazione e la Corte di giustizia sulla compatibilità dell'art. 132 d.lgs. n. 196/2003 con la direttiva 2002/58/CE, pur ritenendo che ai principi espressi nelle sentenze di matrice europea vada attribuito il valore di ulteriore fonte del diritto comunitario, si è specificato che le sentenze della Corte non creano *ex novo* norme comunitarie, ma indicano di queste "*il significato ed i limiti di applicazione*".
Secondo tale Giudice quindi, le sentenze lussemburghesi avrebbero efficacia immediata e diretta "*solo laddove per effetto di tali interpretazioni non residuino negli istituti giuridici regolati concreti problemi applicativi e profili di discrezionalità che richiedano necessariamente l'intervento del legislatore nazionale, e ciò tanto più laddove si tratti di interpretazione di norme contenute in Direttive*".
In definitiva, secondo tale provvedimento, la sentenze della Corte di giustizia avrebbe un effetto "*limitato*", nel senso che "*le interpretazioni proposte dalla citata sentenza Corte di Giustizia Unione Europea Grande Sez., Sent., 02/03/2021, n. 746/18 non possano avere effetti applicativi immediati e diretti, per la indeterminatezza , nella sentenza, del riferimento ai casi nei quali i dati di traffico telematico e telefonico possono essere acquisiti, riferimento genericamente operato ai casi di "lotta contro le forme gravi di criminalità" o di "prevenzione di gravi minacce alla sicurezza pubblica", casi la cui concreta declinazione non può non ritenersi demandata (e venendo di fatto demandata dalla sentenza), in esecuzione ai proposti principi interpretativi della normativa Ue, alla legge nazionale, e non alla elaborazione giurisprudenziale"*.
Viene quindi sì demandata la soluzione della questione all'intervento del legislatore, ma nel frattempo ritenuta applicabile la disciplina attualmente vigente, cioè l'art. 132 Cod. *Privacy*.
Tale secondo provvedimento, se ha indubbiamente il pregio di invocare un intervento legislativo a regolare la materia, non si ritiene tuttavia condivisibile laddove "congela" l'effetto della sentenza lussemburghese in attesa dell'intervento del legislatore e ritiene temporaneamente ancora applicabile la normativa domestica.
Anche accogliendo l'interpretazione seguita dal Giudice romano, secondo cui i principi espressi nelle sentenze della Corte di Giustizia non creano *ex novo* delle norme comunitarie, ma si limitano a indicare "*il significato e i limiti di applicazione*" delle stesse, è indubbio che i principi espressi nel caso H.K (limitazione a reati gravi, autorizzazione da parte di una autorità indipendente) sono del tutto incompatibili con il dettato dell'art. 132 Cod. *Privacy*, che viene quindi travolto dalla pronuncia della Corte.
Non ci sono alternative: non si può applicare l'art. 132 Cod. *Privacy* così com'è formulato in quanto confligge con il significato e i limiti di applicazione della normativa dell'Unione individuati dalla Corte di giustizia; applicarlo caso per caso, seguendo i principi sanciti dalla Corte, vorrebbe dire rimettere la

soluzione alla discrezionalità del giudice e sottrarre la materia alla riserva assoluta di legge, in contrasto con la Costituzione e anche con la Carta dei diritti fondamentali dell'Unione Europea.
Lo stesso articolo 52 della Carta, nel trattare i limiti all'esercizio dei diritti e delle libertà ivi previste, richiede espressamente che tali limiti debbano essere previsti dalla legge e non forgiati dal giudice[24].
In definitiva, l'unica strada percorribile è quella di un urgente intervento del legislatore che disciplini la materia dell'acquisizione e della conservazione dei dati telefonici e telematici, limitandola a tipizzate forme gravi di criminalità e richiedendo il preventivo controllo da parte del giudice.
In un paese di *civil law* come l'Italia, solo il legislatore può disciplinare e delimitare i casi eccezionali in cui è consentita la violazione di un diritto fondamentale dell'individuo come quello alla riservatezza, garantito a livello costituzionale e di normativa e giurisprudenza dell'Unione[25].
I contrasti che stanno sorgendo tra i giudici chiamati a risolvere la spinosa questione dimostrano che l'individuazione dei limiti alla violazione di un diritto fondamentale non può essere demandata alla discrezionalità del giudice.
Nelle more dell'intervento legislativo, i tabulati acquisiti in violazione dei principi tratteggiati dalla sentenza H.K., non potranno che ritenersi "prove illegittimamente acquisite" e quindi essere travolti dalla sanzione dell'inutilizzabilità ai sensi dell'art. 191 c.p.p., rilevabile anche d'ufficio in ogni stato e grado del procedimento.
Si evidenzia infine che la portata di tale pronuncia della Corte di giustizia è destinata ad avere un riflesso non solo nei procedimenti penali, ma anche in quelli civili, tributari e disciplinari in cui, parimenti, non potrà essere fatto alcun utilizzo, ai fini della decisione, di documenti acquisiti in base ad una norma che deve essere disapplicata per contrasto con i principi di diritto dell'Unione Europea.

---

[24] L'art. 52, comma 1, della Carta prevede che "*eventuali limitazioni dei diritti e delle libertà riconosciuti dalla Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*".
[24] Corte di giustizia, Grande Sezione, 2 marzo 2021, C-746/18.
[25] In tal senso si veda F. RUGGIERI, Data Retention *e Giudice di merito penale. Una discutibile pronuncia,* in *Cass. pen.*, Fasc. 6, 1.6.2017, pag. 2483.