

LA CORTE DI LUSSEMBURGO RIBADISCE LO STOP AI TABULATI: UNA FINE ANNUNCIATA

Leonardo Filippi



1. La sentenza 5 aprile 2022 della Grande Camera della Corte giust. U.E.-

La sentenza della Grande Camera della Corte giust. U.E. 5 aprile 2022, G.D. contro *Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, torna sul tema dei tabulati telefonici, telematici e di ubicazione e, dopo la recente pronuncia 2.3.2021, H.K. della stessa Corte, sempre nella sua composizione più autorevole, che riguardava la legislazione estone, ora con una nuova sentenza, in riferimento alla legge irlandese, ribadisce i principi già ripetutamente affermati in passato.

2. La vicenda.-

Anche in quest'occasione, si tratta di una domanda di pronuncia pregiudiziale sull'interpretazione dell'art. 15, § 1, della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 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).

In sintesi i fatti. Nel marzo 2015 G.D. era stato condannato all'ergastolo per l'omicidio di una persona scomparsa nell'agosto 2012 e i cui resti erano stati scoperti solo nel settembre 2013. Nell'appello contro la sua condanna, l'interessato aveva contestato, in particolare, al giudice di primo grado di avere erroneamente ammesso come prova i dati relativi al traffico e i dati relativi all'ubicazione afferenti a chiamate telefoniche, adducendo che la legge irlandese del 2011, che disciplinava la conservazione di tali dati e in base alla quale gli investigatori della polizia nazionale avevano avuto accesso agli stessi, violava i diritti conferitigli dal diritto dell'Unione. Tale appello è attualmente pendente.

Per poter contestare l'ammissibilità di tali prove nel procedimento penale, G.D. intentò inoltre un'azione civile presso l'Alta Corte, irlandese, diretta a far dichiarare l'invalidità di talune disposizioni della legge del 2011. Con decisione del 6 dicembre 2018, l'Alta Corte accolse l'argomento di G.D. e ritenne che l'art. 6, § 1, lett. a), di tale legge fosse incompatibile con l'art. 15, § 1, della Direttiva 2002/58, letto alla luce degli artt. 7 e 8 nonché dell'art. 52, § 1, della Carta di Nizza. L'Irlanda interpose appello avverso tale decisione dinanzi alla Corte suprema irlandese, quale giudice del rinvio e, nel frattempo, il procedimento penale pendente in Irlanda dinanzi alla Corte d'appello fu sospeso fino alla pronuncia della decisione del giudice del rinvio nell'ambito del procedimento civile principale.

Davanti alla Corte suprema irlandese, quale giudice del rinvio, l'Irlanda sostenne che, per determinare se l'ingerenza nel diritto al rispetto della vita privata, sancito all'art. 7 della Carta di Nizza, costituita dalla conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione ai sensi della legge irlandese del 2011 fosse proporzionata, occorreva esaminare gli obiettivi del regime istituito da tale legge nel suo complesso. Inoltre, secondo tale Stato membro, detta legge istituì un quadro dettagliato che disciplinava l'accesso ai dati conservati, in forza del quale l'unità incaricata, in seno alla polizia nazionale, dell'esame preliminare delle domande di accesso godeva di un'indipendenza funzionale rispetto alla polizia nazionale nell'esercizio della sua missione e, di conseguenza, soddisfaceva il requisito di un previo controllo effettuato da un organo amministrativo indipendente. Tale sistema di controllo sarebbe integrato da un procedimento di reclamo e

da un controllo giurisdizionale. Infine, l'Irlanda affermò che, se si dovesse ritenere che la legge del 2011 fosse contraria al diritto dell'Unione, qualsiasi constatazione che ne fosse dedotta dal giudice del rinvio avrebbe dovuto unicamente valere, sotto il profilo dei suoi effetti nel tempo, per il futuro.

Da parte sua, G.D. sostenne che il regime di conservazione generalizzata e indifferenziata dei dati istituito dalla legge irlandese del 2011 nonché il regime di accesso a tali dati previsto dalla stessa legge erano incompatibili con il diritto dell'Unione, come già affermato dalla Corte giust. U.E. 21 dicembre 2016, Tele2 Sverige e Watson e altri.

La Grande Camera della Corte giust. U.E., decidendo sulla questione pregiudiziale, ha precisato che «la direttiva relativa alla vita privata e alle comunicazioni elettroniche non si limita a disciplinare l'accesso a simili dati mediante garanzie dirette a prevenire gli abusi, ma sancisce, in particolare, il principio del divieto della memorizzazione dei dati relativi al traffico e all'ubicazione. La conservazione di tali dati costituisce quindi, da un lato, una deroga a tale divieto di memorizzazione e, d'altro lato, un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, sanciti dagli artt. 7 e 8 della Carta».

Ne consegue l'obbligo del rispetto «non solo dei requisiti di idoneità e di necessità, ma anche di quello relativo al carattere proporzionato di tali misure in relazione all'obiettivo perseguito».

Pertanto, per la Corte, l'obiettivo della lotta alla criminalità grave non può di per sé giustificare il fatto che una misura di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, come quella introdotta dalla direttiva 2006/24, sia considerata necessaria.

Viene, inoltre, ricordato che «vari obblighi positivi sono a carico dei pubblici poteri in forza della Carta, come per esempio l'adozione di misure giuridiche dirette a tutelare la vita privata e familiare, la protezione del domicilio e delle comunicazioni, ma anche la tutela dell'integrità fisica e psichica delle persone, nonché il divieto di tortura e di trattamenti inumani e degradanti. Ad essi spetta pertanto conciliare i vari interessi legittimi e diritti in gioco. Infatti, un obiettivo d'interesse generale non può essere perseguito senza tener conto del fatto che esso deve essere conciliato con i diritti fondamentali interessati dalla misura, effettuando un contemperamento equilibrato tra, da un lato, l'obiettivo di interesse generale e, dall'altro, i diritti di cui trattasi, verificando che l'importanza di detto obiettivo sia correlata alla gravità dell'ingerenza provocata da tale misura».

La Corte ha quindi ribadito principi già affermati ripetutamente nella sua precedente giurisprudenza. Essi sono sostanzialmente tre.

3.1. Il primo principio si articola in diversi punti:

a) Il divieto di «conservazione generalizzata e indifferenziata» dei dati relativi al traffico e dei dati relativi all'ubicazione per finalità di prevenzione delle minacce gravi alla sicurezza pubblica e di repressione della criminalità grave.-

Il primo punto, in ossequio al principio di proporzionalità enunciato dall'art. 52 della Carta dei diritti fondamentali, afferma che l'art. 15, § 1, della menzionata Direttiva 2002/58/CE deve essere interpretato nel senso che esso osta a misure legislative che prevedano, a titolo preventivo, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica, la «conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione». Ne deriva il divieto di una conservazione di tali dati come quella vigente in Italia, che è appunto «generalizzata e indifferenziata», estesa fino a sei anni, in chiave preventiva rispetto alla commissione di eventuali futuri reati.

b) L'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.-

La Corte di giustizia ha chiarito che il predetto art. 15, § 1, letto alla luce degli artt. 7, 8 e 11 e dell'art. 52, § 1, della Carta dei diritti fondamentali, non osta, invece, a misure legislative che prevedano, «per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica», la «conservazione mirata» dei dati relativi al traffico e dei dati relativi all'ubicazione, che però deve essere «delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile».

c) L'ammissibilità di una «conservazione generalizzata e indifferenziata» degli indirizzi IP.-

E' ammessa pure la «conservazione generalizzata e indifferenziata degli indirizzi IP» attribuiti all'origine di una connessione, ma deve essere «per un periodo temporalmente limitato allo stretto necessario».

d) L'ammissibilità di una «conservazione generalizzata e indifferenziata dei dati relativi all'identità civile» degli utenti.-

Senza alcun limite è consentita la «conservazione generalizzata e indifferenziata dei dati relativi all'identità civile» degli utenti di mezzi di comunicazione elettronica, cioè le indicazioni nominative degli utenti.

e) L'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.-

E' consentito infine il ricorso a un' «ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica», esperibile non soltanto dal P.M. ma dal difensore di ogni parte processuale, mediante una decisione dell'autorità competente soggetta a un controllo giurisdizionale effettivo, di procedere, «per un periodo determinato», alla «conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono tali fornitori di servizi».

f) Garanzie comuni a tutte le misure: rispetto delle condizioni e garanzie effettive contro il rischio di abusi.-

La Corte ammonisce però che condizione essenziale è che «tali misure garantiscano, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi è subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongono di garanzie effettive contro il rischio di abusi».

3.2. Il secondo principio riferito alla legislazione irlandese.

Esso chiarisce che l'art. 15, § 1, della stessa Direttiva 2002/58 deve essere interpretato nel senso che esso osta a una normativa nazionale, come quella irlandese, in forza della quale «il trattamento centralizzato delle domande di accesso a dati conservati dai fornitori di servizi di comunicazione elettronica, provenienti dalla polizia nell'ambito della ricerca e del perseguimento di reati gravi, è affidato a un funzionario di polizia, anche qualora quest'ultimo sia assistito da un'unità istituita all'interno della polizia che gode di una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale».

La Corte statuisce anche che, «al fine di garantire, nella pratica, il pieno rispetto delle rigide condizioni di accesso a dati personali», quali i dati relativi al traffico e i dati relativi all'ubicazione, «l'accesso da parte delle autorità nazionali competenti ai dati conservati deve essere subordinato ad un controllo preventivo effettuato o da un giudice o da un organo amministrativo indipendente», e la decisione di tale giudice o di tale organo deve intervenire «a seguito di una richiesta motivata di tali autorità presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di azione penale». E, secondo la Corte, «un funzionario di polizia non è un giudice e non presenta tutte le garanzie d'indipendenza e di imparzialità richieste per poter essere qualificato come organo amministrativo indipendente».

La Corte, quindi, adeguandosi alla sua precedente giurisprudenza, esige che la decisione sull'accesso ai dati conservati sia riservata al giudice o ad un'autorità amministrativa indipendente.

3.3. Il terzo principio ribadisce gli effetti *ex tunc* delle sentenze della Corte di giustizia U.E. e la riserva nazionale sull'ammissibilità della prova derivante dai dati conservati.-

Afferma la Corte di Lussemburgo che il diritto dell'Unione deve essere interpretato nel senso che esso «osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante», in forza del diritto nazionale, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, a causa dell'incompatibilità di tale normativa con l'art. 15, § 1, della Direttiva 2002/58, come modificata dalla Direttiva 2009/136, letto alla luce della Carta dei diritti fondamentali.

Infine, la Corte precisa che «l'ammissibilità degli elementi di prova ottenuti mediante una siffatta conservazione rientra, conformemente al principio di autonomia procedurale degli Stati membri, nell'ambito del diritto nazionale», dovendosi però sempre rispettare i principi di equivalenza (per cui gli individui che fanno valere diritti conferiti dall'ordinamento dell'Unione non devono essere svantaggiati rispetto a quelli che invocano situazioni giuridiche soggettive nazionali) e di effettività (per il quale le norme di diritto interno, rilevanti sul piano processuale, non devono rendere praticamente impossibile o eccessivamente difficile la tutela dei diritti spettanti in forza del diritto U.E.) .

4. Conclusioni.-

Di fronte alla ennesima declaratoria di invalidità di una legislazione che, come quella italiana, prevede una

conservazione «generalizzata e indifferenziata» dei dati telefonici, telematici e di ubicazione, per giunta estesa fino a sei anni, il legislatore deve nuovamente intervenire per rimodellare la disciplina del Codice della *privacy*, introducendo una «conservazione mirata» di tali dati, che però deve essere delimitata, «sulla base di elementi oggettivi e non discriminatori» (ad es. indizi di colpevolezza di gravi reati già commessi o al fine di prevenire la commissione di gravi reati), «in funzione delle categorie di persone interessate» (ad es. indiziati di gravi reati o persone sospettate di essere in procinto di commettere gravi reati) o «mediante un criterio geografico» (ad es. la zona circostante la scena del delitto o gli spostamenti di un soggetto) e comunque «per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile» (ad es. il periodo prossimo al momento di commissione del reato).

Il legislatore dovrebbe pure garantire l'efficienza delle indagini del P.M. e le investigazioni difensive, introducendo nel nostro sistema processuale la possibilità per tutte le parti di rivolgere una «ingiunzione» ai fornitori di servizi di comunicazione elettronica, mediante una decisione dell'autorità competente soggetta a un controllo giurisdizionale effettivo, di procedere, «per un periodo determinato», alla «conservazione rapida» dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono tali fornitori di servizi.

Relativamente, infine, all'utilizzabilità dei dati illegittimamente conservati e/o acquisiti in un processo penale italiano, la Corte richiama le proprie precedenti affermazioni contenute nelle sentenze 2 marzo 2021, *Prokuratuur* e 6 ottobre 2020, *La Quadrature du Net* e altri. In particolare, in quelle occasioni la Grande Camera aveva puntualizzato che «spetta, in linea di principio, al solo diritto nazionale stabilire le regole relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti criminali, di informazioni e di elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati in questione, contraria al diritto dell'Unione, od anche mediante un accesso delle autorità nazionali ai dati suddetti, contrario a tale diritto dell'Unione». Infatti, secondo una consolidata giurisprudenza europea, in assenza di norme dell'Unione in materia, spetta all'ordinamento giuridico interno di ciascuno Stato membro, in virtù del principio dell'autonomia procedurale, stabilire le regole di procedura applicabili ai ricorsi giurisdizionali destinati a garantire la tutela dei diritti riconosciuti ai singoli dal diritto dell'Unione, a condizione però che le regole suddette non siano meno favorevoli di quelle disciplinanti situazioni analoghe assoggettate al diritto interno (principio di equivalenza) e che non rendano impossibile in pratica o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione (principio di effettività).

Per quanto riguarda più in particolare il principio di effettività, occorre ricordare che le norme nazionali

relative all'ammissibilità e all'utilizzazione delle informazioni e degli elementi di prova hanno come obiettivo, in virtù delle scelte operate dal diritto nazionale, di «evitare che informazioni ed elementi di prova ottenuti in modo illegittimo arrechino indebitamente pregiudizio a una persona sospettata di avere commesso dei reati». Il diritto nazionale può raggiungere tale obiettivo «non solo mediante un divieto di utilizzare informazioni ed elementi di prova siffatti, ma anche mediante norme e prassi nazionali che disciplinino la valutazione e la ponderazione delle informazioni e degli elementi di prova, o addirittura tenendo conto del loro carattere illegittimo in sede di determinazione della pena» (sentenza 6 ottobre 2020, *La Quadrature du Net* e altri, cit.).

La Corte di Lussemburgo aveva già sottolineato la necessità di escludere informazioni ed elementi di prova ottenuti in violazione delle prescrizioni del diritto dell'Unione deve essere valutata alla luce, in particolare, del «rischio che l'ammissibilità di informazioni ed elementi di prova siffatti comporta per il rispetto del principio del contraddittorio e, pertanto, del diritto ad un processo equo». Pertanto, il giudice nazionale, il quale consideri che una parte non è in grado di svolgere efficacemente le proprie osservazioni in merito a un mezzo di prova rientrante in una materia estranea alla conoscenza dei giudici e idoneo ad influire in modo preponderante sulla valutazione dei fatti, «deve constatare una violazione del diritto ad un processo equo ed escludere tale mezzo di prova al fine di evitare una violazione siffatta». In conclusione, secondo la Corte, «il principio di effettività impone al giudice penale nazionale di escludere informazioni ed elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con il diritto dell'Unione, od anche mediante un accesso dell'autorità competente a tali dati in violazione del diritto dell'Unione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti di criminalità, qualora tali persone non siano in grado di svolgere efficacemente le proprie osservazioni in merito alle informazioni e agli elementi di prova suddetti, riconducibili ad una materia estranea alla conoscenza dei giudici e idonei ad influire in maniera preponderante sulla valutazione dei fatti» (v., in tal senso, sentenza del 6 ottobre 2020, *La Quadrature du Net* e altri, cit.).

Clicca qui per il testo della sentenza in italiano:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62021CJ0249&qid=1649929347077&from=I>

I

