TRIBUNALE COSTITUZIONALE FEDERALE TEDESCO

2 MARZO 2010

PRESIDENTE: **PAPIER**

REDATTORE: **EICHBERGER**

Servizi di comunicazione elettronica • Fornitori di servizi di comunicazione elettronica
- **Conservazione dei dati**
- **Direttiva 2006/24/CE**
- **Compatibilità**
- **Conservazione dei dati**
- **Sicurezza dei dati**
- **Regolamentazione**
- **Criteri**

La conservazione per un periodo di sei mesi dei dati di traffico relativi alle comunicazioni prevista ai sensi della Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15/03/2006, operata in via precauzionale da parte dei fornitori privati di servizi di comunicazione elettronica, non è di per sé incompatibile con l'articolo 10 della Legge Fondamentale, né vi è, dunque, in principio, incompatibilità con la Direttiva. Il principio di proporzionalità esige che le disposizioni di legge che hanno ad oggetto la conservazione dei dati siano commisurate con la interferenza nell'esercizio dei diritti fondamentali che esse comportano. Si rendono necessarie, perciò, disposizioni sufficientemente definite e chiare sulla sicurezza dei dati, sull'utilizzo dei dati, sulla trasparenza e in materia di tutela giurisdizionale.

Massime.

1. La conservazione per un periodo di sei mesi dei dati di traffico relativi alle comunicazioni prevista ai sensi della Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15/03/2006, operata in via precauzionale da parte dei fornitori privati di servizi di comunicazione elettronica, non è di per sé incompatibile con l'articolo 10 della Legge Fondamentale, né vi è, dunque, in principio, incompatibilità con la Direttiva.

2. Il principio di proporzionalità esige che le disposizioni di legge che hanno ad oggetto la conservazione dei dati siano commisurate con la interferenza nell'esercizio dei diritti fondamentali che esse comportano. Si rendono necessarie, perciò, disposizioni sufficientemente definite e chiare sulla sicurezza dei dati, sull'utilizzo dei dati, sulla trasparenza e in materia di tutela giurisdizionale.

3. La garanzia della sicurezza dei dati e la chiara delimitazione della finalità del potenziale uso dei dati debbono costituire parte intrinseca delle disposizioni del Legislatore federale sull'obbligo di stoccaggio dei dati, in conformità con l'articolo 73 comma 1 n. 7 LF. D'altra parte, la responsabilità della regolamentazione, sia sul versante della garanzia della trasparenza che sul fronte della protezione giuridica, è rimessa alle rispettive autorità competenti.

4. Per quanto riguarda la sicurezza dei dati, è necessaria una regolamentazione chiara che fissi standard di sicurezza vincolanti molto elevati. La legge, inoltre, deve poter recepire le continue innovazioni e scoperte che caratterizzano il settore; essa non deve essere definita sulla base di esigenze meramente economiche.

5. La conservazione e l'utilizzo diretto dei dati sono proporzionali allo scopo solo se hanno la funzione di proteggere beni meritevoli della più alta tutela giuridica. Nell'ambito dell'azione penale, ciò implica il ragionevole

sospetto di essere in presenza di un reato grave. Per i compiti legati alla sicurezza e per l'adempimento delle attività dei servizi segreti, l'autorizzazione all'utilizzo dei dati può essere concessa solo in presenza della prova tangibile dell'esistenza di un pericolo concreto per la vita, per l'incolumità fisica o per la libertà dei singoli, per la stabilità e la sicurezza della Repubblica Federale e di ciascun Land, oppure a fronte di una minaccia generale per gli interessi della collettività.

6. Un utilizzo in forma esclusivamente indiretta dei dati conservati dal fornitore di servizi di telecomunicazioni che associano gli indirizzi IP ai nomi dei proprietari delle connessioni non ha collegamento con la creazione di cataloghi di interessi meritevoli di tutela giuridica e dalla definizione di cataloghi di reati per le forze dell'ordine, per le esigenze di sicurezza e per l'esecuzione dei compiti di intelligence consentiti; esso può essere autorizzato solo nei casi espressamente individuati dalla legge.

Dispositivo.

1. Il § 113-*bis* e 113-*ter* della legge sulle telecomunicazioni (*Telekommunikationsgesetz - TKG*), come modificati dall'articolo 2, comma 6, della legge federale di riforma in materia di sorveglianza telefonica (*Gesetz zur Neuregelung der Telekommunikationsüberwachung*), adottata in attuazione della direttiva 2006/24/CE del 21 dicembre 2007 (Gazzetta federale ufficiale - *Bundesgesetzblatt*, parte I, pag. 3198), violano l'art 10, comma 1 della Legge Fondamentale (*Grundgesetz - GG*) e sono pertanto nulli.

2. Il § 100 g, paragrafo 1, comma 1 del codice di procedura penale (*Strafprozessordnung - StPO*), come modificato dall'articolo 1, comma 11 della legge federale di riforma in materia di sorveglianza telefonica (*Gesetz zur Neuregelung der Telekommunikationsüberwachung*) che implementa la direttiva 2006/24/CE del 21.12.2007 (Gazzetta federale ufficiale - *Bundesgesetzblatt*, parte I, pag. 3198), quando il traffico in questione ricade sotto le previsioni del § 113bis della legge sulle telecomunicazioni, è contrario alle disposizioni dell'articolo 10, comma 1 della LF (*Grundgesetz - GG*) ed è nullo in tale misura.

3. In virtù della ordinanza provvisoria dell'11 marzo 2008 - 1 BvR 256/08 (Gazzetta ufficiale federale - *Bundesgesetzblatt*, parte I, pag. 659), reiterata ed estesa con decisione del 28.11.2008 (Gazzetta federale ufficiale — *Bundesgesetzblatt*, parte I, pag. 2239), da ultimo rinnovata con decisione del 15 novembre 2009 (Gazzetta federale ufficiale - *Bundesgesetzblatt*, parte I, pag. 3.704), è autorizzata la conservazione in via provvisoria dei dati relativi alle comunicazioni da parte dei servizi di comunicazione elettronica accessibili al pubblico e dei fornitori di reti pubbliche di comunicazioni, ma non la loro trasmissione alle autorità richiedenti, nel contesto dell'azione penale ai sensi del § 113 frase 1 comma 1 della legge sulle telecomunicazioni; tali dati debbono essere tempestivamente cancellati ad opera dei fornitori di servizi di comunicazione. Essi non possono essere trasmessi alle autorità richiedenti.

4. La Repubblica federale tedesca deve rimborsare ai ricorrenti le spese sostenute per il procedimento dinanzi al Tribunale costituzionale.

Valori comuni in materia di privacy *e trattamento dei dati personali*

1. Le criticità genetiche della direttiva 2006/24/CE relativa alla conservazione di dati generali o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

Il 2 marzo 2010, il Tribunale costituzionale federale tedesco (BVerG) si è pronunciato in merito alla costituzionalità della legge di attuazione della Direttiva 2006/24/CE sulla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[1].

Il giudizio di incostituzionalità espresso in tale sede arriva a pochi mesi di distanza da un'analoga sentenza della Corte costituzionale romena che ha dichiarato incostituzionale la legge n. 298 del 2008 sul *data retention* per violazione del principio della segretezza della corrispondenza privata, del diritto alla *privacy*, della libertà di espressione e della libertà di circolazione[2]. Il giudizio della Corte di Karlsruhe ripropone due degli elementi cruciali già rilevati all'interno della decisione dell'omologo romeno: da un lato, la Direttiva non viene fatta oggetto di censure e i rilievi critici sono indirizzati in via esclusiva avverso le rispettive leggi nazionali di trasposizione; dall'altro, entrambi i giudizi sembrano sottendere una più generale diffidenza nei confronti del disegno complessivo di conservazione generalizzata dei dati relativi al traffico telefonico e telematico nonché del bilanciamento tra le opposte esigenze di tutela della *privacy* e di sicurezza nazionale, di *data protection* e *data retention*, operato dal legislatore comunitario. In questo quadro, lo spazio per una legge che implementi la Direttiva e che possa, allo stesso tempo, soddisfare i requisiti di costituzionalità individuati dalle due corti, si è rivelato estremamente risicato.

L'intervento del legislatore comunitario inteso ad armonizzare le disposizioni degli Stati membri in tema di conservazione dei dati di riferimento delle comunicazioni telefoniche e telematiche, prende forma nei mesi immediatamente successivi agli attacchi terroristici di Madrid del 2004; ed agli analoghi attacchi che colpiscono Londra nel luglio 2005 fa seguito la definitiva approvazione della Direttiva 2006/24/CE[3]. L'esigenza di incrementare la sorveglianza sul traffico telefonico e telematico è, quindi, strettamente correlata all'obiettivo di approntare una strategia antiterrori-

[1] Bundesverfassungsgericht, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, 2 marzo 2010; il testo della sentenza è disponibile all'indirizzo: *http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.*

[2] Curtea Constituionalã Decizia, 1258, 8 ottobre 2009, pubblicata in *Monitorul Oficial* n. 789 del 23 novembre 2009. La traduzione in inglese (non ufficiale) è reperibile all'indirizzo: *http://www.legiinternet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf.*

[3] « Direttiva del Parlamento europeo e del Consiglio riguardante la conservazione dei dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE ». Per un esame dettagliato della Direttiva in esame, cfr. S. Monteleone, *La tutela dei dati personali nelle comunicazioni elettroniche tra esigenze di Data Protection e obblighi di Data Retention*, in P. Costanzo, G. De Minico, R. Zaccaria (a cura di), *I « tre codici » della Società dell'Informazione*, Torino, 2006, 320 ss.

stica globale che trova nella Gran Bretagna il principale propulsore, fiancheggiato dall'alleato americano; la conservazione dei dati è di fatti intesa a « garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascun membro nella propria legislazione nazionale » (art. 1, comma 1). I *consideranda* della Direttiva danno conto del bilanciamento degli interessi in gioco definito in sede comunitaria: la conservazione dei dati per un periodo di tempo limitato si rende necessaria ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati (considerando 7), ma in capo agli Stati membri grava l'obbligo di « tutelare i diritti e le libertà delle persone fisiche relativamente al trattamento dei dati personali ed, in particolare, il diritto alla vita privata » (considerando 1), nel rispetto dei requisiti previsti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (considerando 9). Inoltre, nella fase dell'accesso ai dati da parte delle autorità competenti, le legislazioni nazionali debbono rispettare i diritti fondamentali quali risultanti dalle tradizioni costituzionali comuni agli Stati membri e dalla CEDU; in particolare, si fa esplicita menzione del principio di « proporzionalità e necessità dell'ingerenza di un'autorità pubblica nel diritto alla riservatezza » affermato nell'art. 8 della CEDU (considerando 25). L'art. 5 della Direttiva precisa che i dati rispetto ai quali incombe l'obbligo di conservazione sono tutti quelli che consentono di rintracciare e identificare la fonte di una comunicazione, la sua destinazione, la data, l'ora e la durata, il tipo di comunicazione e le attrezzature impiegate nonché, in caso di utilizzo di apparecchiature di comunicazione mobile, i dati necessari per individuarne l'ubicazione; sono invece esclusi dal novero delle informazioni soggette a raccolta, i contenuti delle comunicazioni elettroniche e le informazioni consultate attraverso le reti di comunicazione elettronica (art. 1.2), mentre non vengono fatti salvi i dati relativi ai tentativi di chiamata non riusciti (art. 3, comma 2). L'obbligo di raccolta di dati sul traffico si impone ai fornitori di servizi di comunicazione elettronica accessibili al pubblico ed a i fornitori di reti pubbliche di comunicazioni (art. 3) e la durata del periodo di conservazione deve essere stabilita dagli Stati membri, purché resti compresa tra un minimo di sei mesi ed un massimo di due anni dalla data della comunicazione, con possibilità di proroga per un periodo di ulteriori due anni (artt. 6 e 12 della Direttiva). È rimessa alle singole legislazioni nazionali, infine, la scelta della tipologia di misure da adottare per garantire che i dati sul traffico siano conservati in conformità con le disposizioni della Direttiva, nonché la determinazione degli strumenti atti a garantire che i dati siano trasmessi solo alle autorità nazionali competenti (art. 4).

La disciplina della conservazione dei dati prevista dalla Direttiva 2006/24/CE ha innovato le previsioni precedenti, capovolgendo il paradigma delineato e spostando di misura l'equilibrio consolidato fra libertà individuali e collettive. Se, in particolare, la Direttiva 95/46/CE « relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati » e la successiva Direttiva 2002/58/CE « relativa al trattamento dei dati personali e della vita privata nel settore delle comunicazioni elettroniche » si caratterizzavano per un approccio inteso ad assicurare innanzitutto la generale tutela della *privacy* e la protezione dei dati, nella Direttiva del 2006 è il « principio del « più sicurezza e meno *privacy* » che sembra

avere la meglio[4]. I pareri del Garante europeo della protezione dei dati ed i rilievi critici espressi a più riprese dal Gruppo di Lavoro « Articolo 29 »[5] hanno richiamato sovente i principi orientatori per giudicare della legittimità delle ingerenze nella vita privata individuati dall'art. 8 della CEDU e, con particolare riferimento al parametro della necessità della misura « in una società democratica », hanno evidenziato che « il problema fondamentale, attinente alla conservazione dei dati di traffico, è l'automatismo generalizzato di tale operazione, il conservare ''tutto di tutti'', anche di coloro che non sono imputabili di alcunché »[6]. Si presentava, poi, carente, il fronte delle garanzie e della conseguente protezione dei diritti fondamentali, che avrebbe dovuto includere norme chiare sull'accesso ai dati e sull'uso e lo scambio degli stessi, oltre che la precisazione della limitata finalità della raccolta dei dati. Sul versante della proporzionalità, infine, il Garante europeo invitava a ridurre i periodi di conservazione ed a limitare il numero dei dati da memorizzare: gli emendamenti proposti sono stati in larga misura disattesi, specie con riferimento ai tempi di conservazione dei dati, laddove la possibilità di prorogare il periodo massimo di due anni previsto dall'art. 12 della Direttiva « qualora uno stato membro si trovi ad affrontare particolari circostanze che giustifichino tale proroga », compromette in principio i propositi di armonizzazione e dilata in maniera potenzialmente illimitata il termine fissato dall'art. 6 della stessa Direttiva[7].

2. La normativa tedesca di recepimento della direttiva 2006/24/CE.

Il recepimento della direttiva comunitaria in Germania ha avuto luogo con la legge federale *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG* (*VDS-Gesetz*) del 21 dicembre 2007[8], che ha modificato il codice di procedura penale federale (*Strafprozessordnung* - StPO) e la legge federale in materia di sorveglianza telefonica

[4] Così C. Fatta, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Diritto dell'Informazione e dell'Informatica*, in questa *Rivista*, n. 3/2008, 408. Per il punto vedi inoltre F. Cerqua, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, in *Sistema penale e criminalità informatica*, a cura di L. Luparia, Milano, 2009; C. Conti, *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in *Le nuove norme sulla sicurezza pubblica*, a cura di S. Lorusso, Padova, 2008; E. Forlani, *La conservazione preventiva di dati informatici per l'accertamento dei reati*, in *Diritto dell'Internet*, 3/2008, 520 e ss.; M. Gialuz, *La cooperazione informativa quale motore del sistema europeo di sicurezza*, disponibile all'indirizzo: *http://www.openstarts.units.it/dspace/bitstream/10077/3346/1/02Gialuz.pdf*; S. Monteleone, *La tutela dei dati personali nelle comunicazioni elettroniche tra esigenze di Data Protection e obblighi di Data Retention*, cit.

[5] Istituito dall'art. 29 della Direttiva 95/46/CE, il Gruppo di Lavoro « Articolo 29 » è un organo consultivo indipendente che si occupa della protezione dei dati e della vita privata. I suoi compiti sono enumerati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

[6] Cfr. C. Fatta, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Diritto dell'Informazione e dell'Informatica*, in questa *Rivista*, cit.

[7] *Ibidem*.

[8] BGBI I S. 3198, entrata in vigore il 1º gennaio 2008.

(*Telekommunikationsüberwachungsgesetz* - TKG). La legge varata dalla *Große Koalition* emenda la legislazione preesistente, ampliando il novero dei dati soggetti a conservazione, estendendo la possibilità da parte delle autorità statali di accedere a tali dati e diluendo, al contempo, la disciplina che impone all'autorità governativa che ravvisi la necessità di esaminare i dati di illustrare la finalità della consultazione. La *VDS-Gesetz* individua quattro gruppi principali di attori che hanno la facoltà di accedere alle raccolte di dati e stabilisce, inoltre, che qualsiasi ufficio governativo possa consultare i dati di identificazione primaria quali, ad esempio, nome, data di nascita e indirizzo, senza dovere dimostrare quale sia l'interesse pubblico la cui tutela renda necessaria la consultazione. Il periodo di tempo in cui i dati relativi alle comunicazioni devono essere conservati non può superare il termine massimo di sei mesi dalla data della comunicazione stessa[9].

La legge con cui la Germania ha recepito la Direttiva 24/2006, riproducendo in buona sostanza tutte le criticità della Direttiva europea, ha suscitato un diffuso malcontento tale da unificare ampi segmenti della società nel nome della tutela dei diritti digitali e della protezione della *privacy*. A soli due mesi dall'approvazione della *VDS-Gesetz*, si è costituita una nuova ONG, l'*Arbeitskreis Vorratsdatenspeicherung* (Gruppo di lavoro sulla conservazione dei dati), capace di sensibilizzare settori eterogenei della società su temi tecnicamente complessi. Il Tribunale costituzionale è stato sommerso da circa trentacinquemila ricorsi[10] accompagnati dalla richiesta di sospendere la raccolta dei dati per « manifesta incostituzionalità » della legge con ricorso ad una ordinanza cautelare.

La grande attenzione della società civile, in buona parte frutto della massiccia diffusione delle tecnologie digitali per le comunicazioni in Germania, si accompagna ad una riflessione giurisprudenziale di lungo corso sui temi della protezione dei dati e della tutela dei diritti digitali inaugurata dalla cosiddetta sentenza *Mikrozenzus* datata 1969[11] e sviluppata in maniera ancor più organica dalla successiva *Volkszählungsurteil*[12] del 1983. A partire da tale data, la giurisprudenza costituzionale ha sviluppato un *corpus* di principi imperniati sul riconoscimento del diritto all'autodeterminazione informativa (*Recht auf Informationelle Selbstbestimmungen*), ovvero il diritto di controllare l'uso che gli altri fanno delle informazioni personali esercitando un potere di controllo sul flusso dei dati, regolandone le modalità di raccolta e di gestione, ed interrompendo il flusso stesso quando lo si reputi opportuno[13]. La Corte ha ripetutamente precisato, inoltre, che qualsiasi legge che violi *prima facie* un diritto costituzionale deve avere come scopo la protezione di un altro diritto tutelato dalla Costituzione, che la violazione del diritto deve essere necessaria a raggiungere l'obiettivo previsto e che la violazione deve essere altresì proporzionata alla protezione che si ottiene in cambio. Sulla base del dettato della GG, che agli art. 1(1) e 2(1) GG tutela la dignità umana e il diritto alla libertà perso-

[9] Si noti che il limite minimo di sei mesi per la conservazione dei dati fissato dal legislatore comunitario assurge a limite massimo per il legislatore tedesco.

[10] Si noti che nell'elenco dei ricorrenti figura anche il nome del nuovo Ministro della Giustizia Tedesco Sabine Leutheusser-Schnarrenberger.

[11] *Mikrozensus* (1969), 27 BVerfGE.

[12] *Zensus* (1983), 65, 1, BVerfGE.

[13] Cfr. G. Hornung e C. Schnabel, *Data protection in German I: The Population Census Decision and the Right to Informational Self-Determination*, in *Computer Law & Security Review*, n. 85, 2009, 115-122.

nale[14], la giurisprudenza di Karlsruhe ha sviluppato una nozione di *privacy* quale bene collettivo che si sostanzia nella salvaguardia di tre sfere distinte: la *Individualsphäre*, che comprende tutte le informazioni sulle interazioni sociali degli individui; la *Privatsphäre*, che include le informazioni sulla vita privata che generalmente sono accessibili al pubblico; la *Intimsphäre*, che abbraccia tutte le informazioni personali strettamente confidenziali[15]. La *privacy* viene a configurarsi quale declinazione del diritto all'identità personale[16] ed alla dignità, assurgendo a diritto fondamentale ed inalienabile e ricomprendendo, tra gli altri, il diritto alla riservatezza della corrispondenza, la tutela dalla diffamazione, la tutela della *privacy* sessuale ed il diritto alla autodeterminazione informativa.

Con la sentenza del 27 febbraio 2008, il quadro della tutela del diritto alla riservatezza e della protezione dei dati e delle informazioni si è arricchito di un nuovo e prezioso tassello; nel giudizio di costituzionalità sulla Legge sulla protezione della Costituzione del North Rhein Westfalia (*Gesetz über den Verfassungsschutz in Nordrhein-Westfalen*), che autorizzava il monitoraggio segreto di Internet e l'accesso segreto ai sistemi informatici a fini investigativi (cd. *Online Durchsuchung*), la Corte ha « incentrato l'attenzione sui presupposti per l'utilizzo delle misure investigative e sulle garanzie assicurate alla persona » ed ha riconosciuto, accanto al diritto all'autodeterminazione informativa, un « nuovo diritto all'integrità e riservatezza dei sistemi informatici, quali manifestazioni analoghe dell'*Allgemeine Persönlichkeitsrecht* »[17]. Il diritto all'integrità ed alla confidenzialità dei sistemi informatici (*Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme*) ha assunto, così, rilevanza costituzionale[18], finendo per ispessire ulteriormente la tutela della libertà della vita privata apprestata dalla *Grundgesetz*; il giudizio di incostituzionalità espresso dalla Corte ha significativamente rimarcato che « nella tensione tra l'obbligo per lo Stato di tutelare beni giuridici e gli interessi dei singoli al rispetto dei loro diritti garantiti dalla Costituzione, il compito del legislatore è quello di realizzare un bilanciamento tra i contrapposti interessi. Pertanto, la disciplina e l'uso dei [...] nuovi mezzi investigativi tecnologici sono conformi al principio di proporzionalità solo se necessari alla protezione di *importanti e predominanti beni giuridici* »[19].

In questa sede, vale la pena di sottolineare che, a partire dal *Volkszählungsurteil* del 1983, il Tribunale costituzionale non ha riconosciuto la

---

[14] L'art. 1(1) e 2(1) GG garantiscono il diritto al libero sviluppo della propria personalità ed il generale « diritto alla dignità ».

[15] Cfr. C. Degenhardt, *Das Allgemeine Persönlichkeitsrecht*, in *Juristiche Schulung*, n. 32, 1992, 361-368.

[16] Sul punto, cfr., particolarmente, L. Trucco, *Introduzione alla studio dell'identità personale*, Torino, 2004, 232 ss.

[17] Così R. Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht del 27 febbraio 2008 sulla c.d. Online Durchsuchung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona*, in *Riv. trim. dir. pen. econ.*, 2009, 679 ss. Per il punto vedi anche C. Fatta, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Diritto dell'Informazione e dell'Informatica*, in questa *Rivista*, cit., p. 409.

[18] Sul punto, cfr., P. Costanzo, *Una conversazione mondiale continua*, in *Tecniche normative* (*http://www.tecnichenormative.it/draft/extraCost.doc*).

[19] Così R. Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht del 27 febbraio 2008 sulla c.d. online durchsuchung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona*, cit.

privacy quale diritto assoluto, prevedendo, al contrario, la possibilità di comprimere tale diritto quando lo richiedano esigenze imperative di tutela degli interessi collettivi; parallelamente, poi, il giudice ha fornito un elenco tassativo di garanzie al cui rispetto subordinare la compressione del diritto alla riservatezza. Le ingerenze nella *privacy* dei cittadini sono ammesse purché dirette a realizzare un obiettivo legittimo, individuato in maniera limpida ed altamente specifico, nel rispetto del principio di proporzionalità ed a fronte di garanzie procedurali nella gestione del flusso di dati che mettano al riparo da potenziali abusi nel trattamento degli stessi[20]. I provvedimenti potenzialmente lesivi del diritto alla *privacy* sono compatibili con la Costituzione tedesca solo se in linea con tali prescrizioni. In assenza dei succitati parametri di costituzionalità per i cittadini verrebbe meno la possibilità di determinare« *wer, was, wann und bei welcher Gelegenheit über sie weiß* » e un ordine sociale siffatto sarebbe incompatibile con il diritto all'autodeterminazione informativa. Infatti, « *wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist* »[21]. La vitalità della società civile e, per il suo tramite, la vitalità dei processi democratici non può prescindere dalla tutela dei dati riguardanti i rapporti degli individui tra loro e con le istituzioni, i dati circa l'appartenenza a partiti, sindacati, associazioni e movimenti: la *privacy* è una condizione essenziale per potere essere inclusi a pieno titolo nella società civile e nella vita politica. In assenza di una ferma tutela dell'insieme delle informazioni raccolte su ciascun individuo risultano fiaccate le spinte verso la partecipazione civica e la stessa libertà personale è messa a repentaglio[22].

Il *VDS-Gesetz* nella versione definitiva approvata dal *Bundestag* l'8 novembre 2007 non soddisfa, dunque, i requisiti di costituzionalità fissati dalla giurisprudenza del BVerG. In particolare, la legge di recepimento della Direttiva 24/2006/CE non delinea con sufficiente chiarezza lo scopo della registrazione e della eventuale trasmissione dei dati. Se la *VDS-Ge-*

[20] Vedi in particolare: 1969, 27 BVerfGE - *Mikrozensus*; 1893, 65, 1, BVerfGE - *Zensus*; 2005, 113, 348 BVerfGE - *Vorbeugende Telekommunikationsüberwachung*; 2008, 595 BVerfGE - *Online Durchsuchung*.

[21] « Chiunque tema che, in un qualsiasi momento, la propria opinione dissenziente possa essere registrata e conservata, proverà ad evitare di mettere in atto comportamenti tali da generare questo tipo di informazioni. […] Ciò comprometterebbe non solo la libertà di scelta di ciascun individuo, ma anche il benessere della collettività, poiché l'autodeterminazione è il presupposto per la crescita di una società libera e democratica ». Cfr. *Volkszählungsurteil*, BVerfGE 65, 1, par. 43.

[22] Sul punto vedi P. Breyer, *Telecoms data retention and human rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, in *European Law Journal*, 2005, 365 ss. L'Autore osserva in particolare che « *this chilling effect is especially harmful in cases that attract abuses of power, namely in the case of organizations and individuals who are critical of the government or even the political system. Blanket data retention can ultimately lead to restricted political activity, bringing about damage to the operation of our democratic states and thus to society* ».

setz individua tre serie di obiettivi ai quali sacrificare la *privacy* dei cittadini (l'esercizio dell'azione penale, la prevenzione dei crimini gravi e l'espletamento delle funzioni di intelligence da parte dei servizi segreti autorizzato per legge) non illustra tuttavia in quale maniera ed in quale misura la consultazione dei dati raccolti possa contribuire al perseguimento di tali fini. Inoltre, il testo della legge non definisce in maniera univoca quali siano i « crimini gravi » che giustificano la trasmissione dei dati alle autorità pubbliche, mancando sia un elenco delle tipologie di crimine ascrivibile al numero delle infrazioni che giustifichino la compressione del diritto alla *privacy*, sia una lista delle caratteristiche che consentirebbero di individuare tali crimini[23]. Se l'obiettivo della raccolta non è sufficientemente specifico, esso potrà essere definito in maniera esaustiva soltanto *ex post* e si potrà fare ricorso alla conservazione ed alla trasmissione dei dati anche in funzione preventiva, ampliando così la portata e le finalità della Direttiva. La scarsa proporzionalità del provvedimento in esame è aggravata dalla mancata previsione di garanzie procedurali che tutelino gli individui nella fase di trasmissione dei dati[24].

L'11 marzo del 2008 il BVerG[25] ha deciso di non fermare la raccolta dei dati, ma ha imposto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico e a i fornitori di reti pubbliche di comunicazioni il divieto di fornire alle autorità statali le informazioni custodite per sei mesi, con l'obiettivo di sfruttare questo lasso di tempo per potere esaminare i ricorsi e decidere della costituzionalità della *VDS-Gesetz*; in questa circostanza il BVerG riconosceva che la conservazione generalizzata ed indiscriminata dei dati avrebbe potuto avere un effetto deterrente sul ricorso alle comunicazioni elettroniche da parte dei cittadini. Le principali obiezioni sollevate dall'opinione pubblica riguardavano la definizione incompleta del processo di trattamento delle informazioni e la mancata previsione di controlli ad opera di autorità giudiziarie indipendenti al fine di evitare e, eventualmente, perseguire gli abusi; ulteriori critiche si appuntavano sulla mancata previsione di forme di compensazione economica a favore degli operatori sui quali gravava per intero l'onere della implementazione della normativa; la previsione di una generalizzata ed indiscriminata conservazione dei dati sembrava ingenerare inoltre la sensazione che tutti gli utenti fossero potenziali criminali; si arrecava, infine, pregiudizio ad alcune categorie professionali ed a taluni servizi di pubblica utilità per i quali la garanzia dell'anonimato delle comunicazioni appare essenziale (si pensi ad esempio, al segreto professionale cui sono tenuti i medici ed all'attività dei servizi telefonici di pronto intervento); più in generale, si lamentava un bilanciamento tra *data protection* e *data retention* che svilisce la prima esigenza esaltando la seconda.

3. La *privacy* tra disciplina comunitaria e identità costituzionale tedesca.

Per quanto riguarda la pronunzia di merito, la BVerG analizza innanzitutto l'opportunità di riferire la questione preliminare alla Corte di Giu-

[23] Cfr. C. De Simone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, in *German Law Journal*, Vol. 11, n. 3/10, 310 e ss.

[24] *Ibidem*.

[25] BVerfGE 121, 1.

stizia concludendo però come ciò non fosse necessario, sia alla luce dell'articolato della Direttiva che alla luce della sentenza della corte di Lussemburgo del 10 febbraio 2009[26]. Il Tribunale costituzionale prosegue esaminando le norme in materia di protezione dei dati contenute nella legge federale in materia di sorveglianza telefonica e quelle contenute nel codice di procedura penale federale sottolineando come, ai sensi dell'art. 10 della *Grundgesetz*, « la protezione delle comunicazioni non includa soltanto il contenuto ma anche la segretezza delle circostanze in cui la comunicazione ha luogo e specialmente il se, il quando e il numero di volte in cui un individuo contatta o prova a contattare un altro individuo »[27]. Nell'analizzare le basi legali della *VDS-Gesetz*, poi, la Corte sostiene che in linea di principio la conservazione per un periodo massimo di sei mesi possa ritenersi legittima purché riconosciuta come misura eccezionale (« *dass diese eine Ausnahme bleibt* »), poiché tale provvedimento accresce fortemente il rischio che i cittadini siano soggetti ad indagini anche se non hanno commesso alcun reato (« *unabhängig von einer wie auch immer geregelten Ausgestaltung der Datenverwendung das Risiko von Bürgern erheblich steigt, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst Anlass dazu gegeben zu haben* »[28]); per di più, prosegue il giudice, la raccolta e la conservazione dei dati potrebbero ingenerare una sensazione di controllo permanente (« *ein Gefühl des ständigen Überwachtwerdens* ») e di diffuso pericolo (« *diffuse Bedrohlichkeit* »). È lo stesso funzionamento della democrazia tedesca ad essere messo a repentaglio poiché la registrazione indiscriminata dei dati fa sì che i cittadini non siano a conoscenza del numero di informazioni che li riguardano che sono a disposizione delle autorità pubbliche, vivendo, perciò, nel timore costante che queste ultime abbiano cognizione di un numero cospicuo di dati confidenziali[29].

---

[26] L'Irlanda, sostenuta in seguito dalla Slovacchia, ha presentato un ricorso alla Corte di Giustizia contestando la legittimità del provvedimento perché fondato su basi legali errate e, in particolare, sul diritto comunitario e non sulla cooperazione di polizia. Nel febbraio 2009 la Corte di Giustizia ha giudicato tuttavia legittima la Direttiva europea (C-301/06, *Ireland v European Parliament and European Council*). Sul punto vedi C.C. Murphy, *Fundamental Rights and Security: The Difficult Place of the European Judiciary*, disponibile in *http://ssrn.com/abstract=1513611*.

[27] « *Dieser Schutz erfasst dabei nicht nur die Inhalte der Kommunikation. Geschützt ist vielmehr auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist* », par. 189. Con la sentenza n. 81 dell'11 marzo 1993, in tema di tabulati telefonici e della idoneità degli stessi a costituire mezzo di prova del reato di molestie telefoniche, la Corte costituzionale italiana era pervenuta a conclusioni simili, includendo nell'ambito della garanzia apprestata dall'art. 15 della Costituzione la segretezza dei dati esterni alla comunicazione, e sostenendo in particolare che il requisito della confidenzialità della corrispondenza comprende « non solo la segretezza del contenuto, ma anche quella relativa all'identità dei soggetti e ai riferimenti di tempo e di luogo della comunicazione stessa » (Corte Cost. 11 marzo 1993, n. 81, in *Giur. cost.*, 1993, fasc. 2, 731).

[28] Cfr. par. 212.

[29] « *Eine vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten über sechs Monate ist unter anderem deshalb ein so schwerwiegender Eingriff, weil sie ein Gefühl des ständigen Überwachtwerdens hervorrufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der Einzelne weiß nicht, was welche*

Il cuore dell'argomentazione della sentenza sta nella verifica del rispetto del principio di proporzionalità alla luce di quattro criteri che costituiscono il nucleo duro del diritto alla *privacy* così come delineato dalla giurisprudenza tedesca in materia: la sicurezza dei dati, la chiara individuazione della finalità del provvedimento, la trasparenza e la predisposizione di meccanismi di tutela in caso di abusi. Se il livello di sicurezza necessario viene qualificato come « estremamente elevato » senza che si specifichi la tipologia di strumenti cui fare ricorso, per quanto attiene alla determinazione dello scopo della conservazione dei dati il Tribunale costituzionale accorda al legislatore un certo margine discrezionale; esso può, infatti, scegliere di creare un catalogo nuovo di reati *ad hoc* od attingere a quelli esistenti. La qualificazione dei reati come « gravi » deve tuttavia trovare conforto in elementi oggettivi e non può rimandare in via generale a concetti generici. I beni tutelati tramite la raccolta e la conservazione dei dati di riferimento delle comunicazioni telefoniche e telematiche vengono esplicitamente richiamati (si tratta dell'integrità fisica, del bene alla vita e della libertà personale, della sicurezza della Repubblica Federale e del benessere pubblico) e si precisa che l'utilizzo dei dati deve avere luogo solo a fronte del profilarsi di una minaccia concreta; si rende necessaria, cioè, la prova dell'esistenza di un pericolo tangibile e imminente. Inoltre, la Corte dichiara che è necessario garantire per legge che i dati siano valutati immediatamente dopo la consegna all'autorità richiedente e, se giudicati irrilevanti, istantaneamente cancellati. Si ritiene, poi, che la lista dei dati soggetti a raccolta e a trasmissione andrebbe limitata, specie con riguardo alle attività connesse con lo svolgimento di particolari professioni od ai numeri telefonici dedicati ai servizi di pubblica utilità. Quanto al requisito della trasparenza, si richiede la notifica al soggetto interessato del provvedimento in atto; in alternativa, si invoca un controllo giurisdizionale preventivo in modo da scongiurare una compressione grave dei diritti fondamentali. In merito alla prevenzione ed alla sanzione degli abusi, il Tribunale sollecita, infine, la predisposizione di sanzioni effettive e proporzionali contro eventuali usi dei dati che violino la segretezza delle comunicazioni; in assenza di tali strumenti, la tutela dei diritti della personalità (*Allgemeine Persönlichkeitsrecht*) fondata sull'art. 10 GG sarebbe gravemente compromessa[30].

I giudici di Karlsruhe hanno, dunque, stabilito che la legge, con la quale la Germania ha recepito la Direttiva 24/2006, è incostituzionale perché non soddisfa i requisiti di proporzionalità e certezza sopraelencati; in particolare, le disposizioni contestate sono incompatibili con il diritto alla segretezza delle telecomunicazioni di cui all'articolo 10.1 GG. La Corte ha altresì richiesto che tutti i dati conservati sino alla data della sentenza vengano immediatamente cancellati. Il BVerG non ha posto un divieto assoluto alla conservazione dei dati sulle comunicazioni telefoniche ed elettro-

staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können », par. 241.

[30] « *Schließlich setzt eine verhältnismäßige Ausgestaltung wirksame Sanktionen bei Rechtsverletzungen voraus. Würden auch schwere Verletzungen des Telekommunikationsgeheimnisses im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts, auch soweit er in Art. 10 Abs. 1 GG eine spezielle Ausprägung gefunden hat* », par. 252.

niche da parte delle società che forniscono tali servizi, ma ha reclamato la redazione di una nuova norma che sappia affrontare in maniera più efficace la delicata questione della proliferazione dei dati digitali, individuando un nuovo punto di equilibrio tra l'esercizio delle pur necessarie forme di controllo e la tutela del diritto alla riservatezza che sia compatibile con la Legge Fondamentale.

Uno dei passaggi cruciali della sentenza è il paragrafo 218, che contiene tre affermazioni distinte che paiono comporre un « monito » indirizzato al legislatore comunitario e agli altri Stati membri. In esso il giudice di Karlsruhe stabilisce innanzitutto che la conservazione indiscriminata e generalizzata dei dati relativi alle comunicazioni sia incompatibile con l'identità costituzionale e con il principio della conservazione dell'identità (*Identitätsvorbehalt)* quale enunciato dalla Corte in occasione della recente pronuncia sul Trattato di Lisbona[31] (« *Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland […] für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss* »). In secondo luogo, la Corte asserisce che, al fine di rimanere in linea con la tutela dei diritti approntata dalla costituzione tedesca, la registrazione e la conservazione dei dati relativi al traffico telefonico e telematico debbono costituire una eccezione (« *Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt* »). Infine, nello stesso paragrafo il giudice ricorda con preoccupazione che il margine di apprezzamento rispetto alla raccolta di dati effettuata in via precauzionale sta diventando sempre più ridotto in tutta l'Unione Europea (« *durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer* »).

Il richiamo al *Lissabon Urteil* si dimostra particolarmente significativo. Nella sentenza sulla ratifica del Trattato di Lisbona il trasferimento di porzioni di sovranità all'indirizzo dell'Unione Europea è stato ritenuto ammissibile solo fino a quando gli Stati membri conservino « *ihre Fähigkeit zu selbstverantwortlicher politischer und sozialer Gestaltung der Lebensverhältnisse* »[32]; le arene statali continuano a costituire, perciò, lo spazio pubblico destinato a modellare le forme della convivenza civica e politica. Letto in connessione con la necessità che il *data retention* si configuri quale « eccezione », il riferimento al *Lissabon Urteil* vale a rivelare la difficoltà della Corte nell'accettare il sistema complessivo della raccolta e dello stoccaggio generalizzato di dati previsto dalla Direttiva comunitaria, che appare estraneo al nucleo duro dell'identità costituzionale tedesca. « Onorando » la celebre sentenza Solange II del 1986[33], la Corte ha scelto di non contestare la tutela dei diritti umani

[31] 2 BvE 2/08, 2 BvE 5/08, 2 BvR 1010/08, 2 BvR 1259/08, 2 BvR 182/09, 30.06.2009; il testo della sentenza è reperibile all'indirizzo: *http://www.bundesverfassungsgericht.de/entscheidungen/es20090630_2bve000208.html.*

[32] *Ibidem*; « la propria facoltà di modificare autonomamente i modelli politici e sociali della convivenza civile ». Cfr. par. 226, C.

[33] 2 BvR 197/83 del 22 ottobre 1986.

approntata dal legislatore comunitario, ma parallelamente ha dichiarato incostituzionale la legge che recepisce la Direttiva 24/2006 censurando tutte le misure della *VDS-Gesetz* nella misura in cui esso « *exceeded the terms of the Directive, […] until brought in line with German constitutional requirements* »[34]. Sembra trovare concreta applicazione quella « riserva di configurazione nazionale dello spazio pubblico » con cui la Corte ha inteso « sottolineare che in determinati settori il dispiegarsi di un'autentica sfera pubblica discorsiva non può prescindere da un comune trascorso storico — culturale — e valoriale »[35]. E sembra, inoltre, che l'intero l'intervento disegnato dal legislatore comunitario finisca per essere sconfessato perché, se le cautele approntate dal legislatore tedesco non paiono sufficienti, è soprattutto il bilanciamento tra la tutela dei diritti e il fine della repressione dei reati a determinare le censure della Corte risultando in una serie di misure eccessivamente lesive del diritto alla riservatezza. L'archiviazione sistematica appare di per sé inaccettabile[36].

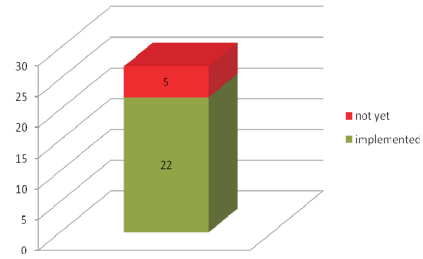
4. *Segue*: *privacy* e conservazione dei dati nella prospettiva europea.

La sentenza del BVerfG sembra fungere da cassa di risonanza ad un movimento di opinione che ha propaggini profonde in Germania ed ha finito per abbracciare l'intera Europa. Se il giudice di Karlsruhe, infatti, ha ricevuto in questa circostanza il più alto numero di ricorsi della sua storia, anche nel resto del Continente la società civile ha mostrato profonda attenzione al problema della tutela della *privacy* accogliendo con diffidenza sia la Direttiva 24/2006 sia le leggi di implementazione che ne hanno dato attuazione. In taluni Paesi le proteste della società civile sono state talmente vibrate da indurre il legislatore a ritardare il recepimento ben oltre i tempi massimi previsti[37]. Sono nati, poi, una serie di

[34] Cfr. C. De Simone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, op. et loc. ult. cit.

[35] Vedi B. Guastaferro, *Il Trattato di Lisbona e la triplice « riserva » apposta dal Bundesverfassungsgericht*, disponibile all'indirizzo *www.astrid-online.it*.

[36] Come è stato osservato in occasione della pronuncia della Corte Costituzionale Romena, « *the only possible way to accord the decision of the Court with the Directive is for the Community act to be amended […]. Any subsequent national measure aimed to implement the Directive should produce the same result in a subsequent reasoning of the Court. A cat-and-mouse game would start between the legislator who needs to implement the Directive and avoid infringement and the Constitutional Court who asserts guardianship of fundamental rights* », cfr. C. Gânj, « *The lives of other judges: Effects of the Romanian data retention judgment* », disponibile in: *http://ssrn.com/abstract=1558043*.



[37] Il seguente schema, ripreso da G. Marcoccio, *La Direttiva europea per la conservazione dei dati di traffico elettronico e telematico per finalità di giustizia e le attuali perplessità sui recepimenti nei Paesi Ue*, disponibile all'indirizzo

network trans-europei con l'obiettivo di tutelare il diritto alla riservatezza in maniera trasversale all'interno del Continente. Come già ricordato, l'Irlanda, cui si è unita successivamente la Slovacchia, ha presentato un ricorso dinanzi alla Corte di Giustizia sostenendo che la Direttiva 2006/24/CE, non essendo finalizzata a migliorare il funzionamento del mercato interno *ex* art. 95 Trattato CE, ma a favorire la raccolta dei dati per scopi di sicurezza pubblica e lotta al terrorismo, avrebbe dovuto essere fondata sul cd. terzo pilastro e non già sul primo. La Corte ha respinto il ricorso[38], sostenendo che compito della Direttiva fosse quello di armonizzare il mercato interno e che, pertanto, il provvedimento sarebbe stato correttamente inquadrato al di fuori della cooperazione giudiziaria e di polizia in materia penale[39]. Anche le autorità garanti nazionali sono intervenute puntualmente a censurare la disciplina comunitaria; peculiare la posizione del Garante per la protezione dei dati personali italiano il quale ha ripetutamente sollecitato il recepimento tempestivo della Direttiva europea, che prometteva di tutelare in maniera più forte il diritto alla *privacy* rispetto alla vigente disciplina italiana soprattutto con riferimento ai tempi di conservazione dei dati; nel mentre, il Garante forniva prescrizioni tecniche indirizzate agli operatori affinché garantissero elevati livelli di sicurezza nella raccolta e nello stoccaggio dei dati ed offriva una serie di indicazioni interpretative della disciplina comunitaria in ordine alla tipologia di dati da conservare, alle finalità perseguibili e alle modalità di acquisizione dei dati[40].

Lo stesso Parlamento Europeo si è attestato su posizioni di difesa del diritto alla *privacy* quando è stato chiamato ad esprimere il proprio pa-

---

www.diritto.it, riproduce la situazione relativa al recepimento della Direttiva 24/2006/CE che avrebbe dovuto essere completato entro il 15 settembre 2007. Anche laddove l'adeguamento ha avuto luogo, peraltro, non sono mancate le tensioni; si pensi, ad esempio, all'annullamento dell'art. 5 delle norme di trasposizione da parte della Corte Suprema Amministrativa della Bulgaria.

[38] Corte giust., 10 febbraio 2009, C-301/06, *Irlanda c. Parlamento europeo e Consiglio dell'Unione europea*.

[39] Va, tuttavia, tenuto presente che il progetto di decisione quadro della Commissione europea in materia di protezione dei dati era stato inizialmente collocato nell'ambito della cooperazione giudiziaria e di polizia in materia penale: cfr. « 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 », (8958/2004 - C6-0198/2004 - 2004/0813(CNS). Si tenga presente inoltre che, con decisione pubblicata il 5 maggio 2010, la High Court di Dublino ha accolto la richiesta della ONG « Digital Rights Ireland » di riferire alla Corte di Giustizia la questione della compatibilità della Direttiva 2006/24/CE con la Carta dei Diritti Fondamentali dell'Unione Europea.

[40] Per il punto vedi C. FATTA, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Diritto dell'Informazione e dell'Informatica*, in questa *Rivista*, 411. Va considerato che gli interventi del Garante per la protezione dei dati personali non sembrano avere sortito gli effetti sperati: è stato osservato che il D.Lgs. n. 109 del 30 maggio 2008 con cui è stata data attuazione alla Direttiva 2006/24/CE non si discosterebbe da un intervento di secca « chirurgia » normativa, senza nulla concedere e/o recepire né delle indicazioni di politica legislativa, né delle specificazioni interpretative contenute sia nella Direttiva che nel Provvedimento del Garante del 17 gennaio 2008. In proposito, cfr. A. STRACUZZI, *Data retention: il faticoso percorso dell'art. 132 Codice Privacy nella disciplina della conservazione dei dati di traffico*, in questa *Rivista*, 2008, 615.

rere sugli accordi PNR[41], SWIFT[42] e ACTA[43], manifestando forti perplessità sul bilanciamento degli interessi previsto in relazione a ciascun provvedimento che molto risente dell'approccio statunitense ai temi della sicurezza e della protezione dei dati personali. È stato osservato che, negli Stati Uniti, all'indomani degli « attacchi terroristici dell'11 settembre e con l'adozione di un organico insieme di misure volte ad affrontare la cosiddetta ''guerra al terrore'', l'esigenza della sicurezza pubblica ha finito

[41] L'accordo UE-USA sull'accesso al Passenger Name Record (PNR) ha avuto una gestazione lunga e piuttosto travagliata. Il 19 novembre 2001 il Congresso americano approvava l'*Aviation and Transportation Security Act*, integrato successivamente dal *Passenger and Crew Manifests Required for Passenger on Flights in Foreign Air Transportations to the United States* pubblicato sul Federal Register il 31 dicembre 2001, ed il *Passenger and Crew Manifests Required for Passenger on Flights in Foreign Air Transportations to or from the United States*, pubblicato sul Federal Register il 25 giugno 2002. Questi provvedimenti stabiliscono che ogni compagnia aerea in volo da e verso gli Stati Uniti debba consentire al *Bureau of Customs and Border Protection* l'accesso alle banche dati telematiche dei sistemi di prenotazione telematica dei voli aerei, il cd. *Passenger Name Record*. Poiché il livello della protezione dei dati affidati al *Bureau of Customs and Border Protection* era potenzialmente lesivo del diritto alla privacy quale tutelato dal diritto comunitario, la Commissione europea negoziava un accordo tra USA ed UE sui dati personali trattati dalle compagnie aeree in occasione della conclusione di un contratto di trasporto con destinazione o transito negli Stati Uniti che fosse rispettoso della normativa comunitaria sul trattamento dei dati e, in particolare, sul trasferimento dei dati ai Paesi Terzi. Il 9 luglio 2004 il Parlamento richiedeva l'annullamento delle decisioni 2004/496/CE del Consiglio e 2004/535/CE della Commissione lamentando una serie di vizi tra cui l'erronea individuazione delle basi legali, la violazione delle norme a tutela della privacy e la violazione di competenza da parte della Commissione. La Corte di Giustizia accoglieva la richiesta di annullamento e pertanto si procedeva all'apertura delle trattative per un nuovo accordo, negoziato questa volta dall'Unione Europea. Anche l'accordo siglato dal Consiglio nel 2007, tuttavia, ha suscitato numerose perplessità e il 5 marzo 2010 il Parlamento Europeo, chiamato ad autorizzarne la ratifica in seguito all'entrata in vigore del Trattato di Lisbona, ha deciso di rimandare il proprio voto.

[42] Il 12 febbraio 2010, facendo ricorso per la prima volta al potere di veto attribuitogli dal Trattato di Lisbona, il Parlamento Europeo ha respinto a larga maggioranza l'accordo transitorio relativo all'accesso ai servizi di messaggistica interbancaria SWIFT da parte del Dipartimento del Tesoro statunitense. Tale misura è prevista dal *Terrorist Finance Tracking Program* (TFTP) nell'ambito dei poteri eccezionali riconosciuti al Presidente degli Stati Uniti dall'*Emergency Economic Powers Act*. Il Parlamento Europeo ha giudicato eccessivamente ampio il margine di discrezione sull'uso dei dati bancari concesso alle autorità statunitensi ed ha bocciato l'accordo adducendo preoccupazioni in materia di *privacy*, proporzionalità e reciprocità. Nel corso della Seduta Plenaria dell'8 luglio 2010, il Parlamento Europeo ha approvato l'Accordo in una nuova versione, giudicata maggiormente garantista. Il testo prevede l'eliminazione dei trasferimenti di dati in blocco, il diritto di ricorso per i cittadini europei e la creazione di un'autorità indipendente che vigili sull'utilizzo dei dati da parte degli Stati Uniti.

[43] L'Accordo sulla lotta alla contraffazione nel commercio (*Anti-Counterfeiting Trade Agreement* - ACTA) è volto a combattere la contraffazione e la pirateria informatica su larga scala e a definire un nuovo quadro legale per la tutela dei diritti sulla proprietà intellettuale. Si tratta di un accordo multilaterale negoziato a porte chiuse tra le parti che contemplerebbe, tra le altre misure, il controllo dei comportamenti individuali sul web e la raccolta degli indirizzi IP; i detentori dei diritti d'autore, infatti, avrebbero la facoltà di controllare ed identificare gli utenti in internet e, in caso di violazione dei diritti sulla proprietà intellettuale, impedire l'accesso alla rete. Il 15 marzo 2010, in occasione della presentazione della relazione Gallo alla *Commissione Mercato Interno e Protezione dei Consumatori* (IMCO), i membri del Parlamento europeo hanno lamentato la scarsa proporzionalità delle misure oggetto di negoziazione e hanno richiesto che gli accordi ACTA contemplino esclusivamente la lotta alla contraffazione e non anche la pirateria informatica

per prevalere quasi indiscriminatamente sulla tutela della *privacy* [...]. A partire, infatti, dall'adozione dell'*USA Patriot Act nell'ottobre 2001, si è assistito all'introduzione di una pletora di disposizioni che hanno significativamente aumentato, in particolare, i poteri di sorveglianza elettronica dei governi. Se, al di là dell'Atlantico, il Patriot Act* costituisce un attacco al bilanciamento tra governo e individuo con un sistematico aggiramento della dottrina consolidata e delle procedure a tutela dell'irragionevole intromissione del governo, non si può dire, purtroppo, che la campana non abbia suonato del pari in Europa »[44].

L'equilibrio costituzionale tra sicurezza e libertà viene energicamente sollecitato dall'emergenza terroristica anche all'interno dell'Unione Europea, con una compressione dei diritti fondamentali, determinata dalle esigenze di sicurezza nazionale, tale da produrre una vera e propria « emergenza civica »[45] agli occhi della società civile europea. Come dianzi rammentato, il Parlamento Europeo ha inteso fare fronte a questo pericolo rinviando al mittente una serie di accordi ritenuti lesivi dei diritti fondamentali e anche la Corte di Giustizia si è attestata su posizioni simili, seppure attraverso censure meramente formali. La Corte tedesca, la cui giurisprudenza ha ampliato il catalogo dei diritti della personalità meritevoli di tutela costituzionale, definendo peraltro le linee fondamentali per un bilanciamento degli interessi compatibile con la Legge Fondamentale, ha ravvisato nella legge di recepimento della direttiva comunitaria una fonte di intollerabili compressioni dei diritti umani in contrasto con il valore della dignità umana; la legge contestata viola la segretezza delle comunicazioni e non offre sufficienti garanzie ai cittadini sull'uso che verrà fatto dei dati raccolti. Esprimendo una sorta di « parere supplementare », che bene sintetizza il tradizionale approccio europeo alla *privacy* e, insieme, il giudizio e i timori dell'opinione pubblica tedesca, il giudice di Karlsruhe ha inteso rammentare il proprio ruolo di baluardo dei diritti umani, specie nei passaggi in cui si è richiamato al *Lissabon Urteil*.

Le cautele con cui la Corte ha inteso suggerire, pur senza affermarla in maniera esplicita, l'idea dell'incompatibilità dello stoccaggio generalizzato dei dati con l'identità costituzionale tedesca, ma, nel contempo, la scelta della Corte di non « calcare la mano », sono forse il sintomo dello sforzo di porsi quale articolazione e centro di trasmissione di un più vasto sistema di tutela dei diritti fondamentali. Quasi che il Tribunale costituzionale tedesco abbia voluto chiarire la propria posizione nel sistema « multilivello » in cui si estrinseca la tutela dei diritti fondamentali in Europa, sistemando le proprie competenze in un punto nevralgico del sistema stesso e rinunciando, tuttavia, ad esigere il primato.

MAURA FOGLIA

---

[44] Cfr. U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008, p. 203.

[45] Cfr. U. PAGALLO, *op. et. loc. ult. cit.*