DIRITTO PENALE CONTEMPORANEO

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

Nota a Corte Giustizia UE, sent. 21 dicembre 2016, Tele2 e Watson, cause riunite C-203/15 e C-698/15

di Oreste Pollicino e Marco Bassini

SOMMARIO: 1. Introduzione. – 2. Uno scenario complesso. – 3. La prima questione pregiudiziale. – 4. La seconda questione pregiudiziale. – 5. Conclusioni.

1. Introduzione.

Dove eravamo rimasti?

Una frase che potrebbe prestarsi a moltissimi contesti, ma che riesce particolarmente efficace per descrivere la continuità con cui la Corte di giustizia, a distanza di poco più di un anno dalla sentenza *Schrems*[1], è tornata a occuparsi del diritto alla privacy, specialmente in ambito digitale.

Prima ancora, come noto, la Corte di giustizia non aveva lesinato sforzi nel codificare, nella sentenza *Google Spain*[2], il diritto alla deindicizzazione dai motori di ricerca e nel pronunciare, nel caso *Digital Rights Ireland*[3], l'annullamento della direttiva 2006/24/CE (c.d. direttiva "Frattini" o "*data retention*") sulla conservazione dei dati personali da parte dei fornitori di servizi di comunicazione elettronica.

Ed è proprio a quest'ultima, storica e controversa decisione e alla sua narrativa che si ricollega la pronuncia che la Grande Sezione della Corte di giustizia ha consegnato il 21 dicembre nelle cause riunite C-203/15 e C-698/15, in cui i giudici europei sono tornati a occuparsi della compatibilità con il diritto dell'Unione delle misure di conservazione dei dati di traffico.

«Se gli uomini fossero angeli, nessun governo sarebbe necessario. Se gli angeli governassero gli uomini, nessun controllo – esterno o interno – sul governo sarebbe necessario. Nel prefigurare un governo di uomini nei confronti di altri uomini, questa è

[1] Corte di giustizia UE, 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*.

[2] Corte di giustizia UE, 13 maggio 2014, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja Gonzàlez*.

[3] Corte di giustizia UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland, Seitlinger e a.*

la difficoltà più grande: prima bisogna permettere al governo di controllare i governati, poi obbligare il governo a controllare se stesso».

Con questa citazione di James Madison si aprono le Conclusioni dell'Avvocato generale[4] nelle cause che hanno visto i giudici del Lussemburgo pronunciarsi. Una citazione che, a ben vedere, coglie nel segno, perché alla radice dell'opera di bilanciamento affidata alla Corte insiste proprio la difficoltà individuata da Madison. La Corte di giustizia era chiamata, infatti, a giudicare la compatibilità con il diritto dell'Unione di disposizioni di diritto interno che obbligavano i fornitori di servizi di comunicazioni elettronica alla conservazione, per un determinato periodo di tempo, di dati di traffico e di ubicazione degli utenti.

Evidente il dilemma, ben rappresentato dallo stesso Avvocato generale. Da una parte, la conservazione dei dati relativi alle comunicazioni consente «al governo di controllare i governati», mettendo a disposizione delle autorità competenti un mezzo di indagine che presenta un'utilità certa nel contrasto ai reati gravi, e in particolare nella lotta contro il terrorismo. Dall'altra, non può non porsi il problema dell'esigenza «di obbligare il governo a controllare se stesso» per quanto riguarda sia la conservazione, sia l'accesso ai dati conservati, tenendo conto delle minacce per il diritto alla privacy, sempre più a "trazione costituzionale" in ambito europeo. Alla base della "difficoltà" più grande, per citare ancora Madison, si colloca la domanda su quale debba essere il punto di equilibrio tra tutela della sicurezza pubblica, specie con riferimento all'esigenza di prevenire attacchi terroristici, per un verso, e protezione della privacy digitale, per altro.

Vi è anche un convitato di pietra che gioca un ruolo da protagonista assoluto lungo il percorso argomentativo della decisione: la già ricordata sentenza dell'8 aprile 2014 nella causa *Digital Rights Ireland*, in cui la Corte di giustizia aveva invalidato la direttiva sulla *data retention* in quanto il periodo di conservazione di dati previsto per fini di protezione dell'ordine pubblico veniva considerato eccessivo e non proporzionato, anche per la vaghezza delle condizioni cui detta conservazione era subordinata[5].

La ragione dell'importanza di questa decisione per la risoluzione del dilemma alla base della pronuncia che si commenta emerge già dai quesiti che i giudici svedesi e britannici hanno posto alla Corte di giustizia. Infatti, seppure in questo caso oggetto diretto dell'interpretazione della Corte fosse una normativa diversa, adottata nel 2002 (direttiva 2002/58/CE), dunque ancor prima della direttiva "Frattini", i giudici nazionali si interrogavano se una legislazione nazionale che prevedesse una conservazione generalizzata e indifferenziata dei dati degli abbonati, utilizzando il

[4] Conclusioni dell'Avvocato generale Saugmandsgaard Øe, 19 luglio 2016.

[5] Per un commento più approfondito si vedano, *ex multis*, i contributi di L. TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it.*, 2014, 8-9, 1850 ss.; R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont. – Riv. trim.*, 2/2014, 178 ss.; F. FABBRINI, *The European Court of Justice Ruling in the Data Rentention Case and its Lessons for Privacy and Surveillance in the U.S.*, 28 *Harvard Human Rights Journal* (2015), 65 ss.

margine di manovra fornito dalla direttiva, si ponesse o meno in contrasto, tra l'altro, con quanto affermato dalla Corte di giustizia nel 2014 nella sentenza *Digital Rights Ireland*.

La risposta della Corte, come si vedrà, non lascia spazio a equivoci. Il margine di manovra che la direttiva riconosce agli Stati membri, integrando una deroga al regime ordinario di tutela della riservatezza, deve infatti essere interpretato in modo restrittivo. Quella in cui la Corte si produce è così un'interpretazione della direttiva 2002/58/CE illuminata non solo dalle "stelle comete" di matrice costituzionale in materia di protezione della privacy digitale, vale a dire gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, che tutelano, rispettivamente, riservatezza e dati personali, ma anche, e forse soprattutto, dalla giurisprudenza, anch'essa di tono costituzionale, della stessa Corte di giustizia, a cominciare proprio da *Digital Rights Ireland*[6].

E, infatti, sebbene lo spazio di azione della Corte di giustizia sia delimitato formalmente dall'interpretazione della direttiva 2002/58/CE, sotto un profilo sostanziale, come bene è stato evidenziato[7], la decisione integra un vero e proprio scrutinio delle legislazioni domestiche da una prospettiva dei diritti fondamentali, in particolare in base agli artt. 7 e 8 della Carta. E la stessa giurisprudenza della Corte di giustizia, con la sentenza *Digital Rights Ireland,* diviene a questo riguardo un parametro di giudizio, ancorché la Corte si premuri di adottare un approccio assai prudente quanto alla sua citazione. Del resto, se si legge questa pronuncia in una chiave meramente politica, l'interrogativo centrale che emerge è se una simile intromissione con il diritto alla privacy e alla protezione dei dati degli individui sia ancora compatibile con il diritto europeo dopo la pronuncia che ha annullato la direttiva sulla *data retention* o non configuri piuttosto un'elusione di quest'ultima decisione, fenomeno che sarebbe agevolato dalla diffusione di normative nazionali[8] che sono parse talora trascurare il giudizio della Corte in *Digital Rights Ireland*[9].

Certo è che la Corte di giustizia, nel fornire un'interpretazione della portata dalla direttiva 2002/58/CE, e in particolare delle deroghe ivi previste al diritto alla riservatezza, sembra essersi esercitata ancora una volta in quell'opera di "rilettura" per

---

[6] È interessante osservare come nella sentenza in oggetto la Corte di giustizia sia tornata a sposare una concezione unitaria degli artt. 7 e 8 della Carta, senza esaminare separatamente i profili inerenti a ciascuno dei diritti interessati, adottando una prospettiva diametralmente opposta, invece, a quella fatta propria, per la prima volta, nella sentenza *Digital Rights Ireland.* Su questo punto sia consentito rinviare a O. Pollicino, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale,* in *Federalismi.it,* 2014, 3, spec. 8.

[7] Così L. WOODS, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber),* in eulawanalysis.blogspot.com, 21 dicembre 2016.

[8] Con riguardo allo scenario britannico e all'applicazione, anche a seguito dell'annullamento della direttiva sulla *data retention*, del Data Protection and Investigatory Powers Act 2014, si v. Independent Reviewer of Terrorism Legislation, *CJEU judgment in Watson,* in www.terrorismlegislationreviewer.independent.gov.uk 21 dicembre 2016.

[9] La circostanza viene sottolineata per esempio, da P. SCHAAR, *New ECJ ruling on data retention: preservation of civil rights even in difficult times!,* in www.eaid-berlin.de, 22 dicembre 2016.

così dire "costituzionalmente orientata", rispetto all'entrata in vigore degli artt. 7 e 8 delle Carta, di cui già si rinveniva traccia nella sentenza *Digital Rights Ireland* e nelle successive pronunce *Google Spain* e *Schrems*[10]. Nulla di nuovo sul piano generale della teoria delle fonti, ma un'interessante dinamica nel processo di ridefinizione di un perimetro "costituzionalmente orientato" o quantomeno *human rights oriented* di disposizioni già in vigore quando la transizione da un'Europa dei mercati a un'Europa dei diritti non si era ancora del tutto completata. Ecco, infatti, prospettarsi alla Corte l'esigenza di rivisitare e precisare l'interpretazione della direttiva del 2002 in modo da renderla compatibile con il contenuto della Carta e della stessa giurisprudenza che ne aveva già fatta applicazione.

2. Uno scenario complesso.

Al centro del rinvio pregiudiziale si colloca l'art. 15 della direttiva 2002/58/CE, adottata in seguito all'entrata in vigore della direttiva 95/46/CE con il precipuo obiettivo di adeguarne l'impianto rispetto all'ambito delle comunicazioni elettroniche. Tale disposizione consente agli Stati membri di derogare al principio di riservatezza per adottare misure necessarie, opportune e proporzionate, in una società democratica, per la salvaguardia di alcuni interessi fra cui la sicurezza dello Stato.

Si tratta di una disposizione che presenta uno stretto collegamento con la direttiva Frattini, la quale era stata adottata, nel 2006, anche per uniformare l'atteggiamento degli Stati membri nel derogare al diritto alla privacy dei cittadini sulla base dell'art. 15. Evidente, infatti, era la preoccupazione che, in carenza di indicazioni univoche, ciascun ordinamento potesse modellare in modo assai differente l'ambito di interferenza legittimato dalla norma ora richiamata.

Due in particolare sono i quesiti che, nell'ambito delle due cause riunite, sono state sottoposti all'attenzione della Corte.

In primo luogo, veniva richiesto alla Corte di giustizia di chiarire se tale disposizione, letta alla luce della Carta, impedisse agli Stati membri di prevedere misure di conservazione generalizzata e indifferenziata dei dati di traffico e dei dati relativi all'ubicazione di abbonati e utenti di servizi di comunicazione elettronica.

In uno dei due procedimenti principali, infatti, era controversa la legittimità di un'ingiunzione adottata dall'autorità svedese delle comunicazioni sulla base della disciplina nazionale, con cui era stato ordinato a Tele2 di provvedere alla conservazione dei dati relativi alle comunicazioni elettroniche.

In secondo luogo, si domandava in via accessoria alla Corte se il medesimo art. 15 impedisse agli Stati membri di prevedere un accesso ai dati personali da parte delle autorità nazionali competenti senza limitare tale accesso alle finalità di lotta alla

[10] Sia consentito segnalare le riflessioni già articolate, in proposito, da O. POLLICINO - M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, 73 ss.

criminalità e senza sottoporlo a un previo controllo da parte dell'autorità giudiziaria o amministrativa. Nel secondo procedimento in via principale, infatti, era contestato il potere del Ministero dell'Interno britannico di imporre ai fornitori di servizi di comunicazione elettronica la conservazione dei dati per un periodo massimo di dodici mesi senza alcun preventivo scrutinio delle autorità competenti.

Sullo sfondo di entrambe le questioni sollevate in via pregiudiziale si coglie un diffuso atteggiamento di incertezza sulle effettive implicazioni della decisione *Digital Rights Ireland* e del conseguente annullamento della direttiva sulla *data retention* rispetto a misure formalmente estranee all'ambito della direttiva e del suo recepimento ma sostanzialmente partecipi della medesima *ratio* che era sottesa alla direttiva Frattini.

3. La prima questione pregiudiziale.

Volendo tradurre in forma semplificata il primo quesito pregiudiziale, si può affermare che alla Corte di giustizia è stato richiesto se una norma come l'art. 15 della direttiva 2002/58/CE esaurisca in modo puntuale il potere (legittimo) delle autorità nazionali di interferire con il diritto alla riservatezza.

La Corte risolve affermativamente una questione preliminare, logicamente precedente al merito del quesito, osservando come le misure legislative adottate dagli Stati membri ai sensi dell'art. 15 rientrano senz'altro nell'ambito di applicazione della direttiva, in quanto hanno ad oggetto un trattamento di dati personali da parte dei fornitori di servizi di comunicazione elettronica.

Non si trattava, invero, di una questione dalla soluzione cristallina o scontata. Infatti, da un lato, l'art. 1, par. 3, della direttiva esclude dal proprio ambito di applicazione le materie della sicurezza pubblica, della difesa e dell'ordine pubblico; dall'altro, l'art. 15 autorizza gli Stati membri all'adozione di misure che limitano la privacy, riferendosi però alle attività proprie degli Stati o delle autorità statali, estranee a settori di attività dei singoli[11]. Nonostante tale disposizione si collochi nell'ambito di un atto che disciplina i servizi di comunicazione elettronica e l'attività dei relativi fornitori, secondo la Corte di giustizia l'unica lettura che preserva un effetto utile all'art. 15 è quella che riconosce che le misure legislative adottate dagli Stati membri rientrano nell'ambito di applicazione della direttiva[12].

---

[11] Sul punto più dettagliatamente anche l'analisi di L. WOODS, *op. cit.*

[12] Va peraltro dato conto, come nota correttamente ancora L. WOODS, *ibidem*, che uno degli argomenti maggiormente dibattuti nell'ambito delle cause concerneva il fondamento della distinzione tra la conservazione di dati effettuata dal fornitore di servizi di comunicazione elettronica e l'accesso ai dati, esclusiva delle autorità di polizia e dei servizi di sicurezza. Questa distinzione, se accolta dalla Corte, avrebbe verosimilmente indotto a considerare soltanto l'attività di conservazione dei fornitori di servizi rientrante nell'ambito di applicazione della direttiva. Tuttavia, la Corte non ha dato credito a questa ricostruzione, optando per una concezione unitaria che considera i due momenti della "conservazione" e dell'"accesso" come espressione di un atto invero complessivamente unitario.

Venendo al merito, la Corte rileva che la norma suddetta costituisce un'eccezione rispetto al divieto di memorizzare dati di traffico senza il consenso degli utenti da parte di qualsiasi soggetto.

Da quanto precede deriva che, consentendo agli Stati membri di derogare al principio che esige la riservatezza delle comunicazioni e dei dati di traffico, l'art. 15 deve formare oggetto di un'interpretazione restrittiva[13]. In quest'ottica, la Corte osserva come le misure adottate ai sensi di tale disposizione devono avere come obiettivo "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". I giudici chiariscono che questa elencazione riveste carattere esaustivo, come si evince dallo stesso tenore letterale della disposizione richiamata. Ne consegue che gli Stati membri non possono adottare misure che interferiscano con la riservatezza degli individui per perseguire finalità diverse da quelle espressamente menzionate dall'art. 15.

Il secondo passaggio cruciale, a seguire, vede la Corte enfatizzare il disposto dell'art. 15, par. 1, laddove la norma afferma l'esigenza di conformare le misure legislative in parola ai principi generali del diritto dell'Unione europea, tra cui i diritti fondamentali. Come a voler rafforzare, quand'anche fosse necessario, l'esigenza di una interpretazione orientata alla tutela dei diritti e dunque, a maggior ragione, restrittiva della potestà di limitare la riservatezza dei dati personali.

A questo punto, la sentenza prende in esame i criteri che le possibili interferenze con i diritti fondamentali tutelati dalla Carta devono rispettare.

La Corte ricorda, anzitutto, che l'art. 52 della Carta riconosce che ogni limitazione all'esercizio dei diritti e delle libertà ivi contemplate deve essere prevista dalla legge e rispettare il loro contenuto essenziale. Le restrizioni necessarie ed effettivamente rispondenti a obiettivi di interesse generale o alla tutela dei diritti altrui, invece, possono essere giustificate nel rispetto del principio di proporzionalità.

La normativa nazionale svedese rispetta questi parametri? La Corte non manca di condurre uno scrutinio accurato.

Dapprima, i giudici notano come la disciplina di cui è controversa la compatibilità con il diritto dell'Unione, legittimando una conservazione generalizzata e indifferenziata, peraltro in maniera continua e sistematica, sia dei dati relativi al traffico sia dei dati relativi all'ubicazione di abbonati e iscritti in rapporto a tutti i mezzi di comunicazione elettronica, rievochi le misure previste dalla direttiva 2006/24/CE. Ecco, dunque, il "tentativo di elusione" che la Corte si ritrova a scongiurare.

In particolare, alla luce dell'ingente quantità e dell'eterogeneità dei dati che devono essere conservati dai fornitori di servizi di comunicazione elettronica, la normativa realizza un'ingerenza nel diritto alla privacy di vasta portata, che la Corte

[13] Di tale criterio era espressione, del resto, il considerando 30 della direttiva 2002/58/CE, a mente del quale "I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari".

giudica particolarmente grave. E ciò in ragione di alcune circostanze peculiari: per esempio, l'idoneità dei dati, per la loro tipologia, a tracciare, se considerati nel loro insieme, un profilo molto preciso della vita privata degli interessati, anche in relazione ad aspetti "sensibili"; ma, soprattutto, la carenza di una notifica agli interessati, idonea a ingenerare la percezione di una sorveglianza costante, che ridonda un'interferenza non solo rispetto al diritto alla riservatezza e alla protezione dei dati personali ma anche, in funzione dello scopo dei servizi di comunicazione elettronica, con riguardo alla libertà di espressione[14].

La Corte trae da queste premesse la conclusione per cui un'incisione così rilevante dei diritti fondamentali degli utenti può trovare ragion d'essere soltanto in un obiettivo altrettanto importante, e segnatamente nella lotta alla criminalità grave.

Ma ciò non significa che in presenza di tale obiettivo decadano le altre tutele: secondo la Corte, anche se questo fosse l'obiettivo sotteso alle misure legislative adottate ai sensi dell'art. 15, si dovrebbe egualmente ritenere non necessaria la previsione di una conservazione generalizzata e indifferenziata dei dati di traffico[15].

Questa osservazione si coniuga a due importanti rilievi svolti dalla Corte di giustizia.

Da un lato, in queste circostanze, le misure che l'art. 15 autorizza a titolo di eccezione finirebbero per costituire la regola, rovesciando l'ordine di priorità indicato dal legislatore europeo.

Dall'altro lato, la Corte osserva che le misure previste dalla normativa nazionale non lasciano spazio alcuna differenziazione, limitazione o eccezione in relazione all'obiettivo perseguito, riguardando in modo invasivo tutti gli individui destinati ad avvalersi di servizi di comunicazione elettronica, a prescindere dalla mera idoneità degli stessi a ingenerare situazioni munite di rilevanza penale.

Dunque, nessuna correlazione è richiesta tra i dati di cui si richiede la conservazione e l'esistenza di una minaccia per la sicurezza pubblica. Tantomeno nessuna limitazione viene indicata, secondo una lacuna già propria della direttiva sulla *data retention*, in relazione al periodo di tempo, all'ambito geografico o alla cerchia di individui cui sarebbe indistintamente applicabile la conservazione dei dati di traffico.

---

[14] In questa direzione la pronuncia della Corte di giustizia sembra riallacciarsi al doppio precedente costituito dalle sentenze del 24 novembre 2011, C-70/2010, *Scarlet c. Sabam* e del 16 febbraio 2012, C-360/10, *Sabam c. Netlog*, che avevano originato dall'adozione, da parte delle autorità belghe, di un ordine di filtraggio dei contenuti in capo ai fornitori dei servizi Internet al fine di prevenire violazioni del diritto d'autore su Internet. Nelle cause in esame, la Corte di giustizia si è soffermata, oltre che sul tema della compatibilità di un simile obbligo *de facto* di sorveglianza con la disciplina dei prestatori di servizi Internet e sulla presunta violazione delle norme a tutela dei dati personali, anche sugli effetti detrimentali per la libertà di manifestazione del pensiero, in ragione del controllo che gli intermediari sarebbero in grado di esercitare sul contenuto dei dati oggetto di raccolta.

[15] A tale riguardo, interessanti i rilievi di L. WOODS, *op cit.*, che nota come la Corte restringa alla sola lotta contro la criminalità grave il novero di fattispecie che giustificano un'intrusione grave ai diritti alla privacy, alla protezione dei dati e alla libertà di espressione, laddove il disposto dell'art. 15, invece, alluda in termini più generali e ampi alla prevenzione di attività criminali.

È abbastanza perché la Corte dichiari che una simile normativa travalica i limiti dello stretto necessario e non può trovare giustificazione nell'art. 15.

Al contrario, questa norma può ben fondare l'applicazione di misure volte a una conservazione mirata di dati di traffico e dati relativi all'ubicazione, per finalità di lotta alla criminalità, qualora la conservazione sia limitata entro necessità in relazione a categorie di dati, mezzi di comunicazione e individui interessati, nonché durata della conservazione.

Così la Corte fornisce un *vademecum* sulle condizioni che legittimano l'applicazione di queste misure.

In primo luogo, occorre che la normativa nazionale definisca, mediante regole chiare e precise, la portata e l'applicazione delle misure di conservazione, fissandone i requisiti anche al fine di permettere agli interessati di averne contezza e di poter proteggere i propri dati.

In secondo luogo, rispetto alle condizioni sostanziali che la normativa nazionale deve soddisfare, la Corte afferma che, per quanto esse possano variare in funzione delle misure adottate, la conservazione deve rispondere a criteri oggettivi, in base a un rapporto tra dati da conservare e obiettivo perseguito.

Da ultimo, la Corte specifica che analoghe cautele devono trovare riscontro in merito alla determinazione dei destinatari potenziali delle misure e delle situazioni in cui esse ricevono applicazione: in base a criteri oggettivi, cioè, che circoscrivano le situazioni idonee a rivelare la connessione con atti di criminalità grave o con un rischio grave per la sicurezza pubblica[16].

4. La seconda questione pregiudiziale.

Alla seconda questione sollevata dal giudice britannico la Corte dedica le sue residuali attenzioni, anche alla luce della soluzione offerta al primo quesito.

La Corte si ricollega, anzitutto, quanto agli obiettivi idonei a giustificare un'interferenza con la riservatezza delle comunicazioni elettroniche, a quanto argomentato in merito al carattere di tassatività degli obiettivi indicati dall'art. 15. Nessun altro obiettivo può giustificare le misure di conservazione, e nella fattispecie, data la gravità dell'interferenza, solo la lotta alla criminalità grave può rilevare.

In seconda battuta, la Corte si sofferma sul principio di proporzionalità, argomentando come l'accesso ai dati garantito alle autorità nazionali competenti deve avvenire entro i limiti dello stretto necessario e in presenza di norme chiare e precise che ne identifichino i presupposti (i.e. circostanze e condizioni).

In tale senso, la Corte evoca l'esigenza che la normativa nazionale si fondi su criteri oggettivi, per esempio circoscrivendo l'accesso ai dati fondato sulla lotta alla

[16] Particolarmente rilevante e al contempo delicato appare il passaggio in cui la Corte di giustizia, al punto 111, annovera, tra le condizioni che fondano l'esistenza di un collegamento oggettivo, anche l'appartenenza a una determinata area geografica in cui la commissione di attività criminali potrebbe presentare un elevato grado di rischio.

criminalità entro una cerchia di persone sospettate di progettare, commettere o aver commesso una violazione grave (o di esservi, ad altro titolo, implicate).

Inoltre, si esplicita l'ulteriore requisito per cui l'accesso delle autorità nazionali ai dati conservati dovrebbe essere subordinato, eccetto il ricorrere di casi d'urgenza, a un controllo preventivo effettuato da un organo giurisdizionale o amministrativo sulla base di una richiesta motivata dall'autorità procedente.

Parimenti, enfasi viene data alla necessità che le autorità informino gli interessati dell'adozione delle misure, a partire dal momento in cui la comunicazione non è suscettibile di compromettere le indagini.

Da ultimo, la conservazione da parte dei fornitori di servizi di comunicazione elettronica richiede l'utilizzo di misure tecniche e organizzative appropriate che consentano di prevenire abusi e alterazioni all'integrità e alla riservatezza dei dati.

Il tutto, ovviamente, entro la cornice dell'ordinamento nazionale in cui un'autorità indipendente ai sensi dell'art. 8, par. 3, della Carta dovrà esercitare i propri poteri di controllo, vigilando sul livello di protezione dei diritti delle persone fisiche.

In conclusione, per la Corte, ogni misura volta alla conservazione dei dati di traffico ordinata dalle autorità nazionali può trovare giustificazione nel diritto dell'Unione e non configura una violazione dei diritti fondamentali di cui gli artt. 7, 8 e 11 della Carta, laddove rispetti le condizioni ora descritte che consentono di limitarne entro i limiti di stretta necessità l'applicazione.

5. Conclusioni.

Occorre, in conclusione, chiedersi se la Corte di giustizia abbia offerto, con la sentenza in commento, un'interpretazione radicalmente innovativa ovvero se, come sembra, non si tratti in realtà di una sentenza che costituisce il naturale (e forse scontato) completamento dell'opera avviata dalla Corte con la demolizione della direttiva 2006/24/CE, che sgombra il campo dalle residue incertezze legate a normative nazionali che non derivassero dalla trasposizione di quest'ultima. E che, tuttavia, regolando una conservazione di dati che si risolve in un trattamento di dati personali, ritrovano un collegamento con il diritto dell'Unione europea. E se questo è il terreno di gioco, è evidente la partita cui la Corte di giustizia sta giocando da ormai quasi tre anni a questa parte: quella della rilettura dello stesso diritto dell'Unione europea e delle normative di recepimento illuminata dalla Carta dei diritti fondamentali, vero baluardo e ago della bilancia della giurisprudenza in epoca digitale della Corte. Al fine di apprezzare fino in fondo l'affondo della Corte di giustizia, la sentenza sembra infatti configurare un definitivo "scacco matto" alla prevalenza delle ragioni di sicurezza pubblica su quelle di protezione della privacy digitale. Un risultato che i giudici ottengono in tre mosse. La prima si è concretizzata nella sentenza del 2014 in cui la Corte aveva annullato una direttiva che sacrificava la tutela dei dati personali sull'altare della lotta al terrorismo internazionale, frutto di un periodo di legislazione emergenziale. La seconda mossa risale all'autunno del 2015, con la sentenza *Schrems*. In questo caso la Corte si era concentrata sui rapporti tra Unione europea e ordinamento

statunitense, pretendendo, una volta elevata, con la prima mossa, l'asticella dello standard europeo di tutela della privacy digitale, che una protezione equivalente fosse garantita dagli Stati Uniti in caso di trasferimento, verso quest'ultimo paese, di dati appartenenti a cittadini europei. Infine, la terza mossa, quella che qui si è commentata: l'obbligo di "prendere sul serio" la tutela della privacy digitale incombe non solo sulle istituzioni europee (*Digital Rights Ireland*) e statunitensi (*Schrems*), ma vincola anche i legislatori degli Stati membri. Scacco matto, dunque, alla proiezione normativa, sempre crescente, e per certi versi comprensibile, dell'ossessione connessa alle esigenze di tutela della sicurezza pubblica, a tutto discapito della protezione della privacy degli utenti.