Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali

di Flavio Guella

Title: Data retention and the circulation of levels of rights' protection in Europe: from constitutional adjudication concerning EU rules to ECJ judgment relevant for national regulation

Keywords: Data retention; Privacy; Dialogue among courts.

1. – Con sentenza del 21 dicembre 2016 la Corte di Giustizia ha aggiunto un ulteriore passaggio nella lunga vicenda che ha avuto ad oggetto la regolazione della conservazione dei dati relativi a comunicazioni telefoniche ed informatiche (c.d. *data retention*). Con questa pronuncia la Corte chiude il cerchio attorno al quale giudici e legislatori europei si sono mossi negli ultimi quindici anni alla ricerca del giusto equilibrio tra riservatezza ed esigenze di pubblica sicurezza. La Grande Sezione, decidendo un rinvio pregiudiziale sulle cause riunite C-203/15 e C-698/15, ha infatti chiarito in che misura il diritto europeo osti a legislazioni nazionali – del tipo di quella britannica e svedese che hanno dato origine alla pronuncia – le quali permettano da un lato la conservazione generalizzata dei dati telefonici per un certo periodo di tempo e, d'altro lato, ammettano l'accesso a tali dati senza adeguate garanzie. Pronunciando in questi termini la Corte di Giustizia di fatto porta ad implementazione un nuovo standard di tutela del diritto alla riservatezza, il cui livello è emerso da un lungo dialogo normativo e giurisprudenziale tra istituzioni europee e Stati membri (sulla vicenda *data retention*, tra i numerosi commenti, si rinvia per un primo inquadramento generale a F. Bestagno, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali*, in *Diritto UE*, 2015, 25 ss. e O. Pollicino, M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel "*reasoning*" dei giudici di Lussemburgo*, in *Dir. informaz. informatica*, 2015, 741 ss.).

La Tele2 Sverige, impresa svedese fornitrice di servizi di comunicazione elettronica, a seguito della precedente invalidazione per effetto della sentenza *Digital RightsIreland* (8 aprile 2014, C-293/12 e C-594/12, EU:C:2014:238) della direttiva 2006/24/CE, che imponeva la conservazione dei dati di traffico per un periodo di tempo minimo, dismetteva la conservazione generalizzata dei dati relativi alle comunicazioni elettroniche, pur se imposta direttamente dalla legge nazionale (*lagen 2003:389 omelektroniskkommunikation*); legge emanata nello spazio di discrezionalità lasciato dalla precedente direttiva 2002/58/CE, ma di contenuto analogo a quello della direttiva del 2006 di cui era stata dichiarata l'invalidità. Analogamente, alcuni cittadini inglesi ricorrevano in giudizio avverso la conservazione dei dati telefonici sulla base del *Data Retention and InvestigatoryPowersAct 2014*, che contiene anch'esso una disciplina conforme alla direttiva del 2006, con la peculiarità – rispetto alla precedente ipotesi – che in questo ordinamento è il Ministro dell'Interno ad adottare, in assenza di qualsivoglia autorizzazione preventiva di un giudice o di un'autorità

amministrativa indipendente, un regime generale di conservazione dei dati (richiedendo l'accessibilità contestualmente alla conservazione).

In esito al giudizio la Grande Sezione del 21 dicembre 2016 ha statuito che l'art. 15, par. 1, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (come modificata dalla direttiva 2009/136/CE), letto alla luce degli articoli 7, 8, 11 e 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che esso osta sia ad una normativa nazionale (come tendenzialmente quella svedese) 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 di qualunque mezzo di comunicazione elettronica, sia ad una normativa nazionale (come tendenzialmente quella britannica, oltre che per specifici profili quella svedese), la quale disciplini la protezione dei medesimi dati senza limitare l'accesso delle autorità nazionali competenti 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 siano conservati nel territorio dell'Unione.

2. – La vicenda è rilevante non solo per la centralità del tema della sicurezza pubblica in connessione con la riservatezza, di grande attualità in un'epoca in cui il ruolo pervasivo delle comunicazioni elettroniche nella vita di ciascuno si confronta con una contestuale difficoltà nel controllo di fenomeni criminali gravi, quali i traffici e l'associazionismo criminale di dimensione transfrontaliera, nonché il terrorismo. Un profilo di rilevanza ulteriore è infatti legato ai meccanismi istituzionali che hanno permesso la fissazione di uno standard comune di tutela della riservatezza, facendo "circolare" negli ordinamenti europei un certo livello di tutela dei diritti fondamentali mediante un costante dialogo tra le corti ed i legislatori.

La questione del *data retention* è paradigmatica di come questo modello dialogico spesso operi, negli anni, fino a costruire un'integrazione europea dei diritti fondamentali che agisce – in assenza di un chiaro disegno preventivo – su singole questioni settoriali (cfr. tra i molti contributi generali sul tema G. de Vergottini, *Oltre il dialogo tra le Corti. Giudici, diritto straniero, comparazione*, Bologna, 2010). Nel caso specifico la questione di fondo cui rispondere in modo uniforme è costituita dal se sia possibile conservare in via generalizzata i dati esterni (c.d. metadati) delle comunicazioni; dati utili per perseguire i crimini, ma che sono in ipotesi raccolti agendo al di fuori di un quadro di indagini in cui è l'autorità inquirente a chiedere *ex post* di mettere sotto controllo determinate utenze, operando quindi *ex ante* una conservazione generalizzata dei dati stessi, cui attingere poi all'occorrenza in sede di indagini. Si trattava pertanto di verificare se e quanto la strumentalità alla sicurezza pubblica della ritenzione dei dati da parte delle compagnie telefoniche per un tempo ulteriore rispetto a quanto strettamente necessario alla fatturazione dei servizi prevalga sulle esigenze della riservatezza.

L'Unione europea era intervenuta nella materia dapprima con la direttiva 2002/58/CE fissando il principio secondo cui i dati relativi al traffico e i dati relativi all'ubicazione devono essere cancellati o resi anonimi qualora non siano più necessari per la trasmissione di una comunicazione. L'art. 15, par. 1, della medesima direttiva introduceva però una deroga a tale principio autorizzando gli Stati membri, ove ciò sia giustificato da uno dei motivi enunciati da tale disposizione (tra cui la sicurezza pubblica e il contrasto alla criminalità), a limitare l'obbligo di cancellazione o di anonimizzazione.

Questa direttiva era intervenuta in un contesto normativo in cui i legislatori nazionali avevano talvolta già disciplinato la materia, come ad esempio nel caso italiano dove il c.d. Codice della privacy aveva fissato in 30 mesi il periodo di conservazione generalizzata dei dati (cfr. l'art. 132 del d.lgs 30 giugno 2003, n. 196 nella sua prima formulazione). Tali opzioni, in sede di prima applicazione della direttiva del 2002, non sembravano per nulla precluse alle autorità nazionali, che potevano conservare discipline di questo genere accedendo ad un'interpretazione della direttiva che riconosceva ampia autonomia procedurale e un esteso margine di apprezzamento agli ordinamenti nazionali, omettendo di dettare più

precise prescrizioni utili per un controllo di proporzionalità (anche se il legislatore italiano stesso, nell'intento di trovare un equilibrio migliore per la tutela della riservatezza alla luce dello sviluppo tecnologico, ha ridotto il termine di conservazione a 24 mesi per i dati telefonici e a 12 mesi per i dati telematici; sulle evoluzioni della disciplina italiana precedenti alla sentenza *Digital Rights* del 2014 cfr. A. Stracuzzi, Data retention*: il faticoso percorso dell'art. 132 Codice Privacy nella disciplina della conservazione dei dati di traffico*, in *Dir. informaz. informatica*, 2008, 585 ss.; S. Aterno, A. Cisterna, *Il legislatore interviene ancora sul* data retention, *ma non è finita - Decreto legislativo 30 maggio 2008, 109*, in *Dir. pen. e processo*, 2009, 282 ss.; A. Rodolfi, *Il regime normativo della* data retention *nell'ordinamento italiano. Stato attuale e problematiche concrete*, in *Ciberspazio e diritto*, 2010, 147 ss.).

3. – In partenza si registra quindi l'assenza di uno standard comune di tutela per la riservatezza in ambito di dati esterni delle comunicazioni elettroniche e l'assenza iniziale – qualora entrino in gioco questioni di pubblica sicurezza – di un'intenzione forte dell'Unione europea di armonizzare la materia, sia verso l'alto (dettando termini massimi di conservazione, a tutela della riservatezza) che verso il basso (dettando termini minimi di conservazione, a tutela della sicurezza comune).

Quest'assenza di uno standard comune non trovava parametri precisi nemmeno nella giurisprudenza della Corte di Strasburgo, che nell'applicare l'art. 8 CEDU sul rispetto della vita privata e familiare a vicende strutturalmente analoghe – fondate sulla violazione della privacy connessa a conservazione e accesso a dati la cui raccolta può essere operata in massa – hanno mantenuto la protezione su livelli necessariamente elastici, rinviando di volta in volta al controllo di proporzionalità.

Così la CEDU non impone un divieto assoluto, pur riconoscendo – sulla base dell'art. 8 – che l'accesso delle autorità nazionali competenti ai dati costituisce un'ingerenza "supplementare" (cfr. Corte EDU, *Leander c. Svezia*, del 26 marzo 1987, serie A n. 116, § 48; *Rotaru c. Romania* [GC], n. 28341/95, § 46, CEDU 2000-V; *Weber e Saravia c. Germania* (dec.), n. 54934/00, § 79, CEDU 2006-XI), e pertanto si devono introdurre regole chiare e precise che disciplinino la portata e l'applicazione della misura invasiva, anche imponendo requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie contro il rischio di abusi, eccessi ed usi illeciti dei dati (cfr. Corte EDU, *Liberty e altri c. Regno Unito*, n. 58243/00, §§ 62 e 63, del 1° luglio 2008; *Rotaru c. Romania*, [GC], n. 28341/95, §§ da 57 a 59). Ciò, in particolare, con un'attenzione più elevata quando i dati personali sono soggetti a trattamento "automatico" (sentenze Corte EDU, *S e Marper c. Regno Unito*, [GC], nn. 30562/04 e 30566/04, § 102, CEDU 2008-V, § 103; *M.K. c. Francia*, n. 19522/09, § 35, del 18 aprile 2013), e quindi nelle ipotesi di raccolta generalizzata dei metadati di traffico telefonico, senza però che la raccolta generalizzata sia necessariamente vietata.

L'Unione europea è quindi libera di porre regole che consentano di operare la conservazione e l'accesso a dati sensibili, eventualmente anche con modalità automatizzate e "di massa", ma dettando quelle garanzie (almeno) procedurali che la CEDU esige come standard minimo di tutela della privacy (standard minimo che vale anche per il diritto UE, secondo l'art. 52, par. 3, prima frase della Carta di Nizza). D'altro lato, l'Unione europea è anche libera di porre uno standard più alto di tutela, restringendo in modo più drastico il trattamento *ex ante* dei dati, da conservare cioè a fini non attuali di tutela della pubblica sicurezza (come disposto dalla seconda frase del citato paragrafo della Carta di Nizza)

4. – A fronte di questo contesto, in prima battuta l'Unione europea ha voluto armonizzare uno standard di tutela della pubblica sicurezza, operando essa stessa un bilanciamento di massima con le esigenze di riservatezza. Se la Direttiva del 2002 continuava infatti a riconoscere un'ampia autonomia procedurale agli Stati e una regola generale di non conservazione fuori delle ipotesi di esigenze di contrasto alla criminalità, proprio per tali fini una nuova direttiva nel 2006 interveniva a ridurre quel margine di discrezionalità

imponendo – in modo uniforme – un termine minimo e massimo di conservazione, nello spazio del quale l'autonomia procedurale degli Stati membri risultava quindi compressa.

La direttiva 2006/24/EC – approvata dopo gli attentati di Londra e di Madrid – ha così imposto che i dati esterni delle telecomunicazioni degli utenti non fossero cancellati dai database dei fornitori del servizio per un minimo di sei mesi, mentre il termine massimi di conservazione veniva fissato a ventiquattro mesi. A tale termine massimo si è conformato il legislatore italiano (come tutt'ora disposto dall'art. 132 del Codice della privacy) e, peraltro, la maggior parte degli ordinamenti europei ha scelto di fissare il termine di conservazione nella fascia alta, tra i dodici e i ventiquattro mesi (mentre in alcuni ordinamenti la direttiva è rimasta inapplicata per ciò che riguarda il termine massimo, ove il legislatore nazionale abbia optato per periodi più lunghi come i tre anni di Irlanda, Lituania e Romania, i cinque anni della Grecia, e i dieci anni della Polonia).

Non in tutti gli Stati membri, tuttavia, il recepimento del termine minimo è stato accettato e non sono mancate le ipotesi in cui istituzioni degli Stati membri ne hanno rilevato il contrasto con il livello nazionale di tutela costituzionale della riservatezza. Particolarmente importante è stato il caso tedesco, in cui la Corte costituzionale con sentenza del 2 marzo 2010, n. 11 (1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08) ha dichiarato l'illegittimità delle norme che prevedevano l'obbligo di conservazione dei dati delle telecomunicazioni per un periodo di sei mesi, al di fuori di qualunque richiesta emersa in sede di indagini preliminari. Il contrasto con la Costituzione nazionale porta quindi all'annullamento della disciplina pur se attuativa della direttiva UE, con una soluzione che è poi stata seguita anche dalla Corte costituzionale della Bulgaria con sentenza 11 dicembre 2008, n. 13627, dalla *Curtea Constituţională* rumena con sentenza del 8 ottobre 2009, dalla Corte Costituzionale della Repubblica Ceca con sentenza del 31 marzo 2011, e dalla Corte Suprema di Cipro con sentenza 1 febbraio 2011 (cfr. A. Di Martino, *Il* Bundesverfassungsgericht *dichiara l'incostituzionalità della* data retention *e torna sul rapporto tra libertà e sicurezza*, in *Giur. cost.*, 2010, 4059 ss.; E. Falletti, *Germania: normativa tedesca sull'archiviazione di dati personali e normativa comunitaria*, in *Foro it.*, fasc. 1, pt. 4, 2011, 60 ss. e R. Flor, *Data retention e limiti al potere coercitivo dello Stato in materia penale: le sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională, in *Cass. penale*, 2011, 1952 ss.).

Le pronunce di incostituzionalità citate sono particolarmente significative perché si pongono in diretto dialogo con la Corte di Giustizia, che in precedenza aveva giudicato non illegittimo il bilanciamento degli interessi raggiunto dalla direttiva del 2006. Le corti costituzionali nazionali chiedono quindi in sostanza alle istituzioni europee di rivedere la posizione assunta con sentenza del 25 febbraio 2009 (C-301/06, *Irlanda c. Parlamento europeo e Consiglio*, su cui cfr. F. Fabbrini, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quad. cost.*, 2009, 419 ss.), la quale aveva fatto salva la conservazione generalizzata dei dati richiesta dal diritto comunitario in quanto rinverrebbe un'adeguata base giuridica nell'art. 95 TCE.

La giurisprudenza costituzionale ceca e tedesca citata si pone così in continuità con le posizioni già assunte in precedenza in tema di mandato di arresto europeo (*BVerfGE*, 113, 273, *Darkanzali*, del 18 luglio 2005), intervenendo sui provvedimenti di recepimento affermandone nel caso specifico la rilevanza esclusivamente interna, considerati da un lato i margini di apprezzamento lasciati dalla direttiva stessa e dall'altro il quadro normativo costituzionale (mentre più drastica è stata la sentenza rumena – n. 1.258/2009, 8 ottobre 2009 – che prende diretta posizione sulla direttiva). Come logica conseguenza, nelle vicende citate non vi è stato rinvio pregiudiziale sulla materia e si è proceduto all'annullamento diretto delle norme interne restrittive del diritto costituzionale alla riservatezza.

5. – Proprio dialogando con queste posizioni assunte dalla giurisprudenza di alcune corti costituzionali nazionali, e in un nuovo giudizio avente ad oggetto la disciplina irlandese e quella austriaca (dove il giudice sceglie di non bypassare il rinvio pregiudiziale), la Corte di Giustizia muta il proprio precedente che aveva affermato la legittimità della direttiva *data retention*. È la Corte di Giustizia quindi a modificare in positivo lo standard di protezione

della riservatezza accolto nella normativa dell'Unione, agendo sul piano giurisprudenziale nell'ambito di un rinvio pregiudiziale di validità e accogliendo lo standard di giudizio già fatto proprio dalle corti costituzionali citate.

Con sentenza dell'8 aprile 2014 (cause riunite C-293/12 e C-594/12, EU:C:2014:238, *Digital RightsIreland e a.*, su cui tra l'ampia dottrina cfr. L. Trucco, *"*Data retention*": la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it.*, 2014, 1850 ss.; G. Tiberi, *La Corte di giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel "dopo-Lisbona"*, in *Quad. cost.*, 2014, 719 ss.; S. Scagliarini, *La Corte di Giustizia bilancia il diritto alla vita privata e lotta alla criminalità: alcuni "pro" e alcuni "contra"*, in *Dir. informaz. informatica*, 2014, 873 ss.; E. Colombo, *"*Data retention*"e Corte di giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della Direttiva 2006/24/CE*, in *Cass. penale*, 2014, 2705 ss.; C.M. Cascione, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione "*data retention*" della Corte di giustizia e gli echi del "*Datagate*"*, in *Nuova giur. civ. commentata*, pt. 1, 2014, 1044 ss.; M. Nino, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di "*data retention*"*, in *Dir. U.E*, 2014, 803 ss.; E. Rossi, *Il diritto alla "privacy" nel quadro giuridico europeo ed internazionale alla luce delle recenti vicende sulla sorveglianza di massa*, in *Dir. com. scambi internaz.*, 2014, 331 ss.), la Grande Sezione ha dichiarato l'invalidità della direttiva 2006/24/CE per contrasto dell'obbligo dei gestori di servizi di telecomunicazione di conservare tutti i dati connessi alle comunicazioni elettroniche (e, su richiesta, di fornirli alle pubbliche autorità) con gli art. 7, 8 e 11 della Carta dei diritti fondamentali; ciò in quanto la conservazione dei dati di traffico, sebbene non riguardi il contenuto delle comunicazioni, nondimeno interferisce con la libertà di espressione, la riservatezza della vita privata e la protezione dei dati personali. Ciò non per una violazione del contenuto essenziale di tali diritti, ma per una mancanza di proporzionalità nelle misure prescritte.

Il nucleo essenziale del diritto alla riservatezza delle proprie espressioni non pubbliche – identificato nella conservazione del contenuto delle comunicazioni – non è intaccato, così come non è leso nel suo nucleo essenziale il diritto alla tutela dei dati personali, posto che già la direttiva 1995/46/CE (e poi la direttiva 2002/58/CE) garantisce modalità di trattamento comprensive di garanzie procedurali minime. La legittimità dell'interferenza, al di là del contenuto essenziale, deve però fondarsi su misure in concreto ragionevoli e proporzionate.

A tale ultimo riguardo, la sentenza *Digital Rights* del 2014 riscontra nella direttiva un livello inadeguato di protezione, posto che l'obiettivo di interesse generale alla base della limitazione dei diritti (ovvero le esigenze di lotta contro il crimine e il terrorismo, bilanciabili con il diritto alla riservatezza in quanto strumentali al diritto alla sicurezza di cui all'art. 6 della Carta) è perseguito dalla direttiva del 2006 con misure adeguate ma non strettamente necessarie. Le norme denunciate hanno infatti ecceduto i limiti della necessarietà in quanto a parere della Corte di Giustizia – che modifica il proprio precedente orientamento mutuando queste osservazioni dalla giurisprudenza costituzionale nazionale tedesca, ceca e rumena – sono altrettanto idonee procedure di conservazione che evitino però un monitoraggio indiscriminato *ex ante*. La raccolta in massa dei metadati sarebbe in particolare una misura eccessiva in quanto idonea ad ingenerare nello spirito delle persone riguardate la sensazione che la loro vita privata costituisca l'oggetto di una sorveglianza continua, evitabile con procedure maggiormente selettive (per una specifica analisi del test di proporzionalità in questa sentenza cfr. A. Vedaschi, *I programmi di sorveglianza di massa nello Stato di diritto. La "*data retention*" al test di legittimità*, in *Dir. pubbl. comp. eur.*, 2014, 1224 ss., in particolare il par. 5.2, e il par. 4. per l'analisi delle sentenze nazionali).

Posta tale presa di posizione della Corte di Giustizia sulla direttiva del 2006, e viste le argomentazioni che l'hanno fondata, rimane la questione del valore che tali argomentazioni assumono rispetto ai diritti nazionali. La sentenza del 2016 qui annotata richiama a fondamento del percorso interpretativo della diversa direttiva del 2002 numerosi passaggi della sentenza *Digital Rights*, qualificando espressamente l'opportunità argomentativa di tali richiami in una logica "per analogia". Sebbene la Grande Sezione del 2014 non abbia inteso enunciare prescrizioni imperative applicabili alle normative nazionali, la pronuncia *Tele2 Sverige* del 2016 rileva quindi come il ragionamento da svolgere rispetto alla direttiva 2002 –

che continua a fissare i confini dell'autonomia procedurale degli Stati membri in materia – sia strettamente legato all'obiettivo perseguito dalla direttiva invalidata, che condiziona quindi l'interpretazione della residua disciplina europea.

6. – Nella sentenza annotata si conclude quindi quella transizione dal giudizio "indiretto" di alcune corti costituzionali nazionali sulla disciplina dell'Unione al giudizio invece operato dalla Corte di Giustizia – dopo aver recepito il nuovo standard di tutela della riservatezza suggerito dal basso – sugli spazi per le discipline nazionali, in un reflusso dell'armonizzazione del livello di tutela verso gli ordinamenti che in precedenza si erano invece conformati alla direttiva del 2006. Se infatti è vero che non vi può essere un'automatica illegittimità del diritto nazionale derivata dalle sentenze della Corte di Giustizia, nella pronuncia del 2016 la Grande Sezione fornisce le necessarie indicazioni su quali strumenti nazionali siano proporzionati ed adeguati per conformarsi al nuovo standard (cfr. per un primo commento alla sentenza 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 *penalecontemporaneo.it*, 9-1-2017).

Si tratta quindi di un rinvio pregiudiziale di interpretazione attuativo del precedente rinvio pregiudiziale di validità, il quale colpisce l'autonomia procedurale degli Stati membri che la direttiva del 2002 aveva lasciato residuare in materia di pubblica sicurezza, riducendo la discrezionalità alla luce delle argomentazioni della pronuncia *Digital Rights*.

Più in particolare, la sentenza *Tele2 Sverige*conferisce un contenuto operativo più preciso di quanto consolidato in precedenza alla regola per cui – come confermato dai considerando 22 e 26 della direttiva 2002/58/CE – il trattamento e la memorizzazione dei dati relativi al traffico sono autorizzati, ai sensi dell'art. 6 della direttiva stessa, soltanto nella misura e per la durata necessaria per la fatturazione dei servizi, per la commercializzazione di questi ultimi e per la fornitura di servizi a valore aggiunto (cfr. sentenza del 29 gennaio 2008, *Promusicae*, C-275/06, EU:C:2008:54, punti 47 e 48). Tale contenuto operativo più preciso è definito restringendo gli spazi per le eccezioni *ex* art. 15, par. 1, imponendo che tali deroghe assumano appunto portata eccezionale (sui cui ambiti cfr. già sentenza del 22 novembre 2012, *Probst*, C-119/12, EU:C:2012:748, punto 23). Si tratta di un'interpretazione restrittiva per cui non solo l'art. 15, par. 1, prima frase, della direttiva 2002/58/CE stabilisce obiettivi di carattere tassativo, in modo che gli Stati non potranno addurre ragioni atipiche rispetto alla pubblica sicurezza – o alle altre ipotesi codificate dalla direttiva – per restringere ragionevolmente la tutela dei diritti fondamentali garantiti dalla Carta (tra cui ovviamente la riservatezza cfr. sentenze del 20 maggio 2003, *Österreichischer Rundfunk e a.*, C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 68; del 13 maggio 2014, *Google Spain*, C-131/12, EU:C:2014:317, punto 68; 6 ottobre 2015, *Schrems*, C-362/14, EU:C:2015:650, punto 38), ma soprattutto si afferma che è necessario un bilanciamento con tali diritti che segua livelli di tutela e modalità operative proporzionate ora delineate dalla Corte di Giustizia stessa.

La sentenza proprio al fine di definire questa proporzionalità riproduce quindi i ragionamenti della pronuncia *Digital Rights* del 2014, per riempire di contenuto la portata delle eccezioni al principio di non conservazione dei dati contenendole – per come previste dalla direttiva 2002 – entro i limiti del rispetto dei diritti fondamentali. Lo standard di tutela accolto ammette quindi che soltanto la lotta contro la criminalità "grave" è idonea a giustificare una misura di eccezione (cfr. sentenza *Digital Rights*, punto 60), ed quindi non violano il diritto dell'Unione solo quelle norme nazionali che conducono ad una conservazione avente ad oggetto dati relativi ad un periodo di tempo e/o a una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una violazione grave, oppure persone che potrebbero, per altri motivi, contribuire, mediante la conservazione dei loro dati, alla lotta contro la criminalità (cfr. ancora per analogia la sentenza *Digital Rights*, punto 59).

Anche se quindi l'art. 15, par. 1, della direttiva 2002/58, letto alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, par. 1, della Carta, non osta a che uno Stato membro adotti una

normativa la quale consenta, a titolo preventivo, la conservazione "mirata" dei dati relativi al traffico per finalità di lotta contro la criminalità grave, ciò deve avvenire appunto a condizione che la conservazione sia selettiva (e quindi strettamente necessaria) per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata della raccolta.

Il livello di proporzionalità fissato con il precedente del 2014 viene peraltro applicato agli spazi di discrezionalità nazionale non solo riguardanti la conservazione dei dati, ma anche l'accesso da parte delle autorità nazionali competenti. Si afferma quindi che viola il diritto dell'Unione quella normativa nazionale che non limiti tale accesso alle sole finalità di lotta contro la criminalità grave, o che non sottoponga l'accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente (cfr. sentenza *Digital Rights*, punto 62, ma anche Corte EDU, 12 gennaio 2016, *Szabó e Vissy c. Ungheria*, CE:ECHR:2016:0112JUD003713814, §§ 77 e 80), o non esiga che i dati siano conservati nel territorio dell'Unione, o non imponga di comunicare appena possibile all'interessato l'avvenuto accesso (cfr. sentenze del 7 maggio 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, punto 52; 6 ottobre 2015, *Schrems*, C-362/14, EU:C:2015:650, punto 95), o non fondi su elementi oggettivi le circostanze in presenza delle quali l'accesso è ammesso (cfr. Corte EDU, 4 dicembre 2015, *Zakharov c. Russia*, CE:ECHR:2015:1204JUD004714306, § 260).

7. – A fronte di questi contenuti, la sentenza *Tele2 Sverige* assume una specifica rilevanza non perché innovativa dei principi della sentenza *Digital Rights*, ma in quanto con questa pronuncia la Corte di Giustizia completa quel ciclo che – attraverso il dialogo con alcune giurisdizioni costituzionali nazionali – ha portato un certo livello di tutela, prima negato dall'Unione europea stessa, ad essere imposto uniformemente a tutti gli Stati membri.

Se infatti ad una fase di forte autonomia procedurale nel porre eccezioni alla regola della non conservazione dei dati per ragioni di pubblica sicurezza era poi succeduta un'armonizzazione verso il basso con la direttiva *data retention*, che imponeva una conservazione generalizzata ed indifferenziata per almeno sei mesi, in direzione contraria – successivamente – la giurisprudenza nazionale di Germania, Repubblica Ceca e Romania aveva contestato la costituzionalità di tali misure, portando la Grande Sezione del 2014 a mutare il proprio orientamento precedente recependo questo diverso standard di tutela della riservatezza nel proprio giudizio di proporzionalità e dichiarando così l'invalidità della direttiva del 2006. Questo punto di approdo riguardante il diritto UE ha posto quindi le premesse per una reinterpretazione del diritto dell'Unione precedente alla direttiva del 2006, in particolare della direttiva 2002 che in passato non era stata applicata in materia di pubblica sicurezza con quella portata limitativa dell'autonomia e discrezionalità degli Stati membri, liberi nel sacrificare fortemente il livello di tutela della riservatezza, che oggi si è invece uniformemente affermata – quasi per un'eterogenesi dei fini – in esito al susseguirsi delle citate vicende.

Il giudizio interpretativo in via pregiudiziale qui annotato è peraltro importante anche su un piano più propriamente giuridico-formale, perché dalla pronuncia pregiudiziale di validità del caso *Digital Rights* relativa alla direttiva del 2006 non è derivata un'automatica ed inevitabile armonizzazione degli ordinamenti nazionali, lo strumento appropriato a tale scopo essendo invece quello del rinvio pregiudiziale interpretativo del residuo diritto dell'Unione vigente dopo l'eliminazione della direttiva invalidata, e quindi le regole e le eccezioni formulate dalla direttiva 2002. Successivamente alla sentenza del 2014 non è infatti sorprendente registrare una forte disomogeneità negli approcci nazionali all'adeguamento, dato che lo strumento del rinvio pregiudiziale di validità non ha potuto fissare con sufficiente puntualità quelle misure adeguate ad una proporzionata conservazione dei dati che solo l'interpretazione del diritto UE di risulta dopo la sentenza *Digital Rights* può enucleare; in altri termini, ragionare esclusivamente sull'eliminazione della direttiva del 2006 produceva rischi di un vuoto normativo, essendo appunto la *data retention* sì sproporzionata ma non radicalmente vietata (ed anzi essenziale per tutelare il diritto alla sicurezza, anch'esso tutelato peraltro dalla Carta di Nizza), di modo che la scelta di numerosi ordinamenti

nazionali è stata quella di non armonizzarsi al nuovo bilanciamento dei diritti operato nel 2014.

Nel panorama europeo possiamo quindi registrare la presenza di ordinamenti che già prima della sentenza 2014 avevano seguito un'interpretazione di maggior tutela della riservatezza per mezzo delle proprie corti costituzionali, il che ha portato al recepimento del livello di tutela oggi accolto in materia anche dall'Unione (Germania, Repubblica Ceca, Romania, Bulgaria e Cipro). D'altra parte, altri Stati membri hanno annullato le norme sulla *data retention* successivamente dalla sentenza *Digital Rights* del 2014, recependo il nuovo orientamento della Corte di Giustizia, come avvenuto ad esempio per l'Austria o la Slovacchia, operando talvolta in via legislativa, talaltra per l'azione diretta della magistratura che ha proceduto a disapplicare od annullare la normativa interna, dando prevalenza al nuovo diritto dell'Unione (come nel caso dei Paesi Bassi, dell'Irlanda, del Belgio e della Slovenia). Altri Stati membri, infine, come i due ordinamenti parte nel giudizio annotato (Svezia e Regno Unito), ma anche ad esempio la Danimarca e l'Italia, hanno conservato fino ad oggi discipline nazionali disarmoniche rispetto ai principi recepiti dalla giurisprudenza della Corte di Giustizia del 2014 (in Italia tra l'altro la Corte costituzionale non ha avuto occasione di affrontare la questione, ed anzi in un giudizio incidentale si è posta la problematica opposta dell'eventuale illegittimità per irragionevolezza dell'imposizione di un vaglio giudiziale preventivo per l'accesso del pubblico ministero alle informazioni concernenti il traffico telefonico; cfr. la sentenza 14 novembre 2006, n. 372 che rimette gli atti ai giudici *a quibus* per una nuova valutazione dopo la novella di cui all'art. 6 del d.l. 27 luglio 2005, n. 144, vicenda su cui si rinvia a E. Bassoli, *Acquisizione dei tabulati vs. privacy: la* data retention*al vaglio della consulta*, in *Diritto dell'Internet*, 2007, 237 ss.).

Si tratta quindi di definire quali condotte attuative debbano essere assunte in tale ultimo gruppo di Stati membri, in particolare per stabilire cosa sia tenuto a rispettare – nella perdurante inerzia dei legislatori nazionali – il singolo operatore delle telecomunicazioni. Da un lato la questione è cioè quella del se il privato fornitore del servizio, destinatario di un diritto nazionale vigente che ancora obbliga a conservare i dati esterni del traffico telefonico e internet, sia tenuto a disapplicare tale obbligo, incorrendo in caso contrario in una responsabilità per violazione della privacy dei propri utenti. D'altra parte, posto che il perdurante onere di conservazione dei dati affligge non solo il diritto alla riservatezza, ma ostacola anche la libera circolazione dei servizi (ponendo costi di servizio aggiuntivi agli operatori, gravati della conservazione e delle relative spese) ci si può chiedere se anche il gestore stesso – non remunerato dall'ordinamento per un onere gestionale illegittimo – possa essere interessato a dismettere la conservazione o proseguirla con richiesta di un risarcimento per il danno economico patito.

La disciplina italiana è senz'altro esposta a tali questioni, posto che è stato mantenuto un obbligo generale di conservazione all'art. 132 del Codice della privacy (circa gli effetti del diritto dell'Unione su tale disposizione, tra i vari contributi cfr. F. Iovene, *"*Data retention*" tra passato e futuro. Ma quale presente?*, in *Cass. penale*, 2014, 4274 ss.; A. Arena, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quad. cost.*, 2014, 722 ss.; R. Flor, *Dalla "*data retention*" al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive "*de jure condendo*"?*, in *Dir. 'informaz. informatica*, 2014, 775 ss.; S. Crespi, *Diritti fondamentali, Corte di Giustizia e riforma del sistema UE di protezione dei dati*, in *Riv. it. dir. pubbl. com.*, 2015, 819 ss., e in particolare il par. 6 per gli effetti sugli ordinamenti nazionali). A fronte di tale obbligo, da un lato la pubblica amministrazione ed i giudici – nelle situazioni in cui può emergere un'esigenza di applicazione o una controversia – devono procedere a disapplicazione per quanto le sentenze del 2014 e (soprattutto) del 2016 consentono di riconoscere effetto diretto alla regola generale di non conservazione dei dati, e quindi facendo salve le regole che ammettono la conservazione per non generali ed indifferenziate esigenze di contrasto alla criminalità (profilo sul quale si rinvia alla valutazione dell'idoneità dell'art 4 *bis* del d.l. 18 febbraio 2015, n. 7, come anche modificato dal d.l. 30 dicembre 2015, n. 210, a porsi come misura adeguatamente selettiva; cfr. P. Caputo, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*,

in *Archivio penale*, 2016, 28 ss.). D'altro lato, ferma la portata estremamente rilevante della giurisprudenza europea citata, l'operatore delle telecomunicazioni – in quanto attore economico privato destinatario di obblighi di leale collaborazione diversi rispetto alle pubbliche autorità – continua ad essere soggetto al diritto vigente nel proprio ordinamento e, quindi, verrà eventualmente sì a causare materialmente un danno alla riservatezza degli utenti, ma tale danno – pur se effettivamente prodotto – nondimeno non sarà qualificabile come ingiusto; ciò in quanto danno non *contra ius* nella misura in cui si richiede al privato di conformare la propria azione all'ordinamento positivo, residuando per lo stesso una mera facoltà di disapplicazione "a proprio rischio", spettando poi al giudice nazionale la valutazione dell'effettiva giustezza di tale scelta.

Proprio grazie a tale ultima sentenza *Tele2 Sverige* la questione pare invece oggi essere certamente risolvibile per le pubbliche autorità nel senso dell'obbligo da parte loro di disapplicare. La sentenza annotata infatti fonda lo standard di tutela della privacy sull'interpretazione delle direttive, consentendo la pacifica qualificazione come diritto dell'Unione della scelta di non ammettere una conservazione generalizzata ed indifferenziata dei dati. Dopo la dichiarazione di invalidità della direttiva *data retention* nel 2014, e prima dell'annotata sentenza del 2016, invece, la disapplicabilità del diritto nazionale che continuava ad imporre la conservazione dei dati appariva più problematica (o quantomeno non così immediata). Ciò perché l'art. 132 del Codice della privacy non può essere inteso come vincolato in senso stretto al diritto europeo (in quanto non solo approvato prima dell'adozione della direttiva 2006, ma perché comunque non strutturato come una disposizione direttamente attuativa di scelte europee bensì come disposizione assunta nell'ambito dell'ampia autonomia procedurale riconosciuta dalla direttiva 2002 nel fissare le eccezioni alla non conservazione fondate su esigenze di pubblica sicurezza; sugli orientamenti della giurisprudenza italiana cfr. ad esempio Trib. Padova, ord. 15-3-2017, Pres. Marassi su cui R. Flor, Data retention*ed art. 132 Cod. privacy:* vexata quaestio, in *penalecontemporaneo.it*, 29-3-2017).

Peraltro, nonostante tale carattere non attuativo, si poteva già affermare che la disciplina italiana vigente dopo la sentenza *Digital Rights* cadesse comunque in un ambito materiale di competenza dell'Unione in quanto – secondo la formula usata dalla Corte di Giustizia – presenterebbe un "collegamento di certa consistenza" con l'ordinamento dell'Unione. In questa prospettiva si poteva quindi già disapplicare la norma italiana dando rilevanza all'art. 51 della Carta nella sua interpretazione più ampia (cfr. le decisioni *Åkerberg*, *Siragusa* e *Pelckmans*, su cui sia consentito rinviare a F. Guella, *Il "collegamento sufficiente" tra disposizione nazionale e ordinamento UE quale perdurante condizione di applicabilità dei diritti fondamentali*, in *Dir. pubbl. comp. eur.*, 2014, 1161 ss. e ai più ampi riferimenti ivi riportati), con la quale si legittima l'utilizzo dei diritti fondamentali dell'Unione non solo per sindacare atti interni formalmente vincolati al diritto derivato europeo da un immediato rapporto di attuazione, ma anche quelli che si pongono come comunque strumentali all'implementazione di scelte normative europee operate in ambiti materiali di competenza dell'Unione.

In altri termini, la sentenza del 2014 aveva eliminato una direttiva per ragioni di tutela dei diritti fondamentali della Carta di Nizza, e il diritto interno poteva essere disapplicato solo riconoscendo che lo stesso – cadendo nell'ambito di operatività del diritto dell'Unione ampiamente inteso – si poneva in diretto contrasto con lo standard di tutela fissato dalla Carta, come interpretata dalla sentenza *Digital Rights*. Al contrario, dopo la sentenza del 2016 qui annotata, tale dubbio interpretativo non ha ragione di sussistere, il rinvio pregiudiziale alla Corte di Giustizia avendo risolto la questione riconducendo ad una direttiva tutt'ora vigente il medesimo standard di tutela, restringendo così uno spazio discrezionale – di autonomia procedurale per gli Stati membri – che la direttiva del 2002 invece in origine dava per sotteso a tutti i casi in cui gli ordinamenti nazionali avessero introdotto eccezioni fondate su ragioni di pubblica sicurezza.