IANUS
Diritto e Finanza

UNIVERSITÀ DI SIENA 1240

Rivista di studi giuridici

https://www.rivistaianus.it

ISSN: 1974-9805

n. 15-16 - giugno-dicembre 2017

LA SENTENZA *TELE2SVERIGE*: VERSO UNA *DIGITAL RULE OF LAW* EUROPEA?

Elisa Spiller

LA SENTENZA *TELE2 SVERIGE*: VERSO UNA *DIGITAL RULE OF LAW* EUROPEA?

Elisa Spiller

Dottoranda in diritto costituzionale presso l'Università degli Studi di Padova

Nel dicembre 2016 la Corte di Giustizia dell'Unione Europea si è pronunciata sul ricorso Tele2 Sverige, *l'ultimo atto di lunga* querelle *in tema di* data retention. *Tale decisione ha chiarito la portata della precedente sentenza* Digital Rights Ireland *all'interno degli ordinamenti nazionali, circoscrivendo il ricorso alla conservazione dei dati di traffico quale misura di contrasto al terrorismo ed altri gravi reati. Ricostruendo gli argomenti proposti dalla giurisprudenza, si andranno ad analizzare i profili inerenti le garanzie dello Stato di diritto. La Corte, infatti, valorizzando la tutela della* privacy *e la protezione dei dati personali ha individuato le condizioni necessarie all'utilizzo delle informazioni elettroniche nell'ambito dell'attività d'indagine, limitando così le interferenze pubbliche nella sfera privata. Una ricognizione di questo paradigmatico percorso contribuirà dunque ad evidenziare i passaggi ermeneutici che hanno permesso di integrare questi mezzi nell'alveo di una* digital rule of law*: dei passi fondamentali per promuovere, anche in tempi così incerti, i valori dello Stato democratico.*

In December 2016, the Court of Justice of European Union decided the case Tele2 Sverige*. This is last act of a long-standing dispute on the retention of data generated or processed by providers of electronic communication services: a set of measures part of the broader international strategy to contrast terrorism and other serious crimes. This essay offers a brief overview on the UE case-law concerning this theme, analyzing the profile of the Rule of Law. The CJEU indeed in* Digital Rights Ireland *opted for a human rights-oriented approach, direct to ensure a high level of protection of privacy, especially with regard to the processing of personal data (Articles 7 and 8 of the Charter). In so doing, the Court provided specific requirements to regulate the storing of metadata and the access by public authorities to this information, limiting the interference of public powers in the private sphere. This study aims to a systematic view of this prominent legal reasoning. The value of these decisions is that they have extended this* Digital Rule of Law *including these measures in the European constitutional framework: these points represent a significant achievement to preserve the very core of a democratic system.*

Sommario:

.

1. Introduzione

Negli ultimi anni, davanti ad un mondo sempre più *digital*, la Corte di Giustizia dell'Unione europea non ha perso occasione per confermare il suo ruolo di *human rights adjudicator*[1]. Con la sua giurisprudenza[2], infatti, sta contribuendo alla fioritura di una vera e propria tradizione costituzionale sui diritti in rete[3], in particolare per quanto riguarda l'elaborazione di un nuovo *digital right to privacy*[4]. Tale riflessione, tuttavia, ha messo in luce la complementare esigenza di individuare le condizioni e i limiti per l'utilizzo di queste nuove informazioni. In un processo di c.d. *datizzazione*, infatti, la loro disponibilità richiede di essere regolamentata, non solo nei confronti dei privati ma anche delle autorità pubbliche, integrando dunque di nuovi profili le garanzie dello Stato di diritto.

Il presente scritto, riprendendo l'ormai paradigmatica *querelle* sulla *data retention*, propone una ricostruzione del percorso svolto fino alla recente sentenza *Tele2 Sverige*[5], evidenziando come un approccio *fundamental rights oriented*[6] abbia contribuito alla parallela elaborazione di una *digital rule of law*. Il tema di fondo, invero, intercetta questioni di immediata attualità. In «*tempo di*

---

[1] CARTABIA, *I diritti in Europa: la prospettiva della giurisprudenza costituzionale italiana*, in *Riv. Trim. Dir. Pubb.*, 2015, par. 2; DE BÚRCA, *After The EU Charter of Fundamental Rights: The Court Of Justice As A Human Rights Adjudicator?*, in *Masst. J. Eur. & Comp. L.*, 2013.

[2] Ci si rifà soprattutto alla sent. 13 maggio 2014, *Google Spain SL e Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12 (diritto all'oblio); alla sent. 8 aprile 2014, *Digital Rights Ireland e a./Minister for Communications, Marine and Natural Resources e a.*, cause riunite C-293/12 e C-594/12 e alla successiva sent. 6 ottobre 2015 *Schrems/Data Protection Commissioner*, C-362/14 (*e-privacy* nell'ambito delle misure sulla *data retention*).

[3] POLLICINO, *Diritto all'oblio e conservazione dei dati. La Corte di Giustizia a piedi uniti: verso un* digital right to privacy, in *Giur. cost.*, 2014, 2949; BRONZINI, *La Carta dei diritti dell'Unione europea come strumento di rafforzamento e protezione dello Stato di diritto*, in *Pol. dir.*, 2016, 20.

[4] POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *federalimsi.it*, 2014; ID., *I nuovi scenari della tutela della privacy nell'era della digitalizzazione alla luce delle recenti pronunce sul diritto all'oblio*, in *federalismi.it*, 2015; BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della* privacy, in *Giur. cost.*, 2016, 289ss; PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016.

[5] Sent. 21 dicembre 2016, *Tele2 Sverige / Post och telestyrelsen e Secretary of State for the Home Department / Watson e al.*, cause riunite C-203/15 e C-698/15.

[6] TIBERI, *Il caso* Tele2 Sverige/Watson: *un'*iconica *sentenza della Corte di Giustizia nella saga sulla* data retention, in *Quad. cost.*, 2017, 436.

ordinario terrorismo»[7] il rapporto tra regola ed eccezione tende a confondersi, e così misure investigative inizialmente straordinarie, assumendo i tratti della normalità, richiedono una più attenta ponderazione[8]. Questa parabola ha interessato, tra le altre, anche la disciplina sulla conservazione dei metadati per attività di contrasto alla criminalità organizzata, rispetto alle quali è stato fondamentale ridefinire i rapporti tra *privacy* e sicurezza, alla ricerca di un diverso punto di equilibrio. In questo contesto, in cui l'utilizzo delle tecnologie si presta ad essere esaltato per le sue inedite potenzialità, diventa necessario infatti reinterpretare e *tradurre*[9] le garanzie costituzionali, attualizzandone la portata a fronte di queste nuove dinamiche.

Ripercorrendo dunque l'evoluzione dell'esperienza europea dall'approvazione della Direttiva 2006/24[10] fino al caso *Tele2*, si andranno ad individuare i passaggi più significativi, evidenziando come la Corte con i suoi interventi abbia contribuito a "normalizzare" l'utilizzo di queste misure attraverso garanzie e limiti compatibili con l'ordinamento democratico.

2. Rule of law e data retention. L'esigenza di normalizzare l'eccezione

La Direttiva 2006/24 «riguardo la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica per il contrasto alla criminalità organizzata» è probabilmente una delle iniziative comunitarie più controverse nella storia dell'Unione. Ad uno sguardo più ampio, tuttavia, il tema della *data retention* ha cominciato a porre importanti interrogati ben prima dell'adozione di tale normativa, già nella prima attuazione delle strategie internazionali per la lotta al terrorismo.

All'indomani dell'11 settembre, su entrambe le sponde dell'Atlantico sono stati approvati provvedimenti straordinari per contenere questo tipo di

[7] Come acutamente definito in DE MINICO, *Le libertà fondamentali in tempo di ordinario terrorismo*, in *federalismi.it*, 2015, 3.

[8] BARTOLI, *Regola ed eccezione nel contrasto al terrorismo internazionale*, in *Dir. pubbl.*, 2010.

[9] LESSIG, *Reading the Constitution in the Cyberspace*, in *Emory Law Review*, 45/3, 1996; SAJÒ - RYAN, *Judicial Reasoning and New Technology*, in POLLICINO - ROMEO (a cura di), *The Internet and Constitutional Law: The protection of fundamental rights and constitutional adjudication in Europe*, Londra - New York, 2016.

[10] Dir. 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la dir. 2002/58/CE.

minacce e salvaguardare la sicurezza pubblica[11]. La caratteristica comune a questi interventi è stata principalmente la loro eccezionalità. Derogando alla normali garanzie costituzionali[12], queste politiche sono state ammesse, infatti, solo per un periodo transitorio, auspicandone il contenimento non appena le condizioni lo avessero consentito. Il susseguirsi degli eventi, tuttavia, racconta una storia ben diversa, in cui il livello di allarme negli anni non ha accennato a diminuire (anzi!) [13]. Con il passare del tempo, si è così avvertita l'esigenza di riconsiderare le premesse e la funzione degli strumenti adottati, onde evitare che le contingenze potessero diventare l'occasione di una prolungata costrizione dello Stato di diritto[14].

La legittimità di simili misure – ora come allora – continua dunque ad essere un argomento sensibile e controverso. Nonostante il capitolo "sicurezza" sia stato assimilato ed integrato da diversi ordinamenti costituzionali[15], il ricorso a mezzi *extra*-ordinari desta ancora serie perplessità. Non è pacifico, infatti, dove collocare il limite ultimo alla loro adozione e, di conseguenza, spesso non è immediato individuare le garanzie minime per un loro buon utilizzo[16].

In quest'aggiornamento della *rule of law*, la ricerca di un nuovo punto di equilibrio per l'Unione europea ha rappresentato un importante banco di

[11] MURPHY, *EU Counter-Terrorism Law. Pre-Emption and the Rule of Law*, Oxford - Portland, 2012; MITSILEGAS, *The Transformation of Privacy in an Era of Pre-emptive Surveillance*, in *Tilburg L. Rev.*, 2015;

[12] VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, in *Dir. pubbl. comp. eur.*, 2014, 1225. Più specificamente, così come constatato dall'Autrice, di fronte alla comune minaccia, se gli Stati Uniti si avevano dichiarato lo *stato di emergenza*, in Europa le Istituzioni comunitarie – e con esse la maggior parte degli Stati membri – erano ricorse alla diversa ipotesi dell'*eccezione costituzionale*: modelli diversi, e tuttavia con esiti sostanzialmente assimilabili.

[13] Si osserva infatti in DE MINICO, *Le libertà fondamentali in tempo di ordinario terrorismo*, come siano cambiati fondamentalmente i tratti stessi del fenomeno: «*quotidianità e sovversività sono quindi i tratti identificativi del terrorismo di oggi, che influenzano in prima battuta il modo di essere del criterio di legittimità, cioè il parametro diretto a orientare il decisore politico, e, per suo tramite, la sua scelta della misura normativa più* reasonable *rispetto alla gravità della situazione*» (3). In tal senso, dunque, sono mutate le caratteristiche della risposta ordinamentale (*ibidem*, 5-8).

[14] JAKAB, *The rule of law, fundamental rights and the terrorist challenge in Europe and elsewhere*, in id., *European Constitutional Language*, Cambridge, 2016, 124-129, 141-142.

[15] TUORI, *The insecure security constitution*, in ID., *European Constitutionalism*, Cambridge, 2015.

[16] JAKAB, *The rule of law, fundamental rights and the terrorist challenge in Europe and elsewhere*, cit., 124-129, 141-142.

prova[17]. Chiamata a ridefinire i rapporti tra controllo pubblico e libertà individuali, la Corte di giustizia si è infatti contraddistinta per un approccio originale[18] – e talora in controtendenza –, contribuendo a riaffermare i valori propri del costituzionalismo europeo, sia nell'attuazione delle strategie internazionali, sia nell'elaborazione di quelle continentali[19].

La conservazione e l'accesso ai metadati prodotti dalle comunicazioni elettroniche si collocano proprio in questo contesto, in un complesso piano di *data surveillance*[20] deciso a sfruttare le potenzialità delle nuove tecnologie per contrastare il fenomeno terroristico. Nel vecchio continente, tuttavia, l'utilizzo di questi strumenti ha cominciato a sollevare particolari domande solo a distanza di qualche anno, in seguito agli attentati di Madrid (2004) e Londra (2005). Fino a quel momento, gli Stati membri avevano adottato autonomamente delle misure di sorveglianza proprie, differenti tra loro in funzione della diverse sensibilità alla questione. Gli attacchi ad alcune città europee avevano però messo in luce i limiti di un approccio così frammentario, lasciando affiorare l'esigenza di una più chiara agenda comune su questi temi[21]. Tali istanze si sono tradotte in proposte preliminari, volte ad elaborare una specifica disciplina comunitaria. Si intendeva, infatti, risolvere in via sussidiaria i problemi emersi nelle singole esperienze

[17] Sent. 30 maggio 2006, *Parlamento europeo/Consiglio dell'Unione Europea (PNR)*, cause riunite C-317/04 e C-318/04; sent. 3 ottobre 2008, *Yassin Abdullah Kadi, Al Barakaat International Foundation/Consiglio*, cause riunite C-402/05 P e C-415/05 P; sent. 21 settembre 2005, *Yusuf, Al Barakaat International Foundation/Consiglio*, causa T-306/01; sent. 21 settembre 2005, *Kadi/Consiglio e Commissione*, causa T-315/01.

[18] FABBRINI, *Human Rights in the Digital Age: The European Court of Justice in the Data Retention Case and Its Lessons for the Privacy and Surveillance in the United States*, in *Harv. Hum. Rts. J.*, 2015.

[19] Consiglio dell'UE, *Dichiarazione sulla lotta al terrorismo*, doc. 7906/04, 31.03.04. In dottrina, *ex multis*, MITSILEGAS, *Transatlantic counterterrorism cooperation and European values*, cit.

[20] MURPHY, *EU Counter-Terrorism Law. Pre-Emption and the Rule of Law*, cit., 147 ss.

[21] Si veda, *in primis*, dir. 2006/24, *Considerando* n. 10 e, per quanto attiene alle precedenti valutazioni di merito, Consiglio dell'UE, *Dichiarazione sulla lotta al terrorismo*, cit., 5-6; Consiglio dell'UE, *EU Plan of Action on Combating Terrorism*, doc. 10586/04, 15.06.04; Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo*, doc. 8958/04, 20.12.2004. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, cit., 1228; in particolare, si evidenzia come, in seguito a quei primi attentati europei si assista ad un vero e proprio «*revirement* securitario», passando da una politica volta ad incoraggiare la *data protection* (segnatamente con le dir. 95/46 e 2002/58) alla graduale legittimazione della *data retention* (in quella che sarà per l'appunto la c.d. Direttiva Frattini).

nazionali, in un percorso che avrebbe avuto come primo esito l'adozione della Direttiva 2006/24.

3. La Direttiva 2006/24: una visione comune oltre i meri costi economici

Ad onor del vero, un tema come la *data retention*, per la sua portata avrebbe meritato fin dall'inizio un approccio unitario, se non altro perché andava a collocarsi in un settore di storica matrice europea quale la tutela della *privacy*.

Il fatto che in un ambito come questo ogni Stato si fosse determinato in modo del tutto indipendente ha posto essenzialmente tre ordini di problemi. Innanzitutto, sul versante della *sicurezza*, un simile *patchwork* normativo si contrapponeva al rafforzamento della cooperazione giudiziaria ed investigativa in materia penale. La conservazione di dati diversi per periodi diversi, infatti, andava ad incoraggiare un utilizzo "selettivo" dei mezzi, convogliando indirettamente le attività criminali verso i sistemi informativi sottoposti ad una disciplina più mite[22]. In secondo luogo, l'imposizione di obblighi così disomogenei moltiplicava i *costi* in capo ai fornitori di servizi[23]. Questi ultimi, a tali condizioni, dovendo comunque garantire un adeguato livello di protezione dei dati conservati[24], si trovavano onerati di numerosi adempimenti, specifici per ogni giurisdizione (una situazione che certo non prometteva di incoraggiare lo sviluppo del mercato interno)[25]. Ultimo ma non ultimo, l'archiviazione di una così vasta quantità di informazioni, costituiva *una forte ingerenza nei diritti* alla *privacy* e alla protezione dei dati personali; e ciò ancor prima di un eventuale accesso da

[22] Una della opzioni considerate anche a livello europeo, infatti, prevedeva l'ipotesi di limitare al conservazione ai soli dati già trattati nell'ambito di erogazione dei servizi, senza definire uno *standard* comune. Tuttavia, si era osservato come una simile scelta avrebbe potuto dirottare le attività criminose verso quei servizi meno interessati alla conservazione di tali informazioni, vanificando l'utilità della misura (rif. Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo*, doc. 15098/04, 23.11.2004).

[23] Dir. 2006/24, *Considerando* nn. 5 e 6.

[24] Dir. 2006/24, art. 7.

[25] Un obiettivo che, per quanto documentato al tempo dell'adozione dell'atto, risulta ancora ben lontano da raggiungere, come rappresentano i dati in seguito emersi nella relazione della Commissione al Consiglio e al Parlamento europeo, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE)*, COM (2011), 28 ss.

parte delle autorità pubbliche. Si finiva, infatti, con il prevedere un trattamento ulteriore proprio laddove escluso dalla disciplina ordinaria[26], favorendo una scelta in aperta contrapposizione non solo con la tradizionale normativa europea sulla *privacy*[27], ma anche con quanto allora recentemente sancito dalla Carta di Nizza[28].

Considerata la politicità del tema, elaborare una risposta a questi problemi si è rivelato un'impresa particolarmente ardua. Contestualizzando la vicenda nel processo di integrazione europea, il Trattato di Maastricht aveva incluso la cooperazione giudiziaria in materia penale nell'ambito delle competenze dell'Unione, ammettendo la possibilità di regolare questi settori, seppur dovendo ricorrere al tradizionale metodo intergovernativo[29]. D'altro canto, per salvaguardare l'*acquis* comunitario, l'art. 47 TUE aveva riconosciuto una *primauté* al primo pilastro[30]; e ciò onde evitare che, di fronte all'alternativa tra diverse basi giuridiche, venisse preferito un ritorno alle procedure del diritto internazionale a discapito dell'esperienza europea. In questa luce, la *data retention* – per i profili di criticità ricordati – presentava delle sfaccettature poliedriche, collocandosi a metà strada tra aree diverse, come una sorta di competenza "interpilastro"[31]. A fronte di quest'incertezza, dunque, nonostante alcuni Governi avessero proposto l'adozione di una decisione nell'ambito delle nuove materie incluse *ex* artt.

[26] Dir. 2006/24, *Considerando* nn. 3 e, specificamente, art. 3 in deroga a quanto previsto dalla dir. 2002/58, artt. 5, 6 e 9.

[27] PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 128-130. Come l'Autore infatti sottolinea, non solo la formulazione del diritto alla *privacy* e alla protezione dei dati personali ha costituito un'attuazione molto evolutiva di quanto previsto dall'art. 8 della CEDU, ma, ben prima del Trattato di Lisbona, la dir. 95/46 ne aveva sancito una tutela completa (così come, peraltro, confermato anche dalla CGUE nella sent. 24 novembre 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) /Administración del Estado*, cause riunite C-468/10, C-469/10, par. 28-29).

[28] GROPPI, *Art. 7*, e DONATI, *Art. 8*, in BIFULCO, CARTABIA, CELOTTO (a cura di), *L'Europa dei diritti*, Bologna, 2001; TIBERI, *Riservatezza e protezione dei dati personali*, in CARTABIA (a cura di), *I diritti in azione*, Bologna, 2007, 368 ss.

[29] *Ex multis*, DANIELE, *Diritto dell'Unione europea*, Torino, 2014, 226 ss.

[30] Più diffusamente, sul punto si rimanda a MASTROIANNI, *Art. 47 TUE*, in TIZZANO (a cura di), *Trattati dell'Unione europea e della Comunità europea*, Milano, 2004, 167.

[31] PALADINI, *I conflitti fra pilastri dell'Unione europea e le prospettive del Trattato di Lisbona*, in *Dir. UE*., 2010, 87-90, 102-105; FONTANELLI, *La Corte di Giustizia e il "favor communitatis". Il percorso della giurisprudenza della Corte di Giustizia delle Comunità europee sul fondamento normativo degli atti dell'Unione*, in *Riv. it. dir. pubbl. comunit.*, 2010.

31, n. 1, lett. c) e 34, n. 2, lett. b) UE[32], Parlamento e Commissione giunsero all'adozione della Direttiva Frattini (2006/24) ancorandola alle previsioni dell'art. 95 CE secondo una prospettiva *market-oriented*[33].

In accordo con la base giuridica così indicata, la portata di questa nuova normativa fu circoscritta alla sola armonizzazione degli obblighi imposti agli operatori[34], uniformando le categorie di dati trattati[35] e riducendo la discrezionalità sui tempi di conservazione[36]. Uno degli aspetti più rilevanti della nuova disciplina, tuttavia, riguardava la natura delle prescrizioni rivolte agli Stati, radicalmente diverse da quanto previsto in precedenza dall'art. 15 della Direttiva 2002/58[37] (c.d. Direttiva sull'*e-privacy*). Tale norma, infatti, solo in casi particolari (quali appunto – tra i vari – la sicurezza nazionale, la difesa, e il contrasto di reati gravi) permetteva di derogare alle ordinarie garanzie per la tutela della *privacy* "elettronica", ammettendo la sospensione dell'obbligo di cancellazione dei metadati. In questi specifici frangenti, dunque, si finiva con il legittimare in via straordinaria il ricorso alla *data retention*, purché ciò avvenisse entro i limiti imposti dal diritto

[32] Nello specifico, un progetto presentato dal Francia, Inghilterra, Regno Unito e Irlanda, *Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detect*, doc. 8958/04, 20.12.2004.

[33] Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo - Base giuridica*, doc. 7688/05, 05.04.2005, spec. 2–7.

[34] Dir. 2006/24, art. 3, includendo – peraltro in termini tutt'altro che restrittivi – i dati necessari per rintracciare e per identificare le fonte e la destinazione di una comunicazione, così da stabilirne la natura, la data, l'ora e la durata, l'ubicazione degli utenti e il tipo di strumentazione utilizzata.

[35] Dir. 2006/24, art. 5.

[36] Dir. 2006/24, art. 6.

[37] Dir. 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 (dir. relativa alla vita privata e alle comunicazioni elettroniche). È nell'adozione di questa direttiva che si avverte per la prima volta il mutato clima del *post* 11 settembre. A differenza della dir. 95/46, infatti, la "novella" del 2002, alla luce degli avvenimenti dell'anno prima, stempera i toni garantisti, limitando tuttavia la possibilità della *data retention* ad una mera facoltà rimessa al legislatore. Sarà solo la dir. 2006/24, dopo i fatti di Madrid e Londra, a cambiare definitivamente la rotta, trasformando un'eventuale eccezione in obbligo. (v. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 129; VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, cit., 1229).

comunitario[38]. Fino a quel momento, pertanto, i singoli interventi statali si erano fondati sull'eccezione contemplata da tale disposizione, nell'esercizio della *facoltà* ivi concessa al legislatore nazionale[39]. Se però la possibilità di ricorrere a tali misure nella previgente regolazione rappresentava un'ipotesi solo eventuale, la nuova Direttiva – con effetti "costitutivi" – la concepiva come un *obbligo*[40], imponendo l'utilizzo di questi strumenti come un normale metodo investigativo per la repressione di gravi reati.

Nel disporre in tal senso, l'atto si limitava a considerare principalmente i profili inerenti la portata degli adempimenti privati, delegando ai singoli Governi la definizione dei presupposti e delle garanzie per ricorrervi[41]. Questa scelta, sebbene inizialmente avvalorata dalla Corte di Giustizia[42], ha continuato però a destare pesanti critiche[43]. La normativa, infatti, aveva imposto degli obblighi destinati a comportare una grave compromissione della *privacy* e del trattamento dei dati senza comunque definire contestualmente un adeguato sistema di garanzie . Il testo, a riguardo, non si spingeva oltre a meri richiami al rispetto dei diritti in questione[44]; cenni,

[38] Dir. 2002/58, art. 15, par. 1, ultimo periodo: «*Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.».* Norma che, in definitiva, andava ad includere anche i principi inerenti la tutela dei diritti fondamentali così come previsi, dapprima, dalla CEDU e dalla tradizione costituzionale degli Stati membri e, in seguito, dalla Carta di Nizza.

[39] Dir. 2002/58, art. 15, par. 1, primo periodo, in cui si legge « Gli Stati membri *possono* adottare disposizioni legislative volte a limitare i diritti e gli obblighi…».

[40] Dir. 2006/24, art. 3, par. 1, in cui diventa: «In deroga agli articoli 5, 6 e 9 della Direttiva 2002/58/CE, gli Stati membri *adottano* misure per garantire che i dati […] siano conservati conformemente alle disposizioni della presente Direttiva»

[41] Dir. 2006/24, art. 4.

[42] Sent. 10 febbraio 2009, *Irlanda/Parlamento e Consiglio*, causa C-301/06, in cui la Corte ha confermato la scelta della base giuridica osservando come la disciplina, limitandosi ai profili privatistici e vincolando la portata delle misure al rispetto del diritto comunitario, potesse (e dovesse: par. 78) essere adottata sui presupposti dell'art. 95 CE. FONTANELLI, *La Corte di Giustizia e il "favor communitatis"*, cit.

[43] BIGNAMI, *Protecting Privacy Against the Police in the European Union : The Data Retention Directive*, in BOT (a cura di), *Melanges en l'Honneur de Philippe Leger: le droit a la mesure de l'homme*, Parigi, 2006; ID, *Privacy and Law Enforcement in the European Union: the Data Retention Directive*, in *Chi. J. Intl. L.*, 2007; FEILER, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, in *EJLT*, 2010; KOSTA, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Protection Directive with the Rights to Privacy and Data Protection*, in *Scripted*, 2013.

[44] Dir. 2006/24, art. 4, ultimo periodo, in cui si legge: «*Le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di*

questi, assolutamente insufficienti a compensare le limitazioni introdotte (soprattutto alla luce di quanto stabilito in merito dalla Carta di Nizza)[45].

Per questi motivi, la Direttiva Frattini è stata oggetto di un acceso dibattito e la discussione sui contenuti da essa ereditati è ancora in là dal sopirsi. Fin dall'inizio, se la Commissione, da un lato, aveva sanzionato severamente i legislatori inadempienti al recepimento[46], dall'altro, le Corti nazionali avevano dichiarato l'illegittimità costituzionale della disciplina di attuazione[47]; una serie di dinamiche che – tutto sommato – hanno invitato ad una più equilibrata revisione della materia.

Nel susseguirsi delle pronunce la complessa natura della disciplina era stata dunque messa in forte discussione. Si è avvertita così l'esigenza di ridefinire i valori in gioco, non limitandosi a considerare i meri interessi economici della prima ora, ma estendendo l'analisi anche ai profili fino a quel momento trascurati, *in primis* la tutela dei diritti. La Corte di giustizia, dunque, finalmente interpellata dalla Corte costituzionale austriaca e dalla Corte suprema irlandese, nel 2012, con la sentenza *Digital Rights Ireland*, ha

---

necessità e di proporzionalità sono definite da ogni Stato membro nella legislazione nazionale, con riserva delle disposizioni in materia del diritto dell'Unione europea o del diritto pubblico internazionale e in particolare della CEDU, secondo l'interpretazione della Corte europea dei diritti dell'uomo.»

[45] Anche il mero riferimento all'esigenza di includere le previsioni nella legislazione nazionale, senza soffermarsi sulle caratteristiche minime dell'atto di recepimento, è stato oggetto di analisi. Nella ricostruzione offerta dell'AG nel caso *Tele2 Sverige*, infatti, anche la sola individuazione di una corretta base giuridica risulta problematica, a fronte del fatto che lo stesso significato della parola "legge" o di locuzioni tipo "misura legislativa" può assumere un significato diverso nei singoli contesti nazionali, individuando fonti con un diverso grado di specificità e vincolatività (*Tele2 Sverige*, Conclusioni AG, par. 144ss.)

[46] Sent. 26 novembre 2009, *Commissione/Grecia*, causa C-211/09; Sent. 26 novembre 2009, *Commissione/Irlanda*, causa C-202/09; sent. 4 febbraio 2010, *Commissione/Svezia*, causa C-185/09; sent. 29 luglio 2010, *Commissione/Austria*, causa C-189/2009. In particolare, inoltre, va ricordata un'ulteriore procedura che, in seguito, ha visto coinvolta nuovamente la Svezia, condannata al pagamento di una somma forfettaria di 3 milioni di euro (sent. 30 maggio 2013, *Commissione/Svezia*, causa C-270/2011).

[47] Si erano, infatti, pronunciate nel frattempo la Corte suprema amministrativa bulgara (2008); la Corte suprema rumena (2009); il Tribunale costituzionale federale tedesco (2009); la Corte suprema cipriota (2011) e la Corte costituzionale ceca (2011); senza contare i ricorsi pendenti al momento del rinvio alla CGUE, avanti la Corte costituzionale polacca (2011) e la Corte costituzionale slovacca (2012). In dottrina si rimanda a KOSTA, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Protection Directive with the Rights to Privacy and Data Protection*, cit.; DURICA, *Directive on the Retention of Data on Electronic Communication in the Rulings of the Constitutional Courts of the EU Member States and Efforts for its Renewed Implementation*, *TQL*, 2013; VEDASCHI - LUBELLO, *Data Retention and its Implications for the Fundamental Right to Privacy*, *Tilburg L. Rev.*, 2015, 22–26.

colto l'occasione per rispondere alla numerose perplessità emerse fino ad allora. Incentrando lo scrutinio sugli artt. 7, 8 e 52, § 1 della Carta, questa pronuncia – unitamente alla successiva giurisprudenza – ha gradualmente messo a fuoco due prospettive complementari. Enfatizzando, infatti, gli aspetti inerenti la legittima limitazione delle libertà fondamentali, dapprima, ha elaborato più *precise condizioni procedurali* per l'utilizzo di queste misure, limitandone poi il ricorso – sotto il profilo sostanziale – *solo per interventi circoscritti e mirati*.

4. Precise condizioni procedurali…

Come accennato, le Corti nazionali avevano messo in luce quanto la normativa europea fosse finita con il "normalizzare" le misure di *data retention* senza corredarle delle opportune guarentigie. Auspicando una più attenta ponderazione degli interessi coinvolti, tali previsioni erano state censurate a più riprese perché eccessivamente intrusive rispetto alla tutela della sfera privata: un'indicazione che le CGUE ha accolto e sviluppato.

A riguardo, non si può trascurare come il mutato assetto istituzionale abbia contribuito alla maturazione di questa diversa sensibilità. Il Trattato di Lisbona, infatti, riconoscendo pieno valore alla Carta di Nizza, aveva confermato la centralità del proprio *bill of rights* nell'ambito del diritto europeo. Alla luce di queste evoluzioni, la giurisprudenza sulla competenza svelava dunque tutta la sua fragilità, ora mostrando – addirittura – delle profonde contraddizioni[48]. Dal piano nazionale la questione *costituzionale* ha acquisito, pertanto, una rilevanza *europea*, dovendosi chiarire se e in che misura le istituzioni comunitarie potessero limitare con i loro atti la portata dei diritti fondamentali previsti dalla Carta[49].

[48] Riprendendo, infatti, le considerazioni svolte in precedenza – in occasione della sent. *Irlanda/Parlamento e Consiglio* – nel ricorso *Digital Rights Ireland* è stato proposto un ulteriore motivo sulla corretta individuazione della base giuridica. La Corte nella sua decisione, analizzando dapprima la questione alla luce degli artt. 7 e 8, non arriva a decidere del punto ma nelle Conclusioni dell'AG Cruz Villalòn il problema viene affrontato in modo più compiuto: l'ingerenza della conservazione nella sfera della vita privata era sproporzionata per una misura volta alla sola tutela del mercato interno e, allo stesso tempo, l'unico presupposto che avrebbe permesso di confermare la legittimità della base giuridica non avrebbe potuto essere altro se non l'art. 95 CE (par. 102).

[49] L'AG, infatti, introducendo le proprie conclusioni, esordisce sottolineando come i due ricorsi offrano alla Corte «*le offre l'occasione di pronunciarsi sulle condizioni alle quali è* costituzionalmente *possibile per l'Unione europea prevedere una limitazione all'esercizio dei diritti fondamentali nel senso particolare di cui all'articolo 52, paragrafo 1, della Carta dei*

A tal proposito la Corte formalmente non arriva a discostarsi dalla sua precedente decisione[50]. Tuttavia, facendo leva su questi nuovi elementi, si è prodigata in un'attenta rivalutazione delle questioni in oggetto. Pur riconoscendo l'importanza di armonizzare gli oneri imposti ai gestori privati, ha evidenziato come essi, da soli, costituissero un motivo insufficiente a giustificare simili ingerenze nella vita privata[51]. Questa prima constatazione ha permesso, dunque, di riconsiderare la portata della Direttiva nella sua totalità, approfondendone l'analisi in dialogo con quanto affermato dalle magistrature nazionali.

Il paradosso cui aveva condotto la scelta del fondamento giuridico era ormai evidente. Incardinando la disciplina nell'ambito del primo pilastro, la Direttiva aveva finito per regolare soprattutto i profili inerenti la tutela del mercato, evitando di limitare ulteriormente l'autonomia nazionale in altri settori. A motivo di questa decisione, però, la struttura dell'articolato risultava precaria, soprattutto quanto alla tutela dei diritti[52]. Comprensibilmente – è vero – non si potevano pretendere in tal senso prescrizioni puntuali e dettagliate, poiché si sarebbe finiti per invadere le già menzionate competenze penali. Tuttavia, risultava difficile giustificare la mancanza di quegli "obblighi indicativi" che avrebbero dovuto orientare l'operato dei singoli Stati affinché questi ultimi si facessero custodi di alcune imprescindibili garanzie minime.[53]. Il margine concesso alla discrezionalità del legislatore nazionale, infatti, da un lato, rischiava di tradursi in un recepimento deficitario rispetto ai canoni previsti dalla Carta (e prima ancora dalla tradizione costituzionale europea)[54]. E, dall'altro, anche quando la

---

diritti fondamentali dell'Unione europea» (par. 1). Un ruolo istituzionale – quello di giudice costituzionale – che in questi casi non solo viene implicitamente ammesso dalla CGUE ma che le viene riconosciuto anche dalle Corti nazionali che ad essa di sono rivolte, come sottolineato da VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto*, cit., 1241 e TIBERI, *Il caso* Tele2/Sverige/Watson, cit., 437.

[50] Anche alla luce di quanto esposto nella nota precedente, la Corte non arriva a riconsiderare il proprio orientamento sul punto della competenza comunitaria (par. 71), decide di analizzare la questione soltanto alla luce di quanto previsto dalla Carta.

[51] *Digital Rights Ireland*, Conclusioni, par. 102.

[52] VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto*, cit., 1229-1232; BIGNAMI, *Protecting Privacy Against the Police in the European Union : The Data Retention Directive*, cit., 113 ss.

[53] *Digital Rights Ireland*, Conclusioni, par. 125; Sentenza, par. 54 e 65.

[54] Come si avrà modo di constatare nell'analisi svolta sulla portata delle normative nazionali nel caso *Tele2 Sverige*, spesso queste si erano determinate ad includere nel novero dei reati presupposto fattispecie di minor gravità, estendendo dunque le ingerenze nei diritti *ex* artt. 7 e 8 ben oltre i fini originariamente previsti dalla Dir. (*Tele2 Sverige*, Conclusioni, par. 230).

locale attuazione delle norme avesse privilegiato un approccio garantista, questo non avrebbe comunque potuto compensare le effettive carenze della disciplina comunitaria[55]. In altri termini, si è arrivati a concludere che – in quanto prescrittivo di specifiche limitazioni – l'atto avrebbe dovuto avere un'elaborazione coerente anche sotto il profilo delle tutele, includendo almeno dei criteri chiari e oggettivi[56].

I parametri della Carta di Nizza hanno quindi fornito un'utile lente per rinvenire le carenze della Direttiva 2006/24; una riflessione che – come si vedrà in seguito – risulterà fondamentale per la declinazione di una *digital rule of law* europea, rivolta non solo alle istituzioni comunitarie ma anche agli Stati membri.

Le misure di *data retention*, come già ricordato, erano causa di ingerenze particolarmente gravi nei diritti sanciti dagli artt. 7 e 8 della Carta[57]. Per garantire quindi un minimo *standard* di tutela, la Direttiva avrebbe dovuto innanzitutto regolare – almeno per principi – le procedure necessarie all'utilizzo dei metadati[58]. Nell'*ecologia* dell'atto avrebbero perciò dovuto trovare spazio previsioni volte ad individuare riferimenti oggettivi, in modo tale da assicurare un effettivo controllo sulle condizioni preordinate alla conservazione e all'accesso[59]. Quanto al rispetto dei diritti, tuttavia, il testo si limitava a prevedere che le normative nazionali avrebbero dovuto «*rispettare pienamente i diritti fondamentali che risultano dalle tradizioni costituzionali comuni degli Stati membri e che sono garantiti dalla CEDU*»[60], richiamando poi, genericamente i contenuti delle direttive 96/45 e 2002/58[61]. A fronte del

[55] *Digital Rights Ireland*, Conclusioni, par. 126-131; Sentenza, par. 58-68.

[56] VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto*, cit., 1239.

[57] Invero, tanto nei ricorsi della sent. *Digital Rights Ireland*, quanto in quelli successivi – nel caso *Tele2 Sverige* – le doglianze erano state sollevate non solo con riferimento a questi due articoli ma anche e soprattutto richiamando i diritti tutelati dall'art. 11, in materia di libertà di espressione. Tuttavia, nonostante qualche accenno a quest'ultimo (specificamente in *Tele2 Sverige*, par. 101), secondo la logica della "maggiore esposizione" (VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto*, cit., 1235), l'indagine si è concentrata principalmente su queste due disposizioni, in tema di *privacy* e protezione dei dati personali.

[58] Rispetto a questo passaggio è interessante notare come le argomentazioni sviluppate dalla Corte – quanto meno formalmente – si discostino dalla Conclusioni presentate dall'AG. Mentre quest'ultimo, infatti, ricorrendo al concetto di "qualità della legge" mutuato dalla giurisprudenza della Corte EDU, si è ampiamente soffermato sulle caratteristiche necessarie ad un sostanziale rispetto del principio di legalità (par. 108 ss.), la CGUE sviluppa le riflessioni senza ricorrere a tali precedenti, rafforzando la propria autonomia come Corte dei diritti.

[59] *Digital Rights Ireland*, Sentenza, par. 61.

[60] Dir. 2006/24, *Considerando* n. 25.

[61] Dir. 2006/24, art. 7.

sacrificio richiesto, in definitiva, indicazioni così vaghe sembravano confermare – anziché smentire – questa fragilità di sistema, tanto da lasciare aperta la domanda su quali avrebbero dovuto essere, in effetti, le procedure per poter ottenere l'accesso ai dati in modo legittimo.

Queste garanzie sono state in qualche modo elaborate attraverso un ragionamento *a contrario*, delineando le carenze della disciplina sulla sicurezza del trattamento dei dati e sulle condizioni di accesso e di utilizzo delle informazioni. A tal proposito, quanto al momento della conservazione, è interessante sottolineare, come si possa documentare un "ritorno" alla logica garantistica del primo "pacchetto privacy" (Dir. 95/46 e Dir. 2002/58). Per assicurare un più elevato livello di tutela, la Corte ha insistito sull'esigenza di dislocare i *database* sul territorio dell'Unione, così da poter affermare in via diretta gli *standards* e la giurisdizione comunitaria[62]. Quanto all'accesso, invece, ci si è soffermati principalmente sui presupposti all'azione di polizia, in termini di legittimazione, pertinenza e controllo. *In primis*, si è osservato come non fosse stato previsto alcunché circa l'opportunità di prestabilire e limitare l'utilizzo di questi strumenti solo a determinati soggetti[63], mancando così di individuare in modo chiaro le autorità potenzialmente abilitate a ricorrervi[64]. In secondo luogo, si è notato come non fossero stati nemmeno contemplati dei limiti all'ulteriore utilizzo dei dati ottenuti[65], ammettendo indirettamente che, una volta disponibili, gli stessi potessero finire per soddisfare fini diversi da quelli per cui erano stati conservati. Infine – quanto all'osservanza dei più elementari meccanismi di *checks and balances* – si era tralasciato il fatto che l'accesso avrebbe dovuto essere subordinato all'autorizzazione di un giudice o di una autorità indipendente[66]. Si è, quindi, incoraggiato un ritorno a forme di controllo effettivo, onde evitare che l'affermarsi delle autocertificazioni potesse tradursi in un opaco autoreferenzialismo degli inquirenti[67]. In altri termini, non si è fatto altro che confermare la centralità del principio di legalità e

[62] *Digital Rights Ireland*, Sentenza, par. 68.

[63] *Digital Rights Ireland*, Sentenza, par. 62.

[64] Commissione europea, relazione della Commissione al Consiglio e al Parlamento europeo, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE),* cit., 10 ss.; COCQ - GALLI, *Comparative law paper on data retention regulation in sample of EU Member States*, 2013, 13ss.

[65] *Digital Rights Ireland*, Sentenza, par. 61.

[66] *Digital Rights Ireland*, Sentenza, par. 62.

[67] Commissione europea, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE),* cit., 10 ss.; COCQ - GALLI, *Comparative law paper on data retention regulation in sample of EU Member States*, cit., 13ss.

della riserva di giurisdizione anche per queste misure, in pieno accordo con le tradizionali garanzie dello Stato di diritto.

La sentenza *Digital Rights*, rilevando queste ed altre[68] lacune, è giunta a dichiarare l'invalidità dell'intera Direttiva e il principale merito di questa pronuncia è quello di aver individuato dei principi di tutela anche per le procedure inerenti la *data retention*. Con quella prima vittoria si sperava dunque che quanto stabilito in sede europea avrebbe trovato spazio a livello nazionale, affinando una maggior sensibilità per questa nuova *digital rule of law*[69].

5. …solo per interventi circoscritti e mirati

L'annullamento della Direttiva 2006/24 ha segnato senz'altro un punto di non ritorno. Per la prima volta, infatti, è stata dichiarata l'invalidità di un intero atto perché contrario alle previsioni della Carta di Nizza: una conclusione che certo prometteva di aver un suo peso nella futura regolamentazione della materia. A riguardo, la sentenza *Digital Rights* ha sviluppato un'attenta analisi sui diritti garantiti dagli artt. 7 e 8 della Carta, accostando ai profili procedurali relativi all'accesso più stringenti limitazioni sul piano sostanziale[70].

A tal proposito, oltre ad un intendimento meno formale della c.d. "qualità della legge"[71], i parametri offerti dal § 1 dell'art. 52 della Carta hanno permesso di soffermarsi sulla portata dei principi di necessità e proporzionalità[72], concentrando l'analisi sulla compatibilità della *data retention* con il contenuto essenziale dei diritti considerati.

Quest'ulteriore dimensione d'indagine ha il merito di arricchire e completare i precedenti rilievi, andando ad individuare dei limiti perentori

[68] *Infra* par. 5.

[69] ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?* in *Quad. Cost*., 2014; VON DANWITZ, *The Rule of Law in the Recent Jurisprudence of the ECJ*, in *Fordham ILJ*, 2014, 1332-1333.

[70] POLLICINO, *Diritto all'oblio e conservazione dei dati*, cit., par. 1. La Corte, infatti, come osserva l'Autore, per la prima con questa sentenza ha affrontato in modo distinto il profilo relativo alla possibile violazione di diritti – e la riflessione sui loro contenuti essenziali – e il giudizio di proporzionalità: un ragionamento che, così strutturato, ha permesso – come si vedrà – di ammettere il ricorso alle misure di *data retention*, purché nel rispetto dei principi e limiti previsti dal diritto europeo quanto ai fini e alle garanzie.

[71] *Digital Rights Ireland*, Conclusioni, 20.

[72] *Digital Rights Ireland*, Sentenza, par. 45 ss.

all'utilizzo di queste misure «*all'interno di una società democratica*»[73]. Si è osservato, infatti, come i dati conservati, presi nel loro insieme, permettano una puntuale profilazione degli individui interessati, portando a conclusioni molto precise riguardo la loro vita privata. Una situazione (e una sensazione[74]) di continua sorveglianza, dunque: l'esatto opposto di quanto affermato dal principio di riservatezza su cui si è da sempre fondato il contenuto della *privacy*. Si è reso necessario, pertanto, comprendere a quali condizioni sia ammissibile il ricorso a questi sistemi di controllo.

Un'analisi sommaria dell'intera dinamica avrebbe forse portato a concludere che il momento più insidioso quanto alla tutela della sfera privata si concentrasse nell'autorizzazione all'accesso, sottovalutando invece l'incidenza della semplice conservazione dei dati. Sebbene simili argomenti avessero trovato spazio in una pronuncia del 2005[75], tale impostazione, alla luce delle successive evoluzioni giurisprudenziali circa la portata di queste misure, non poteva più essere né condivisa né giustificata. Venivano archiviati, infatti, i dati di traffico di pressoché tutta la popolazione europea dotata di un'utenza[76]: una condizione che certo sollecitava ad un attento scrutinio circa la necessarietà e la proporzionalità degli obblighi imposti. Si è cominciato ad intuire come il momento stesso della conservazione rappresentasse di per sé un'insidia alle garanzie dell'art. 8 e così (indirettamente) dell'art. 7[77]. Un ulteriore trattamento dei metadati laddove

[73] Letteralmente dall'art. 15, par. 1, dir. 2001/58. A fronte del fatto che l'utilizzo delle misure di *data retention* era stato effettivamente esteso anche a reati di minor gravità (basti pensare all'inclusione, da parte del *Regulation of Investigatory Powers Act* inglese di fattispecie come il «*benessere economico del Regno Unito*», piuttosto che «*la prevenzione dei danni alla salute fisica o mentale nei casi di emergenza*» o le «*indagini sui casi di errori giudiziari*») si è avvertito il rischio che l'adozione di questi mezzi in termini estensivi, astrattamente, potesse davvero avere delle implicazioni preoccupanti. In tal senso, è interessante richiamare un passaggio delle Conclusioni dell'AG Saugmandsgaard Øe, in cui ipotizza che le misure di sorveglianza adottate contro il terrorismo vengano rivolte alla prevenzione dei disturbi psichiatrici, stigmatizzando questa categoria di persone, oppure – in uno scenario più *orwelliano* – siano volte ad individuare gli oppositori al Governo in carica (par. 257-258). Un quadro che, per quanto ipotetico, rappresenta in modo efficace il nòcciolo della questione.

[74] *Digital Rights Ireland*, Sentenza, par. 37; *Tele2 Sverige*, Sentenza, par. 100.

[75] *Irlanda c. Parlamento e Consiglio*, Sentenza, par. 80-84.

[76] Dir. 2006/24, art. 5. *Digital Rights Ireland*, Sentenza, par. 56-57.

[77] In particolare, nelle Conclusioni dell'AG – poi, peraltro, riprese dalla Corte – merita particolare attenzione la riflessione fatta circa la durata della conservazione e l'eccessiva discrezionalità concessa al legislatore statale a riguardo. A fronte del fatto che la disciplina prevista dalla dir. 2006/24, Nonostante rispetto all'ordine logico delle questioni differisca, la piena cognizione di questa dimensione del problema è accuratamente riportata tanto nelle Conclusioni dell'AG, quanto nella decisione della Corte. Per un approfondimento

la Direttiva 2002/58 ne prevedeva la cancellazione – oltre alle criticità legate agli accessi *secundum legem* – apriva infatti anche nuovi scenari di rischio, legati al possibile uso illecito delle informazioni[78].

Tale situazione ha invitato a riconsiderare lo stato dell'arte, evidenziando soprattutto le possibili linee evolutive per la disciplina della materia. Quanto all'opportunità di individuare limiti sostanziali all'utilizzo di queste misure, va riscontrato come la Direttiva 2006/24, da un lato, avesse escluso la possibilità di registrare e conservare il contenuto delle comunicazioni[79] e, dall'altro, avesse comunque previsto la presenza di *standards* di protezione minimi per il trattamento dei dati personali[80]. Pur comportando delle gravi ingerenze, la normativa dunque non sembrava scalfire il contenuto essenziale dei diritti in questione e questo permetteva – quanto meno in astratto – di ammettere la *data retention*, purché nel rispetto dei principi che via via si andavano esplicitando. Tuttavia, ponendo in deroga la disciplina prevista dalle direttive 96/45 e 2002/58, ed imponendo degli obblighi specifici laddove era stata prevista solo un'eventuale facoltà, la portata e l'utilizzo di tali mezzi avrebbero dovuto essere limitati al minimo necessario[81]. Pur riconoscendo infatti l'utilità di detti sistemi per il contrasto alla criminalità organizzata, un simile obiettivo d'interesse generale non era in grado di giustificare di per sé la necessarietà della misura. Sarebbe servito, invece, individuare in modo oggettivo la relazione tra la minaccia temuta e le informazioni conservate[82], nonché le situazioni in cui ricorrere alle stesse[83].

Sotto questi profili gli arresti del caso *Digital Rights* sono stati integrati e completati dalla recente sentenza *Tele2 Sverige*. Invalidata la "Direttiva madre", infatti, erano rimaste comunque in vigore le leggi statali che ne avevano dato attuazione, le quali molto spesso avevano ereditato – quando ancora non aggravato[84] – i vizi contestati alla normativa europea. Si trattava dunque di chiarire come e a che condizioni la legislazione nazionale dovesse

---

comparatistico tra le due argomentazioni, si rimanda a TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. It.*, 2014.

[78] *Digital Rights Ireland*, Sent., par. 66. Tele2 *Sverige*, Sentenza, par. 122. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto*, cit., 1230-1231).

[79] Dir. 2006/24, art. 5, par. 2.

[80] Dir. 2006/24, art. 7.

[81] *Digital Rights Ireland*, Sentenza, par. 51-52; *Tele2 Sverige*, Sentenza, par.116-120.

[82] *Digital Rights Ireland*, Sentenza, par. 58.

[83] *Digital Rights Ireland*, Sentenza, par. 59.

[84] BIGNAMI, *Privacy and Law Enforcement in the European Union: the Data Retention Directive*, cit., 233; VEDASCHI - LUBELLO, *Data Retention and its Implications for the Fundamental Right to Privacy*, cit., 20; COCQ - GALLI, *Comparative law paper on data retention regulation in a sample of EU Member States*, cit., 11.

conformarsi ai principi elaborati dalla giurisprudenza comunitaria, delineando soprattutto in concreto i limiti al legittimo utilizzo delle misure in questione. A tal proposito, se individuare le carenze procedurali poteva essere un'operazione agile, delineare dei limiti perentori all'utilizzo della *data retention* ha richiesto qualche ulteriore riflessione. Come ricordato con riferimento alla Direttiva, la conservazione generalizzata e indifferenziata dei metadati avrebbe continuato a coinvolgere una tale quantità di persone che quella che si sarebbe voluta come un'*eccezione* si sarebbe, di fatto, trasformata nella *regola*[85]. Bisognava dunque riconsiderare le situazioni idonee ad ammettere il ricorso a questi strumenti, onde evitare la legittimazione di un regime di sorveglianza. L'obbligo di *data-collecting* – si osservava – veniva infatti prescritto in un momento in cui gli utenti interessati potevano non avere nulla a che fare con i fenomeni criminosi che si intendeva perseguire[86]: una circostanza sufficiente ad insistere per un risoluto invito alla cautela.

Premesso che il periodo di conservazione avrebbe dovuto essere parametrato in funzione di criteri oggettivi[87] – senza così sconfinare in quegli eccessi di discrezionalità in precedenza ammessi dalla Direttiva Frattini – era necessario ora ricostruire il quadro normativo entro cui si sarebbe andati a ragionare. Con il venir meno di tale disciplina, il riferimento

---

. [85] Già nella sent. *Digital Rights Ireland*, si è osservato come, rispetto alla dir. 2006/24, l'«*articolo 3, in combinato disposto con l'articolo 5, paragrafo 1, della stessa, la conservazione di tutti i dati relativi al traffico riguardante la telefonia fissa, la telefonia mobile, l'accesso a Internet, la posta elettronica su Internet nonché la telefonia via Internet. Pertanto, essa concerne tutti i mezzi di comunicazione elettronica il cui uso è estremamente diffuso e di importanza crescente nella vita quotidiana di ciascuno. Inoltre, conformemente all'articolo 3, la Direttiva riguarda tutti gli abbonati e gli utenti registrati. Essa implica pertanto un'ingerenza nei diritti fondamentali della quasi totalità della popolazione europea.*» (par. 56). La pronuncia *Tele2 Sverige*, riprendendo il punto, ha dunque concluso che qualora la normativa nazionale, in accordo con le prescrizioni invalidate, fosse finita con il prevedere una conservazione generale e indifferenziata dei metadati, «*porta alla conseguenza che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce la regola, quando invece il sistema istituito dalla Direttiva 2002/58 esige che tale conservazione dei dati sia l'eccezione*» (par. 104), violando il principio di necessità.

[86] DE MINICO, *Le libertà fondamentali in tempo di ordinario terrorismo*, cit., 4. L'Autrice sottolinea, infatti, come, in generale, l'utilizzo dei mezzi di contrasto al terrorismo chieda di mediare tra valori antagonisti in base alla proporzionalità di inveramento del rischio. Questo implica che la valutazione, dunque, consideri situazioni *disallineate in ragione del tempo, disomogenee nel sacrificio e nel vantaggio:* si nota come «*infatti, il danno attuale e certo sopportato dal detentore del diritto alla riservatezza ha un peso maggiore del vantaggio procurato ai titolari del diritto alla sicurezza*».

[87] *Digital Rights Ireland*, par. 63-64.

era tornato ad essere l'art. 15 della Direttiva 2002/58, rispristinando dunque la *facoltà* di adottare le misure in questione solo per specifici motivi di interesse pubblico. La previgente regolamentazione, tuttavia, aveva lasciato agli Stati una certa discrezionalità nell'individuare i reati presupposto, ammettendo dunque la possibilità di un'interpretazione estensiva delle ipotesi inizialmente contemplate. Questa autonomia era stata intesa in vari modi, tant'è che ad un'indagine trasversale si è potuto osservare come la scelta di criteri differenti avesse finito con l'includere fattispecie tra loro molto diverse per natura e gravità[88]. Alla luce dei principi di necessità e proporzionalità (questa volta approfonditi per l'individuazione di un vero e proprio limite[89]) era chiaro che non tutti i crimini, ma solo quelli più gravi potessero ammettere il ricorso a simili strumenti[90]. Con una sentenza "additiva"[91], la Corte ha dunque integrato la portata dell'art. 15 con i principi elaborati dalla sua precedente giurisprudenza, limitando l'utilizzo di queste misure soltanto alle ipotesi menzionate dalla norma, da intendersi come esaustive[92]. A questo primo limite, si sono aggiunte ulteriori considerazioni circa la necessità di una relazione tra i dati raccolti e i soggetti interessanti, escludendo – a differenza del passato – che la conservazione possa essere rivolta nei confronti dell'intera popolazione. Non più misure generali, dunque, ma interventi mirati sulla base di fondati sospetti, prevendendo inoltre, senza pregiudizio delle indagini, il dovere d'informativa nei confronti degli interessanti, così da assicurare *ex post* un effettivo esercizio del diritto al ricorso[93].

La saga sulla *data retention*, dunque, sembra giungere ad un approdo in assoluta controtendenza con il generale clima securitario degli ultimi anni[94]. La Corte di giustizia, infatti, elaborando in via ermeneutica condizioni e

[88] Si rimanda inoltre alla relazione della Commissione al Consiglio e al Parlamento europeo, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE)*, cit., 6 ss.; COCQ - GALLI, *Comparative law paper on data retention regulation in a sample of EU Member States*, cit., 11.

[89] POLLICINO - 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*, *Dir. Pen. Contemporaneo*, 2017, spec. 6-9.

[90] *Tele2 Sverige*, Sentenza, par. 115.

[91] TIBERI, *Il caso* Tele2 Sverige/Watson: *un'*iconica *sentenza della Corte di Giustizia nella saga sulla* data retention, in *Quad. cost.*, 2017, 436.

[92] *Tele2 Sverige*, Sentenza, par. 90 e 115.

[93] *Tele2 Sverige*, Sentenza, par. 121.

[94] POLLICINO - VIGEVANI, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza* Tele2 Sverige *della Corte di giustizia UE*, in *Forum QC*, 16 gennaio 2017.

limiti per queste misure, ha contribuito a normalizzarne l'utilizzo secondo le garanzie proprie dello Stato di diritto.

6. Conclusioni

Quello che si prospetta ora è uno scenario incerto sotto molti punti di vista[95]. L'elaborazione delle garanzie sulla *data retention* si è accompagnata infatti ad un sempre crescente stato d'allarme, e bisognerà quindi attendere per vedere le reazioni che accompagneranno il recepimento dei principi elaborati dalle sentenze *Digital Rights Ireland* e *Tele2 Sverige*[96].

Quel che è certo è che questa giurisprudenza ha contribuito a rafforzare la tenuta della *rule of law* lì dove la serietà della minaccia e le potenzialità dei mezzi rischierebbero di far arretrare delle conquiste di civiltà che innervano la cultura giuridica europea[97]. I parametri individuati in via ermeneutica, infatti, con il tempo si stanno affermando come una sorta di paradigma: criteri per valutare non solo la "bontà" delle normative interne ma anche il livello di tutela assicurato dai Paesi terzi. Nell'ambito delle relazioni esterne, infatti, dopo la cassazione degli accordi con gli Stati Uniti nel già citato caso *Schrems*[98], la

[95] Soffermandosi solo sulle iniziative europee, basti richiamare la recente approvazione della dir. 2016/817/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e della dir. (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. Per alcuni accenni in dottrina si rimanda a RUBECCHI, *Sicurezza, tutela dei diritti fondamentali nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it*, 2016; TIBERI, *La Direttiva UE sull'uso dei dati del codice di prenotazione (PNR) nella lotta al terrorismo e ai reati gravi*, in *Quad. Cost.*, 2016, 591.

[96] ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?* cit.; TIBERI, *Il caso* Tele2 Sverige/Watson: *un'*iconica *sentenza della Corte di Giustizia nella saga sulla* data retention, cit., 437.

[97] Da un punto di vista prospettivo, infatti, questi arresti hanno contribuito a tornare a quell'approccio garantista che da sempre ha contraddistinto l'esperienza europea in materia di *protezione* dei dati personali (VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto*, cit., 1241). Non da ultimo, i principi sanciti nella pronuncia *Digital Rights Ireland*, hanno costituito una sorta di *trait-d 'union* tra la giurisprudenza della CGUE e l'esperienza della Corte europeo dei diritti dell'uomo, la quale ne ha ripreso i passaggi nella sua successiva sent. 12 gennaio 2016, *Szabó e Vissy/Ungheria*, par. 68.

[98] *Schrems/Data Protection Commissioner*, C-362/14, già riportata in apertura (nota n. 1).

Corte ha confermato il proprio orientamento anche nella sua ultima pronuncia relativa alle intese con il Canada per il trattamento dei dati PNR[99].

Non è questa la sede per valutare l'opportunità di una simile proiezione "globale" degli *standards* comunitari[100]. Quel che qui interessa è il merito della riflessione svolta: il fatto che per la sua sensibilità, l'esperienza continentale si stia consolidando come una vera e propria "lezione"[101]. Affermando la portata delle libertà individuali in questi nuovi scenari, essa ha gradualmente ridefinito i limiti delle ingerenze pubbliche nella sfera privata, contrastando un ormai troppo ripetuto paradigma del controllo totale. Si va, dunque, verso una *digital rule of law* europea? Forse. Il traguardo raggiunto, per quanto precario, non sembra essere di poco conto.

[99] *Parere 1/15*, 26 luglio 17, Avis-1/15

[100] *Ex multis*, KUNER, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, in *Legal Studies Reasearch Paper Series*, 14/2016; SCHULHOFER, *An international right to privacy? Be careful what you wish for*, in *IJCL*, 2016.

[101] FABBRINI, *Human Rights in the Digital Age: The European Court of Justice in the Data Retention Case and Its Lessons for the Privacy and Surveillance in the United States*, cit.

BIBLIOGRAFIA

Articoli:
ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?* in *Quad. Cost*., 2014
BARTOLI, *Regola ed eccezione nel contrasto al terrorismo internazionale* in *Dir. pubbl.*, 2010
BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della* privacy, in *Giur. cost.*, 2016
BIGNAMI, *Privacy and Law Enforcement in the European Union: the Data Retention Directive*, in *Chi. J. Intl. L.*, 2007
BIGNAMI, *Protecting Privacy Against the Police in the European Union : The Data Retention Directive*, in BOT (a cura di), *Melanges en l'Honneur de Philippe Leger: le droit a la mesure de l'homme*, Parigi, 2006
BRONZINI, *La Carta dei diritti dell'Unione europea come strumento di rafforzamento e protezione dello Stato di diritto*, in *Pol. dir.*, 2016
CARTABIA, *I diritti in Europa: la prospettiva della giurisprudenza costituzionale italiana*, in *Riv. Trim. Dir. Pubb*., 2015
COCQ - GALLI, *Comparative law paper on data retention regulation in sample of EU Member States*, 2013
DANIELE, *Diritto dell'Unione europea*, Torino, 2014
DE BÚRCA, *After The EU Charter of Fundamental Rights: The Court Of Justice As A Human Rights Adjudicator?*, in *Masst. J. Eur. & Comp. L.*, 2013
DE MINICO, *Le libertà fondamentali in tempo di ordinario terrorismo*, in *federalismi.it*, 2015
DONATI, *Art. 8*, in BIFULCO, CARTABIA, CELOTTO (a cura di), *L'Europa dei diritti*, Bologna, 2001
DURICA, *Directive on the Retention of Data on Electronic Communication in the Ruling of the Constitutional Courts of the EU Member States and Efforts for its Renewed Implementation*, in *TQL*, 2013
FABBRINI, *Human Rights in the Digital Age: The European Court of Justice in the Data Retention Case and Its Lessons for the Privacy and Surveillance in the United States*, in *Harv. Hum. Rts. J.*, 2015
FEILER, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, in *EJLT*, 2010
FONTANELLI, *La Corte di Giustizia e il "favor communitatis". Il percorso della giurisprudenza della Corte di Giustizia delle Comunità europee sul fondamento normativo degli atti dell'Unione*, in *Riv. it. dir. pubbl. comunit.*, 2010
GROPPI, *Art. 7*, in BIFULCO, CARTABIA, CELOTTO (a cura di), *L'Europa dei diritti*, Bologna, 2001
JAKAB, *The rule of law, fundamental rights and the terrorist challenge in Europe and elsewhere*, in id., *European Constitutional Language*, Cambridge, 2016
KOSTA, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Protection Directive with the Rights to Privacy and Data Protection*, in *Scripted*, 2013
KUNER, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, in *Legal Studies Reasearch Paper Series*, 14/2016
LESSIG, *Reading the Constitution in the Cyberspace*, in *Emory Law Review*, 45/3, 1996
MASTROIANNI, *Art. 47 TUE*, in TIZZANO (a cura di), *Trattati dell'Unione europea e della Comunità europea*, Milano, 2004

MITSILEGAS, *The Transformation of Privacy in an Era of Pre-emptive Surveillance*, in *Tilburg L. Rev.*, 2015
MURPHY, *EU Counter-Terrorism Law. Pre-Emption and the Rule of Law*, Oxford-Portland, 2012
PALADINI, *I conflitti fra pilastri dell'Unione europea e le prospettive del Trattato di Lisbona*, in *Dir. UE*., 2010
PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016
POLLICINO - 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 *Dir. Pen. Contemporaneo*, 2017
POLLICINO - VIGEVANI, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza* Tele2 Sverige *della Corte di giustizia UE*, in *Forum QC*, 16 gennaio 2017
POLLICINO, *Diritto all'oblio e conservazione dei dati. La Corte di Giustizia a piedi uniti: verso un* digital right to privacy, in *Giur. cost.*, 2014
POLLICINO, *I nuovi scenari della tutela della privacy nell'era della digitalizzazione alla luce delle recenti pronunce sul diritto all'oblio*, in *federalismi.it*, 2015
POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *federalismi.it*, 2014
RUBECCHI, *Sicurezza, tutela dei diritti fondamentali nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it*, 2016
SAJÒ - RYAN, *Judicial Reasoning and New Technology*, in POLLICINO-ROMEO (a cura di), *The Internet and Constitutional Law: The protection of fundamental rights and constitutional adjudication in Europe*, Londra-New York, 2016
SCHULHOFER, *An international rights to privacy? Be careful what you wish for*, in *IJCL*, 2016
TIBERI, *Il caso* Tele2 Sverige/Watson: *un'*iconica *sentenza della Corte di Giustizia nella saga sulla* data retention, in *Quad. cost.*, 2017
TIBERI, *La Direttiva UE sull'uso dei dati del codice di prenotazione (PNR) nella lotta al terrorismo e ai reati gravi*, in *Quad. Cost.*, 2016
TIBERI, *Riservatezza e protezione dei dati personali*, in CARTABIA (a cura di), *I diritti in azione*, Bologna, 2007
TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. It.*, 2014
TUORI, *The insecure security constitution*, in id., *European Constitutionalism*, Cambridge, 2015
VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, in *Dir. pubbl. comp. eur.*, 2014
VON DANWITZ, *The Rule of Law in the Recent Jurisprudence of the ECJ*, in *Fordham ILJ*, 2014

Decisioni Cgue:
Commissione/Austria, 29 luglio 2010, causa C-189/2009
Commissione/Grecia, 26 novembre 2009, causa C-211/09
Commissione/Irlanda, 26 novembre 2009, causa C-202/09
Commissione/Svezia, 30 maggio 2013, causa C-270/2011
Commissione/Svezia, 4 febbraio 2010, causa C-185/09
Digital Rights Ireland e a./Minister for Communications, Marine and Natural Resources e a., 8 aprile 2014, cause riunite C-293/12 e C-594/12

Google Spain SL e Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 13 maggio 2014, C-131/12
Irlanda/Parlamento e Consiglio, 10 febbraio 2009, causa C-301/06
Parere 1/15, 26 luglio 17, Avis 1/15
Parlamento europeo/Consiglio dell'Unione Europea (PNR), 30 maggio 2006, cause riunite C-317/04 e C-318/04
Schrems/Data Protection Commissioner, 6 ottobre 2015, C-362/14
Tele2 Sverige/Post och telestyrelsen e Secretary of State for the Home Department / Watson e a., 21 dicembre 2016, cause riunite C-203/15 e C-698/15
Yassin Abdullah Kadi, Al Barakaat International Foundation/Consiglio, 3 ottobre 2008, cause riunite C-402/05 P e C-415/05 P

Decisioni Tribunale UE:
Yusuf, Al Barakaat International Foundation/Consiglio, 21 settembre 2005, causa T-306/01
Kadi/Consiglio e Commissione, 21 settembre 2005, causa T-315/01

Decisioni Corte Europea dei Diritti dell'Uomo:
Szabó e Vissy/Ungheria, 12 gennaio 2016

Documenti UE:
Consiglio dell'UE, *Dichiarazione sulla lotta al terrorismo*, doc. 7906/04, 31 marzo 2004
Consiglio dell'UE, *EU Plan of Action on Combating Terrorism*, doc. 10586/04, 15 giugno 2004
Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo*, doc. 8958/04, 20 dicembre 2004
Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo*, doc. 15098/04, 23 novembre 2004.
Commissione al Consiglio e al Parlamento europeo, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE),* COM (2011)
Consiglio dell'UE, *Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detect*, doc. 8958/04, 20 dicembre 2004.
Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo - Base giuridica*, doc. 7688/05, 5 aprile 2005
Direttiva 2002/58/CE, del 12 luglio 2002
Direttiva 2006/24/CE, del 15 marzo 2006