Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche: l'orientamento della Corte di Giustizia tra principio di proporzionalità, criterio di "gravità" e definizione di autorità indipendente

di Emilio Minniti

Title: Processing of personal data and protection of privacy in the electronic communications sector: the orientation of the European Court of Justice between the principle of proportionality, the criterion of "seriousness" and the definition of independent authority

Keywords: Personal Data; Privacy; Telecommunications.

1. – L'articolo 15, paragrafo 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), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre

DPCE online
ISSN: 2037-6677

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 le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo.

L'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale.

Questo è il *decisum* cui perviene la Corte di Giustizia dell'Unione Europea, Grande Sezione, con riferimento alla domanda di pronuncia pregiudiziale sollevata, ai sensi dell'articolo 267 TFUE, dal Riigikohus (Corte suprema, Estonia) in relazione al procedimento penale contro H.K.

Con la sentenza del 6 aprile 2017, il Viru Maakohus (Tribunale di primo grado di Viru, Estonia) ha condannato H.K. a una pena detentiva di due anni per aver commesso, nel periodo compreso tra il 17 gennaio 2015 e il 1° febbraio 2016, otto furti di prodotti alimentari e di altri beni materiali di valore compreso tra EUR 5,20 e EUR 2.100,00, per aver utilizzato la carta bancaria di un terzo, causando a quest'ultimo un danno di EUR 3.941,82, e per aver commesso atti di violenza nei confronti di soggetti partecipanti ad un procedimento giudiziario a suo carico.

Nel pronunciare la condanna di H.K. il Tribunale di primo grado estone si è basato, tra l'altro, su una serie di processi verbali che vertono su

dati relativi a comunicazioni elettroniche, ai sensi di quanto disposto dal paragrafo 2 dell'articolo 111 della legge relativa alle comunicazioni elettroniche (Elektroonilise Side Seadus), che l'autorità incaricata dell'indagine aveva raccolto presso un fornitore di servizi di telecomunicazioni nel corso del procedimento istruttorio, dopo aver ottentuto a tal fine l'autorizzazione del Viru Ringkonnaprokuratuur (Procura Distrettuale di Viru, Estonia), sulla base dell'articolo 901 del Codice di Procedura Penale.

Nello specifico, in data 2 novembre 2015, la Procura Distrettuale di Viru ha autorizzato l'autorità inquirente a ordinare all'impresa di telecomunicazioni di fornire i dati di cui al paragrafo 2 dell'articolo 111 della legge sulla comunicazione elettronica, al fine di accertare la trasmissione, in data 21 settembre 2015, di telefonate e messaggi mediante due numeri di telefono cellulare utilizzati da H.K., la loro durata, la modalità di trasmissione, i dati personali e l'ubicazione del mittente e del destinatario. Sulla base dei dati ottenuti dall'impresa di telecomunicazioni in virtù di tale autorizzazione, l'autorità inquirente, in data 4 novembre 2015, ha redatto un verbale nel quale erano indicati i ripetitori telefonici nel cui raggio d'azione era stato utilizzato il numero di abbonato adoperato da H.K. il 21 settembre 2015 dopo le ore 19:00. Il pubblico ministero, con tale verbale ed unitamente ad altri mezzi di prova, ha inteso dimostrare in giudizio che H.K. era l'autrice del furto perpetrato il 21 settembre 2015. In data 25 febbraio 2016 la Procura Distrettuale di Viru ha nuovamente autorizzato l'autorità inquirente a ordinare all'impresa di telecomunicazioni di fornire, in relazione a sette numeri di telefono utilizzati da H.K. nel periodo compreso tra l'1 marzo 2015 ed il 19 febbraio 2016, i dati di cui al paragrafo 2 dell'articolo 111 della legge sulla comunicazione elettronica, ai fini dell'indagine su un reato di cui all'articolo 303, paragrafo 1, del Codice Penale (Karistusseadustik) Sulla base dei dati ottenuti in ragione di tale autorizzazione, che indicavano i giorni in cui H.K. aveva chiamato i

DPCE online
ISSN: 2037-6677

coimputati ed aveva ricevuto chiamate dai medesimi, nonché le date in cui H.K. aveva inviato loro messaggi e ne aveva ricevuti da essi, è stato redatto il verbale del 15 marzo 2016 con il quale pubblico ministero ha inteso dimostrare in giudizio, unitamente ad altri mezzi di prova, che H.K., dalla primavera del 2015, aveva ripetutamente minacciato per telefono i coimputati. Il 20 aprile e il 6 maggio 2016 l'autorità inquirente, sempre in forza della suddetta autorizzazione, ha redatto altri verbali relativi ai dati ottenuti dall'impresa di telecomunicazioni, nei quali sono annotate le stazioni base nella cui copertura, nelle date del 4, del 27 e del 31 agosto 2015 nonché dall'1 al 3 settembre 2015, sono partite telefonate dai sei numeri di abbonato utilizzati da H.K. e sono state ricevute telefonate dagli stessi. Sulla base di tali verbali, unitamente ad altri mezzi di prova, i pubblico ministero ha inteso dimostrare in giudizio che H.K. era l'autrice dei sei furti perpetrati nelle date sopra indicate. Contestualmente, sulla base di un'autorizzazione rilasciata dalla Procura Distrettuale di Viru per reati di cui all'articolo 200, paragrafo 2, punti 7, 8 e 9, del Codice Penale (furto a mano armata e con violazione di domicilio), il 20 aprile 2016 l'autorità inquirente ha redatto un verbale in cui figurano i dati relativi alle stazioni base nel cui raggio di copertura, nel periodo compreso tra il 16 ed il 19 gennaio 2015, sono partite telefonate da due numeri di abbonato utilizzati da H.K. e sono state ricevute telefonate dai medesimi. Sulla base di detto verbale, unitamente ad altri mezzi di prova, il pubblico ministero ha inteso dimostrare che H.K. era la persona che, dal 17 al 19 gennaio 2015, aveva prelevato denaro contante con la carta bancaria della vittima da un distributore automatico di banconote.

Il 17 novembre 2017 la Tartu Ringkonnakohus (Corte d'appello di Tartu, Estonia) ha respinto l'appello contro la sentenza del Viru Maakohus presentato da H.K., la quale ha successivamente proposto un ricorso contro tale decisione dinanzi alla Riigikohus (Corte suprema, Estonia), contestando, tra l'altro, l'ammissibilità dei processi verbali redatti in base ai

dati ottenuti presso il fornitore di servizi di comunicazioni elettroniche. Nel ricorso, infatti, si sostiene come, sulla base di quanto stabilito dalla sentenza *Tele2 e Watson*, le disposizioni dell'articolo 111 della legge relativa alle comunicazioni elettroniche che prevedono l'obbligo dei fornitori di servizi di conservare dati relativi alle comunicazioni, nonché l'utilizzazione di tali dati ai fini della condanna, siano contrari all'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11, nonché dell'articolo 52, paragrafo 1, della Carta.

Viene pertanto sollevata la questione della conformità a quanto disposto dall'articolo 15, paragrafo 1, della direttiva 2002/58, della raccolta dei dati posti alla base dei processi verbali e, dunque, della loro effettiva ammissibilità come prova.

In considerazione di tale problema interpretativo, ma anche in relazione alle perplessità emerse rispetto alla possibilità di considerare il pubblico ministero estone come un'autorità amministrativa indipendente, il Riigikohus ha sospeso il procedimento sottoponendo alla Corte di giustizia europea le seguenti questioni pregiudiziali: se l'articolo 15, paragrafo 1, della direttiva 2002/58 debba essere interpretato, alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta, nel senso che, in un procedimento penale, l'accesso di autorità nazionali a dati che consentano di rintracciare e identificare la fonte e la destinazione di una comunicazione telefonica a partire dal telefono fisso o mobile del sospettato, di determinare la data, l'ora, la durata e la natura di tale comunicazione, di identificare le apparecchiature di comunicazione utilizzate, nonché di localizzare il materiale di comunicazione mobile utilizzato, costituisce un'ingerenza nei diritti fondamentali sanciti dai suddetti articoli della Carta di gravità tale che detto accesso debba essere limitato, nel contesto della prevenzione, della ricerca, dell'accertamento e del perseguimento dei reati, alla lotta contro le forme gravi di criminalità, indipendentemente dal periodo al quale si riferiscono i dati conservati cui le autorità nazionali hanno accesso;

DPCE online
ISSN: 2037-6677

se l'articolo 15, paragrafo 1, della direttiva 2002/58 debba essere interpretato, sulla scorta del principio di "proporzionalità" enunciato nella sentenza del 2 ottobre 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788), punti da 55 a 57, nel senso che, qualora la quantità dei dati menzionati nella prima questione, ai quali le autorità nazionali hanno accesso, non sia grande (sia per il tipo di dati che per la loro estensione nel tempo), la conseguente ingerenza nei diritti fondamentali può essere giustificata, in generale, dall'obiettivo della prevenzione, della ricerca, dell'accertamento e del perseguimento dei reati, e che quanto più notevole è la quantità di dati cui le autorità nazionali hanno accesso, tanto più gravi devono essere i reati perseguiti mediante tale ingerenza; se il requisito indicato nel secondo punto del dispositivo della sentenza del 21 dicembre 2016, *Tele2 e Watson* (C-203/15 e C-698/15, EU:C:2016:970), secondo cui l'accesso ai dati da parte delle autorità nazionali competenti dev'essere soggetto ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, implichi che l'articolo 15, paragrafo 1, della direttiva 2002/58 deve essere interpretato nel senso che può considerarsi come un'autorità amministrativa indipendente il pubblico ministero, il quale dirige il procedimento istruttorio e che, per legge, è tenuto ad agire in modo indipendente, restando soggetto soltanto alla legge e verificando, nell'ambito del procedimento istruttorio, sia gli elementi a carico sia quelli a discarico relativi all'indagato, ma che successivamente, nel procedimento giudiziario, rappresenta la pubblica accusa.

2. – La Corte di Giustizia, nel dare risposta alle domande pregiudiziali poste dal giudice del rinvio, evidenzia come i paragrafi 2 e 4 dell'articolo 111 dell'Elektroonilise Side Seadus (legge relativa alle comunicazioni elettroniche) impongano ai fornitori di servizi di comunicazioni elettroniche un obbligo di conservare per il periodo di un anno, in maniera generalizzata e indifferenziata, i dati relativi al traffico e all'ubicazione

riguardanti la telefonia fissa e mobile. Tali dati consentono, in particolare, di rintracciare e di identificare la fonte e la destinazione di una comunicazione a partire da un telefono fisso o mobile, di stabilire la data, l'ora, la durata e la natura di tale comunicazione, di identificare le apparecchiature di comunicazione utilizzate, di localizzare il telefono mobile senza che una comunicazione sia necessariamente trasmessa, nonché di accertare la frequenza delle comunicazioni dell'utente con determinate persone in un dato periodo.

Tra questi dati, infatti, figurano: il numero telefonico del chiamante nonché il nome e il recapito dell'abbonato; il numero telefonico del chiamato nonché il nome e il recapito dell'abbonato; in caso di utilizzo di servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero selezionato nonché il nome e il recapito dell'abbonato; la data e l'ora di inizio e fine di una chiamata; il servizio di telefonia fissa o mobile utilizzato; il codice identificativo internazionale di abbonato di telefonia mobile (IMSI) del soggetto chiamante e del soggetto chiamato; il codice identificativo internazionale di apparecchiatura di telefonia mobile (IMEI) del soggetto chiamante e del soggetto chiamato; l'etichetta di ubicazione all'inizio della chiamata; i dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione nel periodo in cui vengono conservati i dati sulle comunicazioni; nel caso di servizi prepagati anonimi, la data e l'ora della prima attivazione della carta e l'etichetta di ubicazione del luogo in cui è stata effettuata l'attivazione.

In relazione a ciò la Corte ha rilevato come l'accesso a un insieme di dati relativi al traffico o all'ubicazione possa consentire di trarre conclusioni molto precise sulla vita privata dei soggetti i cui dati sono stati conservati, in riferimento soprattutto alle abitudini della vita quotidiana, ai luoghi di soggiorno permanenti o temporanei, agli spostamenti giornalieri o di altro tipo, alle attività esercitate, alle relazioni sociali e agli ambienti frequentati (sul tema la Corte rimanda alla sentenza del 6 ottobre 2020, La

DPCE online
ISSN: 2037-6677

Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 117).

Pertanto, in considerazione di tali circostanze, la Corte afferma come soltanto gli obiettivi della lotta contro le forme "gravi" di criminalità o della prevenzione di "gravi" minacce per la sicurezza pubblica sono atti a giustificare l'accesso delle autorità pubbliche ad un insieme di dati relativi al traffico o all'ubicazione, suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali utilizzate da quest'ultimo, e che quindi siano tali da consentire di trarre conclusioni precise sulla vita privata dei soggetti interessati (sul tema la Corte rimanda alla sentenza del sentenza del 2 ottobre 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punto 54), 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.

Riconnettendosi alla precedente giurisprudenza sul tema (*cfr Tele2 e Watson* , C-203/15 e C-698/15, EU:C:2016:970; *Ministerio Fiscal*, C-207/16, EU:C:2018:788) i giudici hanno ribadito come una tale ingerenza nei diritti fondamentali prodotta dall'acquisizione dei dati in questione sia giustificabile esclusivamente nell'ambito del contrasto alla criminalità "grave", integrando concettualmente il dispositivo dell'articolo 15 della direttiva 2002/58/CE, secondo il quale "gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, 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 dell'uso non autorizzato del sistema di comunicazione

elettronica […]" (*cfr* G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministerio Fiscal in *Osservatorio Costituzionale AIC*, Fasc. 3/2018, 458).

Quanto alla questione dell'incidenza della durata del periodo per il quale viene richiesto l'accesso ai dati, sebbene la Corte affermi di concordare, in linea di principio, con il giudice del rinvio circa la sussistenza di un rapporto tra l'estensione temporale dell'accesso e l'entità dell'ingerenza nella vita privata del soggetto, questa precisa, tuttavia, come la quantità dei dati disponibili e le informazioni concrete sulla vita privata della persona interessata siano aspetti che possono essere adeguatamente valutati soltanto dopo la consultazione dei dati suddetti. Poiché, ad ogni modo, l'autorizzazione all'accesso interviene necessariamente prima che i dati vengano visionati, la valutazione della gravità dell'ingerenza costituita dall'accesso si effettua essenzialmente in termini generali in funzione del rischio per l'afferente alla categoria di dati richiesti.

In ultimo, in riferimento alla terza questione pregiudiziale sollevata dal giudice del rinvio, relativa alla compatibilità con l'art. 15 della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, dell'individuazione del pubblico ministero estone quale autorità competente ad autorizzare l'accesso ai dati relativi al traffico e all'ubicazione ai fini di un'istruttoria penale, la Corte precisa preliminarmente come spetti al diritto nazionale stabilire le condizioni alle quali i fornitori di servizi di comunicazioni elettroniche debbano accordare l'accesso ai dati. Tuttavia, al fine di soddisfare il principio di proporzionalità, i giudici affermano come un tale accesso possa essere consentito con l'obbiettivo del contrasto alla criminalità, soltanto per i dati di soggetti sospettati di progettare, di commettere o di aver commesso un illecito grave, e che esso debba essere necessariamente subordinato ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente (sul tema la Corte rimanda alla sentenza del

DPCE online
ISSN: 2037-6677

6 ottobre 2020, *La Quadrature du Net e a.*, C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 189 e alla giurisprudenza *ivi* citata). Quanto ai requisiti che definiscono il concetto di autorità amministrativa indipendente, la Corte riprende l'orientamento esplicitato dall'Avvocato Generale nel paragrafo 105 delle sue conclusioni, individuando due specifici presupposti: tale autorità non deve essere soggetta a istruzioni o pressioni esterne che possano influenzarne le decisioni; detta autorità, in virtù del proprio *status* e dei compiti che le sono conferiti, deve soddisfare un requisito di obiettività nell'ambito del controllo da essa effettuato, ossia deve offrire garanzie di imparzialità. L'entità amministrativa indipendente, quindi, deve essere in grado di garantire un giusto equilibrio tra gli interessi dell'indagine contro la criminalità e il rispetto dei diritti fondamentali, della vita privata e della protezione dei dati personali dei soggetti interessati dall'accesso. Essa deve evidenziare terzietà rispetto al soggetto che richiede l'accesso ai dati, e ricoprire una posizione di neutralità nei confronti delle parti del procedimento penale. In riferimento a tali criteri, dunque, il pubblico ministero non può essere considerato quale autorità amministrativa indipendente, in quanto questi dirige il procedimento di indagine ed esercita l'azione penale. La Corte non considera sufficiente a conferirgli lo *status* di terza parte rispetto agli interessi in gioco la circostanza che il pubblico ministero sia tenuto a verificare gli elementi a carico e quelli a discarico, a garantire la legittimità del procedimento istruttorio e ad agire unicamente in base alla legge ed al suo convincimento. Quanto all'eventualità, considerata dal giudice del rinvio nelle sue domande pregiudiziali, di supplire all'assenza di un controllo preliminare effettuato da un'autorità indipendente mediante un controllo successivo, effettuato da un giudice, la Corte precisa come il controllo indipendente debba intervenire anteriormente a qualsiasi accesso, salvo situazioni di giustificata urgenza, nel qual caso questo deve comunque avvenire entro tempi brevi. Un controllo successivo, infatti, non

consentirebbe di impedire un accesso ai dati in questione eccedente i limiti dello stretto necessario.

3. – La sentenza in oggetto offre una lettura in chiave "costituzionale" dell'art. 15 della Direttiva 2002/58/CE che si inserisce nel quadro della giurisprudenza precedente (*Digital Rights Ireland*, *Schrems*, *Tele2 e Watson*) contribuendo a definire in maniera più netta i termini del bilanciamento tra la tutela del diritto alla privacy e alla protezione dei dati personali e l'esigenza di conservare e utilizzare tali dati al fine di garantire la sicurezza. In questa prospettiva, la sentenza *H.K.* consente inoltre di escludere ogni ipotesi interpretativa orientata ad individuare nella decisone sul caso *Ministerio Fiscal* una sorta di "*revirement*" rispetto a quanto sancito dalla precedente sentenza *Tele2 e Watson*, in relazione al requisito della gravità del reato (*cfr* G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministerio Fiscal in *Osservatorio Costituzionale AIC*, Fasc. 3/2018, 464).

Sebbene la Carta di Nizza abbia codificato l'*habeas data*, ossia l'equivalente dell'*habeas corpus* nell'ambito della società e della dimensione digitale, la costante evoluzione tecnologica e il recente rafforzamento delle esigenze di sicurezza rispetto alla diffusa minaccia terroristica hanno evidenziato la necessità di tutelare la *privacy* su diversi ed importanti piani (in dottrina v. C. SARTORETTI, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in *Federalismi.it*, Luglio 2019, 10 e SS). Con la sentenza *Schrems* del 6 ottobre 2015, causa C-362/14, la Corte di Giustizia europea ha rivendicato la necessità di affermare e difendere la sovranità digitale dell'Unione, stabilendo l'invalidità dell'accordo commerciale con gli Stati Uniti basato sul regime del cosiddetto *safe-harbour*, in quanto si era consentito alle aziende americane un uso improprio dei dati degli utenti europei transitati su *server* statunitensi. La decisione sul caso *Digital Rights Ireland*, viceversa, ha disposto

DPCE online
ISSN: 2037-6677

l'annullamento della Direttiva 2006/24/CE, relativa alla conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, che aveva modificato la precedente 2002/58/CE con l'obbiettivo di creare un quadro normativo in materia di *data retention* unitario e non più frammentato e diversificato su base statale. La Corte ha tuttavia ritenuto che le disposizioni contenute in essa non superassero il test di "proporzionalità", in quanto producevano una compressione dei diritti fondamentali non circoscritta a quanto strettamente necessario. Da tale pronuncia è dunque scaturita una ri-espansione di quanto disposto in materia dalla Direttiva 2002/58/CE, che ha nuovamente posto gli Stati membri di fronte alla necessità di individuare correttamente il perimetro concesso alle legislazioni nazionali dai margini derogatori previsti dall'art. 15. Le sentenze *Tele2 e Watson*, *Ministerio Fiscal* e *H.K.* rispondono a tale esigenza, disegnando un quadro sostanzialmente unitario e coerente. La decisione sul caso *Tele2 e Watson* stabilisce che il margine di manovra che la direttiva riconosce agli Stati membri al fine di integrare una deroga al regime ordinario di tutela della *privacy* debba essere interpretato in senso chiaramente restrittivo, giungendo ad implementare concettualmente il dispositivo dell'art. 15, il quale "osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione". Contestualmente, i giudici hanno sancito che l'art. 15 debba essere interpretato nel senso che esso "osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione

generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica".

La Corte di Giustizia dell'Unione Europea ha dunque stabilito che soltanto la necessità di contrastare forme di criminalità "grave" possa giustificare una significativa ingerenza nei diritti fondamentali e che tale ingerenza debba essere sottoposta ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente (cfr G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministerio Fiscal in *Osservatorio Costituzionale AIC*, Fasc. 3/2018, 458 e ss; I. Cameron, *A. Court of Justice Balancing data protection and law enforcement needs: Tele2 Sverige and Watson* in *Common Market Law Review,* Vol. 54, Issue 5 (2017),1467-1495; O. Pollicino; M. Bassini, *La Corte di Giustizia e una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico,* in *Diritto Penale Contemporaneo,* 3 e ss).

La sentenza *H.K.* ha confermato e consolidato le linee di fondo di questo impianto interpretativo, e consente pertanto alla dottrina di escludere retrospettivamente "letture" della decisone del 2 ottobre 2018 sul caso *Ministerio Fiscal* orientate all'individuazione di un mutamento di prospettiva rispetto alla preminenza del criterio della "gravità". Nell'ambito di quest'ultima pronuncia, infatti, si è registrato un riferimento al principio di proporzionalità volto a conferire legittimità ad un'ingerenza non grave nel quadro di un procedimento relativo ad un reato di altrettanto ridotta gravità. L'analisi della sentenza *H.K.*, in ultima analisi, permette di registrare il consolidamento di un preciso orientamento della Corte di Giustizia dell'Unione Europea, volto ad interpretare in chiave "restrittiva" le possibilità di ingerenza in merito al diritto alla *privacy* e alla protezione dei dati personali, concesse al legislatore nazionale.

DPCE online
ISSN: 2037-6677

Emilio Minniti
Università degli Studi Internaz. di Roma
emilio.minniti@unint.eu