Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Osservatorio sulla giurisprudenza

Diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali e sovrastatali europee. Il caso della *Data Retention Directive*

di Luca Curicciati *

1. Introduzione

Nella società moderna, caratterizzata da costanti e celeri sviluppi tecnologici, comprendere in che modo si possa tutelare adeguatamente il diritto alla riservatezza individuale rappresenta una questione fondamentale. In particolare, la grande diffusione degli *smartphone* e dei *social network* ha fatto in modo che si possa venire a conoscenza, molto più facilmente rispetto a qualche decennio fa, di aspetti rilevanti della vita privata di ogni persona. È evidente che questa "spettacolarizzazione" del privato riceva impulsi importanti dal singolo individuo, il quale

* Dottore in Giurisprudenza, Università degli Studi di Bari "A. Moro". Contributo sottoposto a doppio referaggio anonimo (*double blind peer review*).

spontaneamente posta in rete informazioni che attengono la sua vita personale: opinioni, relazioni sociali, abitudini, esperienze lavorative.

Probabilmente, e per certi versi anche inconsapevolmente, la società attuale sta perdendo la concezione e il valore della tutela della propria riservatezza, non percependo come la protezione dei dati personali rappresenti uno snodo fondamentale anche per altri diritti**.** Va posta in luce anche la potenziale attitudine degli algoritmi dei motori di ricerca sul web a rivelare, associando gli elementi delle stringhe di ricerca degli utenti, dati personali e sensibili. In tale prospettiva si ricordi ad esempio la sentenza "*Google Spain*"[1], decisiva per qualificare l'attività di un motore di ricerca come "trattamento di dati personali", e per definire l'obbligo del gestore di eliminare, su richiesta dell'interessato, dall'elenco dei risultati di una ricerca effettuata a partire dal nominativo di una persona, dei collegamenti verso pagine contenenti dati sensibili. Speciale attenzione va dedicata anche ai c.d. *cookies*, dati raccolti durante la navigazione dell'utente su internet e che possiedono una rilevante valenza sotto il profilo statistico e permettono la "profilazione" dell'utente. Appare evidente non soltanto l'importanza di tale attività sotto il profilo del diritto alla riservatezza, ma anche per l'utilizzo potenzialmente pregiudizievole dei dati.

Alla luce di tali considerazioni, il diritto alla riservatezza, classificato da Norberto Bobbio (1997) nella categoria dei c.d. "diritti di quarta generazione", ovvero quei diritti legati allo sviluppo dell'informatica e del-

[1] Corte Giustizia UE, *Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González* (causa C131/12 del 13 maggio 2014).

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Osservatorio sulla giurisprudenza

le telecomunicazioni, ricopre oggi un ruolo centrale per regolare le relazioni umane, ed è efficacemente "inglobato" all'interno del nostro patrimonio giuridico. Tuttavia, ormai troppo spesso, i cittadini rivestono il ruolo di "spettatori inermi" rispetto a politiche nazionali ed internazionali che pongono in discussione alcuni dei nostri diritti fondamentali.

In un contesto storico come quello attuale è giusto che a prevalere sia il principio per cui *salus rei publicae suprema lex esto*, e quindi ogni deroga ai diritti fondamentali deve essere accettata in quanto rivolta a garantire una maggiore sicurezza, o sarebbe più opportuno, alla luce di emergenze come quella terroristica che assume sempre più i caratteri dell'ordinarietà e non dell'eccezionalità, riorganizzare la tutela delle nostre garanzie per evitare che possano configurarsi abusi come quelli che hanno riguardato il diritto alla riservatezza?

Per rispondere a tale domanda, un importante ambito di analisi è rappresentato dai limiti entro i quali sono considerate ammissibili possibili violazioni a tale diritto allo scopo di tutelare interessi statali e sovrastatali confliggenti (Bonetti 2006; De Vergottini 2004 a e b). Cruciale, a tal fine, è lo studio degli sviluppi normativi e giurisprudenziali europei degli ultimi anni, a partire dal celebre caso della *Data retention directive*, a cui è dedicato questo scritto, fino alla più recente "sentenza Teledue" della Corte Giustizia UE del 21 dicembre 2016, con cui la Grande Sezione della Corte ha stabilito che gli Stati membri non possono imporre ai fornitori di servizi di comunicazione elettronica un obbligo generale e indifferenziato di conservazione dei dati relativi al traffico e all'ubicazione degli utenti, in assenza del consenso degli stessi. Si può solo prevedere, a titolo preventivo, una conservazione mirata allo scopo esclusivo di combattere gravi fenomeni di criminalità, a condizione che la stessa si

limiti a quanto necessario per quello che attiene le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone implicate e la durata di conservazione prevista (Pollicino e Bassini 2017).

In ragione della complessità e della costante evoluzione che caratterizza tale diritto risulta opportuno, prima di esaminare gli aspetti principali della sentenza con cui la Corte di Giustizia dell'Unione europea ha sancito l'invalidità della c.d. *Data Retention Directive*, fornire una breve ricostruzione storica del diritto alla riservatezza, utile per contestualizzare, a grandi linee, il tema oggetto di questo scritto. Infine, l'analisi comparativa della giurisprudenza di alcune Corti costituzionali statali, ha lo scopo di analizzare l'impatto della Direttiva 2006/24/CE all'interno degli ordinamenti nazionali, valutando i differenti orientamenti emersi, soprattutto in seguito alla pronuncia della Corte di Giustizia.

2. Il diritto alla riservatezza delle comunicazioni

Al termine della *26th International Conference on Privacy and Personal Data Protection*, Stefano Rodotà afferma che:

> la *privacy* si presenta come un elemento fondamentale della società dell'eguaglianza. Senza una forte tutela dei dati riguardanti le convinzioni politiche o l'appartenenza a partiti, sindacati, associazioni, i cittadini rischiano di essere esclusi dai processi democratici: così la *privacy* diventa una condizione essenziale per essere inclusi nella società della partecipazione. Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo. Diventa così evidente che la *privacy* è uno strumento necessario per difendere la società

della libertà, e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale (Rodotà 2004).

La storia del diritto alla riservatezza è uno dei casi sintomatici di "trapianto" di istituti giuridici da un Paese ad un altro e di circolazione di modelli giuridici. Infatti tale diritto trae le sue origini dall'esperienza statunitense: nel 1890, in un saggio dal titolo *The right to privacy*, del senatore Warren e del giudice Brandeis (Brandeis e Warren 1890), si ritrova la prima definizione di *privacy*, ovvero «*the right to be let alone*», in cui si propone di considerare illecito civile (*tort*) la lesione della *privacy* dell'individuo.

L'opera rappresenta una pietra miliare in materia in quanto è la prima monografia giuridica a riconoscere l'esistenza di questo autonomo diritto. Prima di allora le esigenze di tutela della vita privata, seppur avvertite a livello sociale, non trovano un riconoscimento giuridico, venendo ricondotte all'interno delle logiche di diversi diritti, quali il diritto alla reputazione e all'onore. L'importanza del saggio si evince dalla volontà di proteggere l'essenza del diritto alla *privacy* non per il valore che esso ha rispetto alla dimensione pubblica, ma per l'importanza che esso possiede nella dimensione privata del titolare del diritto.

Attualmente negli USA la *privacy* non si configura come un diritto fondamentale dell'individuo, ma come un diritto del consumatore, da bilanciare con le esigenze delle imprese. A dimostrazione di ciò, la competenza a vigilare sull'aderenza dei comportamenti delle aziende su quanto dichiarano nelle proprie *privacy policy* e sul rispetto delle leggi sulla *privacy* appartiene alla FTC (*Federal Trade Commission*), agenzia deputata alla tutela dei consumatori negli USA. La natura settoriale del si-

stema statunitense ha mostrato tutta la sua fragilità a seguito degli attentati dell'11 settembre del 2001, nel momento in cui il governo americano, approvando una legislazione d'emergenza di contrasto al terrorismo, ha posto in essere una indebita compressione del diritto alla *privacy* dei cittadini americani in nome della sicurezza nazionale.

Nell'odierna società dell'informazione, il concetto di riservatezza risulta indissolubilmente legato a quello del diritto alla protezione dei dati personali. In particolar modo negli ultimi anni è stato possibile assistere ad una vera e propria consacrazione di questo diritto all'interno di testi normativi sia nazionali che sovrastatali. Quello che caratterizza tale nozione in primo luogo è l'impossibilità di individuare elementi statici e predeterminati che possano definirlo nel tempo. Infatti il diritto alla riservatezza, definito anche come diritto alla *privacy*, si presenta come un concetto estremamente mutevole e particolarmente correlato a situazioni attinenti da un lato la sfera sociale dell'individuo e, dall'altro, l'evoluzione tecnologica.

A tal proposito, basti pensare che all'interno del Codice civile italiano non esiste nessuna norma che definisca esplicitamente questo diritto. Questa assenza ha erroneamente generato l'idea che tutto ciò che attiene la riservatezza dell'individuo non è suscettibile di tutela all'interno del nostro ordinamento, ma già nella Costituzione italiana vi sono richiami a disposizioni di carattere generale (come gli artt. 2 e 3) o specifiche (come gli artt. 13, 14, 15). Il riferimento all'art. 2 Cost. risulta particolarmente pertinente sotto il profilo del riconoscimento e della garanzia dei diritti inviolabili dell'uomo, per il legame che si instaura tra persona e formazioni sociali, per la esplicita previsione di doveri inderogabili di solidarietà economica, politica e sociale. L'art. 3 invece, nel riconoscere

l'eguaglianza giuridica e nello stabilire l'impegno positivo a rimuovere gli ostacoli che impediscono ai consociati di godere effettivamente dell'eguaglianza e della libertà, pone in rilievo il valore della persona umana ed il principio personalista. Ragion per cui il combinato realizzato tra queste due norme è utile per affermare, seppur indirettamente, l'inviolabilità di tale diritto. In particolare, se si considera la *privacy* come aspetto legato alla libertà personale, essa da un lato implica una sorta di "libertà negativa", ovvero la garanzia che nessun altro possa intromettersi nella sfera privata del titolare della libertà stessa, e, dall'altro, una "libertà positiva", intesa come possibilità di attribuire al soggetto titolare del diritto l'autonomia di intervenire di fronte a comportamenti altrui che possano ledere la propria posizione sociale (Baldassarre 1997) .

In ambito europeo è solo con la direttiva 95/46/CE – relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati (Flor 2015; Bignami 2007; Benedizione e Paris 2015) - che per la prima volta viene fissato uno standard di tutela obbligatoriamente vincolante per gli Stati appartenenti all'UE. Questa direttiva rappresenta uno snodo cruciale se si vuol capire come l'Unione europea sia in grado di tutelare la nostra *privacy* permettendo congiuntamente la libera circolazione delle informazioni tra gli Stati membri. La sfida più importante cui la società e le istituzioni europee sono chiamate a rispondere è proprio questa: riuscire a dimostrare che un equo bilanciamento tra queste due differenti esigenze è possibile. Ogni giorno, infatti, imprese, enti pubblici e singoli cittadini trasmettono grandi quantità di dati personali attraverso i confini nazionali all'interno dell'UE. Un eventuale conflitto di norme nazionali sulla protezione dei dati presenti in vari paesi interromperebbe gli scambi internazionali,

frenando il mercato e il processo di integrazione economica e sociale. I principi della direttiva sono poi stati acquisiti e fatti propri dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea[2] che tutela la protezione dei dati di carattere personale.

L'importanza di questo diritto si evince anche dalle garanzie introdotte in relazione alla tutela degli individui e al trattamento dei propri dati personali da molte delle Costituzioni europee di ultima generazione. Si pensi ad esempio alla Costituzione svizzera del 1999, il cui art. 13, 2° co., dispone che «ognuno ha diritto d'essere protetto da un impiego abusivo dei suoi dati personali» o alla Costituzione spagnola del 1978, il cui art. 18, 4° co., stabilisce che «la legge limita l'utilizzazione dell'informatica al fine di garantire l'onore, l'intimità personale e familiare dei cittadini ed il pieno esercizio dei loro diritti».

Lo sviluppo della società dell'informazione comporta, tra le sue conseguenze, l'introduzione di nuovi servizi di comunicazione elettronica. In quest'ottica il Parlamento europeo e il Consiglio dell'Unione europea hanno provveduto ad adottare la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di

[2] «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.»

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione. Il diritto alla riservatezza, a seguito della sempre più costante e innovativa diffusione di nuove tecniche di comunicazione a distanza che si basano sull'utilizzo di Internet (es. Skype, Messenger, Whatsapp), ha mutato la propria fisionomia, ragion per cui si è reso necessario un adeguamento delle sue tutele che possa conformarsi alle recenti innovazioni tecnologiche.

L'informazione rappresenta ormai un importante fattore economico. È chiaro che individuare in maniera accurata le caratteristiche della domanda dei consumatori permette alle industrie di fornire un'offerta conforme alle necessità del mercato. In tale contesto risulta palese come tutta la miriade di informazioni che viene veicolata da Internet venga considerata dagli operatori economici alla stessa stregua di un prodotto fondamentale per garantire incrementi produttivi costanti[3]. Se quindi la

[3] Si pensi ad esempio agli *smartwatch*, orologi intelligenti che oltre ad effettuare telefonate, inviare e ricevere sms, disporre di navigatore GPS e mantenere contatti attraverso i *social network*, consentono anche di monitorare i passi ed il battito cardiaco, una funzionalità, peraltro proposta anche da alcune marche di *smartphone* (*iPhone* Apple), pensata per gli amanti del *fitness*. Federprivacy, associazione italiana che promuove con ogni mezzo la divulgazione, la conoscenza ed il rispetto delle normative vigenti in materia di *privacy e data protection* rende nota la possibilità di rivelare abitudini, gusti, comportamenti, desideri senza esserne consapevoli attraverso l'utilizzo di *app* scaricabili dagli *store* sul web. Un recente studio, condotto dall'Università di Pisa con la collaborazione dell'Università dell'Essex (UK) e l'Harvard Medical School e Massachusetts Institute of Technology (USA), ha dimostrato come il cuore possa essere un vero e proprio portale per la rivelazione delle emozioni. Oggi oltre che inviare messaggi sul proprio *smartphone* o *smartwatch* con annunci che rispecchiano le nostre ultime ricerche, i nostri gusti e le nostre abitudini, è anche scientificamente possibile determinare che tipo di emozione si

privacy dei cittadini è posta sempre più a rischio, di contro le crescenti criticità derivanti dal progresso tecnologico hanno reso provvidenziale l'approvazione del nuovo Regolamento europeo sulla *privacy*.

Il 27 aprile 2016 il testo del Regolamento UE 2016/679 è stato siglato dal Presidente del Parlamento europeo e dal Presidente del Consiglio e il 4 maggio 2016 è stato pubblicato, in tutte le lingue ufficiali dell'Unione, sulla Gazzetta Ufficiale dell'Unione Europea. Entrato in vigore il 25 maggio 2016, sarà effettivamente applicato a partire dal 25 maggio 2018, data che inoltre indica l'abrogazione della Direttiva 95/46/CE ma non determina il venir meno degli effetti prodotti dagli atti e dalle decisioni adottate durante la sua vigenza. Al contrario, essi "restano in vigore" fino alla loro modificazione, sostituzione o abrogazione.

L'obiettivo principale del nuovo Regolamento è quello di assicurare una disciplina uniforme di protezione dei dati personali ed una applicazione coerente delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Tale scopo può essere raggiunto sia attraverso una serie di disposizioni fondamentali contenute nel Regolamento, sia affidando un ruolo decisivo alle autorità di controllo e al Comitato europeo di protezione dati.

Nonostante la predisposizione di simili misure, il Regolamento in molte parti consente al legislatore statale di adottare normative nazionali. Se è vero che, da un lato, una scelta simile favorisce un approccio

provi osservando un determinato prodotto in vetrina o assistendo ad esempio a una partita di calcio o a un concerto.

"flessibile" in un contesto uniformemente applicato, dall'altro evidenzia la necessità di differenziare tra i diversi casi in cui l'intervento del legislatore nazionale sia facoltativo o obbligatorio. È chiaro che la legislazione europea e nazionale incompatibile con il Regolamento necessiti di un adeguamento che sia il più celere possibile, ovviamente nel rispetto delle materie nelle quali è predisposta una riserva di competenza in favore degli Stati.

Come già scritto precedentemente l'entrata in vigore del nuovo Regolamento porterà alla abrogazione della Direttiva 95/46/CE. Tale scelta trova la sua ragion d'essere sia nelle trasformazioni sociali e nello sviluppo tecnologico dei due decenni che ci separano dall'adozione della Direttiva 95/46, sia in una visione che pone al centro della protezione dei dati personali l'interesse pubblico europeo. Il nuovo Regolamento, quindi, è introdotto in un sistema che indubbiamente riconosce la protezione dei dati personali come diritto fondamentale della persona, fermo restando che il rispetto di questo diritto sia da bilanciare con la sua funzione sociale e con altri diritti di pari livello (Pizzetti 2016).

Tra le principali novità introdotte si segnalano nuove disposizioni sul diritto all'oblio, sul consenso chiaro ed informato al trattamento dei dati personali, l'obbligo di informare il titolare dei dati quando gli stessi risultino violati e l'introduzione della figura dei DPO (*Data Protection Officer*), esperti di *privacy* delegati a verificare la compatibilità delle attività aziendali con il rispetto delle norme europee per le società aventi un elevato numero di dipendenti e sanzioni pecuniarie sino a 20 milioni di euro o al 4% del fatturato annuo per le società e le amministrazioni che non rispettino i parametri stabiliti dall'Unione.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Ai fini di questo scritto è necessario menzionare inoltre la Direttiva UE/2016/680 relativa alla protezione dei dati personali delle persone fisiche per quanto concerne il trattamento e la circolazione dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali che abroga la decisione quadro 2008/977/GAI del Consiglio.

La condivisione dei dati e delle informazioni tra le forze dell'ordine e le autorità giudiziarie dei diversi Paesi membri rappresenta uno strumento fondamentale per garantire la sicurezza nell'Unione europea. I dati raccolti per finalità di prevenzione e di polizia in un Paese possano essere trasmessi nel resto d'Europa e, eventualmente, all'estero purché le rispettive autorità giudiziarie e di polizia garantiscano, nel trattamento dei dati personali di tutte le persone fisiche, un adeguato livello di tutela che non violi il diritto alla *privacy*. Gli Stati membri dovranno dare attuazione alla Direttiva entro il 6 maggio 2018 e saranno tenuti a rispettare una serie di obblighi tra cui quello di tutelare i diritti e le libertà fondamentali delle persone fisiche.

La Direttiva UE 680/2016 riafferma ancora una volta, inequivocabilmente, l'idea secondo cui tutta la disciplina europea in materia di privacy debba essere rispettata anche da parte della autorità giudiziarie e di polizia. Sebbene gli ultimi avvenimenti di matrice terroristica pongano certamente in discussione tali garanzie, l'idea di ribadire con forza i parametri entro i quali esercitare le prerogative attribuite *ex lege* appare come una chiara manifestazione del principio secondo cui non è necessario rinunciare alla *privacy* per garantire maggiore sicurezza.

Questo tema, tuttavia, non costituisce un elemento di novità nell'ambito delle discussioni attinenti le limitazioni applicate ai diritti

del singolo individuo durante situazioni emergenziali. In tale contesto, la riservatezza di ciascun soggetto può essere facilmente "sacrificata" in nome del bene comune, ovvero la sicurezza nazionale, come dimostra la *Data Retention Directive*, che aveva l'obiettivo di armonizzare le normative interne degli Stati membri in relazione alla conservazione di dati generati o trattati da provider di servizi di comunicazione elettronica garantendo la disponibilità degli stessi ai fini della prevenzione, individuazione e perseguimento di reati gravi.

La direttiva – oggetto del giudizio di numerose Corti costituzionali nazionali, oltre che della stessa Corte di Giustizia – costituisce un caso di studio di particolare interesse per quanto attiene il tema del bilanciamento tra esigenze statali e il diritto alla *privacy*, alla cui analisi sono dedicati i paragrafi che seguono.

3. Il diritto alla riservatezza delle comunicazioni e l'emergenza terrorismo: la *Data Retention Directive* innanzi alla Corte di Giustizia dell'Unione europea

La sentenza della Corte di Giustizia dell'Unione europea dell'8 Aprile 2014, che ha dichiarato l'invalidità della Direttiva 2006/24/CE[4], meglio conosciuta come *Data Retention Directive*, riguardava le disposizioni del-

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

la direttiva volte a garantire la conservazione dei dati di traffico telefonico e telematico, i dati relativi all'ubicazione e quelli necessari all'identificazione dell'abbonato. Tali elementi infatti, pur non attingendo al contenuto della conversazione, forniscono comunque indicazioni importanti sulle comunicazioni intrattenute da ciascuno, sui loro destinatari e sulla loro frequenza, realizzando conseguentemente una forte ingerenza nella vita privata dei cittadini, considerato che la conservazione e il successivo utilizzo degli stessi avverrebbe ad insaputa dell'interessato (Cerqua 2014; Guild e Carrera 2014; Marin 2016).

Se, in linea di massima, il contrasto a gravi forme di criminalità (si pensi alle organizzazioni terroristiche) e le esigenze di pubblica sicurezza possono contribuire a rendere parzialmente condivisibile lo scopo della direttiva, secondo la Corte le disposizioni presentate non sarebbero conformi ai limiti imposti dal principio di proporzionalità. Tale principio rappresenta il punto cardine della pronuncia, come si può ben comprendere dalla volontà della CGUE di delimitare in maniera precisa l'utilizzo di questi elementi, fermo restando il rispetto di alcune garanzie essenziali, come, ad esempio, la subordinazione di tali limitazioni all'autorizzazione di organi giudiziari o enti amministrativi indipendenti. E mira, del resto, a non sottrarre tali dati alle garanzie di protezione accordate dalle autorità nazionali considerata l'esigenza di mantenere i dati stessi all'interno del territorio dell'U.E. (Sperti 2009; Vedaschi e Lubello 2015; Fabbrini 2015).

È evidente, a tal proposito, l'influenza dello scandalo *Datagate*, emerso a seguito delle sconcertanti rivelazioni di Edward Snowden relative alle attività segrete di monitoraggio delle comunicazioni private sistematicamente poste in essere dalla NSA statunitense.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Colpisce poi constatare come, tanto l'Avvocato Generale, quanto la Corte di Giustizia, seppur argomentando in maniera differente, giungano alla stessa conclusione circa la compatibilità della disciplina con la Carta dei diritti fondamentali. Infatti, mentre il primo ritiene che la legislazione in materia non regolamenti con sufficiente precisione le condizioni di accesso e impiego dei dati conservati, la Corte argomenta direttamente sulla proporzionalità della disciplina. Inoltre la straordinaria importanza della pronuncia risulta ancor più evidente se si considera che la CGUE raramente dichiara l'invalidità di un intero atto comunitario.

La vicenda trae origine da due distinte controversie giudiziarie nazionali sviluppatesi in Irlanda e in Austria che, in ragione del loro comune oggetto, sono state processualmente riunificate e hanno portato ad un'unica risposta della Corte europea. Più precisamente, nella causa C-293/12, la ricorrente nel procedimento principale è stata una società avente come scopo statutario la protezione dei diritti umani nel contesto delle moderne tecnologie di comunicazione, la Digital Rights Ireland Ltd. La *High Court* irlandese ha sollevato una serie di questioni pregiudiziali soffermandosi in particolar modo sulla necessità di compiere un bilanciamento adeguato tra la necessità di garantire la sicurezza e il corretto funzionamento del mercato interno e l'esigenza di garantire la libertà di circolazione[5], il rispetto della vita privata[6], la protezione dei dati personali[7], e la

[5] Art. 21 Trattato sul funzionamento dell'Unione europea (TFUE).

[6] Art. 7 Carta dei diritti fondamentali dell'UE.

[7] Art. 8 della Carta dei diritti fondamentali dell'UE.

libertà di espressione[8]. Nella causa C-594/12 invece, è stata la *Verfassungsgerichtshof* austriaca, che, per rispondere ai ricorsi con cui il governo della Carinzia e 11.130 privati cittadini hanno chiesto l'annullamento della legge interna di recepimento della direttiva, ha sollecitato a sua volta la Corte di Giustizia per comprendere se il sistema di raccolta dei dati sia compatibile con il diritto al rispetto della vita privata, con il diritto alla protezione dei dati personali e con il diritto alla libertà di espressione, diritti tutelati dalla Carta dei diritti fondamentali.

Investita di tali questioni, la Corte di giustizia ha argomentato la sua decisione segnalando in primo luogo una contrapposizione evidente tra l'art. 1 e l'art. 5 della direttiva oggetto d'esame della Corte e l'art. 7, l'art. 8 e l'art. 11 della Carta dei diritti fondamentali dell'UE. Le prime due norme infatti stabiliscono il divieto di conservare il contenuto delle conversazioni avvenute attraverso i canali elettronici. Tuttavia i dati sottoposti all'obbligo di conservazione (es. la durata e tipo di comunicazione o il nome e indirizzo dell'utilizzatore), permettono di tracciare profili abbastanza definiti riguardo i soggetti che utilizzano i mezzi di comunicazione, generando una violazione della riservatezza e della tutela dei dati personali.

Per rispondere a tali interrogativi i giudici hanno richiamato l'art. 52 della Carta Europea dei diritti fondamentali, constatando come le lesioni prodotte dalla direttiva siano gravi ma non sufficienti a violare il contenuto essenziale dei diritti richiamati. In particolar modo per quanto concerne il diritto alla riservatezza si segnala come sia espressamente vieta-

[8] Art. 11 della Carta dei diritti fondamentali dell'UE.

to conservare il contenuto delle comunicazioni; inoltre, la presenza di direttive[9] che regolamentano con chiarezza la disciplina, ha escluso la possibilità che eventuali violazioni del diritto alla protezione dei dati personali non vengano evidenziate. In secondo luogo, la Corte di Giustizia si è occupata di verificare se la limitazione dei diritti suddetti riguardasse effettivamente finalità di interesse generale. A tal proposito i giudici ritenevano necessario chiarire la distinzione sussistente tra scopo formale e scopo materiale della direttiva. Più precisamente, mentre lo scopo formale dichiarato è stato quello di armonizzare le disposizioni degli Stati membri relative agli obblighi gravanti sui fornitori di servizi di comunicazione elettronica concernenti la conservazione di determinati dati da essi trattati o generati, lo scopo materiale è stato individuato nella volontà di garantire la disponibilità delle informazioni a fini di indagine, accertamento e perseguimento di reati gravi.

La Corte sottolinea come la genesi dell'UE sia legata all'esigenza di realizzare un mercato comune, obiettivo ricollegabile al "primo pilastro" e che solo nel 1992 l'Unione ha ottenuto il potere di regolamentare atti sulla materia della cooperazione giudiziaria e di polizia in materia penale, ovvero il "terzo pilastro". La relazione col primo pilastro risulta più chiara nel momento in cui si osserva l'obiettivo complessivo della conservazione dei dati. Fornendo un unico standard regolamentare, sarebbe risultato più semplice per i fornitori di servizi fare affari in più giurisdi-

[9] Dir. 1995/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e Dir. 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche..

zioni, seguendo una sola regolamentazione e non una differente a seconda dello Stato interessato. Il maggior bisogno di sicurezza legato alla minaccia terroristica ha spinto l'UE verso l'adozione di nuove strategie che hanno comportato un rafforzamento delle modalità di collaborazione fra il controllo alla criminalità e le strutture di sicurezza, ragion per cui si è giunti alla formulazione di questa direttiva. Ad ogni modo, una volta chiarito che la lotta al terrorismo è lo scopo fondamentale della *Data Retention*, è indubbio che lo stesso costituisca un obiettivo di interesse generale.

Proseguendo nella verifica ex art. 52 della Carta, la Corte ha esaminato la proporzionalità della disciplina. Nello svolgere tale controllo, il giudice europeo deve stabilire l'ampiezza del margine di discrezionalità delle istituzioni dell'Unione europea nel caso concreto: margine che, a seconda delle circostanze, può essere più o meno ampio. In proposito, viene esplicitamente richiamata la giurisprudenza della CEDU in materia: nella celebre sentenza *Marper vs U.K.* del 2008, riguardante un caso significativo di conservazione dei dati personali (impronte digitali e DNA) per fini investigativi e di repressione dei crimini, il giudice di Strasburgo ha affermato che generalmente il margine di discrezionalità spettante in materia alle autorità nazionali varia in considerazione della natura del diritto garantito, della gravità dell'ingerenza e degli obiettivi perseguiti dalla misura.

La Corte di Lussemburgo ha dichiarato che, nel caso di specie, trattandosi di aspetti fondamentali concernenti la vita delle persone, il margine di proporzionalità doveva essere ristretto. Nello specifico la Corte ha osservato come la direttiva 2006/24 imponga la conservazione di tutti i dati sul traffico riguardanti telefoni fissi, cellulari, navigazione internet

e posta elettronica, coinvolgendo l'intera popolazione europea. Infatti è necessario sottolineare che la conservazione non riguarda esclusivamente i dati degli utenti sospettati di avere legami con la criminalità organizzata o con il terrorismo, ma anche quelli di tutte le persone che hanno usufruito dei servizi di comunicazione elettronica nel territorio degli Stati membri, non escludendo neppure le comunicazioni soggette a segreto professionale.

La Corte ha proseguito evidenziando l'assenza di un criterio oggettivo con cui le autorità nazionali competenti potessero ottenere l'accesso ai dati raccolti. Infatti nell'art. 1 della Direttiva si pone soltanto un generico richiamo a reati "gravi" (ma non specificati), non disciplinando le condizioni sostanziali e procedurali attraverso cui le competenti autorità nazionali possano avere accesso alle informazioni memorizzate. L'accesso ai dati per cui non è subordinato al previo controllo di un giudice o di un ente amministrativo indipendente. Per quanto attiene il periodo temporale di conservazione delle informazioni raccolte, la direttiva stabilisce un limite minimo (6 mesi) e massimo (24 mesi), ma non detta alcun criterio oggettivo per la determinazione dello stesso caso per caso, né introduce una distinzione tra categorie di dati a seconda delle persone interessate e all'eventuale utilità dei dati rispetto all'obiettivo perseguito. Inoltre la durata della conservazione è posta nell'arco temporale succitato, ma non sono specificati i criteri oggettivi in base ai quali la stessa durata debba essere determinata, in modo da garantire la sua limitazione allo stretto necessario.

Infine, relativamente alla questione della sicurezza dei dati personali raccolti, secondo la Corte non sono previste sufficienti garanzie contro il pericolo di abuso e contro qualsiasi accesso e utilizzo illegittimo dei dati,

anzi rileva come la direttiva autorizzi i fornitori di servizi a tenere conto di considerazioni economiche in sede di determinazione del trattamento di sicurezza da applicare e non garantisce la distruzione irreversibile dei dati dati al termine della loro durata di conservazione. In secondo luogo, la disciplina comunitaria non impone che le informazioni sul traffico siano conservate dai fornitori di servizi nel territorio dell'Unione Europea, così consentendo di eludere agevolmente il controllo sui dati personali, richiesto dall'art. 8.3 della Carta dei Diritti Fondamentali dell'UE da parte di una autorità indipendente, controllo che costituisce una componente essenziale della protezione degli individui con riguardo al trattamento dei loro dati personali.

Alla luce delle considerazioni esposte, la Corte di Giustizia ha dichiarato invalida l'intera disciplina contenuta nella Direttiva 2006/24/CE, in quanto ha oltrepassato i limiti imposti dal rispetto del principio di proporzionalità, in riferimento agli art. 7, 8 e 52.1 della Carta. Il giudice europeo non ha dichiarato illegittima la raccolta dei dati in sé, ma ha sottolineato il difetto di proporzionalità della normativa proposta rispetto al diritto fondamentale alla riservatezza. L'obbligo di conservazione diviene incompatibile con il diritto dell'UE nel momento in cui non sono delineate le tipologie di soggetti i cui dati sono conservati. Ragion per cui una sorveglianza generalizzata e preventiva delle comunicazioni e l'utilizzo dei relativi dati secondo le modalità previste dalla direttiva risulta incompatibile con i diritti fondamentale al rispetto della vita privata e alla protezione dei dati personali (Vecchio 2014).

La pronuncia della Corte di Giustizia ha contribuito a mostrare la complessità e l'inscindibilità del rapporto tra tutela della riservatezza ed esigenze di sicurezza. La dichiarazione di invalidità dell'intera disciplina

inoltre ha esentato la Corte dal rispondere alle ulteriori questioni pregiudiziali, aprendo nuovi scenari anche per quello che attiene la legislazione nazionale di recepimento della stessa.

4. Il bilanciamento tra diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali.

Come anticipato, la *Data Retention Directive* è stata oggetto del giudizio, oltre che della Corte di Giustizia, anche di numerose Corti costituzionali europee. Nell'ambito della giurisprudenza costituzionale, è possibile individuare tre differenti *modus operandi* da parte delle Corti.

Un primo criterio, esaminato nel paragrafo precedente, è quello prescelto dalle Corti irlandese e austriaca, che, rinviando la questione di interpretazione delle leggi di attuazione della Data retention directive" alla Corte di Giustizia, hanno mostrato un atteggiamento "cooperativo" con la Corte europea, riconoscendone un ruolo quasi "super-costituzionale".

Altre Corti invece, come ad esempio quella bulgara o ceca, hanno optato per un atteggiamento che si potrebbe definire "sovranistico", dichiarando incostituzionali le leggi di attuazione della medesima direttiva.

Infine la Corte costituzionale slovena, rispetto alle Corti costituzionali citate precedentemente ha optato per una sospensione del procedimento attinente la questione di costituzionalità in attesa di una decisione della Corte di Giustizia dell'Unione europea, già chiamata ad esprimersi sulla compatibilità della Direttiva *Data Retention* con gli articoli 7 ed 8 della

Carta dei diritti fondamentali dell'Unione europea, mostrando quindi un atteggiamento divergente dalle altre Corti. La Corte costituzionale slovena si colloca ad un livello intermedio tra i due sopracitati *modus operandi*, in quanto, pur non escludendo la sua competenza a esprimersi su questioni concernenti la materia, ha ritenuto più opportuno attendere la pronuncia della Corte di Giustizia (Raducu 2014; Romboli 2014; Benedizione e Paris 2015).

Con riferimento alle decisioni di costituzionalità "sovranistiche", è interessante constatare un *modus operandi* comune tra le Corti costituzionali della Bulgaria[10], della Romania[11] e della Repubblica Ceca[12]. In particolar modo la Corte costituzionale bulgara e quella romena hanno evidenziato l'eccessiva vaghezza della direttiva in rapporto ad una disciplina particolarmente complessa come quella della tutela dei dati personali, procedendo alla disapplicazione delle leggi di esecuzione. La Corte costituzionale ceca invece, sollevando ugualmente delle perplessità relative alla compatibilità della direttiva con la Costituzione ceca e con la Carta Europea dei diritti fondamentali, ha dichiarato l'incostituzionalità delle leggi di esecuzione mutuando l'impianto argomentativo della Corte costituzionale tedesca sulla conservazione dei dati.

[10] Decisione n.13627 dell'11 dicembre 2008 del Supremo Tribunale Amministrativo bulgaro; per un riassunto in lingua inglese http://www.aip-bg.org/.

[11] Decisione n. 1258 della Corte costituzionale romena, dell'8 ottobre 2009, in *Romanian Official Journal*, 23-11-2009, n. 789 (consultabile anche nella versione inglese sul sito: www.legi-internet.ro).

[12] Sentenza della Corte costituzionale ceca del 22 marzo 2011 riguardante la legge n. 127/2005 e il decreto 485/2005 consultabile in http://www.concourt.cz/.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Nello specifico, per quel che ha riguardato la decisione della Corte costituzionale bulgara, a parere dei ricorrenti, l'art. 5 del Regolamento[13] con cui la Bulgaria ha attuato la Direttiva, ha dato la possibilità di realizzare violazioni del diritto alla *privacy* dei cittadini, in quanto l'accesso e la conservazione dei dati, permesso per operazioni investigative è stato formulato in maniera troppo vaga e imprecisa, non fornendo le adeguate garanzie previste dalla Costituzione bulgara ai sensi dell'art. 32[14] e anche dall'art. 8 della Carta Europea dei Diritti fondamentali. La Corte costituzionale bulgara ha evidenziato l'importanza della procedura relativa alla conservazione dei dati; tuttavia, la causa che ha portato all'annullamento di alcune norme previste dal Regolamento di attuazione è da ricollegare alla insufficiente chiarezza delle previsioni normative considerate.

La Corte costituzionale rumena, con sentenza n. 1258 dell'8 ottobre 2009 ha annullato la legislazione nazionale di attuazione[15] della direttiva sulla conservazione dei dati in quanto incompatibile con le disposizioni costituzionali che proteggono la libertà di movimento[16], il diritto alla vita privata[17], la segretezza della corrispondenza[18] e la libertà di espressio-

[13] Regolamento n.40 del Ministero degli Interni del 07/01/2008.

[14] «La *privacy* dei cittadini è inviolabile. Ognuno dovrebbe essere protetto da illecite interferenze per quello che attiene la propria vita privata, la propria famiglia, e contro ogni violazione relativa alla sua dignità, al suo onore e alla sua reputazione.»

[15] La normativa nazionale di recepimento (l. n. 298/2008 e l. n. 506/2004) viene ritenuta in contrasto con l'art. 26 della Costituzione, che tutela il diritto alla *privacy*.

[16] Art. 25 Cost. Romania: «Il diritto alla libertà di movimento è garantito sul territorio nazionale. La legge pone in essere le condizioni necessarie alla tutela di questo diritto».

[17] Art. 26 Cost. Romania: «L'autorità pubblica rispetta il diritto alla vita privata e l'intimità dei cittadini» .

ne[19]. La Corte ha ritenuto che il tentativo del governo di giustificare la conservazione obbligatoria dei dati delle telecomunicazioni in nome di presunte minacce alla sicurezza nazionale non era sufficiente per ammettere misure di tal genere, e nel farlo ha richiamato la sentenza *Klass vs. Germany*[20], in cui si afferma il principio per cui l'adozione di misure di sorveglianza prive di garanzie adeguate può portare a «distruggere la democrazia invece di difenderla».

Nell'ottobre del 2011 la Commissione europea ha chiesto al governo rumeno di introdurre nuove leggi di recepimento della direttiva *Data Retention*, affermando come, in caso contrario, l'UE avrebbe posto in essere una procedura di infrazione, come previsto dall'art. 258[21] del TFUE. Effettivamente una nuova legge è stata formulata ma successivamente respinta dal Senato rumeno, a seguito di un pesante attacco mediatico e anche dopo la mancata approvazione dell'Autorità di protezione dei dati del Paese, adducendo come motivazione che gli articoli relativi ai servizi di sicurezza erano ancora troppo vaghi.

[18] Art. 28 Cost. Romania: «La segretezza di lettere, telegrammi, o altre comunicazioni postali, comunicazioni telefoniche ed ogni altro tipo di comunicazione è inviolabile».

[19] Art. 30 Cost. Romania: «La libertà di espressione di pensieri, opinioni, creazioni, resa sia in forma scritta, in forma orale, mediante immagini o mediante suoni o attraverso qualsiasi altra forma è inviolabile».

[20] Corte Europea dei diritti dell'uomo, *Klass and others v Federal Republic of Germany*, 6 settembre 1978.

[21] «La Commissione, quando reputi che uno Stato membro abbia mancato a uno degli obblighi a lui incombenti in virtù dei trattati, emette un parere motivato al riguardo, dopo aver posto lo Stato in condizioni di presentare le sue osservazioni.»

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

A seguito delle pronunce dei loro colleghi bulgari, romeni, tedeschi, ciprioti anche i giudici della *Ústavní soud* della Repubblica Ceca hanno accolto le ragioni di quanti evidenziavano le possibili falle di un sistema massivo di raccolta preventiva dei dati informatici ed elettronici, dichiarando l'incostituzionalità dei provvedimenti normativi interni che davano attuazione alle previsioni contenute nella Direttiva 2006/24/CE.

Nel ricostruire gli elementi che hanno portato alla pronuncia dei giudici cechi può essere utile ricordare che la vicenda si inserisce nel quadro di una procedura di controllo inaugurata da un gruppo di cinquantuno deputati che lamentavano l'incostituzionalità della legge n. 125/2005 ("Legge sulle comunicazioni elettroniche"). I ricorrenti sostenevano che imporre ai gestori dei network di telecomunicazioni l'obbligo di registrare tutti i dati relativi alle comunicazioni effettuate per mezzo di sms, mail, internet, ecc. comporta una chiara violazione dell'art. 8 della Convenzione europea dei diritti dell'uomo.

La Corte costituzionale ceca ha optato per un percorso logico non basato solo sulla giurisprudenza nazionale, ma ha mostrato una grande attenzione anche a prospettive derivanti da precedenti giurisprudenziali della Corte europea dei diritti dell'uomo e di altri sistemi costituzionali. Partendo da questo presupposto i giudici costituzionali, ribadendo in primo luogo il riconoscimento del diritto all'inviolabilità delle comunicazioni private, hanno richiamato il medesimo percorso giuridico indicato dalla giurisprudenza costituzionale tedesca[22]. Così, per risolvere la questione relativa alle modalità di intervento su provvedimenti che hanno origine

[22] Sentenza 1 BvR 256/08 del Bundesverfassungsgericht, del 2 marzo 2010.

da una previsione europea, i giudici di Brno hanno statuito la rilevanza esclusivamente interna dell'applicazione della direttiva europea, ribadendo inoltre come la medesima rinvii al legislatore nazionale la scelta delle modalità più opportune all'adempimento degli obblighi costituzionali.

La condotta dei giudici cechi è utile per analizzare anche lo sviluppo delle interpretazioni e delle relazione degli ordinamenti. Se infatti è vero che la dichiarazione di incostituzionalità si è rivelata utile per bloccare e rivedere l'applicazione di una normativa con non pochi punti critici, per contro è apparsa discutibile la scelta di mutuare l'impianto argomentativo della decisione tedesca sulla conservazione dei dati e di non utilizzare lo strumento del rinvio pregiudiziale. A parere della Corte infatti l'adesione della Repubblica ceca all'UE non priva la stessa della competenza a giudicare sulla costituzionalità delle leggi. Tale condotta posta in essere nei confronti della giurisdizione del Lussemburgo non rispetta *in primis* quell'obbligo di leale collaborazione che dovrebbe ispirare le relazioni tra i giudici, principio invece rispettato sia dall'Irlanda e dall'Austria e, *in secundis*, contravviene gli obblighi imposti dalla giurisprudenza europea sulla base dell'art. 264 TFUE[23] (Vecchio 2014).

Infine, come anticipato, la Corte costituzionale slovena adotta un atteggiamento intermedio tra quello "cooperativo" e "nazionalistico". Infatti, con l'ordinanza della Corte costituzionale slovena del 26 settembre 2013, la Corte costituzionale ha sospeso il procedimento attinente una questione di costituzionalità sollevata in relazione alla legge sulla comu-

[23] «Se il ricorso è fondato, la Corte di giustizia dell'Unione europea dichiara nullo e non avvenuto l'atto impugnato. Tuttavia la Corte, ove lo reputi necessario, precisa gli effetti dell'atto annullato che devono essere considerati definitivi.»

nicazioni elettroniche, precedentemente entrata in vigore per attuare la direttiva *Data Retention*, fino alla decisione della Corte di giustizia dell'Unione europea nelle cause C-293/12 (rinvio della *High Court irlandese*) e C-594/12 (il rinvio da parte della Corte costituzionale austriaca). In particolare, l'ordinanza ha riguardato un ricorso relativo alla violazione del diritto alla riservatezza (art. 37-38 Cost. [24]), della libertà di circolazione (art. 32 Cost.[25]), della libertà di manifestazione del pensiero (art. 39 Cost. [26]) e del principio di presunzione di innocenza (art. 27 Cost. [27]), per effetto

[24] Art. 37: "È garantita la segretezza della corrispondenza e degli altri mezzi di comunicazione. Solo la legge può stabilire che, in base a un provvedimento del tribunale, sia permesso che per un determinato periodo non si rispetti la tutela della segretezza della corrispondenza e di degli altri mezzi di comunicazione e l'inviolabilità della sfera privata dell'uomo, qualora ciò sia reso indispensabile per l'inizio o la prosecuzione di un procedimento penale o per la sicurezza dello Stato».

Art. 38: "È garantita la protezione dei dati personali. È vietato l'uso dei dati personali in contrasto con lo scopo della loro raccolta. La legge definisce la raccolta, l'elaborazione, lo scopo dell'uso, il controllo e la protezione dei dati personali. Ognuno ha il diritto di venire a conoscenza dei dati personali raccolti che lo riguardano e il diritto di tutela giurisdizionale contro il loro abuso».

[25] «Ognuno ha il diritto di circolare e di soggiornare liberamente, di lasciare il Paese e di farvi ritorno in qualsiasi momento. Tale diritto può essere limitato dalla legge soltanto se sia necessario per garantire lo svolgimento di un procedimento penale, per impedire la diffusione di malattie contagiose, per assicurare l'ordine pubblico ovvero se lo richiedano gli interessi della difesa dello Stato. La legge può limitare agli stranieri l'ingresso nel Paese e la durata del soggiorno in esso.»

[26] «È garantita la libertà di espressione dei propri pensieri, di discorsi e interventi pubblici, di stampa e di altre forme di informazione ed espressione pubblica. Ognuno può liberamente raccogliere, accettare e divulgare notizie e pareri. Ognuno ha il diritto di ricevere informazioni di carattere pubblico per le quali ha qualche interesse legale fondato sulla legge, salvo nei casi stabiliti dalla legge.»

dell'applicazione delle disposizioni della legge di attuazione della normativa europea, che dispongono la conservazione, anche preventiva, dei dati elettronici.

> La Corte costituzionale, pur non escludendo la propria competenza a giudicare sulla costituzionalità di atti normativi di attuazione delle fonti europee, ha affermato tuttavia che la questione di costituzionalità relativa alla legge slovena dipendesse direttamente dalla compatibilità della direttiva sulla conservazione di dati con gli art. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, che corrispondono, sul piano interno, agli art. 37 e 38 della Costituzione slovena. La decisione sulla costituzionalità della legge necessita di una preventiva risoluzione della questione di compatibilità tra direttiva 2006/24/CE e Carta dei diritti dell'UE, competenza che, come ha sottolineato la Corte slovena, spetta esclusivamente alla Corte di Giustizia. (Dicosola, 2016)

La decisione della Corte rappresenta una parte importante nel dibattito riguardante la necessità e la proporzionalità dell'uso di misure e tecnologie di sorveglianza da parte delle forze dell'ordine e delle agenzie di *intelligence*. Il 3 luglio 2014, la Corte costituzionale slovena ha annullato gli articoli della legge sulle comunicazioni elettroniche adottati al fine di attuare la direttiva 2006/24 e ha ordinato agli operatori elettronici di distruggere tutte le informazioni in loro possesso. Nella decisione principale, la Corte Costituzionale ha rilevato che con l'annullamento della di-

[27] «La persona accusata di illecito si considera innocente finché la sua colpa non venga provata mediante sentenza passata in giudicato.»

rettiva, veniva meno l'obbligo per lo Stato membro di recepirla nel proprio ordinamento giuridico.

La Corte slovena, nell'ordinanza con la quale ha sospeso il procedimento, in primo luogo ha ribadito la propria facoltà di valutare le misure nazionali di attuazione della direttiva, anche se, ai sensi dell'articolo 267 del TFUE, la Corte di giustizia detiene la competenza esclusiva sulla questione della validità della direttiva. Il suo compito principale è stato quindi quello di valutare se, in assenza dell'obbligo creato per il legislatore nazionale di porre in essere una legislazione di attuazione dalla direttiva 24/2006, la normativa possa ugualmente rimanere nel sistema giuridico sloveno. La Corte Costituzionale slovena in primo luogo ha affermato che la vasta conservazione dei dati, attuata senza criteri ben definiti, è stata sproporzionata. Se il compito del giudice è quello di affidare la tutela dei diritti fondamentali alla Corte di giustizia, si deve allo stesso tempo continuare a collaborare per garantire l'attività della Corte di giustizia (Bardutzky 2014).

5. Osservazioni conclusive

Alla luce della breve analisi proposta in questo studio, appare evidente come il diritto alla *privacy* sia ormai totalmente "inglobato" all'interno del nostro patrimonio giuridico e che, in questa fase di trasformazione ed evoluzione tecnologica, possa costituire la "bussola" con cui orientarsi all'interno del sistema normativo. La formazione di nuovi diritti, quali ad esempio il diritto all'oblio non è altro che la conseguenza di considerazioni precedenti sviluppatesi appunto sul diritto alla riservatezza.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

La sentenza della Corte di Giustizia sul caso della *Data Retention Directive* e le decisioni delle Corti costituzionali sulle leggi di attuazione della stessa hanno rafforzato infatti la convinzione che le limitazioni applicabili a tale diritto, debbano essere poste con la massima chiarezza e con le minime limitazioni. L'idea stessa di comprimere le garanzie relative al diritto alla riservatezza per fronteggiare problemi o per garantire altri diritti costituisce un messaggio errato che viene diffuso da alcuni Stati con la massima convinzione. Risulterebbe invece più opportuno considerare, in una prospettiva oggettiva e più critica, che i dati raccolti talvolta si rivelano poco utili alle esigenze effettivamente palesate.

Sebbene sia ormai chiaro che una efficace lotta contro gravi forme di criminalità dipenda sempre più frequentemente dall'uso di strumenti d'indagine ad alto contenuto tecnologico, ciò non legittima un utilizzo indiscriminato e incontrollato dei dati. Tra questi le c.d. perquisizioni *online* occupano uno spazio che impegna la riflessione del processualista per la peculiarità del diritto fondamentale che la loro pratica comprime e per il fatto di assommare le caratteristiche di diversi strumenti di indagine. È quindi compito del legislatore intervenire, regolando con una disciplina *ad hoc* un equo bilanciamento, alla luce del principio di proporzionalità, tra diritti costituzionalmente protetti: quello alla riservatezza informatica da un lato e quello alla repressione dei reati dall'altro.

Nell'attuale assetto della società dell'informazione e di internet non è possibile pensare di affrontare le sfide poste dalle nuove tecnologie senza poter sfruttare le loro potenzialità. La questione da porsi riguarda i limiti entro i quali può operare il legislatore (nazionale ed europeo) nella compromissione dei diritti fondamentali. Al riguardo, l'art. 52 della Carta dei diritti fondamentali dell'Unione europea, identifica proprio nel

principio di proporzionalità il criterio guida fondamentale, sia sul piano ermeneutico che su quello delle scelte normative del legislatore, delimitandone l'area di discrezionalità.

Per queste ragioni le linee guida ricavabili dalla lettura combinata delle sentenze della Corte di Giustizia sui casi *Google Spain, Data retention e Teledue* potrebbero costituire la base idonea a consentire il giudizio di bilanciamento fra le esigenze contrapposte. Infatti, con la sentenza *Teledue,* la Corte di Giustizia completa quel ciclo che, anche per merito del dialogo instauratosi tra alcune giurisdizioni costituzionali nazionali, ha portato al raggiungimento di uno *standard* di tutela applicato uniformemente a tutti gli Stati membri.

È opportuno ricordare che alcuni ordinamenti, già prima della pronuncia della Corte di Giustizia del 2014 avevano seguito un'interpretazione di maggior tutela della riservatezza per mezzo delle proprie Corti costituzionali, il che ha portato al recepimento del livello di tutela oggi accolto in materia anche dall'Unione. D'altra parte, altri Stati membri come l'Austria, hanno annullato le norme sulla conservazione dei dati in un secondo momento, recependo il nuovo orientamento della Corte di Giustizia emerso a seguito della pronuncia oggetto dello scritto. Altri Stati invece, tra cui Danimarca e Italia, hanno scelto di conservare discipline nazionali non omogenee rispetto ai principi recepiti dalla giurisprudenza della Corte di Giustizia del 2014. Si tratta quindi di definire quali condotte attuative debbano essere assunte in tale ultimo gruppo di Stati membri e, a tal proposito, la sentenza *Teledue* riveste un ruolo fondamentale, non ammettendo una conservazione generalizzata ed indifferenziata dei dati.

Bibliografia

Alpa, G., G. Resta (2006), *Le persone e la famiglia. Vol 1: Le persone fisiche e i diritti della personalità* , in R. Sacco (cur.), *Trattato di diritto civile*, Milano: Utet giuridica, pp. 97-108.

Baldassarre, A. (1997), *Diritti della persona e valori costituzionali*, Torino: Giappichelli.

Bardutzky, S. (2014), *The timing of dialogue: Slovenian Constitutional Court and the Data retention Directive*, in www.verfassungblog.de (consultato il 14/04/2016)

Benedizione, L., E. Paris (2014), *Bilanciamento e dialogo fra le Corti: la Corte di giustizia dichiara invalida la Data Retention directive*, in www.dirittocomparati.it (consultato 14/04/2016)

Benedizione, L., E. Paris (2015), *Preliminary Reference and Dialogue Between Courts as Tools for Reflection on the EU System of Multilevel Protection of Rights: The Case of the Data Retention Directive,* in *German Law Journal*, 16(6), pp. 1727-1769.

Bignami, F. (2007), *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, in *Chicago Journal of International Law*, pp. 233-255.

Bobbio, N. (1997), *L'età dei diritti*, Torino: Einaudi.

Bonetti, P. (2006), *Terrorismo emergenza e costituzioni democratiche*, Bologna: il Mulino

Brandeis, S., L. Warren (1890), *The right to Privacy*, in *Harvard Law Review,* Vol. IV, n. 5.

Carnevale, P. (2002), *Emergenza bellica e sospensione dei diritti costituzionalmente garantiti. Qualche prima considerazione anche alla luce dell'attualità*, in *Giurisprudenza costituzionale*, pp. 4509-4528.

Cerqua, F. (2014), *La Corte di giustizia dichiara invalida la direttiva sulla*

data retention: brevi osservazioni, in www.dirittopenaleeuropeo.it (consultato il 14/04/2016).

Daniele, M. (2016), *La triangolazione delle garanzie processuali fra diritto dell'Unione europea, CEDU, e sistemi nazionali*, in www.penalecontemporaneo.it. (consultato il 14/04/2016).

De Vergottini, G. (2004 a), *Guerra e costituzione*, Bologna: il Mulino.

De Vergottini, G. (2004 b), *La difficile convivenza fra libertà e sicurezza. La risposta delle democrazie al terrorismo* , in *Rassegna Parlamentare*, pp. 427-454.

Dicosola, M. (2014), *La data retention directive e il dialogo tra Corti costituzionali e Corte di giustizia nel sistema multilivello europeo*, in www.diritticomparati.it (consultato il 14/04/2016).

Dicosola, M. (2016), *Gli Stati dell'Europea centro-orientale tra identità nazionale e costituzionalismo europeo*, in *La cittadinanza europea*, n. 1.

Fabbrini, F. (2015), *Human Rights in the Digital Age. The European Court of Justice Ruling in the Data Retention case and its Lessons for Privacy and Surveillance in the U.S.A*, in *Harvard Human Rights Journal*, vol. 28, pp. 65-95.

Ferro, G. (2014), *Riflessioni sul cammino "costituzionale" della Corte di giustizia dell'Unione europea*, in www.ambientediritto.it (consultato il 14/04/2016).

Flor, R. (2015), *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia*, in G. Resta, V. Zeno-Zencovich (cur.), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, in http://romatrepress.uniroma3.it/ita/ (consultato il 20/12/2016).

Groppi, T. (cur.) (2006), *Democrazia e terrorismo*, Napoli: Editoriale Scientifica.

Guild. E., S. Carrera (2014), *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive*, CEPS Liberty and Security in Europe Papers, n. 65.

Mantelero, A. (2015), *Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso Google: ricordare e dimenticare nella digital economy*, in G. Resta, V. Zeno-Zencovich (cur.), *Il diritto all'oblio su Internet dopo la sentenza Google Spain, in* http://romatrepress.uniroma3.it/ita/ (consultato il 20/12/2016).

Papademetriou, T., *European Union: ECJ invalidates Data Retention directive*", in www.libraryofcongress.gov (consultato il 14/04/2016).

Pizzetti, F. (2015), *Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain*, in G. Resta, V. Zeno-Zencovich (cur.), *Il diritto all'oblio su Internet dopo la sentenza Google Spain, in* http://romatrepress.uniroma3.it/ita/ (consultato il 20/12/2016).

Pizzetti, F. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, vol. 2, Torino: Giappichelli

Pollicino, O. (2014), *Interpretazione o manipolazione? La Corte di Giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it*, n. 3.

Pollicino, O. (2015), *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo?*, in G. Resta, V. Zeno-Zencovich (cur.), *Il diritto all'oblio su Internet dopo la sentenza Google Spain, in* http://romatrepress.uniroma3.it/ita/ (consultato il 20/12/2016).

Pollicino, O., M. Bassini (2017), *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in www.penalecontemporaneo.it (consultato il 10/02/2017).

Prevosti, O. (2014), *Tutela della privacy come presupposto della libertà: due recenti sentenze della Corte di Giustizia dell'Unione Europea a difesa della riservatezza individuale*, in www.osservatorioaic.it (consultato il 10/02/2017).

Raducu, I. (2014), *Deferential Dialogues between the Court of Justice and Domestic Courts Regarding the Compatibility of the EU Data Retention Directive with (Higher?) National Fundamental Rights Standards*, University of

Luxembourg Law Working Paper, n. 2014-03.

Rauhoffe J., D.M. Sithigh (2014), *The Data Retention Directive Never Existed*, University of Edinburgh School of Law Research Paper Series, n. 2014/34.

Resta, G. (2014), *Dignità, persone, mercati*, Giappichelli: Torino, pp. 73-96.

Rodotà, S. (2004), *Privacy, libertà, dignità*, in www.garanteprivacy.it (consultato il 14/04/2016).

Romboli, R. (2014), *Corte di giustizia e giudici nazionali: il rinvio pregiudiziale come strumento di dialogo*, in www.rivistaaic.it, n. 3 (consultato il 14/04/2016).

Savino, M. (2008), *Libertà e sicurezza nella lotta al terrorismo: quale bilanciamento?*, in *Giornale di diritto amministrativo*, fasc. 4, pp. 211-217.

Scaffardi, L. (2013), *Nuove tecnologie, prevenzione del crimine e privacy: alla ricerca di un difficile bilanciamento*, in A. Torre (cur.), *Costituzioni e sicurezza dello Stato*, Santarcangelo di Romagna: Maggioli, pp. 425-439.

Sperti, A. (2009), *Il Terrorist Surveillance Program e le sue delicate implicazioni sul piano costituzionale*, in *Quaderni costituzionali*, pp.105-108.

Vecchio, F. (2014), *L'ingloriosa fine della direttiva Data Retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy*, in www.diritticomparati.it (consultato il 14/04/2016).

Vecchi, F. (n.d.), *Un nuovo capitolo nella "saga" del Data retention: la Corte costituzionale della Repubblica ceca dichiara l'incostituzionalità degli atti di attuazione della direttiva 2006/24/CE*", in www.unikore.it (consultato il 14/04/2016).

Vedaschi A., V. Lubello (2015), *Data Retention and its Implications for the Fundamental Right to Privacy*, in *Tilburg Law Review*, pp. 14-34.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Osservatorio sulla giurisprudenza

Abstract

Right to privacy and security in the jurisprudence of National and Supranational European Courts. The "Data Eetention Directive" case

The "Data Retention Directive" (2006/24/EC) states the obligation for providers of publicly available electronic communications services or of public communications networks to retain traffic and location data for six months up to two years for the purpose of the investigation, detection and prosecution of serious crime. This article analyses the decision of the European Court of Justice about the compatibility of the "Data direction directive" with the European fundamental rights, and proposes an analysis of the different approaches came from some National Constitutional Courts, called to express their opinions about the national sustainability of the Directive.

Keywords: Privacy; data retention; suspension of fundamental rights; European Court of Justice; security.