LA CORTE DI GIUSTIZIA CONSIDERA LA DIRETTIVA EUROPEA 2006/24 SULLA C.D. "DATA RETENTION" CONTRARIA AI DIRITTI FONDAMENTALI. UNA LUNGA STORIA A LIETO FINE?

Roberto Flor

Abstract

L'epocale sentenza della Corte di Giustizia sulla c.d. data *retention* ha invalidato la direttiva 2006/24, in quanto non compatibile con i limiti imposti dal rispetto del principio di proporzionalità, alla luce degli artt. 7, 8 e 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea. Ne consegue che se le norme interne dei singoli Stati, come nel caso italiano, non rispettano gli standards ricavabili dalla sentenza, esse dovrebbero essere disapplicate per contrasto con il diritto europeo. La soluzione più immediata, ma purtroppo ad effetto "locale", vede come protagonista il legislatore nazionale, il quale dovrebbe intervenire ed adattare l'attuale disciplina agli standards elaborati dalla Corte di Giustizia. Sarebbe però maggiormente auspicabile un intervento del legislatore europeo, nell'ambito di una più ampia politica criminale dell'Unione, considerando l'utilità e, spesso, l'indispensabilità della *data retention* nell'odierna società dell'informazione, in particolare per prevenire e accertare gravi reati lesivi di importanti beni giuridici.

1. Una premessa necessaria.

Il 18 aprile 2011 la Commissione europea ha presentato la relazione al Consiglio ed al Parlamento europeo avente ad oggetto la "Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24)"[1].

L'analisi della Commissione si è basata sulle comunicazioni relative al recepimento dell'atto europeo trasmesse da venticinque Stati membri.

In Repubblica Ceca, Germania e Romania le rispettive Corti costituzionali avevano dichiarato incostituzionali le leggi nazionali di attuazione della stessa direttiva[2].

Il rapporto ha evidenziato, *in primis*, che quest'ultima ha assicurato che la maggior parte degli Stati membri provvedessero alla conservazione dei dati, ma non ha garantito di per sé che i dati conservati fossero immagazzinati, estratti e usati nel pieno rispetto del diritto alla vita privata e del diritto alla protezione dei dati personali.

In secondo luogo, essendo stata delegata agli Stati la previsione delle garanzie per i diritti fondamentali, esso ha rilevato la carenza di un approccio comune, anche con riferimento alla limitazione delle finalità della *data retention*, ai periodi di conservazione e alle previsioni di contributi economici statali per gli operatori e i fornitori di servizi destinatari dell'obbligo di conservazione dei dati.

In terzo luogo, la Commissione, prendendo atto, da un lato, proprio del caso irlandese – a seguito del quale la questione della validità della direttiva è stata rimessa alla Corte di Giustizia[3] – e, dall'altro lato, dell'intervento del Garante europeo per la protezione dei dati personali – il quale ha affermato che la direttiva «non ha armonizzato la legislazione nazionale» e che il ricorso alle informazioni conservate non si limita allo stretto necessario per contrastare i reati gravi[4] – ha sollevato dubbi sul rispetto della vita privata e della riservatezza e ha evidenziato la necessità di norme più severe anche in materia di sicurezza e protezione dei dati, basandosi sulle critiche, emerse anche a seguito delle citate sentenze delle Corti costituzionali nazionali, all'obbligo di conservazione dei dati così come previsto dalla legislazione vigente.

La Commissione, però, ha sostenuto l'indispensabilità della *data retention* nell'ambito delle investigazioni per l'accertamento e la prevenzione di gravi reati[5], anche tramite una più recente statistica[6], nonché attraverso la presentazione di un documento in cui dimostra la necessità della conservazione dei dati per la lotta contro gravi forme di criminalità[7]

Per questo motivo, e in un momento storico di massima allerta contro attacchi terroristici, essa ha sottolineato l'opportunità di esaminare la conservazione dei dati nell'UE alla luce dei principi di necessità e proporzionalità, tenuto conto e nell'interesse della sicurezza nazionale, del buon funzionamento del mercato interno e del rafforzamento del rispetto della vita privata, nonché del diritto fondamentale alla protezione dei dati personali, proponendo la revisione del quadro giuridico in materia di conservazione dei dati sulla base di alcune raccomandazioni, fra le quali: a) sostenere e disciplinare la conservazione dei dati quale misura di sicurezza; b) garantire la proporzionalità nell'intero processo di immagazzinamento, estrazione e uso dei

[1] V. COM(2011) 225 definitivo

[2] Su tali vicende, anche per gli opportuni riferimenti bibliografici, si consenta di rinviare a R. Flor, *Le recenti sentenze del Bundesverfassungsgericht e della Curtea Constituțională sul data retention*, in L. Violante, T. Galiani, A. Merli, *Oggetto e limiti del potere coercitivo dello Stato nelle democrazie costituzionali*, in *Annali della facoltà giuridica*, Camerino, 2013, 308-329 e R. Flor, Data retention *e limiti al potere coercitivo dello Stato in materia penale: le sentenze del Bundesverfassungsgericht e della Curtea Constituțională,* in *Cass. pen.*, 2011, 1952-1969; cfr. altresì R. Flor, *Data retention rules under attack in the European Union? (Po sulmohen rregullat mbi ruajtjen e të dhënave në Bashkimin Evropian?)*, in *Illyrius*, 2012, 69-86; R. Flor, *La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del Bundesverfassungsgericht e della Curtea Constituțională su investigazioni ad alto contenuto tecnologico e* data retention, in L. Picotti, F. Ruggieri, *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, 32-49.

[3] Vedi infra, 2.

[4] Cfr. COM(2011) 225 definitivo, 33, nota 126.

[5] Gli stessi Stati membri, in generale, hanno affermato che la conservazione dei dati è «quanto meno utile, e in alcuni casi indispensabile, per prevenire e contrastare la criminalità, compresa la protezione delle vittime e l'assoluzione degli imputati innocenti». La Repubblica ceca, ad esempio, ha considerato la conservazione dei dati «assolutamente indispensabile in un gran numero di casi»; la Slovenia ha indicato che l'assenza di dati conservati «paralizzerebbe l'attività delle agenzie di contrasto»; l'Ungheria ha affermato che era «indispensabile nelle attività ordinarie [delle agenzie di contrasto]»; il Regno Unito ha descritto la disponibilità di dati relativi al traffico come «assolutamente essenziale … per condurre indagini riguardanti il terrorismo e i reati gravi». Vedi COM(2011) 225 definitivo, 25, nota 105.

[6] Vedi http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/statistics_on_requests_for_data_under_the_data_retention_directive_en.pdf

[7] Vedi http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf

dati[8].

Alla data di presentazione del rapporto sulla valutazione dell'applicazione della direttiva sulla c.d. *data retention* erano stati proposti ricorsi riguardanti la conservazione dei dati anche dinanzi alle Corti delle leggi di Bulgaria, Cipro e Ungheria[9].

Più di recente, con l'ordinanza del 26 settembre 2013 la Corte costituzionale slovena[10], dovendosi pronunciare in merito ad una questione di costituzionalità relativa alla legge sulle comunicazioni elettroniche, adottata dal Parlamento sloveno nel 2012, in attuazione della citata direttiva europea, ha sospeso il giudizio in attesa della sentenza interpretativa della Corte di Giustizia, richiesta dalle Corti irlandese e austriaca[11].

L'epocale sentenza in commento della Corte di Giustizia giunge, dunque, in un delicato momento storico, in cui il ricorso alle "investigazioni tecnologiche"[12] e all'accessibilità a dati ed informazioni trasmesse per via telefonica e telematica deve confrontarsi con le esigenze di accertamento dei reati e di ricerca della prova, da un lato, e di rispetto delle garanzie e dei diritti inviolabili dei cittadini, dall'altro lato, nel contesto più ampio della riforma in atto, a livello europeo, di tutta la disciplina in materia di tutela della *privacy*, attraverso un *corpus* unico di norme[13].

[8] Nell'ambito della valutazione d'impatto di una futura proposta in materia di conservazione dei dati, nel rispetto del principio di proporzionalità e con l'obiettivo di contrastare i reati gravi, la Commissione ha fatto riferimento: alla coerenza tra la limitazione delle finalità della conservazione dei dati e le categorie di reati per le quali si possono consultare e usare i dati conservati; alla maggiore armonizzazione ed eventuale riduzione dei periodi di conservazione obbligatoria dei dati; alla garanzia di un controllo indipendente delle richieste di accesso e del regime generale di conservazione dei dati e di accesso agli stessi applicato in tutti gli Stati membri; alla limitazione delle autorità autorizzate a consultare i dati; alla riduzione delle categorie di dati da conservare; agli orientamenti in materia di misure di sicurezza tecniche e organizzative per l'accesso ai dati, comprese le procedure di trasmissione; alla elaborazione di procedure di quantificazione e di notifica per agevolare il confronto dell'applicazione e la valutazione di uno strumento futuro. Sul possibile "impatto" di una revisione della disciplina giuridica *in subiecta materia*, che coinvolge anche Stati terzi, si veda il rapporto finale "*Research study into evidence of potential impacts of options for revising the Data Retention Directive*"commissionato dalla Direzione Generale Affari Interni (*Directorate-General Home Affairs - DG HOME*) in: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf.
Sull' "emergenza terrorismo" ed il delicato bilanciamento fra "sicurezza nazionale" e tutela dei diritti fondamentali, vedi anche "*The right to privacy in the digital age*" - Report dell' *Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37, 30 giugno 2014, in cui si evidenzia come spesso strumenti tecnologici destinati ai *digital communications surveillance programmes* trovino giustificazione proprio nella lotta al terrorismo. E' emblematica, proprio in questo contesto, l'esperienza dello Stato di Israele, che vive da 65 anni una c.d. "politica di perenne emergenza", la quale si è tradotta nell'adozione di strumenti straordinari destinati alla "sorveglianza segreta" attraverso intercettazioni e monitoraggi di dati personali, compresi quelli sensibili, non solo di sospetti terroristi, ma anche di una più ampia parte della popolazione civile. Nell'attuale società globalizzata, "dominata" e "dipendente" dalle nuove tecnologie sarebbe utopistico ritenere che una simile "attività preventiva" e di accertamento avvenga senza ricorrere agli stessi strumenti tecnologici. Una parte della dottrina ha ben evidenziato, con riferimento all'esperienza israeliana, il ruolo che dovrebbe avere il parlamento rispetto al potere esecutivo, nonché quello delle Corti Supreme, al fine di monitorare le misure da adottare, vagliare le motivazioni e i fini, la loro temporaneità e proporzionalità. Si veda, anche per gli opportuni riferimenti bibliografici, I. Marchi, *Quando l'emergenza non è più l'eccezione. L'esperienza dello Stato di Israele tra terrorismo e tutela dei diritti umani*, in *Ind. pen*., 2013, 705 – 736.

[9] Cfr. COM(2011) 225 definitivo, 23.

[10] U-I-65/13-16 (reperibile in inglese in http://www.us-rs.si/media/u-i-65-13.-.order.pdf). E' utile evidenziare che la Corte costituzionale slovena non ha escluso la propria competenza nel giudicare la legittimità costituzionale della legge di attuazione della direttiva, ma ha rilevato che la questione dipende dalla compatibilità della direttiva con gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (corrispondenti agli artt. 37 e 38 della Costituzione slovena). Nel caso di specie, considerando che erano già pendenti, in relazione alla medesima direttiva, i due ricorsi sollevati in via pregiudiziale dalla *High Court* irlandese e dalla Corte costituzionale austriaca, essa ha ritenuto di dover sospendere il giudizio, in attesa della pronuncia della Corte europea. Questa vicenda ha dimostrato come il dialogo fra le Corti, nell'attuale sistema europeo multilivello, sia divenuto tanto complesso quanto raffinato ed avanzato, soprattutto in relazione a settori la cui regolamentazione è fortemente di ispirazione europea. Cfr. E. Kosta, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection*, in *SCRIPTed,* 10:3, 2013, 339 (http://script-ed.org/?p=1163)

[11] Vedi infra, 2.

[12] Cfr. ampiamente R. Flor, *Perspectiva para novos modelos de "investigação tecnológica" e proteção de direitos fundamentais na Era da Internet – O chamado "ciberterrrorismo" como um primordial exemplo, em conjunto a problemas de definição e a luta contra terrorismo e os crimes cibernéticos* in *Revista Brasileira De Ciências Criminais*, 99, 2012, 69-100, reperibile altresì in inglese, con integrazioni bibliografiche: R. Flor, *Perspective for new types of "technological investigation" and protection of fundamental rights in the Era of Internet. The so-called "cyberterrorism" as a prime example, between problems of definition and the fight against terrorism and cybercrime*, in *Delito, pena, politica criminal y tecnologìas de la informatiòn en las modernas ciencias penales*, Salamanca, Ediciones Universidad de Salamanca, 2012, 51-76. Vedi anche R. Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung* in *Riv. trim. dir. pen. ec.*, 3, 2009, 695-716. Più di recente, in particolare con riferimento alle c.d. "*Online Searches*", cfr. F. Iovene, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont.*, 22 luglio 2014.

[13] Si fa riferimento alle concrete iniziative europee. In questa sede basti il rinvio a:
http://ec.europa.eu/justice/data-protection/index_en.htm

2. I fatti all'origine dei procedimenti principali.

Nelle cause C-293/12 e C-594/12 la Corte ha dovuto affrontare la questione della validità della direttiva 2006/24/CE[14] (che modifica la direttiva 2002/58/CE) 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, la quale prevede, in particolare, l'obbligo a carico ai fornitori di servizi nella società dell'informazione di raccogliere e conservare, per un periodo di tempo determinato, i dati generati o trattati nell'ambito delle comunicazioni telefoniche e telematiche effettuate dai cittadini europei per il perseguimento di gravi reati e ai soli fini di indagine.

In estrema sintesi, nella causa C-293/12, la ricorrente (*Digital Rights Ireland Ltd* - DRI), società volta alla promozione ed alla protezione dei diritti civili e dei diritti dell'uomo, in particolare nel contesto delle moderne tecnologie di comunicazione, ha presentato un ricorso contro due ministri del governo irlandese (*Minister for Communications, Marine and Natural Resources* e *Minister for Justice, Equality and Law Reform*), il comandante della polizia irlandese, l'Irlanda e l'*Attorney General* dello Stato irlandese, chiedendo l'annullamento dei provvedimenti in base ai quali i fornitori di servizi di telecomunicazioni erano tenuti a conservare i dati, ritenendoli incompatibili con la Costituzione irlandese e con il diritto dell'Unione e sollevando, perciò, la questione di legittimità della stessa direttiva 2006/24 rispetto alle previsioni della Carta e/o della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Nella causa C-594/12, il sig. Seitlinger ha presentato dinanzi al *Verfassungsgerichtshof* austriaco un ricorso simile, fondato sull'art. 140, par. 1, del *Bundes-Verfassungsgesetz* (B-VG), lamentando l'incostituzionalità dell'art. 102 *bis* del *Telekommunikationsgesetz* del 2003 (TKG), che prevede l'obbligo in capo ai fornitori di servizio di conservare dati di traffico telefonico e telematico.

3. Le questioni pregiudiziali.

La Corte di Giustizia ha dovuto valutare, in primo luogo, se la limitazione dei diritti dei ricorrenti derivante dalle disposizioni di cui agli artt. 3, 4 e 6 della direttiva 2006/24/CE che riguardano, rispettivamente, gli obblighi di conservazione dei dati, le regole di accesso ai dati ed i periodi di conservazione, fosse incompatibile con l'art. 5, par. 4, TUE in quanto non proporzionata, non necessaria o non adeguata per il perseguimento degli obiettivi legittimi, ossia per garantire la disponibilità dei dati di traffico telefonico e telematico a fini di indagine, accertamento e perseguimento di reati gravi e/o per garantire il corretto funzionamento del mercato interno dell'Unione europea.

Più precisamente la Corte ha dovuto affrontare le seguenti questioni:

- se la direttiva 2006/24/CE è compatibile con il diritto dei cittadini di circolare e soggiornare liberamente nel territorio degli Stati membri sancito dall'art. 21 TFUE;
- se la direttiva 2006/24/CE è compatibile con il diritto al rispetto della vita privata sancito dall'art. 7 della Carta dei diritti fondamentali dell'Unione europea e dall'art. 8 della

[14] La direttiva 2006/24 modifica, in realtà, in modo significativo la disciplina applicabile ai dati attinenti alle comunicazioni elettroniche risultante dalle direttive 95/46 e 2002/58, prevedendo che gli Stati membri introducano un obbligo di raccolta e conservazione dei dati di traffico e di ubicazione, che si inserisce nel quadro delle restrizioni al diritto alla protezione dei dati personali previste dagli artt. 13, par. 1, della direttiva 95/46 e 15, par. 1, della direttiva 2002/58. La direttiva 2006/24 ha, infatti, come primo obiettivo quello di armonizzare le normative nazionali che già impongono ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione obblighi di conservazione dei dati «a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale».

Convenzione europea dei diritti dell'uomo[15];

- se la direttiva 2006/24/CE è compatibile con il diritto alla protezione dei dati di carattere personale sancito all'art. 8 della Carta;

- se la direttiva 2006/24/CE è compatibile con il diritto alla libertà di espressione sancito dall'art. 11 della Carta e dall'art. 10 della CEDU;

- se la direttiva 2006/24/CE è compatibile con il diritto ad una buona amministrazione contemplato dall'art. 41 della Carta;

- in che misura i Trattati – in particolare il principio di leale collaborazione di cui all'art. 4, par. 3, TUE – impongono al giudice nazionale di esaminare e valutare la compatibilità delle misure statali volte a trasporre la direttiva 2006/24/CE con le garanzie previste dalla Carta, ivi compreso il suo art. 7.

Nella causa C-594/12 il *Verfassungsgerichtshof*, inoltre, ha sottoposto alla Corte un'ulteriore questione, relativa ai rapporti fra gli artt. 8 e 52 della Carta e, da un lato, la direttiva 95/46/CE sulla tutela dei dati personali e il regolamento CE n. 45/2001, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati; dall'altro lato, i cambiamenti e le evoluzioni derivanti dalle norme successive di diritto derivato.

Infine, tenuto conto della clausola di corrispondenza di cui all'art. 52, par. 3, della Carta, i giudici austriaci hanno sollevato la necessità di valutare se e come la giurisprudenza della Corte europea dei diritti dell'uomo relativa all'art. 8 CEDU possa fornire indicazioni interpretative rilevanti.

I giudici austriaci si sono interrogati, infine, anche sui rapporti che intercorrono tra l'art. 8 della Carta e le tradizioni costituzionali degli Stati membri in relazione all'art. 52, par. 4, della Carta.

4. La decisione della Corte di Giustizia.

La sentenza della Corte di Giustizia affronta, per la prima volta, la delicata questione concernente il bilanciamento fra le esigenze di repressione ed accertamento dei reati e la tutela dei diritti fondamentali dell'individuo, che possono essere fortemente limitati dagli obblighi di conservazione dei dati di traffico telefonico e telematico nella società informazione.

La decisione risulta essere epocale ed ha un forte impatto non solo sul diritto dell'Unione, ma anche sugli ordinamenti nazionali e sulle attività investigative che si basano sull'acquisizione di dati e informazioni presso i *service providers*.

[15] Questa "corrispondenza" è già stata evidenziata dall'avvocato generale Pedro Cruz Villalón (lo stesso della causa in esame) nelle conclusioni presentate il 14 aprile 2011 relative alla causa C-70/10 (vedi infra, 5), in cui ha proposto la riformulazione della questione nei termini che seguono. Il giudice del rinvio aveva formulato la sua prima questione pregiudiziale quale interpretazione di varie disposizioni del diritto derivato dell'Unione «alla luce degli artt. 8 e 10 della CEDU». Ex art. 6, n. 3, TUE, «[i] diritti fondamentali, garantiti dalla [CEDU] (…) fanno parte del diritto dell'Unione in quanto principi generali». Anzitutto, il medesimo art. 6 TUE inizia precisando, al par. 1, co. 1, che la Carta «ha lo stesso valore giuridico dei trattati», come la Corte non ha mancato di sottolineare negli ultimi sviluppi della sua giurisprudenza. «Poiché i diritti, le libertà e i principi enunciati nella Carta hanno quindi, di per sé stessi, un valore giuridico, oltretutto di primo rango, il ricorso ai principi generali sopra menzionati non è più necessario, nei limiti in cui i primi possono identificarsi nei secondi». Questo è stato dunque un primo elemento a favore dell'esame della questione alla luce delle disposizioni della Carta, piuttosto che con riferimento a quelle della CEDU. Inoltre, l'art. 52, par. 3, della Carta prevede che «[l]addove [essa] contenga diritti corrispondenti a quelli garantiti dalla [CEDU], il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione», restando inteso che «[tale] disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa». Orbene, secondo l'avvocato generale «nelle circostanze della causa principale, i diritti garantiti dall'art. 8 CEDU corrispondono, ai sensi dell'art. 52, par. 3, della Carta, a quelli garantiti dagli artt. 7 (Rispetto della vita privata e della vita familiare) e 8 (Protezione dei dati di carattere personale) della Carta, così come i diritti garantiti dall'art. 10 CEDU corrispondono a quelli garantiti dall'art. 11 della Carta (Libertà di espressione e d'informazione), nonostante le differenze relative, rispettivamente, alle formulazioni impiegate e alle nozioni utilizzate». L'avvocato generale ha pertanto proposto di modificare la questione del giudice del rinvio sostituendo il riferimento agli artt. 8 e 10 CEDU con quello agli artt. 7, 8 e 11 della Carta, in combinato con l'art. 52, n. 1, della stessa, come interpretati, ove necessario, alla luce degli artt. 8 e 10 CEDU. Cfr. R. Flor, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, *in Dir. pen. cont.*, 20 settembre 2012

4.1. *La compatibilità della direttiva 2006/24 con gli artt. 7, 8 e 11 della Carta dei diritti fondamentali dell'Unione europea.*

Le disposizioni della direttiva ritenute contrarie ai diritti fondamentali del rispetto della vita privata e della vita familiare, della protezione dei dati di carattere personale e della libertà di espressione e di informazione sono quelle previste in deroga agli artt. 5, 6 e 9 della direttiva 2002/58/CE, relative in particolare all'obbligo di conservazione dei dati di traffico telefonico e telematico (art. 3)[16], alle procedure e alle garanzie inerenti all'accesso ai dati (art. 4)[17] – che avrebbero dovuto essere definite da ogni Stato membro nel pieno rispetto delle previsioni della CEDU, secondo l'interpretazione della Corte europea dei diritti dell'uomo – nonché alle stesse categorie di dati da conservare (art. 5)[18].

La Corte ha rilevato che il trattamento di tali dati, compresa la loro archiviazione, consente di trarre precise conclusioni sulla vita privata dei cittadini europei, sulle loro abitudini giornaliere, sui luoghi di residenza permanente o temporanea, sui loro movimenti e le loro attività, così come sulle loro relazioni sociali.

Pertanto, la c.d. *data retention* invade direttamente e specificatamente i diritti garantiti dall'art. 7 della Carta, mentre il trattamento di tali dati comprime i diritti previsti dall'art. 8 della Carta, non rispettando i requisiti di tale ultima disposizione, considerando la giurisprudenza della stessa Corte di Giustizia (vedi C-92/09 e C-93/09).

Inoltre, anche se la direttiva non consente di archiviare i dati relativi ai contenuti delle comunicazioni, le sue previsioni hanno comunque un effetto sul possibile utilizzo dei mezzi di comunicazione da parte degli utenti e sull'esercizio della loro libertà di espressione (ex art. 11 della Carta), nonché permettono un possibile controllo *ex post* delle attività personali e professionali dei cittadini europei che, seppur esercitato soltanto a posteriori in occasione dell'impiego delle informazioni, minaccia in modo permanente, e per tutto il periodo della loro conservazione, il diritto alla riservatezza.

La Corte ha evidenziato che la verifica dell'esistenza di una interferenza rispetto al diritto alla riservatezza non coinvolge necessariamente le questioni relative alla natura del dato (sensibile o meno) o al fatto che la persona coinvolta sia o meno disturbata dal trattamento delle informazioni (vedi C-465/00, C-138/01, C-139/01). In altri termini il solo obbligo, in capo al *provider*, di conservare i dati per un periodo di tempo definito, nonché la previsione della possibilità di accesso a tali dati da parte delle autorità nazionali, costituiscono di per sé una interferenza nei diritti fondamentali garantiti dall'art. 7 della Carta e dall'art. 8 CEDU.

[16] «In deroga agli art. 5, 6 e 9 della direttiva 2002/58/CE, gli Stati membri adottano misure per garantire che i dati di cui all'art. 5 della presente direttiva, qualora siano generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati, da fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione nell'ambito della loro giurisdizione, siano conservati conformemente alle disposizioni della presente direttiva. 2. L'obbligo di conservazione stabilito dal par. 1 comprende la conservazione dei dati specificati all'art. 5 relativi ai tentativi di chiamata non riusciti dove tali dati vengono generati o trattati e immagazzinati (per quanto riguarda i dati telefonici) oppure trasmessi (per quanto riguarda i dati Internet) da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione nell'ambito della giurisdizione dello Stato membro interessato nel processo di fornire i servizi di comunicazione interessati». La direttiva non richiede la conservazione dei dati per quanto riguarda le chiamate non collegate.

[17] «Gli Stati membri adottano misure per garantire che i dati conservati ai sensi della presente direttiva siano trasmessi solo alle autorità nazionali competenti, in casi specifici e conformemente alle normative nazionali. Le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di 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».

[18] A titolo esemplificativo si pensi ai dati necessari per rintracciare e identificare la fonte di una comunicazione (numero telefonico chiamante, nome e indirizzo dell'abbonato o dell'utente registrato), per l'accesso Internet, posta elettronica e telefonia via Internet, per rintracciare e identificare la destinazione di una comunicazione, per determinare la data, l'ora e la durata di una comunicazione (che comprendono, ad esempio, anche data e ora del *log-in* e del *log-off* del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato), per determinare il tipo di comunicazione o il servizio Internet utilizzato, per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione (*Cell ID*) nel periodo in cui vengono conservati i dati delle comunicazioni.

4.2. *L'applicazione del principio di proporzionalità per la tutela del nucleo essenziale dei diritti fondamentali coinvolti.*

Ex art. 52, par. 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà da essa riconosciuti devono essere previste dalla legge e non pregiudicare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

La questione riguarda, dunque, la verifica relativa, da un lato, all'esistenza di una finalità di interesse generale o all'esigenza di tutelare le libertà e i diritti altrui e, dall'altro lato, al rispetto del nucleo essenziale dei diritti fondamentali in gioco.

E' vero che la direttiva non si applica al contenuto delle comunicazioni elettroniche, ivi incluse le informazioni consultate utilizzando una rete di comunicazioni elettroniche.

E' altresì vero che l'art. 7 della direttiva dispone che ogni Stato membro avrebbe dovuto provvedere affinché i fornitori di servizi adottassero alcuni principi di sicurezza, ivi comprese misure tecniche e organizzative dirette ad evitare la cancellazione non solo accidentale, ma anche illecita dei dati, la loro alterazione non autorizzata o l'accesso illegale alle informazioni, nonché a garantire che essi vengano distrutti alla fine del periodo di conservazione, fatta eccezione per quelli consultati e conservati.

Sul piano dell'esistenza di un interesse generale riconosciuto dall'Unione, la Corte ha rilevato che la direttiva contribuisce alla lotta contro gravi crimini e, dunque, a tutelare la pubblica sicurezza. Essa, infatti, si propone l'obiettivo di armonizzare le disposizioni degli Stati membri relative agli obblighi, per i fornitori di servizi, di conservazione di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale.

Lo stesso art. 6 della Carta sancisce i diritti fondamentali alla libertà ed alla "sicurezza", che possono essere minacciati da fenomeni criminali gravi, come il terrorismo internazionale o la criminalità organizzata[19].

Risulta pertanto incontestabile, secondo la Corte, che sussista un oggettivo interesse generale dell'Unione.

Il principio di proprozionalità richiede, però, che le iniziative delle istituzioni europee siano appropriate al fine di raggiungere i legittimi obiettivi, perseguiti attraverso la disciplina giuridica in esame, purché, utilizzando le parole dei Giudici, non superino i limiti «di quanto è appropriato e necessario» per raggiungere quegli obiettivi.

Le scelte discrezionali del legislatore europeo, pertanto, possono essere limitate, in quanto dipendenti da una serie di fattori, compresi quelli relativi alla natura dei diritti fondamentali in gioco, a natura, grado e gravità dell'interferenza ed agli obiettivi da raggiungere attraverso quest'ultima.

In altri termini la Corte ha dovuto valutare l'importante ruolo attribuito alla tutela dei dati personali rispetto all'estensione della grave intrusione causata dalle disposizioni della direttiva 2006/24 e, in particolare, dagli obblighi di conservazione dei dati.

La Corte ha ammesso che le tecnologie informatiche e i mezzi di comunicazione elettronica possono essere estremamente utili nell'ambito delle attività di indagine, permettendo alle autorità nazionali di avere maggiori opportunità nella lotta alla criminalità grave. In questo senso gli obblighi di conservazione dei dati dovrebbero essere considerati appropriati al raggiungimento degli obiettivi perseguiti dalla direttiva europea.

La Corte, però, ha anche evidenziato che il rispetto della vita privata richiede che le deroghe e i limiti relativi alla protezione dei dati personali devono essere applicati solo ed esclusivamente in casi di stretta necessità.

Anche se la lotta contro gravi crimini risulta essere essenziale per assicurare la sicurezza pubblica, e la sua efficacia può dipendere da un largo uso di moderne tecniche investigative, la "necessità" di archiviare i dati di traffico per il raggiungimento di un "interesse generale", anche

[19] E' la stessa Corte che richiama le esigenze di contrasto a questi fenomeni criminali gravi, facendo riferimento al diritto alla "sicurezza", inteso quale «mantenimento della pace» e «sicurezza pubblica».

se di tale portata, non è di per sé giustificata.

Il legislatore europeo avrebbe dovuto imporre chiare e precise regole relative all'applicazione della *data retention*, prevedendo, secondo i Giudici, standard minimi di garanzia per assicurare al cittadino europeo, o alla persona i cui dati sono archiviati, una effettiva protezione contro i rischi di abusi o di accesso illegale alle informazioni, soprattutto in casi come quello in esame, in cui il trattamento dei dati avviene in modo automatizzato ed è intrinsecamente "pericoloso"[20].

Sulla stretta necessità della forte limitazione dei diritti fondamentali portata dalla direttiva, dunque, la Corte è giunta alle seguenti conclusioni.

I. La direttiva richiede l'applicazione della *data retention* a tutti i dati di traffico connessi a qualsiasi mezzo comunicativo che viene utilizzato oggi da tutti in ogni attività giornaliera. Gli stessi obblighi di archiviazione riguardano i dati di ogni utente registrato. Pertanto essa si applica, in modo generalizzato, a tutti gli utenti e a tutti i mezzi di comunicazione elettronica, così come a tutte le modalità di traffico di dati (via telefono, Internet, e-mail ecc.) senza differenziazioni, limiti o eccezioni rispetto all'obiettivo di contrastare la criminalità grave. Inoltre, tale archiviazione ha ad oggetto dati di persone che, nemmeno indirettamente, si trovano nella situazione di dare adito a procedimenti penali o di essere collegate, anche solo in modo remoto, a reati gravi, anche in situazioni in cui non sussistono prove che la loro condotta possa in qualche modo far sospettare un loro coinvolgimento. Inoltre essa non prevede alcuna eccezione, con la conseguenza che si trova ad essere applicata anche alle persone le cui comunicazioni sono soggette, in base alle norme di diritto nazionale, all'obbligo del segreto professionale.

II. La direttiva non prevede alcun rapporto tra i dati oggetto dell'obbligo di conservazione e una minaccia per la sicurezza pubblica. In particolare, tale obbligo non è limitato a: a) dati relativi a un determinato periodo di tempo e/o una particolare zona geografica e/o ad un cerchio di persone che possono essere coinvolte, in un modo o nell'altro, in un crimine grave; b) a persone che potrebbero, per altri motivi, contribuire, grazie alla conservazione dei loro dati, alla prevenzione, accertamento e perseguimento di reati gravi.

III. La direttiva non prevede alcun limite oggettivo, sostanziale o procedurale[21], per l'accesso ai dati da parte delle competenti autorità nazionali e per il successivo utilizzo a fini di prevenzione, accertamento [o nell'ambito di procedimenti penali] riguardanti reati che, in considerazione della portata e della invasività della interferenza con i diritti fondamentali di cui agli artt. 7 e 8 della Carta, siano di una gravità tale da giustificare una limitazione a questi diritti. Al contrario, la direttiva fa riferimento in modo generale, ex art. 1, par. 1, a «reati gravi» come «definiti dagli Stati membri», e non prevede che l'accesso ai dati avvenga dopo l'esame di un giudice o di una autorità amministrativa indipendente, la cui decisione possa, a seguito di una richiesta motivata presentata nel quadro delle procedure di prevenzione o accertamento di gravi reati, o nell'ambito di procedimenti penali, limitare l'accesso ai dati e il loro utilizzo a quanto è strettamente necessario ai fini del raggiungimento dell'obiettivo perseguito. Non si rinviene per gli Stati, peraltro, nessuno specifico obbligo di prevedere tali limiti.

IV. Per quanto riguarda il periodo di archiviazione dei dati, la direttiva fa riferimento ad un lasso di tempo minimo (6 mesi) e massimo (24 mesi) senza distinguere le categorie di dati e la loro possibile utilità per il raggiungimento degli obiettivi perseguiti, ovvero in accordo con le persone coinvolte. Inoltre, il "periodo finestra" non è basato su criteri oggettivi al fine di assicurare che sia limitato alla stretta necessità. Ne consegue che l'interferenza con i diritti fondamentali in esame avviene senza limiti o regole precise.

V. Con riferimento alla sicurezza ed alla protezione dei dati oggetto dell'obbligo di archiviazione, la direttiva non prevede misure di garanzia sufficienti – come richieste, invece, dagli artt. 7 e 8 della Carta – in specie contro il rischio di abusi, accesso illegale o uso non autorizzato, nonché in relazione alla molteplicità e diversità di dati che devono essere archiviati, alla natura dei medesimi ed ai rischi connessi alla loro integrità, confidenzialità e genuinità. La direttiva, inoltre, non prevede l'obbligo per gli Stati membri di disciplinare elevati standard di sicurezza, permettendo in tal modo ai *providers* di poter seguire criteri di mera economicità

[20] Si consideri che anche il nostro d.lgs n. 196/2003 (Codice Privacy) all'art. 15 (Danni cagionati per effetto del trattamento), prevede che «chiunque cagioni danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c.» (che riguarda proprio la responsabilità per l'esercizio di attività pericolose).

[21] L'art. 4 della direttiva, infatti, lascia agli Stati membri il compito di definire le regole procedurali da seguire e i requisiti sostanziali per garantire l'accesso e la comunicazione dei dati.

per assicurare la protezione delle informazioni[22]. Infine, la direttiva non richiede che i dati in questione debbano essere conservati all'interno dell'Unione europea, con la conseguenza che non è possibile ritenere che il controllo, espressamente richiesto dall'art. 8, par. 3 della Carta, da parte di un'autorità indipendente in conformità con le esigenze di tutela e sicurezza dei dati, possa essere pienamente garantito[23].

Per tutte queste ragioni la Corte ha invalidato la direttiva 2006/24, in quanto non compatibile con i limiti imposti dal rispetto del principio di proporzionalità, alla luce degli artt. 7, 8 e 52, par. 1, della Carta.

5. Conclusioni necessariamente provvisorie e questioni aperte.

Non è certo la prima volta che la Corte di Giustizia ha dovuto affrontare la delicata questione relativa al bilanciamento fra le diverse esigenze, da un lato, di tutela dei diritti fondamentali e, dall'altro, di perseguimento e prevenzione di attività illecite e di reati.

In almeno due precedenti recenti[24] la Corte ha valorizzato, in particolare, i diritti fondamentali tutelati dagli artt. 8 e 11 della Carta, oltre alla libertà di impresa (ex art. 16 della Carta) per garantire la loro prevalenza nel bilanciamento con le esigenze di tutela della proprietà intellettuale in Internet, le cui violazioni costituiscono, in molti Stati, un illecito penale[25].

Cercando di sintetizzare, in entrambi i casi essa ha affermato che l'ingiunzione diretta, da parte di un giudice nazionale ad un *service provider,* di adottare sistemi di filtro per impedire agli utenti di utilizzare sistemi di *file sharing* in violazione delle norme in materia di diritto d'autore, comprime in modo sproporzionato tali diritti.

Le ragioni di queste decisioni si fondano sul fatto che un sistema di filtro adottato da un fornitore di servizi presuppone l'identificazione degli utenti e, nell'ambito delle comunicazioni elettroniche, i *file* che appartengono al traffico *peer-to-peer* e i *file* che contengono opere sulle quali i titolari dei diritti di proprietà intellettuale affermino di vantare diritti. Tale sistema è in grado di determinare, dunque, quali tra questi *file* sono scambiati in modo illecito, procedendo al blocco delle relative condivisioni. Questo tipo di sorveglianza attiva e preventiva, senza limiti di tempo e a totale carico, sul piano economico, del prestatore di servizi, richiederebbe un'osservazione attiva sulla totalità delle comunicazioni elettroniche e, indistintamente, degli utenti che si avvalgono del servizio. In questi casi, dunque, la Corte ha bene evidenziato che non può desumersi che la tutela del diritto di proprietà intellettuale, sebbene sia sancita dall'art. 17, par. 2, della Carta, sia intangibile e assoluta, rispetto alla tutela di altri diritti fondamentali, come quelli previsti dagli artt. 8, 11 e 16 della Carta.

In una più recente pronuncia[26], invece, la Corte ha ritenuto che i diritti fondamentali riconosciuti dal diritto dell'Unione devono essere interpretati nel senso che non ostano a che sia vietato, con un'ingiunzione pronunciata da un giudice ad un fornitore di accesso ad Internet, di concedere ai suoi abbonati l'accesso ad un sito Internet che metta in rete materiali protetti

[22] Il c.d. "criterio di economicità" era già stato evidenziato, in senso critico, dalla Corte costituzionale tedesca nella citata sentenza del 2 marzo 2010 sulla *data retention* (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), *on-line* in http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html Per un primo commento in italiano si consenta il rinvio a R. Flor, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul* data retention, in *Ciberspazio e diritto*, 11, 2 , 2010 , 359-392.

[23] La Corte ha aderito alle conclusioni dell'avvocato generale Pedro Cruz Villalón presentate il 12 dicembre 2013, secondo il quale la direttiva 2006/24 impone agli Stati membri di provvedere affinché i dati siano conservati in conformità ad essa. Egli ha comunque osservato che ciò è richiesto solo per permettere che tali dati e ogni altra informazione necessaria ad essi collegata «possano essere trasmessi immediatamente alle autorità competenti su loro richiesta». La direttiva lascia liberi gli Stati di disciplinare le misure di protezione e sicurezza dei dati conservati, tenendo presente che l'utente non è informato in relazione al trattamento di tali dati. La carenza di informazione può, dunque, indurre i cittadini europei, secondo i giudici, alla convinzione che la loro vita sia costantemente sorvegliata.

[24] Corte di Giustizia dell'Unione europea, 24 novembre 2011 (C-70/10) e 16 febbraio 2012 (C -360/10).

[25] Si consenta di rinviare a R. Flor, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, Padova, 2010 che, con riferimento a fenomeni criminali che trovano in Internet un mezzo formidabile per la loro commissione, oppure l'ambiente ideale di manisfestazione, riporta la disciplina penale di alcuni paesi (in particolare Italia, Germania, Francia, Spagna, Regno Unito, Svezia e Stati Uniti d'America). Con riferimento alle cause C-70/10 e C-360/10 vedi l'art. 87, n. 1, primo e secondo comma, della legge belga 30 giugno 1994 (*Belgisch Staatsblad,* [27] luglio 1994), sul diritto d'autore e sui diritti connessi, il quale prevede quanto segue: «Il presidente del *tribunal de première instance* (…) consta[ta] l'esistenza e [ordina] la cessazione di qualsiasi violazione del diritto d'autore o di un diritto connesso. [Può] altresì emanare un provvedimento inibitorio contro intermediari i cui servizi siano utilizzati da un terzo per violare il diritto d'autore o un diritto connesso».

[26] Corte di Giustizia dell'Unione europea, 27 marzo 2014 (C-314/12).

senza il consenso dei titolari dei diritti, qualora tale ingiunzione non specifichi quali misure il fornitore d'accesso deve adottare e quest'ultimo possa evitare sanzioni per la violazione di tale ingiunzione dimostrando di avere adottato tutte le misure ragionevoli. A condizione, tuttavia, che da un lato, le misure adottate privino inutilmente gli utenti di Internet della possibilità di accedere in modo lecito alle informazioni disponibili e, dall'altro, che tali misure abbiano l'effetto di impedire o, almeno, di rendere difficilmente realizzabili le consultazioni non autorizzate dei materiali protetti e di scoraggiare seriamente gli utenti di Internet che ricorrono ai servizi del destinatario di questa stessa ingiunzione dal consultare tali materiali messi a loro disposizione in violazione del diritto di proprietà intellettuale, circostanza che spetta alle autorità e ai giudici nazionali verificare.

Pur trattandosi di questioni pregiudiziali sull'interpretazione delle direttive 2000/31/CE sul commercio elettronico, 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, 2004/48/CE sul rispetto dei diritti di proprietà intellettuale, 95/46/CE sul trattamento dei dati personali e 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, esse hanno, di fatto, posto in discussione l'uso di taluni mezzi tecnologici "invasivi" rispetto alla tutela dei diritti fondamentali, ferma restando la validità degli atti europei[27].Con la sentenza sulla c.d. *data retention,* invece, la Corte di Giustizia ha invalidato la direttiva 2006/24, aprendo nuovi scenari sia a livello europeo che a livello nazionale.

Il dato positivo risiede nel fatto che la Corte ha indicato al legislatore europeo, soprattutto in un momento di riflessione sulla riforma della disciplina in materia di tutela della riservatezza e dei dati personali, la strada da percorrere per garantire i diritti fondamentali dell'individuo, senza necessariamente, in verità, dover totalmente rinunciare agli strumenti tecnologici indispensabili per la prevenzione e la repressione di gravi reati[28].

L'aspetto negativo, invece, risiede nel fatto che molti paesi europei, compresa l'Italia, si trovano a dover affrontare immediatamente la delicata questione relativa alla "validità" delle rispettive norme nazionali di attuazione della direttiva, sulla base delle quali vengono svolte importanti attività investigative per l'accertamento e la prevenzione dei reati.

Lo scenario attuale è aggravato dalla disomogeneità delle singole previsioni statali con

[27] E' degna di nota una recente sentenza della Corte di Giustizia (13 maggio 2014, C-131/12), la quale ha affermato la prevalenza dei diritti tutelati dagli artt. 7 e 8 della Carta, in determinate condizioni, rispetto alla libertà di espressione e agli interessi economici dei *providers,* rafforzando in questo modo la posizione giuridica della persona interessata, benchè non fosse pacifico poter ricavare dalle norme della direttiva, intepretate alla luce delle disposizioni dalla Carta, un diritto "generalizzato" all'oblio (vedi, in questo senso, le conclusioni dell'Avvocato Generale Niilo Jääskinen presentate il 25 giugno 2013). Il Giudice nazionale ha chiesto, in sostanza, se i diritti dell'interessato alla rettifica, alla cancellazione, al congelamento dei dati e all'opposizione al trattamento, previsti, dagli artt. 12, lett. b), e 14, lett. a) della direttiva 95/46 possano corrispondere ad un vero e proprio "diritto all'oblio". In questa sede è opportuno, seppure brevemente, riportare il fatto. Il 5 marzo 2010, il sig. Costeja González, cittadino spagnolo, ha presentato dinanzi all' *Agencia Española de Protección de Datos* un reclamo contro il quotidiano *La Vanguardia Ediciones SL* e contro Google Spain e Google Inc., in quanto gli utenti di Internet, introducendo il suo nome in «Google Search», ottenevano dei *link* verso due pagine del quotidiano pubblicate nel 1998, sulle quali figurava un annuncio di rilevanza giudiziaria. Egli chiedeva, quindi, che fosse ordinato al quotidiano di sopprimere o modificare tali pagine, oppure di ricorrere a taluni strumenti forniti dai motori di ricerca per proteggere i dati, ordinando altresì a Google Spain o a Google Inc. di eliminare o di occultare le informazioni personali, in modo che cessassero di comparire tra i risultati di ricerca. Il reclamo è stato accolto parzialmente. L'AEPD, infatti, ha ordinato ai soli gestori del motore di ricerca di rimuovere i dati e di provvedere ad impedire l'accesso alle informazioni. Essa ha ritenuto, da un lato, che la grave ingerenza nei diritti fondamentali tutelati dagli artt. 7 e 8 della Carta non può essere giustificata dal semplice interesse economico del fornitore del servizio. Dall'altro lato, però, poiché la soppressione di *link* dall'elenco dei risultati potrebbe, a seconda della natura e del tipo di informazione, avere ripercussioni sul legittimo interesse degli utenti ad avere accesso a quest'ultima, occorrerebbe ricercare un "giusto equilibrio" fra i diritti fondamentali coinvolti. In estrema sintesi la Corte, nella causa avente ad oggetto la domanda di pronuncia pregiudiziale proposta dall'*Audiencia Nacional* (Spagna), con decisione del 27 febbraio 2012, nel procedimento Google Spain SL, Google Inc. contro l'AEPD e il sig. Mario Costeja González, ha affermato che l'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione dei presupposti di applicazione degli artt. 12, lett. b), e 14, co. 1, lett. a), della direttiva 95/46, possono ordinare al gestore del servizio (Google) di cancellare, dall'elenco di risultati che appare a seguito di una ricerca, i *link* verso pagine *web* pubblicate da terzi e contenenti informazioni relative a una persona. Il fornitore del servizio è obbligato, inoltre, a sopprimere gli stessi *link* anche nel caso in cui il nome o le informazioni non vengano previamente o simultaneamente cancellati dalle pagine *web* del quotidiano, eventualmente anche quando la loro pubblicazione sia di per sé lecita. Sulla base dell'interpretazione di tali prescrizioni, dettate dall'art. 6, co. 1, lett. da c) a e), direttiva 95/46, un trattamento di dati inizialmente lecito potrebbe divenire, con il tempo, incompatibile con la direttiva, qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura in particolare nel caso in cui i dati risultino inadeguati, non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità e al medesimo tempo trascorso. E'agevole notare che, secondo la Corte, i diritti fondamentali di cui agli artt. 7 e 8 della Carta prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico degli utenti a trovare l'informazione in occasione di una ricerca *online* relativa ad una persona determinata. Ferme restando, secondo i Giudici, le eccezioni legate, ad esempio, al ruolo ricoperto da tale persona nella vita pubblica, che potrebbe giustificare la prevalenza dell'interesse degli utenti ad avere accesso all'informazione. Per quanto riguarda la situazione italiana *in subiecta materia* basti il rinvio al recente provvedimento del Garante Privacy, 10 luglio 2014, n. 353.

[28] Vedi supra, 4.2., punti I-V.

riferimento sia al periodo di archiviazione dei dati, sia alla disciplina procedurale da seguire per l'accesso alle informazioni e per il loro successivo utilizzo, sia all'autorità competente ad effettuare tali operazioni[29].

Nel nostro ordinamento, ad esempio, l'art. 132 d.lgs. n. 196 del 2003 prevede che i dati relativi al traffico telefonico siano conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, siano conservati dal fornitore per dodici mesi dalla data della comunicazione.

Entro tali termini i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore, i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'art. 391-*quater* c.p.p., ferme restando le condizioni di cui all'art. 8, co. 2, lett. f), per il traffico entrante.

Tralasciando le disposizioni relative allo svolgimento delle investigazioni preventive previste dall'art. 226 delle norme di cui al d.lgs. n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati[30], il Codice Privacy prevede, ex art. **132**-*bis,* **che i** fornitori istituiscano procedure interne per rispondere alle richieste effettuate in conformità alle disposizioni che disciplinano forme di accesso ai dati personali degli utenti[31].

Ad una prima lettura è agevole notare che, nell'ambito dello spazio discrezionale lasciato dalla direttiva ai legislatori nazionali, il legislatore italiano abbia optato, in primo luogo, per la

[29] Vedi ad esempio, COM(2011) 225 definitivo, 10, tab. 2, relativa all'accesso ai dati (procedure e condizioni), secondo cui quattordici Stati membri elencano tra le autorità competenti i servizi di sicurezza o di intelligence o le forze militari, sei Stati membri le autorità fiscali e/o doganali e tre Stati membri le autorità di frontiera. Uno Stato membro consente ad altre autorità pubbliche di consultare i dati, previa autorizzazione per finalità specifiche previste dalla legislazione secondaria. In undici Stati membri è necessaria l'autorizzazione giudiziaria per ogni richiesta di accesso ai dati conservati. In tre Stati membri l'autorizzazione giudiziaria è necessaria nella maggior parte dei casi. Quattro altri Stati membri richiedono l'autorizzazione di un'autorità di alto livello, ma non di un giudice. In due Stati membri l'unica condizione prevista sembra essere la necessità di presentare la richiesta per iscritto. Sui periodi di conservazione quindici Stati membri specificano un solo periodo per tutte le categorie di dati. uno Stato membro (Polonia) indica un periodo di conservazione di due anni, uno indica 1,5 anni (Lettonia), dieci indicano un anno (Bulgaria, Danimarca, Estonia, Grecia, Spagna, Francia, Paesi Bassi, Portogallo, Finlandia, Regno Unito) e tre indicano sei mesi (Cipro, Lussemburgo, Lituania). Cinque Stati membri hanno definito periodi di conservazione diversi per le varie categorie di dati: due Stati membri (Irlanda, Italia) indicano due anni per i dati relativi alla telefonia fissa e mobile e 1 anno per i dati relativi all'accesso Internet, alla posta elettronica su Internet e alla telefonia via Internet; uno Stato membro (Slovenia) indica 14 mesi per i dati relativi alla telefonia e otto mesi per i dati relativi a Internet; uno Stato membro (Slovacchia) indica un anno per la telefonia fissa e mobile e sei mesi per i dati relativi a Internet; uno Stato membro (Malta) indica un anno per i dati relativi alla telefonia fissa, mobile e via Internet e sei mesi per l'accesso Internet e la posta elettronica su Internet. Uno Stato membro (Ungheria) conserva tutti i dati per un anno, eccetto i dati sui tentativi di chiamata non riusciti, che sono conservati per sei mesi. Uno Stato membro (Belgio) non ha previsto un periodo di conservazione specifico per le categorie di dati stabilite dalla direttiva. Vedi COM(2011) 225 definitivo, 15, tab. 3.

[30] In questo ambito si consideri che il co. 4-*ter* della stessa disposizione prevede: «il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel co. 1 dell'art. 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato art. 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi». Il successivo co. 4-*quater* dispone, invece: «Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-*ter* deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'art. 326 c.p.» I provvedimenti adottati ai sensi del comma 4-*ter* sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.

[31] Per completezza è opportuno evidenziare che l'inosservanza dell'obbligo di conservazione dati comporta l'applicazione di una sanzione amministrativa in capo al fornitore dei servizi. L'art. 162-*bis* (Sanzioni in materia di conservazione dei dati di traffico) Codice Privacy prevede, infatti, quanto segue: «salvo che il fatto costituisca reato e salvo quanto previsto dall'art. 5, co. 2, del decreto legislativo di recepimento della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006, nel caso di violazione delle disposizioni di cui all'art. 132, co. 1 e 1-*bis*, si applica la sanzione amministrativa pecuniaria da 10.000 euro a 50.000 euro». Il citato art. 5, co. 2, invece, dispone: «salvo che il fatto costituisca reato, l'omessa o l'incompleta conservazione dei dati ai sensi dell'art. 132, co. 1 e 1-*bis*, del Codice, è punita con la sanzione amministrativa pecuniaria da euro 10.000 ad euro 50.000, che può essere aumentata fino al triplo in ragione delle condizioni economiche dei responsabili della violazione. Nel caso di assegnazione di indirizzo IP che non consente l'identificazione univoca dell'utente o abbonato si applica la sanzione amministrativa pecuniaria da 5.000 euro a 50.000 euro, che può essere aumentata fino al triplo in ragione delle condizioni economiche dei responsabili della violazione. Le violazioni sono contestate e le sanzioni sono applicate dal Ministero dello sviluppo economico».

previsione di un obbligo generale valido per l'accertamento e la repressione dei "reati", senza individuare categorie specifiche di fattispecie penali che devono ritenersi "gravi".

In secondo luogo, non sono previsti obblighi particolari di sicurezza nel trattamento e nell'archiviazione dei dati che possano corrispondere ad "elevati standard" in considerazione dello sviluppo tecnologico o di *best practices* riconosciute a livello sovranazionale.

In terzo luogo, per l'acquisizione dei dati il legislatore ha previsto il decreto motivato del pubblico ministero.

In quarto luogo, le procedure "interne" per rispondere alle richieste di accesso ai dati sono state lasciate sostanzialmente nelle mani del *provider*, anche se il Garante Privacy italiano è intervenuto in più occasioni prescrivendo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, ai sensi degli artt. 17, 123 e 132 d.lgs 196 del 2003, l'adozione di specifici accorgimenti e misure in grado di garantire un "elevato" livello di protezione dei predetti dati di traffico[32].

A questo punto appare logico chiedersi quale valore assumono i dati acquisiti presso il *provider* o, meglio, "consegnati" dal *provider*, all'interno del processo penale[33]. Quali sono le garanzie legate alla genuinità, integrità e veridicità del dato se le stesse "procedure interne" possono essere non previste in modo chiaro e preciso dalla legge, ma lasciate alla "valutazione" dei *providers* o, come è avvenuto in Italia, a prescrizioni del Garante, che però possono essere attuate dai fornitori del servizio in modo diverso e con margini di discrezionalità organizzativa, tecnica ed economica? Gli *stress* a cui sono sottoposti gli istituti processuali coinvolti sono superabili? E qual è il destino dei procedimenti in atto – che incide sulla stessa utilizzabilità dei dati – i quali potrebbero basarsi proprio sull'acquisizione delle informazioni di traffico telefonico o telematico oggetto della *data retention*? Infine, quali sono le prospettive *de jure condendo,* anche sul piano del diritto penale sostanziale? E' opportuno che il legislatore nazionale intervenga in tempi rapidi per adeguare la disciplina italiana ai "rilievi" di illegittimità della direttiva e di grave interferenza nei diritti fondamentali dell'individuo evidenziati dalla Corte?

Alla luce della sentenza della Corte di Giustizia queste brevi osservazioni costituiscono, anzitutto e *de jure condito*, questioni "aperte", con cui l'interprete dovrà necessariamente confrontarsi, in quanto influiscono in modo determinante sulle riflessioni connesse alla "validità" della disposizione italiana in rapporto al diritto europeo ed al rispetto dei diritti fondamentali previsti dalla Carta.

Da un lato, la fonte "gerarchicamete" superiore è stata dichiarata invalida per il contrasto con i diritti fondamentali, ritenuti compromessi ben oltre il limite posto dal rispetto del loro contenuto essenziale e del principio di proporzionalità.

[32] Con i provvedimenti del 17 gennaio 2008, 24 luglio 2008 e 29 aprile 2009, con cui ha disposto più proroghe per l'adempimento da parte dei fornitori di servizi, il Garante ha preso atto anche delle modifiche normative intervenute dalla data di entrata in vigore del d.lgs n. 196 del 2003 e, in particolare, di quelle introdotte con la l. n. 48 del 2008, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001, che ha modificato l'art. 132 del Codice, prevedendo una specifica ipotesi di conservazione temporanea dei dati relativi al traffico telematico a fini di svolgimento di investigazioni preventive o di accertamento e repressione di reati. In materia è successivamente intervenuto il d.l. 2 ottobre 2008, n. 151 (convertito con modificazioni dall'art. 1 della l. n. 186 del 2008). Gli adempimenti in capo ai *providers* hanno avuto ad oggetto, ad esempio, prescrizioni per l'adozione di sistemi di autenticazione e autorizzazione, di cifratura e protezione, nonché per la conservazione separata dei dati oltre che per la cancellazione di questi ultimi e per il controllo delle operazioni. Tali prescrizioni, però, pur apparendo stringenti, e pur risultando importanti nel settore oggetto di studio, lasciano sostanzialmente nelle mani del fornitore la definizione concreta delle procedure tecniche, che coinvolge la "consegna" dei dati alle autorità investigative. Le stesse misure di *audit* originariamente prescritte sono generiche e fanno riferimento alla «garanzia di completezza, immodificabilità e autenticità delle registrazioni», o all'adozione di «dispositivi non alterabili», ovvero a locuzioni del tipo «prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche» oppure, ancora, «l'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati». L'esito dell'attività di controllo deve (solo) essere comunicato alle persone e agli organi legittimati ad adottare decisioni e a esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società e messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria. Tali prescrizioni esprimono le difficoltà relative alla previsione di ulteriori adempimenti, oltre all'obbligo di conservazione dei dati, che comportano impegni organizzativi, strutturali ed economici per i fornitori di servizi.

[33] Alcune criticità sulla c.d. *data retention*, a livello statale (nel caso di specie Germania), ma considerando la prospettiva europea, sono state evidenziate già da U. Sieber, *Straftaten und Strafverfolgung im Internet*, München, 2012, C 128 – C 136. Ulteriori criticità, anche in relazione alla collaborazione fra settori pubblico e privato nella lotta alla criminalità (non solo informatica), sono state messe in risalto dal rapporto "*Comprehensive Study on Cybercrime*" dell'UNODC (*draft* febbraio 2013), in http://www.unodc.org/.

Dall'altro lato, la disposizione italiana, già più volte modificata[34], non è oggi in grado di assicurare il rispetto degli standard elaborati dalla Corte di Giustizia.

Ferme le delicate questioni sui limiti temporali della conservazione dei dati e sulle procedure di accesso e di acquisizione delle informazioni, le criticità principali riguardano, *in primis*, l'individuazione dei "gravi" reati "presupposto", nonché la definizione dei presupposti oggettivi che possano giustificare la *data retention*. In secondo luogo, la valutazione sull'esistenza di un *fumus commissi delicti* dovrebbe essere lasciata ad un organismo indipendente (giudice) attraverso la previsione di una procedura snella e "tempestiva", che consenta comunque un accertamento concreto sulla sussistenza del reato "presupposto", basato su elementi indiziari (provvedimento motivato dell'autorità giudiziaria su richiesta del pubblico ministero, anche su istanza del difensore dell'imputato), che può pervenire ex post, in un lasso di tempo comunqe breve, esclusivamente in ipotesi di urgenza (ad esempio quando sussistono elementi oggettivi e concordanti relativi alla preparazione di attentati terroristici), purchè vi sia una definizione: a) di un elevato livello delle "misure di sicurezza" da adottare e delle procedure da seguire per la conservazione, l'estrazione e, eventualmente, la cancellazione dei dati al termine del procedimento o del trattamento; b) di apposite sanzioni di inutilizzabilità del materiale probatorio acquisito in modo illecito o in caso di mancato rispetto del "principio di necessità" nel trattamento dei dati (ad esempio quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato o le persone a lui collegate solo in caso di indispensabilità).

La soluzione più immediata, ma purtroppo ad effetto "locale", vede come protagonista il nostro legislatore, il quale dovrebbe intervenire ed adattare l'attuale disciplina agli standard elaborati dalla Corte di Giustizia.

Sarebbe però maggiormente auspicale un intervento del legislatore europeo, nell'ambito di una più ampia politica criminale dell'Unione. La stessa individuazione dei fenomeni criminali gravi e di natura transnazionale, nonché la conseguente definizione dei "reati presupposto", potrebbe trovare una base legale nell'art. 83, par. 1, TFUE.

Il *valore aggiunto* riguarda, da un lato, l'efficacia, per la forza vincolante delle fonti per gli Stati membri; dall'altro lato le *garanzie,* che devono circondare la produzione di norme penali (legittimazione democratica e trasparenza del procedimento legislativo, controllabilita` politica, da parte dei Parlamenti nazionali durante la fase « ascendente » dei fondamentali principi di sussidiarieta` europea e di proporzionalita`, ex art. 5 TUE e Protocollo applicativo n. 2 allegato al TFUE, piena controllabilita` giudiziaria di tali presupposti da parte della Corte di Giustizia ed, indirettamente, delle giurisdizioni nazionali nella fase applicativa).

L'epocale sentenza della Corte di Giustizia, di cui si condivide l'iter argomentativo e motivazionale, che fonda le proprie basi nel percorso già intrapreso da numerose Corti costituzionali europee, si scontra con la complessità dell'attuale società dell'informazione, governata dalla inarrestabile rivoluzione informatica e dalla esasperata velocità evolutiva delle tecnologie, che hanno trasformato i dati e le informazioni in "beni immateriali" di inestimabile valore.

Nell'attuale assetto sociale ed economico il ricorso a strumenti investigativi a "contenuto tecnologico" e alla *data retention* risulta indispensabile, per prevenire e per accertare gravi reati lesivi di importanti beni giuridici. Ma proprio la complessità di questo assetto richiede che il bilanciamento fra le contrapposte esigenze di tutela, per il raggiungimento di un fine di interesse generale, avvenga anche sulla base di un rapporto dialogico con le scienze extragiuridiche, con gli "operatori" del diritto e con la società civile.

[34] L'art. 132 Codice Privacy, prima dell'attuazione della direttiva 2006/24/Ce, è stato modificato dal d.l. 24 dicembre 2003, n. 354, convertito con modificazioni dalla l. 26 febbraio 2004, n. 45, ed ha subito ulteriori modifiche con il d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, dalla l. 31 luglio 2005, n. 155 (recante misure urgenti per il contrasto del terrorismo internazionale), dal d.l. 31 dicembre 2007, n. 248, convertito, con modificazioni, dalla l. 27 febbraio 2008, n. 31 e, infine, dalla l. 18 marzo 2008, n. 48, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001. La direttiva europea 2006/24/Ce ha trovato formale attuazione con il d.lgs 30 maggio 2008, n. 109, che ha previsto le categorie di dati da conservare per gli operatori di telefonia e di comunicazione elettronica.