DIPARTIMENTO DI SCIENZE POLITICHE

CATTEDRA DI DIRITTO DI INTERNET

La giurisprudenza della Corte di giustizia dell'Unione europea sulla privacy: un fronte ancora aperto sui colossi del web

RELATORE
Prof.Pietro Falletta

Jacopo Verzaschi
Matr. 074462

ANNO ACCADEMICO

2016/2017

INDICE

CAPITOLO 4

LA CORTE DI GIUSTIZIA E IL TRASFERIMENTO DEI DATI DALL'UNIONE AGLI STATI UNITI

4.1 La sentenza Schrems della Corte di Giustizia, Grande Sezione, 6 ottobre 2015, causa 362/14

4.2 Il procedimento principale e le questioni pregiudiziali

4.3 La natura delle decisioni della Commissione

4.4 La posizione assunta dalla Corte di Giustizia

Conclusioni

INTRODUZIONE

Intendimento del presente lavoro è quello di dimostrare come nel mondo di Internet sia evidente, forse ancora più che in altri campi, l'esigenza di contemperare interessi giuridici e beni da tutelare, attraverso un bilanciamento non sempre facile da operare.

Oltre ad una obiettiva difficoltà di porre in essere tale bilanciamento, occorre prendere atto che esso muta nel tempo, perché mutevoli sono le condizioni politiche e sociali, che impongono al legislatore di intervenire in maniera differente, a seconda delle necessità che si prospettano.

Dopo aver illustrato il concetto di privacy sia nella sua accezione generica e nel diritto comune, si cercherà di rapportarlo al mondo dell'informatica e delle telecomunicazioni, ponendo in risalto le difficoltà di calibrare esigenze apparentemente contrapposte: da una parte la libera circolazione delle informazioni e la libertà di informazione, agevolate dalle enormi prerogative di Internet, quale veicolo di notizie e dati potenzialmente illimitato; dall'altra, la tutela del diritto alla privacy; della tutela dei dati personali e più in generale della vita privata.

Di tutto questo si è resa interprete la Corte di Giustizia, che, con tre pronunce a distanza di breve tempo l'una dall'altra, ha orientato il legislatore europeo verso la difesa strenua della privacy e della garanzia che il trattamento dei dati personali avvenga attraverso adeguate forme di protezione.

I fatti terroristici che avevano animato il legislatore al momento della adozione di una normativa in un certo qual modo derogatoria rispetto alle modalità di raccolta, trattamento e trasferimento dati di cui alle precedenti direttive, a vantaggio della tutela della sicurezza nazionale, cedono il passo ad una impostazione che vede la centralità dell'uomo e della sua individualità. In alcun modo la dimensione individuale e il patrimonio di informazioni che lo connotano, possono essere sacrificate, rispetto ad un controllo generalizzato ed indiscriminato di dati e informazioni, che atteggiandosi ad un controllo di massa, appare, per ciò solo, inaccettabile.

La Corte ha affermato e difeso il diritto all'oblìo, inteso come il diritto a non vedere diffuse, a meno che non sussistano particolari motivi, notizie che siano di pregiudizio all'onore di una persona, per tali intendendosi principalmente i precedenti giudiziari di una persona. A meno che non si tratti di casi particolari ricollegabili a fatti di cronaca ed anche in tali casi la pubblicità del fatto deve essere proporzionata all'importanza dell'evento ed al tempo trascorso dall'accaduto.

Si rinnova, così, una nuova sensibilità sul tema della privacy, ed un atteggiamento, quello della Corte di Giustizia, che, in adesione alle doglianze di molti Stati dell'Unione, ha censurato modalità di raccolta e trattamento dati, sollevando interrogativi sulla adeguatezza degli strumenti normativi ed imponendo al legislatore europeo di ripronunciarsi, colmando il vuoto generato dalla declaratoria di invalidità della direttiva 2006/24/CE.

Il lavoro cercherà, poi, di porre in evidenza il ruolo delle autorità nazionali quali soggetti indipendenti nel valutare le domande poste da un soggetto riguardo al trattamento di dati personali che lo riguardano - dati

trasferiti da uno Stato membro verso un paese terzo preposto al trattamento – laddove l'interessato faccia valere il diritto e la normativa di quel paese non garantisca un livello di protezione adeguato.

Elemento comune alle pronunce oggetto di analisi è senz'altro la valorizzazione della Carta dei diritti fondamentali dell'Unione europea, che, all'art. 52 della Carta prevede che: "Ogni eventuale limitazione ai diritti fondamentali garantiti deve essere prevista dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

Punto di approdo del legislatore europeo, è il Regolamento 2016/679, nuovo Regolamento europeo in materia di dati personali, ispirato ai principi enunciati dalla Corte di Giustizia, che ha senz'altro recepito le istanze dei legislatori di alcuni Stati dell'Unione, sollecitate da una dottrina particolarmente sensibile al tema della privacy e al bilanciamento degli interessi a favore della tutela dei dati personali.

In Italia, uno dei giuristi che senz'altro si è fatto artefice di questo percorso è Stefano Rodotà, al quale spetta il merito della presentazione della «Dichiarazione dei diritti in Internet», elaborata dalla Commissione per i diritti e doveri relativi ad Internet, presentata all'Internet Governance Forum nel novembre 2015 in Brasile, destinata ad avere visibilità oltre i confini dell' Italia; non è insomma una legge invocabile davanti a un giudice, ma, al tempo stesso, ha rappresentato e rappresenta un valore di mozione di indirizzo, in grado di orientare le scelte delle Istituzioni italiane ed europee.

Secondo Rodotà, in Rete ha ancora una certa fortuna l'idea che internet non abbia bisogno di regole, ma egli ritieni che si tratta di una posizione smentita dai fatti. Siamo pieni di regole, molte delle quali rappresentano delle vere e proprie limitazioni della libertà. E' necessario riequilibrare i diritti.

«Internet ha contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e tra queste e le Istituzioni. Ha cancellato confini e ha costruito modalità nuove di produzione ed utilizzazione della conoscenza. ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l'organizzazione del lavoro. Ha consentito lo sviluppo di una società più ampia e libera. Internet deve essere considerata una risorsa globale che risponde al criterio della universalità.

L'Unione europea è oggi la regione del mondo dove è più elevata la tutela costituzionale dei dati personali, esplicitamente riconosciuta dall'art. 8 della Carta dei diritti fondamentali, che costituisce il riferimento necessario per una specificazione dei princìpi riguardanti il funzionamento di Internet, anche in una prospettiva globale.»

Questa dichiarazione dei diritti in Internet è fondata sul pieno riconoscimento di libertà, uguaglianza, dignità, e diversità di ogni persona. La garanzia di questi diritti è condizione necessaria perché sia assicurato il funzionamento democratico delle Istituzioni, e perché si eviti il prevalere di poteri pubblici e privati che possano portare a duna società della sorveglianza, del controllo e della selezione sociale. Internet si configura come uno spazio sempre più importante per l'autorganizzazione delle persone e dei gruppi e come uno strumento essenziale per promuovere la partecipazione individuale e collettiva ai processi democratici e

l'eguaglianza sostanziale. I princìpi riguardanti Internet tengono conto anche del suo configurarsi come uno spazio economico che rende possibili innovazione, corretta competizione e crescita in un contesto democratico.

«Una Dichiarazione dei diritti di Internet è strumento indispensabile per dare fondamento costituzionale a princìpi e diritti nella dimensione sovranazionale»[1].

[1] Dal preambolo della Dichiarazione dei diritti in Internet

CAPITOLO 1

1. PRIVACY ED INTERNET

1.1. Le origini del diritto alla privacy.

Leggendo l'opera Monografica «The right to privacy»[2], pubblicata sulla rivista Harward Law rewiev nel 1890, si prende atto che il concetto di privacy quale protezione dei dati personali, rappresenta il culmine di un percorso dottrinale e giurisprudenziale che vede il suo epicentro negli Stati Uniti, Paese da cui provenivano i giuristi Warren e Brendeis, autori dell'opera citata. E' a loro che si deve il primo riconoscimento del concetto di privacy quale diritto autonomo, sganciato dai tradizionali concetti di onore e reputazione, a vantaggio di una nozione propria, focalizzata e concentrata sulla intimità dell'uomo. La grande novità consiste in una visione che esula dal diritto di proprietà e dagli aspetti economici ad essa connessi. La nuova impostazione, secondo i giuristi, nasce dalla consapevolezza del fatto che la normativa volta a sanzionare la diffamazione e la calunnia è in funzione della tutela dell'onore e della reputazione, ma che alla base di ciò la Common law afferma e riconosce un diritto generale alla privacy, quale diritto di decidere se ed in quale misura svelare la propria intimità a terzi, con il divieto di chiunque di pubblicare dati e informazioni personali senza il consenso dell'interessato. Questo diritto prescinde dalle forme di comunicazione o dalle modalità espressive attraverso le quali quei contenuti trovano estrinsecazione. Ed è, altresì, altra cosa rispetto al diritto d'autore, in relazione al quale la normativa mira a tutelare gli utili derivanti dall'utilizzo di opere e lavori propri.

Secondo i due giuristi il diritto alla privacy, così inteso, è sganciato, allora, dal diritto di proprietà dell'opera, che sia artistica o letteraria. Ne costituisce la prova la mancata accordata tutela, da parte di alcuni Tribunali dell'epoca, ad opporsi alla pubblicazione di lettere private, sul presupposto che esse difettassero del connotato di composizione letteraria, e, per ciò solo, non fossero meritevoli di protezione.
Di qui la convinzione che esista un generale diritto dell'individuo ad essere lasciato solo, accordando protezione alla propria intimità ed interiorità, ed il riconoscimento della violazione della privacy quale illecito civile, cui riconoscere tutela, e, dunque, risarcibilità, posto che il diritto permane fino alla pubblicazione dei dati o dei fatti, da parte dell'interessato, ovvero tramite il consenso da questi prestato.
Il silenzio del legislatore statunitense negli anni successivi rivela il disorientamento e l'impreparazione di tradurre in diritto positivo questa nuova impostazione, ma gli scritti della metà degli anni '60 dimostrano come la strada fosse stata tracciata[3]: partendo dalla Common law viene così sancita la distinzione tra diritto alla riservatezza e diritto alla proprietà privata, riconoscendo il valore della interiorità umana, così da poter invocare il diritto alla privacy, in un certo qual modo contrapposto al primo emendamento della Costituzione americana, che riconosce la libertà di stampa.

[2] S. D. Warren e L. Brandeis The right to privacy, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
[3] A. Westin, Privacy and freedom, The Bodley Head Ltd, 1970 .

Di questo percorso ha risentito anche l'Europa, così che il legislatore europeo, con la direttiva 95/46/CE ha sancito la tutela alla protezione dei dati personali quale diritto fondamentale della persona, da riconoscersi tanto nell'ordinamento comunitario, quanto all'interno dei singoli Stati membri, attraverso la fissazione di misure standard di tutela che ogni Stato è obbligato a garantire. Successivamente, la Carta di Nizza, all'art. 8 ha affermato che «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. 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. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

Come si vedrà di seguito, le sentenze della Corte di Giustizia oggetto di commento sono in linea con il modello di regolamentazione che riconosce la privacy come diritto fondamentale, rispetto ad un atteggiamento, quello degli Stati Uniti (nonché dell'Unione europea), che appare paradossale, o, per lo meno oggetto di riflessione: lo stesso Stato che ha lottato ai fini di delineare un modello di privacy quale diritto da salvaguardare a tutti i costi, ha successivamente messo in discussione l'assolutezza di siffatte conclusioni dopo l'attentato terroristico dell'11 settembre 2001, a vantaggio delle esigenze di sicurezza nazionale. Le sentenze della Corte di Giustizia, lontane dalla emotività di quel periodo di terrore, recuperano quella visione di tutela piena ed efficace della privacy, ritenendo indebite le compressioni subìte dalle libertà e dai diritti dei cittadini.

Il termine inglese privacy richiama significati plurimi e può accostarsi ai concetti di «riservatezza», «privatezza». L'evoluzione del suo significato ha fatto sì che con la parola «*privacy*» oggi debba intendersi tanto il diritto di essere lasciati in pace o di proteggere la propria sfera privata, quanto il diritto di controllare l'uso e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione.[4]

La privacy ha assunto una importanza tale, da essere considerata, soprattutto nella accezione di diritto alla protezione dei dati personali, un diritto fondamentale delle persone, strettamente correlato alla tutela della dignità umana, come sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea[5].

E' questo un importante riferimento normativo a tutela della propria libertà individuale rispetto alle ingerenze di un'autorità pubblica, al di fuori delle ipotesi previste dal legislatore a tutela della sicurezza nazionale, della pubblica sicurezza, del benessere economico del paese, dell'ordine o della prevenzione dei reati, ovvero della protezione della salute o della morale.

L'art. 8 comma 1 della Carta dei diritti fondamentali recita:«1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. 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

[4] In http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1663787
[5] In http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1663787

previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

L'evoluzione del concetto di privacy è stata anche frutto dell'elaborazione giurisprudenziale. La giurisprudenza decise di identificare tale diritto nella tutela delle situazioni e vicende strettamente personali e familiari, le quali, anche laddove accadute fuori dal domicilio domestico, non rivestono un interesse socialmente apprezzabile[6].

Detta affermazione è divenuta fondamentale per il bilanciamento tra riservatezza e diritto di cronaca, in quanto la linea di confine tra privacy e diritto all'informazione di terzi è oggi condizionata dalla popolarità del soggetto, pur precisando che anche soggetti famosi conservano tale diritto, però limitatamente a fatti che non hanno niente a che vedere con i motivi della propria popolarità.

Successivamente, la giurisprudenza di legittimità, pur non riconoscendo espressamente un diritto alla riservatezza, ha ammesso il diritto ad un tutela in tale ambito, riconoscendo che nel nostro ordinamento il diritto alla privacy aveva cittadinanza[7].

Inizialmente, quindi, la riservatezza era più che altro un diritto riconosciuto alle persone note. L'Italia fu uno degli ultimi Stati in Europa ad approvare una legge di tutela della privacy di applicazione generale, la legge 675/1996, oggi contenuta nel Codice in materia di protezione dei dati personali (Codice della privacy) cioè il d.lgs. 196/2003, secondo il quale la privacy non è solo il diritto a non vedere trattati i propri dati senza consenso, ma anche l'adozione di cautele tecniche ed organizzative che tutti, comprese le persone giuridiche, devono rispettare per procedere in maniera corretta al trattamento dei dati altrui[8].

Detta normativa, considerata la più completa a livello europeo, dedica la prima parte ai principi generali, dettando le definizioni essenziali per la comprensione della normativa, tra le quali quelle di dato personale e di trattamento[9].La privacy, intesa nel modo sopra descritto, deve trovare il giusto contemperamento con il diritto di cronaca e il diritto all'informazione costituzionalmente garantito; questa, allora, la difficoltà, e cioè quella di stabilire il corretto compromesso tra i due interessi.

In effetti, anche il diritto all'informazione, inteso non soltanto come diritto di cronaca, ma anche come diritto alla manifestazione del pensiero, trova un suo riconoscimento nella Costituzione, essendo tutelato dall'articolo 21. Il consenso esplicito al trattamento dei dati che riguardano l'interessato, è l'atto giuridico attraverso il quale si realizza il bilanciamento tra i due interessi, come sancito dal Codice in materia di

[6] Corte di cassazione, 22 dicembre 1956, n. 4487
[7] Corte di cassazione, del 27 maggio 1975, n. 2129
[8] In http://brunosaetta.it/privacy/privacy-o-diritto-alla-riservatezza-e-protezione-dei-dati-personali.html
[9] Vengono recepite le direttive 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati; nonché la direttiva 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.

protezione dei dati personali; consenso, peraltro revocabile, in virtù del quale egli mantiene il controllo sulle informazioni che lo riguardano.

La giurisprudenza ha chiarito che, in tema di attività giornalistica è, però, consentito il trattamento dei dati personali, la comunicazione e la diffusione anche senza il consenso dell'interessato e, con riferimento ai dati sensibili e giudiziari, senza nemmeno la preventiva autorizzazione del Garante, purché vengano rispettati i limiti sanciti in ordine al diritto di cronaca e cioè l'essenzialità della notizia e il suo interesse pubblico**,** con l'unica eccezione dei dati relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti pubblici.[10]

1.2 Privacy ed internet: evoluzione del quadro normativo

La adozione di una disciplina normativa unitaria per tutti i mezzi di comunicazione elettronica deriva dal processo di digitalizzazione, che ha inevitabilmente posto nuovi profili giuridici da affrontare e risolvere.

Si pensi ad esempio, all'art. 15 della Costituzione, ai sensi del quale «La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria [cfr. art. 111 c. 1] con le garanzie stabilite dalla legge», nonché all'art. 21 della medesima Carta costituzionale, secondo cui «Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. La stampa non può essere soggetta ad autorizzazioni o censure. Si può procedere a sequestro soltanto per atto motivato dell'autorità giudiziaria nel caso di delitti, per i quali la legge sulla stampa espressamente lo autorizzi, o nel caso di violazione delle norme che la legge stessa prescriva per l'indicazione dei responsabili. In tali casi, quando vi sia assoluta urgenza e non sia possibile il tempestivo intervento dell'Autorità giudiziaria, il sequestro della stampa periodica può essere eseguito da ufficiali di polizia giudiziaria, che devono immediatamente, e non mai oltre ventiquattro ore, fare denunzia all'Autorità giudiziaria. Se questa non lo convalida nelle ventiquattro ore successive, il sequestro s'intende revocato e privo di ogni effetto. La legge può stabilire, con norme di carattere generale, che siano resi noti i mezzi di finanziamento della stampa periodica. Sono vietate le pubblicazioni a stampa, gli spettacoli e tutte le altre manifestazioni contrarie al buon costume. La legge stabilisce provvedimenti adeguati a prevenire e a reprimere le violazioni». Ebbene, sulla rete questa distinzione rinvenibile dagli articoli citati è destinata a venir meno, posto che trovano applicazione entrambi i princìpi nello stesso tempo[11]. L'intento di agire sul mondo del web, anche nella forma di regole comuni in ordine ai comportamenti degli utenti, nonché nel ricorso al filtraggio e al controllo dei contenuti, viene limitato a specifici settori, quale quello della privacy.

Il problema di garantire la privacy si è posto e continua a porsi in maniera incessante e preponderante, proprio in Internet, dove la diffusione dei dati è facile e veloce. Inoltre, tale problema è strettamente legato al tema della sicurezza informatica, attesa la frequenza di furti di dati attraverso la rete.

[10] Corte di cassazione, sez. III, 12 ottobre 2012, n. 17408
[11] M. Mensi e P. Falletta, Il Diritto del Web, Casi e materiali, ed. Cedam, Padova, 2015

Lo spyware, ad esempio, è un programma che, installandosi spesso in maniera fraudolenta nei personal computer delle vittime, provvede a copiare ed inviare dati personali (pagine visitate, account di posta, gusti ecc) a terzi che successivamente li rielaboreranno e rivenderanno per i loro fini economici.

E' stata la modernizzazione e l'informatizzazione di tali nuove modalità di comunicazione ad imporre che gli Stati adeguassero i rispettivi ordinamenti, estendendo la tutela ad un nuovo concetto di privacy, rispetto ad un passato in cui la tutela atteneva alla tradizionale corrispondenza ed alla comunicazione telegrafica e telefonica.[12]

La trasversalità e transnazionalità di internet pone anche un problema in ordine alle legislazioni straniere, nonchè alla normativa da applicare, posto che una violazione commessa in rete produce effetti in molti paesi nello stesso momento.

Il diritto alla privacy, allora, si è dovuto e deve continuare a misurarsi con l'evoluzione della rete e della tecnologia, anche tenuto conto della definizione di internet, da intendersi «quale moltitudine di reti che collegano milioni di utenti mediante computer e altri dispositivi al fine di trasmettere informazioni attraverso una varietà di linguaggi, noti come protocolli».[13] Internet, dunque, quale strumento che consente di navigare ed usufruire di contenuti attraverso legami (definiti link) ed ulteriori servizi accessibili.

Il primo atto normativo attraverso cui il legislatore europeo ha inteso tutelare la privacy è la direttiva 95/46/CE, con cui il Parlamento e il Consiglio hanno imposto che gli Stati membri garantiscano, in conformità alle disposizioni della direttiva stessa, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali. Il considerando 3 racchiude la consapevolezza da parte della istituzione, di contemperare la libera circolazione delle merci, delle persone, dei servizi e dei capitali, nonché la libera circolazione dei dati personali da uno Stato membro all'altro, con la salvaguardia dei diritti fondamentali della persona.

L'apertura del mercato, l'integrazione economica e sociale, allora, gli elementi da cui trarre allora, come inevitabile conseguenza, un considerevole aumento degli scambi di dati personali tra tutti i soggetti della vita economica e sociale degli Stati membri, siano essi privati o pubblici;

La direttiva, poi, pone come condizione, che il livello di tutela dei diritti e delle libertà fondamentali sia equivalente presso tutti gli Stati membri, e, allo stesso tempo, riconosce la necessità, per raggiungere tale obiettivo, di un intervento della Comunità per avvicinare le legislazioni.

Il considerando 25 afferma che i principi di tutela si esprimono, da un lato, nei vari obblighi a carico delle persone, autorità pubbliche, imprese, agenzie o altri organismi responsabili del trattamento, obblighi relativi in particolare alla qualità dei dati, alla sicurezza tecnica, alla notificazione all'autorità di controllo, alle circostanze in cui il trattamento può essere effettuato e, dall'altro, nel diritto delle persone, i cui dati sono

[12] In http://brunosaetta.it/privacy/privacy-o-diritto-alla-riservatezza-e-protezione-dei-dati-personali.html
[13] M. Mensi e P. Falletta, Il Diritto del Web, Casi e materiali ed. Cedam, Padova, 2015

oggetto di trattamento, di esserne informate, di poter accedere ai dati, e chiederne la rettifica, o di opporsi al trattamento in talune circostanze.

La direttiva, poi, si sofferma sul concetto di trattamento dei dati, da intendersi, secondo l'art. 2 «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione»; il quale trattamento, per considerarsi lecito, deve presupporre non soltanto il consenso dell'interessato, ma deve essere effettuato per tutelare un interesse essenziale alla vita della persona a cui si riferiscono i dati.

L'art. 28, poi, attribuisce una serie di prerogative alle autorità nazionali di controllo in ordine alla legittimità del trattamento, sancendone la piena indipendenza nell'esercizio delle funzioni loro attribuite.

Gli Stati membri dispongono che le autorità di controllo siano consultate al momento dell'elaborazione delle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali.

La norma conferisce alle predette autorità poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo; di intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali; di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie. È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.

Il medesimo articolo, poi, conferisce a qualsiasi persona, o associazione che la rappresenti, il diritto di presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda. Qualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 della direttiva citata, venendo successivamente informata che una verifica ha avuto luogo.

Il percorso normativo è successivamente proseguito con la direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, che prevedeva l'armonizzazione delle disposizioni degli Stati membri atte a garantire un livello equivalente di tutela dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel

settore delle telecomunicazioni, nonché a garantire la libera circolazione di tali dati e delle apparecchiature e dei servizi di telecomunicazione all'interno della Comunità.

La direttiva richiamata è stata abrogata dalla direttiva 2002/58. L'art. 3 dispone che "la presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità"; non si cita più il settore delle telecomunicazioni ma il più ampio ed omnicomprensivo settore delle comunicazioni elettroniche.

La modifica normativa nasce, secondo il Parlamento europeo, dalla necessità di adeguarsi «agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica, in guisa da fornire un pari livello di tutela dei dati personali e della vita privata agli utenti dei servizi di comunicazione elettronica accessibili al pubblico, indipendentemente dalle tecnologie utilizzate».

Si riportano due passi ritenuti rilevanti, ove rileva l'importanza di una limitata conservazione nel tempo delle comunicazioni registrate e, comunque, per un periodo non superiore a quanto necessario:

«il divieto di memorizzare comunicazioni e i relativi dati sul traffico da parte di persone diverse dagli utenti o senza il loro consenso non è inteso a vietare eventuali memorizzazioni automatiche, intermedie e temporanee di tali informazioni fintanto che ciò viene fatto unicamente a scopo di trasmissione nella rete di comunicazione elettronica e a condizione che l'informazione non sia memorizzata per un periodo superiore a quanto necessario per la trasmissione e ai fini della gestione del traffico e che durante il periodo di memorizzazione sia assicurata la riservatezza dell'informazione"; "la riservatezza delle comunicazioni dovrebbe essere assicurata anche nel quadro di legittime prassi commerciali. Ove necessario e legalmente autorizzato, le comunicazioni possono essere registrate allo scopo di fornire la prova di una transazione commerciale"; "le parti in comunicazione dovrebbero essere informate sulla registrazione, il suo scopo e la durata della sua memorizzazione preventivamente alla stessa. La comunicazione registrata dovrebbe essere cancellata non appena possibile ed in ogni caso non oltre la fine del periodo durante il quale la transazione può essere impugnata legittimamente».

E' in questa direttiva che compare il termine «*spyware*», programma che, installandosi spesso in maniera fraudolenta nei personal computer delle vittime, provvede a copiare ed inviare dati personali (pagine visitate, account di posta, gusti ecc) a terzi che successivamente li rielaboreranno e rivenderanno per i loro fini economici.

L' art. 15 della direttiva prevede al paragrafo 1, da parte degli Stati membri, limitazioni e restrizioni di diritti ed obblighi nella «misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica» e per la «prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare

misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo».

L'evoluzione del percorso normativo in sede europea è culminato nella direttiva 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, la quale, in particolare, ha previsto l'obbligo degli Stati membri di provvedere affinché le categorie di dati elencati nell' articolo 5 della medesima, siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione.

E' questo il punto che, come si vedrà nel proseguio della trattazione, sarà oggetto di censura da parte della Corte di Giustizia.

Alla forza propulsiva delle pronunce della Corte di Giustizia, oggetto del presente lavoro, hanno fatto seguito il regolamento europeo in materia di protezione dei dati personali e la direttiva UE 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

1.3 **Sicurezza e dati personali: l'inversione di rotta della Corte di Giustizia dell'Unione europea**

Lo sviluppo tecnologico e le potenzialità da questo offerte hanno messo in risalto le lacune dell'impalcatura della normativa e la sua incapacità a bilanciare coerentemente beni giuridici diversi, soprattutto dopo l'entrata in vigore del Trattato di Lisbona, che ha elevato il diritto alla protezione dei dati personali a diritto fondamentale dell'Unione.

Si è dovuto constatare l'inadeguatezza della direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati rispetto alle nuove esigenze maturate, che rendevano ancora più evidente la mancanza di omogeneità, da parte degli Stati membri, di adattare all'interno dei rispettivi ordinamenti, una normativa piuttosto frammentata e insoddisfaciente.

L'inadeguatezza del quadro normativo e la necessità di porre un rimedio, intervenendo in via legislativa, si è resa all'evidenza, quando il flusso e il trasferimento continuo dei dati personali attraverso Internet ha dovuto fare i conti con gli attentati terroristici, a partire dall'11 settembre 2001, da quando, cioè, si è ritenuto che la privacy dovesse recedere a favore della sicurezza nazionale

Gli Stati Uniti, attraverso il *Patriot Act*, hanno così ridefinito il sistema giuridico dei diritti dei cittadini, facendo prevalere la sicurezza nazionale rispetto a ogni altro diritto fondamentale, compreso fra tutti il diritto alla protezione dei dati personali[14].

[14] Il Patriot Act, proprio per rispondere alle minacce alla sicurezza nazionale poste dal terrorismo, ha decisamente ristretto i diritti e le libertà dei cittadini; legittimando l'ampliamento delle intercettazioni delle linee telefoniche e informatiche, attraverso un incremento dei poteri degli organi di polizia e delle autorità federali.

Anche il legislatore europeo è intervenuto in relazione a quei bisogni che si imponevano in quel determinato contesto sociale, caratterizzato, successivamente al 2001, dall'attacco terroristico di Londra, che, insieme a quello di Madrid, imponeva la necessità di adottare misure efficaci in materia di conservazione dei dati relativi alle comunicazioni.

Il rischio di un sistema tutto volto alla raccolta e conservazione indiscriminata e di massa dei dati è esploso con il caso *Datagate*[15] .

A distanza di qualche anno da quegli attentati, ed impressionati dalla portata del caso *Datagate*, la Corte di Giustizia ha sentito la necessità di riespandere diritti fino a quel momento compressi, benchè già sanciti e riconosciuti[16].

Così, se il rapporto tra sicurezza nazionale e privacy, apparso da sempre come conflittuale, dapprima, e di fronte alle minacce del terrorismo, pendeva a favore della prima, ha successivamente finito per risolversi, invertendo il bilanciamento tra la sicurezza nazionale e il rispetto della privacy e delle libertà fondamentali a favore di queste ultime, in virtù di un approccio differente da parte della Corte di Giustizia.

[15] Il giornale britannico The Guardian il 5 giugno 2013 iniziò a pubblicare le rivelazioni di Edward Snowden, che fece emergere un sistema di controllo e monitoraggio gestito dall'*NSA*, in accordo con le più importanti compagnie telefoniche e operatori Internet.

[16] Vedasi il Trattato di Lisbona, nonchè la Carta di Nizza che, all'art. 8 aveva riconosciuto autonoma tutela al diritto alla protezione dei dati personali (art. 8); vedasi anche l'art. 16 TFUE, che estende il diritto alla protezione dei dati personali a tutte le materie di competenza dell'Unione e l'art. 39 TUE con riguardo alle materie di politica estera e sicurezza comune.

CAPITOLO 2

LA DIRETTIVA 2006/24/CE E L'INTERVENTO DELLA CORTE DI GIUSTIZIA

2.1 Il sistema di conservazione dei dati connessi alle comunicazioni elettroniche

Con le decisioni riunite C-293 e C-594 dell'8 aprile 2014 la Corte di Giustizia, segnando una inversione di tendenza rispetto all'orientamento giurisprudenziale del passato, ha annullato la direttiva 2006/24/CE che imponeva ai gestori di servizi di telecomunicazioni l'obbligo di conservazione di tutti i dati relativi alle comunicazioni elettroniche, nonché di fornirli, ove richiesto, alle autorità investigative e alla magistratura, per fini di accertamento e repressione dei reati gravi. La sentenza, di fatto, recepisce e fa proprie le critiche rivolte alla normativa europea, da parte degli organi giurisdizionali di alcuni Stati membri, alcuni dei quali si erano pronunciati sancendo la incostituzionalità delle rispettive leggi di recepimento della direttiva. Alcuni di essi, rilevando sin da subito le criticità evidenziate, si erano rifiutati di trasporre la direttiva nel proprio contesto normativo nazionale, ravvisando l'assenza di una precisa elencazione dei soggetti legittimati a richiedere tali dati, nonchè la genericità dell'espressione «reato grave».

Secondo la direttiva 2006/24/CE del Parlamento europeo e del Consiglio - afferente «la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE» – gli Stati membri dovevano garantire la conservazione dei dati sulle telecomunicazioni dei cittadini per un minimo di sei mesi fino a una massimo di ventiquattro mesi. In vigenza della predetta direttiva, la polizia e le agenzie di sicurezza avevano il permesso di richiedere accesso ad alcuni dettagli quali l'indirizzo IP, il tempo di utilizzo di e-mail, le chiamate telefoniche, nonché gli sms inviati e/o ricevuti. Soltanto un Tribunale aveva il potere di consentire l'accesso alle predette informazioni.

Per comprendere le ragioni della inversione di tendenza a cui ha aderito la Corte di Giustizia, appare utile risalire alle ragioni politiche che avevano indotto il legislatore europeo a legiferare nei termini di cui alla direttiva 2006/24/CE.

Nel delineare uno strumento normativo come quello della direttiva del 2006, il legislatore era stato senz'altro condizionato dalla situazione venutasi a creare all'indomani degli attentati terroristici di Londra e Madrid. Il clima di paura instaurato a seguito di quegli eventi aveva indotto a privilegiare l'esigenza della sicurezza nazionale, da anteporre agli altri beni, sia pure anch'essi di rilevanza costituzionale.

Alla stessa stregua, il giudice europeo, nel pronunciarsi nei termini di invalidità della direttiva 2006/24/CE, ha risentito del condizionamento delle rivelazioni di Edward Snowden[17], che ha fatto emergere un vero e proprio sistema di sorveglianza di massa[18].

A distanza di otto anni, e di fronte ad una soglia di attenzione rispetto agli attacchi terroristici sempre alta, ma psicologicamente più lontana da quei tragici accadimenti, la Corte ha ritenuto che la totale generalizzazione e l'eccessiva l'indeterminatezza dell'ingerenza nei dati personali e più in generale nei diritti fondamentali, non poteva essere giustificata, o, in qualche misura tollerata, da nessuna esigenza di sicurezza nazionale.

Il predetto atto normativo è stato così oggetto della pronuncia giudiziale 8 aprile 2014 da parte della Corte di Giustizia, nelle cause riunite C-293/12 e C-594/12.

Le domande di pronuncia giudiziale vertevano sulla validità della direttiva richiamata; in particolare, la domanda proposta nella prima causa atteneva alla legittimità di misure legislative e amministrative nazionali irlandesi riguardanti la conservazione di dati relativi a comunicazioni elettroniche; nella seconda, invece, la questione concerneva la compatibilità della legge attuativa della direttiva 2006/24 nel diritto interno austriaco con la legge costituzionale federale.

La direttiva non autorizzava la conservazione del contenuto delle comunicazioni né delle informazioni consultate, consentita solo in presenza di uno specifico mandato dell'autorità giudiziaria.
Il giudizio che ci occupa veniva sollecitato dall'Alta Corte Irlandese e dalla Corte Costituzionale austriaca.

La Corte ha analizzato il contesto normativo, richiamando la direttiva 95/46CE, relativa alla tutela delle persone fisiche con riguardo sia al trattamento dei dati personali sia alla libera circolazione di tali dati. Essa è volta a garantire la tutela delle libertà e dei diritti fondamentali delle persone fisiche e specificamente del diritto alla vita privata, con riferimento al trattamento dei dati personali. Il trattamento, peraltro, secondo l'art. 17, deve avvenire attraverso l'adozione – da parte del responsabile del trattamento – di misure tecniche ed organizzative appropriate, nonché di un livello di sicurezza appropriato. L'obiettivo, quello di difendersi dalla diffusione e da accessi non autorizzati, ovvero da dalla distruzione accidentale, dalla perdita accidentale o dall'alterazione, "segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di dati personali".

L'altra fonte normativa di riferimento della Corte, la direttiva 2002/58/CE concernente il trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche, mira ad armonizzare le disposizioni degli Stati membri necessarie per garantire un livello omogeneo dei diritti e delle libertà

[17] Informatico e attivista statunitense, divenuto famoso per aver rivelato l'esistenza di programmi di sorveglianza di massa da parte del Governo britannico e di quello americano.
[18] O. Prevosti, 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, settembre 2014.

fondamentali, con particolare riguardo al diritto alla vita privata ed alla riservatezza, nonchè al trattamento dei dati personali nel settore delle comunicazioni elettroniche.

2.2 I Procedimenti principali e le questioni pregiudiziali nella sentenza «Data retention»

2.2.a Le cause: C-293/12 e C-594

La questione principale atteneva al ricorso innestato da una società irlandese asseritamente proprietaria di un telefono cellulare, registrato il 3 giugno 2006 e da essa utilizzato a decorrere da pari data, ricorso con cui veniva contestata la legittimità sia di disposizioni legislative che di atti amministrativi nazionali attinenti alla conservazione di dati relativi a comunicazioni elettroniche. Il giudice interno chiedeva che la Corte di Giustizia dichiarasse la nullità della direttiva 2006/24/CE, che attribuisce l'obbligo ai fornitori di servizi di telefonia, di conservare i dati sul traffico telefonico e sull'ubicazione, entro un determinato arco temporale, a fini di prevenzione, accertamento, indagini o perseguimento dei reati e di protezione della sicurezza dello Stato. Il giudizio interno veniva, così, sospeso, decidendo, il giudice interno, di sottoporre alla Corte le questioni pregiudiziali poi affrontate. Nelle questioni pregiudiziali poste, il giudice interno aveva chiesto di verificare se la limitazione dei diritti della società ricorrente in relazione all'utilizzo della telefonia mobile non fosse incompatibile con il principio di proporzionalità ed adeguatezza, che impongono di adottare misure e restrizioni equilibrate rispetto agli obiettivi perseguiti. Alla Corte di Giustizia veniva altresì richiesto di esprimersi in ordine alla compatibilità dell'obbligo di conservazione dei dati sul traffico e sull'ubicazione entro un certo arco temporale, con il diritto ad una buona amministrazione, con il rispetto della vita privata, della protezione dei dati personali, nonché con il diritto a circolare e soggiornare liberamente nel territorio degli Stati membri.

La Corte veniva anche investita della questione di valutare in che misura i Trattati ed il principio di leale collaborazione impongano al giudice nazionale di esaminare e verificare la compatibilità delle misure nazionali volte a trasporre la direttiva 2006/24/CE con le garanzie previste dalla Carta e specificamente dall'articolo 7.

La Corte suprema irlandese, all'interno di una fattispecie in cui si contestava tanto la direttiva, quanto l'atto nazionale di recepimento, aveva così sollevato le questioni pregiudiziali sopra riportate, chiedendo di verificare se la disciplina europea bilanciasse adeguatamente la necessità di garantire la sicurezza e il corretto funzionamento del mercato interno e la necessità di garantire la libertà di circolazione, così come protetta dall'art. 21 del Trattato sul funzionamento dell'Unione europea, il rispetto della vita privata, secondo l'art. 7 della Carta europea dei diritti fondamentali; la protezione dei dati personali, secondo l'art. 8 della Carta europea dei diritti fondamentali, nonché il diritto ad una buona amministrazione, ai sensi dell'art. 41 della Carta europea dei diritti fondamentali.

Il giudice interno, ha, poi, con la terza questione, aveva altresì chiesto in che misura i Trattati e, in particolare il principio di leale collaborazione di cui all'art. 4, paragrafo 3, TUE imponessero al giudice

nazionale di esaminare e valutare in autonomia la compatibilità tra le misure nazionali volte a trasporre la direttiva 2006/24/CE con le garanzie previste dalla Carta.

Nell'altra causa oggetto di decisione, cioè la C-594/12, la questione all'origine della domanda di pronuncia giudiziale traeva origine da numerosi ricorsi con cui il governo della Carinzia e numerosi cittadini avevano chiesto l'annullamento della normativa interna di recepimento della direttiva 2006/58/C, inducendo la Corte costituzionale austriaca a chiedere se il sistema di raccolta dei dati fosse 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 tutelati dalla Carta dei diritti fondamentali. Specificamente, le questioni pregiudiziali poste concernevano la verifica della compatibilità della direttiva 2006/24/CE con gli articoli 7,8,11 della Carta.

In particolare, richiamando l'art. 52 della Carta, secondo cui «Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui», la questione atteneva a verificare se le lesioni prodotte dalla direttiva non violassero il contenuto essenziale dei diritti sopra richiamati.

2.3 La posizione assunta dalla Corte di Giustizia

La Corte ha ravvisato nella direttiva - in particolare nella parte in cui impone ai fornitori dei servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica, di conservare i dati necessari per rintracciare e identificare la fonte di una comunicazione e la destinazione della stessa, al fine di stabilire, ora, durata, e tipologia di comunicazione – una ingerenza nei diritti sanciti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione, posto che la pratica della conservazione può interferire con il diritto alla riservatezza, alla protezione dei dati personali, nonché con la libertà di espressione.

Secondo la Corte, l'accertamento dell'ingerenza nella vita privata, prescinde dalla circostanza che si tratti di dati sensibili, ovvero che gli interessati abbiano subito inconvenienti a causa di detta ingerenza, che appare *in re ipsa*, ed alla quale segue una ulteriore ingerenza nel diritto fondamentale al trattamento dei dati personali, consistente nell'accesso da parte delle autorità nazionali competenti ai dati. Così, anche gli artt. 4 e 8 della direttiva, nel prevedere regole relative all'accesso delle autorità nazionali competenti ai dati, sono costitutivi di una invasione rispetto ai diritti garantiti dall'art. 7 della Carta.

La Corte ha acclarato così, l'esistenza di una ingerenza nei diritti sanciti dagli artt. 7 e 8 della Carta, tenuto conto del fatto che la predetta conservazione dei dati può ledere ed il loro ulteriore utilizzo condizionare i soggetti interessati, inducendoli a sentire la propria vita privata bersaglio di continuo controllo ed intrusione. Verificata l'esistenza di una siffatta invasione, i giudici si sono posti il problema di valutarne la legittimità secondo le regole dell'ordinamento europeo.

Ciò posto, i giudici si sono dovuti porre la domanda di stabilire se quella invasione fosse giustificata, nonchè rispettosa del principio di proporzionalità, canone interpretativo contenuto nel medesimo articolo 52. L'analisi della direttiva, infatti, non può non tener conto di quella disposizione normativa, proprio nella misura in cui prevede che la legge possa limitare l'esercizio dei diritti e delle libertà riconosciuti dalla Carta stessa, sia pure nel rispetto del loro contenuto essenziale e del principio di proporzionalità. Ed allora, in ordine alla verifica sulla legittimità dell'interferenza, è risultato necessario valutare il rispetto dei parametri posti dal principio di proporzionalità.

Pertanto, le condizioni imprescindibili per ritenere valida la direttiva sono il perseguimento di un obiettivo di interesse generale e la necessità della limitazione all'esercizio dei diritti e delle libertà riconosciuti dall'ordinamento. La conservazione dei dati per permettere alle autorità nazionali competenti di disporre di un eventuale accesso agli stessi è stata ritenuta coerente con le finalità di interesse generale previste dall'art. 52 della Carta. Mentre, dunque, con riguardo al perseguimento di un obiettivo di interesse generale, i giudici hanno rilevato – come si evince dal considerando 7 della direttiva 2006/24 - che i dati relativi all'uso delle comunicazioni elettroniche costituiscono uno strumento valido ed efficace nella lotta e nella prevenzione della criminalità organizzata, la Corte ha invece ritenuto che parecchie circostanze denotano incontrovertibilmente che le norme oggetto di denuncia eccedono i limiti rispetto a quello che appare necessario a garantire la sicurezza.

In particolare, secondo la Corte, sono vaghi i criteri per definire oggettivamente quali siano i crimini da perseguire attraverso la conservazione e il trattamento dei dati; nonché insufficienti le condizioni e le procedure previste per evitare che, attraverso la raccolta di dati si possano innestare abusi.

Ulteriori profili di vulnerabilità della direttiva, la mancanza di un elenco di fattispecie eccezionali escluse dall'obbligo di conservazione; la latitanza di norme idonee a garantire sicure modalità di trattamento dei dati raccolti, e la scelta legislativa di una raccolta di dati di massa, e, per ciò solo, indiscriminata, che, coinvolgendo in maniera indiscriminata tutti i soggetti, è stata ritenuta esorbitante rispetto ai pur legittimi obiettivi di lotta al crimine e al terrorismo.

Allo stesso tempo, però, l'indagine ha verificato che la misura adottata non è stata rispettosa del principio di proporzionalità, che impone di adottare un provvedimento non eccedente quanto è opportuno e necessario per conseguire lo scopo prefissato. Alla luce di tale principio, infatti, nel caso in cui l'azione amministrativa coinvolga plurimi interessi da contemperare, occorre adottare la soluzione che comporti il minor sacrificio possibile; secondo questa prospettiva, il principio di affidamento appare elemento sintomatico della legittimità dell'azione amministrativa e della discrezionalità in relazione all'effettivo bilanciamento degli interessi.[19] Il principio richiamato, di matrice comunitaria, esige che gli atti delle istituzioni dell'Unione europea non travalichino i limiti di quanto è sufficiente e idoneo al raggiungimento dell'obiettivo

[19] Consiglio di Stato, sez. IV, 26 febbraio 2015, n. 964

perseguito[20]. Se da una parte la Corte ha osservato che la lotta contro la criminalità [21]organizzata e il terrorismo è di vitale importanza per la sicurezza pubblica, allo stesso tempo, ha rilevato che un tale obiettivo, per quanto rilevante, non può giustificare che una misura di conservazione, quale quella della direttiva 2006/24, sia da considerare necessaria, dovendo, le deroghe e le limitazioni alla tutela dei dati personali essere contemplate nei limiti dell'indispensabile. La sproporzione della misura adottata dalla direttiva, secondo la Corte, si evince anche dalla circostanza per cui essa si applica anche a persone non sottoposte ad indagini penali, ed in assenza di un giudizio, nonché di qualsiasi indizio da cui trarre un collegamento tra la condotta dell'interessato ed ipotesi di reati gravi.

Questa eccessiva estensione del suo ambito di applicazione, e l'assenza di una relazione tra i dati di cui si prevede la conservazione e una minaccia per la sicurezza pubblica, stride con la necessità, invece, rilevata dalla Corte, di dover delimitare la conservazione dei dati, e l'arco temporale, ad una circoscritta area geografica, nonché ad un numero limitato di persone.

Come sopra accennato, la Corte ha rilevato anche l'assenza di un parametro oggettivo che consenta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fine di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riferimento all'intensità dell'invasione nei diritti fondamentali di cui agli artt. 7 e 8 della Carta, essere reputati sufficientemente gravi da giustificare, e, dunque, legittimare tale ingerenza. In sostanza, la direttiva si limita a rinviare all'art. 1 par. 1, in modo generico ai reati, così come individuati da ogni Stato membro, all'interno del proprio diritto interno.

Difetta la direttiva, secondo la Corte di Giustizia, anche di un criterio idoneo a consentire la limitazione del numero di persone autorizzate ad accedere e ad utilizzare i dati oggetto di controllo e conservazione per quanto strettamente necessario alla luce dell'obiettivo perseguito.

Manca la garanzia della conservazione dei dati all'interno del territorio dell'Unione, e con il rischio di trasferimento degli stessi al di fuori, e conseguente perdita di controllo da parte dei titolari e delle autorità preposte; né è garantita la cancellazione irreversibile dei dati al termine del periodo di conservazione.

In altre parole, e per concludere, mancano nella direttiva 2006/24 norme chiare e precise idonee a limitare ragionevolmente e nel rispetto del principio di proporzionalità, l'invasione nella sfera dei diritti tutelati dagli art. 7 e 8 della Carta.

Viene così ribadito il principio giuridico secondo cui non esistono diritti assoluti; o meglio, la pienezza di ogni diritto non è mai data a prescindere, ma occorre sempre un bilanciamento in concreto tra interessi contrapposti; nel caso di specie, la pubblica sicurezza non prevale sulla protezione dei dati a priori, ma va correttamente bilanciata con gli altri diritti in gioco.

[20] In questo senso vedasi Corte di Giustizia, C-343/09 EU:C:2010:419, punto 45
[21] Corte di Giustizia, C-473/12 EU:C:2013:715, punto 39

La Corte censura la natura indiscriminata della misura di sorveglianza e la possibilità di detta libertà di accesso da parte delle autorità ai dati conservati**,** con una chiara presa di posizione contraria alla sorveglianza di massa[22].

Il principio espresso non afferma una incompatibilità assoluta tra la raccolta e la conservazione dei dati a fini di sicurezza e le norme europee, bensì che debbano essere introdotte regole puntuali e stringenti, compatibili e rispettose del principio di proporzionalità.

2.4 Gli effetti della sentenza sui singoli ordinamenti interni

Il problema che si è posto successivamente alla sentenza attiene agli effetti della pronuncia all'interno degli ordinamenti degli Stati membri, che, in ossequio al diritto europeo, hanno, nel frattempo recepito la direttiva invalidata.

Occorre chiedersi se il provvedimento giudiziario oggetto di trattazione sia per ciò solo idoneo a porre rimedio alle problematiche derivanti dalla adozione della direttiva annullata.

In presenza di normative nazionali ancora in vigore, la problematica, a cascata, coinvolge anche gli operatori del settore: essi, da una parte dovrebbero conservare i dati per non trovarsi in violazione di legge, ma nel contempo tale conservazione attualmente deve considerarsi illegale, e quindi potrebbe sorgere una responsabilità per violazione della privacy (che in alcuni Stati è un reato). In tal senso i fornitori potrebbero anche decidere di cancellare i dati fin da subito.

Nulla quaestio in ordine a quegli Stati che non hanno recepito la direttiva, con la conseguenza che l'annullamento sana, in una certa misura, il mancato recepimento. Il problema, invece, si pone per quei Paesi che non soltanto abbiano recepito la direttiva con un atto interno, ma che non provvedano ad eliminare la norma interna che regola il sistema di conservazione dei dati censurato dalla Corte di Giustizia.

In effetti, l'inefficacia della direttiva non comporta automaticamente la caducazione delle norme in contrasto, anche se potrebbero essere disapplicate da subito dai giudici; ed evidentemente, le legislazioni nazionali vanno modificate solo per quanto riguarda gli aspetti in contrasto col diritto europeo.

Non è mancato chi, al fine di dirimere la questione, facendo leva sull'art. 51 della Carta, ai sensi del quale "Le disposizioni della presente Carta si applicano alle istituzioni e agli organi dell'Unione nel rispetto del principio di sussidiarietà come pure agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione. Pertanto, i suddetti soggetti rispettano i diritti, osservano i principi e ne promuovono l'applicazione secondo le rispettive competenze"*,* ritenga disapplicabile la normativa interna contrastante con la Carta.

In realtà, delle due l'una: o la direttiva è *self executing,* così che, non essendoci bisogno di attuazione, la norma interna adottata dallo Stato membro non può essere considerata attuativa, e non può, quindi, ricadere,

[22] In http://brunosaetta.it/privacy/corte-europea-e-data-retention-no-alla-sorveglianza-digitale-di-massa.html

nell'art. 51 della Carta; ovvero non è *self executing*, ed allora non può essere oggetto di disapplicazione, In tal caso, è il diritto nazionale chiamato a predisporre i necessari rimedi per elidere il contrasto con la Carta fondamentale dei diritti.

La tematica coinvolge anche lo Stato italiano, che ha recepito la direttiva invalidata con l'art. 132 del codice della privacy, che dispone: «Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico, sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. 1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni.3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del giudice su istanza del pubblico ministero o del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-quater del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante».

Il meccanismo da applicare dovrebbe rinvenirsi nella questione di costituzionalità da porre ai sensi dell'art. 117, comma 1, ai sensi del quale "La potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonchè dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali".

In altre parole, la Corte Costituzionale dovrebbe essere adita al fine di dichiarare l'incostituzionalità dell'art. 132 del d.lgs. 196/2003, posto che, alla luce della sentenza della Corte di Giustizia, non sarebbe rispettosa della riserva di giurisdizione introdotta dall'art. 15 comma 3 della Cost., secondo cui la limitazione della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

Residuerebbero, poi, in capo alla norma interna, le critiche mosse alla direttiva oggetto di recepimento, e cioè l'irragionevole sproporzione rispetto al fine perseguito e per la mancata elencazione delle ipotesi in cui è ammissibile una siffatta restrizione della concorrenza.

La strada della declaratoria di incostituzionalità, pur avendo il merito di elidere definitivamente l'incertezza giuridica derivante dagli effetti dell'annullamento della direttiva sulle norme interne che quella direttiva recepivano, sarebbe, peraltro, lunga, determinando una situazione di stallo e di dubbi interpretativi per un arco temporale forse eccessivamente lungo.

La strada della disapplicazione appare, a parere di chi scrive, non soltanto conveniente in termini di efficacia temporale, ma anche giuridicamente corretta, nella misura in cui le norme interne non possono trovare ancora spazio nell'ordinamento giuridico: nel momento in cui le modalità di raccolta e trattamento dei dati con cui sono state concepite, mancano della copertura normativa europea che aveva legittimato una deroga alle garanzie riconosciute dalle direttive precedenti, il giudice ordinario, dovrebbe provvedere a disapplicare l'art. 132 del codice della privacy, senza ulteriori rinvii ad altre istanze in sede giudiziaria.

Peraltro, nemmeno si creerebbe un vuoto normativo, essendosi riespanse le regole di cui alle due direttive precedenti, che dovrebbero poter operare senza il regime derogatorio censurato dalla Corte di Giustizia, che costituisce la parte invalidata della direttiva 2006/58/CE.

La norma ha subito diversi rimaneggiamenti, ma non è mai piaciuta molto al Garante per la protezione dei dati personali, contrario alla raccolta di una così grande quantità di dati da conservare per un periodo così lungo. «Questa sentenza va nella direzione da noi sempre auspicata di una più marcata tutela dei diritti". I dati di traffico non sono informazioni neutre ma rivelano molto di tutti noi, della nostra vita privata. Una indifferenziata conservazione di questi dati per periodi molto lunghi espone quindi a grandi rischi. Con la sua decisione la Corte sottolinea, inoltre, l'esigenza che i dati oggetto di conservazione per ragioni di giustizia restino nel territorio dell'Ue con evidente riferimento alle recenti vicende del Datagate. La sentenza opera un riequilibrio tra due valori, sicurezza e privacy, che in questi anni si erano decisamente disallineati. Occorrerà una revisione dell'attuale sistema nel segno del principio di proporzionalità e delle»[23].

[23]A. Soro, Presidente dell'Autorità garante per la privacy http://www.repubblica.it/tecnologia/2014/04/08/news/corte_giustizia_ue_conservazione_dati-83025720/

CAPITOLO 3

LA CORTE DI GIUSTIZIA E IL DIRITTO ALL'OBLIO

3.1 Il concetto di oblìo anche alla luce della sentenza «Google Spain»

Il diritto all'oblio prevede la non diffondibilità, a meno che non sussistano particolari motivi, di notizie che siano di pregiudizio all'onore di una persona, per tali intendendosi principalmente i precedenti giudiziari di una persona. A meno che non si tratti di casi particolari ricollegabili a fatti di cronaca ed anche in tali casi la pubblicità del fatto deve essere proporzionata all'importanza dell'evento ed al tempo trascorso dall'accaduto.
Nella seconda accezione, l'oblio si correla al periodo di permanenza della notizia on – line.
E' stato rintracciato un ulteriore significato che identifica il diritto all'oblio con il diritto di rettifica e di cancellazione dei dati personali o di opposizione al trattamento degli stessi, secondo quanto previsto dall'art. 12 della direttiva 95/46CE.
Nell'analisi e nell'approfondimento di questa tematica, appare opportuno osservare che la rete reca con sé due elementi dai quali non può prescindersi: la velocità di circolazione dei dati e la loro permanenza. Entrambi generano conseguenze importanti, tenuto conto del fatto che questo modo di informare attraverso supporti che restano integri e resistono al passato, impone di verificare se la persistenza di informazioni riferibili ad un dato soggetto siano compatibili con il loro diritto a vederle "scomparire".
E' la resistenza della tecnologia al passato che ha imposto ai legislatori europei di soppesare il diritto all'informazione con il diritto a non vedersi danneggiati da dati e informazioni pregiudizievoli relativi a condotte pregresse e non più rilevanti per la società.
Non vi è chi abbia correttamente affermato che la privacy non è il diritto all'oblìo, ponendo l'accento, nel bilanciamento con il diritto all'informazione, sulle funzioni pubbliche ricoperte, sul ruolo nella società, e sulla fiducia eventualmente da riporre nelle qualità etico morali di un determinato soggetto.
Le competizioni elettorali sono quelle che forse meglio spiegano il rapporto tra la trasparenza e la totalità delle informazioni e il diritto alla propria identità personale, intesa come dominio della propria sfera privata[24]
L'oblìo è stato oggetto di decisioni in sede giurisdizionale. La Corte di cassazione ha affermato che «il soggetto titolare dei dati personali oggetto di trattamento deve ritenersi titolare del diritto all'oblìo anche in caso di memorizzazione nella rete Internet, mero deposito di archivi dei singoli utenti che accedono alla rete e cioè, titolari dei siti costituenti la fonte dell'informazione. A tale soggetto, invero, deve riconoscersi il relativo controllo a tutela della propria immagine sociale che, anche quando trattasi di notizia vera, e a fortiori se di cronaca, può tradursi nella pretesa alla contestualizzazione e aggiornamento dei dati e, se del

[24] G. De Minico, La Privacy non è il diritto all'oblìo, in Europa, 11 novembre 2010

caso, avuto riguardo alla finalità di conservazione nell'archivio ed all'interesse che la sottende, finanche alla relativa cancellazione».[25]

La giurisprudenza, dunque, con pronunce già risalenti nel tempo, ha riconosciuto il diritto all'oblìo al soggetto a cui i dati si riferiscono, e cioè il divieto alla divulgazione di notizie obsolete, dimenticate o non note alla generalità dei consociati.

La portata dei princìpi enunciati appare tanto generale da ritenersi estendibile ai gestori dei motori di ricerca, titolari del trattamento dei dati raccolti. [26]

La Corte di Giustizia, con la sentenza del 13 maggio 2014 causa C-131/12, si è soffermata sugli obblighi ricadenti in capo a chi gestisce i motori di ricerca, a tutela dei dati personali di coloro i quali non vogliono consentire la indicizzazione e la pubblicazione in modo indefinito delle informazioni che li riguardano.[27]

Alla domanda se esista un conflitto tra due diritti fondamentali quali il diritto all'informazione e quello alla privacy, e specificamente all'oblìo, il Garante alla tutela dei dati personali ha affermato che «La sentenza della Corte di Giustizia ha tentato di individuare un giusto equilibrio tra l'interesse a reperire facilmente informazioni in rete ed il diritto all'oblìo degli utenti. Per tale ragione è stata prevista soltanto la possibilità di ottenere la rimozione di un link che veicola l'informazione ove associato ad un nominativo, von la conseguenza che la notizia continuerà ad essere reperibile ed accessibile utilizzando, ad esempio, altre chiavi di ricerca. La tutela dell'oblìo, lungi dall'essere una questione puramente culturale, impedisce a soggetti privati quali i motori di ricerca, che perseguono interessi puramente economici, di avere il potere di fornire una rappresentazione distorta della personalità e dell'identità degli utenti».[28]

3.2 Il procedimento principale e le questioni pregiudiziali

La fattispecie concreta posta al vaglio del giudice interno era stata innestata da un cittadino spagnolo che, dopo essere stato interessato, nel 1998, da una procedura di riscossione coattiva di crediti previdenziali, a distanza di tanti anni, lamentava la circostanza per la quale, qualunque utente di Internet, digitando nel motore di ricerca del gruppo Google il suo nome, otteneva un link recante le pagine di un quotidiano che ospitava un annuncio, menzionante il suo del ricorrente, per una vendita all'asta di immobili connessa ad un pignoramento effettuato per riscuotere i crediti previdenziali sopra menzionati.

La domanda, rivolta sia nei confronti della testata giornalistica che del gruppo Google Spain e Google Inc, consisteva nella richiesta di sopprimere e modificare le pagine richiamate, affinchè i suoi dati non apparissero più, o, comunque, ricorrere ad adeguati sistemi di protezione, idonei ad occultarli. La motivazione con cui l'interessato avanzava detta pretesa risiedeva nel fatto che il pignoramento era stato

[25] Corte di cassazione sez. III, 5 aprile 2012, n. 5525 in http://www.dirittoegiustizia.it/news/17/0000068206/Il_diritto_all_oblio_su_internet_in_Italia_prescrizioni_del_Garante_per_la_privacy.html

[26] In http://www.dirittoegiustizia.it/news/17/0000068206/Il_diritto_all_oblio_su_internet_in_Italia_prescrizioni_del_Garante_per_la_privacy.html

[27] R. Cosa e L. Viola in http://sicurezzaegiustizia.com/diritto-all-oblio-il-caso-google-spain/

[28] A. Soro Presidente dell'Autorità garante per la privacy http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3619799

definito molti anni prima, così che la sua menzione a distanza di tanto tempo dopo era priva di qualunque rilevanza.

Il ricorso, respinto rispetto alla testata giornalistica – tenuto conto del fatto che la pubblicazione doveva intendersi legittima, in quanto ordinata dal Ministero del Lavoro e dagli Affari sociali – veniva, invece, accolto nella parte in cui era diretto contro Google Spain e Google Inc, ritenendosi l'Agenzia di protezione dei dati autorizzata ad ordinare la rimozione dei dati nonché il divieto di accesso qualora la localizzazione e la loro diffusione ledano il diritto alla protezione dei dati personali e la dignità delle persone.

Avverso la predetta decisione Google Spain e Google Inc. proponevano due ricorsi separati, riuniti dall'Autorità giurisdizionale spagnola in un unico procedimento, poi sospeso, ritenendo di dover sottoporre alla Corte di Giustizia le questioni pregiudiziali rilevate.

Lasciando in disparte le questioni pregiudiziali che concernevano l'ambito territoriale di applicazione della direttiva 95/46/CE e della normativa spagnola sulla protezione dei dati personali, le altre questioni poste all'attenzione della Corte di Giustizia riguardavano specificamente le attività dei motori di ricerca. In particolare, se l'attività di Google Search - quale fornitore di contenuti di localizzazione ed indicizzazione delle informazioni, nonché memorizzazione temporanea, laddove siano presenti dati personali - sia attività rientrante nella nozione di trattamento di dati personali, ed eventualmente se la società di gestione debba essere considerata responsabile del trattamento dei dati personali contenuti nelle pagine web da essa indicizzate.

Residuavano due ulteriori questioni pregiudiziali, subordinate alla risposta affermativa all'ultimo quesito riportato; il giudice interno chiedeva se l'Autorità indipendente, al fine di tutelare i diritti alla riservatezza e all'identità personale, potesse ordinare direttamente a Google Search di rimuovere dai propri indici un'informazione pubblicata da terzi, senza anche doversi rivolgere al titolare della pagina web contenente l'informazione.

L'ultima questione atteneva alla portata del diritto di cancellazione e/o opposizione al trattamento di dati in relazione al diritto all'oblìo, e cioè se il diritto di cancellazione, rettifica e/o opposizione implicasse, per l'interessato, la possibilità di rivolgersi direttamente a chi gestisce il motore di ricerca, facendo valere la propria volontà di non rendere conosciute ai fruitori di Internet informazioni pregiudizievoli, quandanche pubblicate da terzi lecitamente.

3.3 La posizione assunta dalla Corte di Giustizia

Il presupposto normativo da cui partire è la direttiva 95/46/CE, che mira a proteggere le libertà e i diritti fondamentali delle persone fisiche, con particolare riguardo alla vita privata, rispetto al trattamento dei dati personali, provvedendo ad eliminare, al contempo, gli ostacoli alla libera circolazione di tali dati.

Partendo dalla definizione dell'art. 2, lettera d) della direttiva citata che definisce il responsabile del trattamento come «la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento e dei responsabili», la Corte ha affermato la piena riconducibilità del gestore del motore di ricerca alla definizione testè richiamata.

Secondo la Corte, infatti, il trattamento svolto dai motori di ricerca si distingue e si aggiunge a quello effettuato dagli editori di siti web, che consiste nel fare apparire tali dati su una pagina Internet.
La delicatezza della questione della tutela dei dati personali è ancora più pregnante laddove si consideri che, qualora il motore di ricerca sia sollecitato partendo dal nome del soggetto interessato, si rendono accessibili dati anche a quegli utenti che non avrebbero trovato la pagina web su cui i dati sono pubblicati.
Viene sancito così l'obbligo per il gestore del motore di ricerca, in presenza di precise condizioni, di provvedere alla soppressione dei link che rimandano a pagine web contenenti informazioni, anche allorquando la loro pubblicazione sia, di per sé lecita.
Ben può essere, allora, che, anche in presenza di una pubblicazione legittima di quelle informazioni, venga censurata non la pubblicazione in sé, quanto piuttosto la persistenza di quei dati e di quelle informazioni che hanno perso qualsiasi rilevanza.
Questa riflessione deriva anche dall'aver preso atto della facilità di riproduzione delle informazioni contenute in un sito, su altri siti web, con la conseguenza che dover rivolgersi preventivamente o contestualmente a tutti gli editori web per la cancellazione delle informazioni pubblicate cozzerebbe anche con il principio di effettività della tutela.
Occorre anche tener conto, secondo la Corte, che talvolta, gli editori del web, qualora il trattamento dei dati sia effettuato per finalità giornalistiche, possano beneficiare delle deroghe di cui all'art. 9 della direttiva 95/46, con la conseguenza che l'interessato potrebbe esercitare le prerogative a difesa dei propri dati personali, di cui agli artt. 12 lettera b) e 14, comma 1, lettera a) solo nei confronti dei gestori dei motori di ricerca e non anche nei riguardi degli editori.
La sentenza si è soffermata anche sulla disciplina della direttiva nella parte in cui regola il rapporto diretto tra interessato e responsabile del trattamento: l'art. 14 comma 1 lettera a) attribuisce al primo il diritto di opporsi in qualunque momento al trattamento dei dati che lo riguardano, in presenza di «motivi preminenti e legittimi derivanti dalla sua situazione particolare salvo disposizione contraria prevista dalla normativa nazionale», dando luogo ad una dialettica all'interno della quale effettuare la necessaria ponderazione di interessi e la valutazione delle circostanze che connotano la situazione concreta del soggetto interessato.
Secondo l'art. 12 lettera b) e 14 comma 1 lettera a) le domande con cui ci si oppone al trattamento dei dati e si chiede l'oscuramento o la loro cancellazione vanno presentate direttamente al responsabile del trattamento, il quale è chiamato a valutarne la fondatezza ed eventualmente a porre fine allo stesso. Nel caso ciò non avvenga, l'interessato può adire l'Autorità di controllo o l'Autorità giudiziaria.
Secondo la pronuncia in esame, Internet è strumento di informazione e comunicazione ontologicamente differente dalla carta stampata, non potendo soggiacere ai medesimi controlli e regole di quest'ultima, posto che il pregiudizio arrecabile da contenuti inerenti a una persona, tanto più condensati attraverso una ricerca nominativa, è certamente maggiore rispetto a quello cagionato da violazioni della libertà di stampa.
Secondo il ragionamento della Corte di Giustizia, dalle prescrizioni di cui all'art. 6 paragrafo 1, lettere c),d),e), della direttiva 95/46, ben è possibile che un trattamento di dati inizialmente lecito, possa,

progressivamente cozzare con la direttiva, laddove tali dati non siano più necessari in rapporto alle finalità per le quali sono stati trattati; ed uno dei parametri per accertare se ricorra detta situazione è proprio la pertinenza dei dati anche in rapporto al tempo trascorso.

I diritti fondamentali sanciti dagli artt. 7 e 8 della Carta prevalgono tanto sull'interesse economico del gestore del motore di ricerca, quanto sull'interesse degli utenti a reperire l'informazione.

E' evidente, però, che detta valutazione non può che avvenire in concreto, dal momento che l'interesse pubblico di una informazione, nonché la sua attualità e rilevanza possono senz'altro dipendere dal ruolo ricoperto dall'interessato nella vita pubblica, al punto da giustificare l'ingerenza nel suoi diritti fondamentali.

Nella ricerca costante di un giusto equilibrio tra l'interesse degli utenti all'accesso alle informazioni e il rispetto della vita privata e della protezione dei dati personali, la Corte ha sancito, di norma, la prevalenza di questi ultimi, benchè tale equilibrio possa derivare dalla natura dell'informazione, dall'interesse che quella notizia riveste, dal grado di popolarità e dal ruolo che l'interessato ricopre nella vita pubblica.

Alla stessa stregua, non è così tollerabile, allora, che, a distanza di ben sedici anni, nel digitare un nome proprio su un motore di ricerca, si rimandi a pagine web riportanti notizie, la cui pubblicazione, benchè lecita, manca dei requisiti di attualità ed interesse che ne legittimerebbero la persistenza nel mondo digitale, senza peraltro, che sia necessario che l'inclusione dell'informazione arrechi necessariamente un pregiudizio.

Diritto all'oblio, dunque, da intendersi quale diritto a pretendere che i propri dati personali non vengano trovati on line.

Ricapitolando, sono questi i principali punti espressi dalla Corte di Giustizia:

- Il gestore di un motore di ricerca raccoglie dati ai sensi della direttiva 95/46/CE;
- Le operazioni di estrazione, registrazione, organizzazione dei dati - prima della conservazione nei loro server – operazioni contemplate nella direttiva, vanno considerate come trattamento ai sensi della direttiva medesima;
- Sussiste l'obbligo per il gestore del motore di ricerca, in presenza di precise condizioni, di sopprimere dall'elenco dei risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona[29].

Non è mancato chi abbia mosso delle critiche a questa impostazione, chiedendosi se, non sia irragionevole la distinzione tra editore web e motore di ricerca, laddove l'obbligo di rimozione dei link viene imposto solo al gestore del motore di ricerca e non anche all'editore web. Occorre anche chiedersi se sia ragionevole che sia il motore di ricerca, a dover e a poter valutare il bilanciamento che si impone tra il diritto all'oblio e la libertà di informazione[30].

Infatti, la Corte non obbliga il gestore del motore di ricerca a dare seguito alle richieste dell'interessato, consentendogli di valutare autonomamente in ordine alla cancellazione dei risultati contestati.

[29] Comunicato stampa n. 70/14, Lussemburgo, 13 maggio 2014, in www.curiaeuropea.eu

[30] R. Cosa e L. Viola in http://sicurezzaegiustizia.com/diritto-all-oblio-il-caso-google-spain/

L’attribuzione di una siffatta prerogativa, che consente al gestore di essere arbitro all’interno del processo di bilanciamento tra la protezione dei dati personali e il diritto all’informazione ha sollevato perplessità[31].

[31] M. Mensi e P. Falletta in Il diritto del web, Casi e materiali ed. Cedam, Padova, 2015

CAPITOLO 4

LA CORTE DI GIUSTIZIA E IL TRASFERIMENTO DEI DATI DALL'UNIONE AGLI STATI UNITI

4.1 La sentenza Schrems della Corte di Giustizia, Grande Sezione, 6 ottobre 2015, causa 362/14

Nella terza sentenza oggetto della presente trattazione, la Corte di Giustizia ha censurato la decisione 2000/520/CE della Commissione europea, nella parte in cui consente il trasferimento dei dati personali dall'Unione europea agli Stati Uniti, in violazione dei parametri definiti dalla direttiva 95/46/CE.

Si tratta della Decisione della Commissione, del 26 luglio 2000, adottata a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti.

L'art. 25 della direttiva 95/46/CE vieta il trasferimento dei dati personali verso altri Paesi, a meno che lo Stato che li riceve non abbia un adeguato livello di protezione.

4.2 Il procedimento principale e le questioni pregiudiziali

La vicenda ha tratto origine dal contenzioso incardinato da un cittadino austriaco, iscritto alla rete sociale Facebook. In proposito, chi, all'interno dell'Unione europea intenda utilizzare tale rete, deve sottoscrivere un contratto con Facebook Ireland, società controllata di Facebook Inc, situata, quest'ultima negli Stati Uniti, così che i dati personali degli utenti Facebook interni all'Unione vengono trasferiti negli Stati Uniti, su server di Facebook Inc., e lì sono oggetto di trattamento.

Con la sua domanda, il cittadino interessato chiedeva che la predetta Autorità, nell'esercizio delle proprie prerogative, impedisse a Facebook Ireland di trasferire i dati presso i server dell'altra società situata negli Stati Uniti, affermando l'inadeguatezza del sistema di protezione statunitense rispetto alle attività di controllo esercitate dalle autorità pubbliche. L'affermazione della inadeguatezza prospettata era motivata dalle rivelazioni di Edward Snowden relativamente alle attività di intelligence degli Stati Uniti, messe in atto dalla National Security Agency (NSA).

La denuncia veniva respinta sul presupposto che tutte le questioni sulla adeguatezza della protezione dei dati personali negli Stati Uniti erano già stati oggetto di decisione da parte della Commissione europea; in particolare, la decisione 2000/520 aveva affermato un adeguato livello di protezione dei dati personali da parte degli Stati Uniti.

La decisione era oggetto di ricorso da parte dell'interessato, che adiva la Corte di appello, la quale, pur riconoscendo nella sorveglianza elettronica e nelle intercettazioni dei dati, una attività indispensabile per la tutela dell'interesse pubblico, rilevava eccessi considerevoli messi in atto dalla NSA proprio in relazione alle rivelazioni del sig. Snowden.

La Corte d'appello, movendo dal presupposto che la tutela della vita privata e l'inviolabilità del domicilio, garantiti dalla Costituzione irlandese, possano essere oggetto di ingerenza laddove quest'ultima sia

proporzionata e conforme ai requisiti previsti dalla legge, ha constatato come l'accesso massiccio e indifferenziato, effettuato, peraltro, su larga scala da parte della NSA, pongano seri dubbi sul rispetto dell'adeguato livello di protezione previsto tanto dal diritto interno, quanto dall'art. 25 della direttiva 95/46/CE.

Di qui la sospensione del processo per sottoporre alla Corte di Giustizia le questioni pregiudiziali da esaminare

In particolare, la questione era volta a verificare se l'Autorità indipendente - preposta alla tutela dei dati personali e competente a decidere sul merito di una denuncia presentata con cui si sosteneva che il diritto e la prassi di un Paese terzo presso il quale venivano trasferiti i dati personali (nel caso di specie gli Stati Uniti d'America) non prevedano adeguate tutele per i soggetti interessati - fosse assolutamente vincolata dalla constatazione in senso contrario dell'Unione contenuta nella decisione 2000/520, ovvero conservasse la propria prerogativa di condurre un propria indagine sulla questione alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520.

In altre parole, con la prima questione la Corte veniva chiamata a decidere se le prerogative di un' autorità indipendente, garante delle protezione dei dati personali, chiamata a decidere su una denuncia presentata in ordine alle modalità di conservazione e gestione dei dati, fossero implicitamente limitate dal rispetto della decisione della Commissione contenente la avvenuta constatazione di un adeguato livello di protezione garantito.

La seconda, invece poneva la questione se tale autorità avesse un autonomo potere di indagine, anche alla luce degli accadimenti successivi alla pubblicazione della decisione.

4.3 La natura delle decisioni della Commissione

Prima ancora di comprendere il significato e la portata della sentenza della Corte di Giustizia, appare utile soffermarsi sulla natura delle decisioni della Commissione, dal momento che l'oggetto della pronuncia concerne la validità o meno della decisione 2000/520/CE.

L'art. 288 TFUE afferma che «La decisione è obbligatoria in tutti i suoi elementi. Se designa i destinatari è obbligatoria soltanto nei confronti di questi».

La definizione riportata incide sulla tradizionali impostazione secondo cui si connotava quale atto sostanzialmente amministrativo, essendo indirizzato a destinatari determinati.

La disposizione, così come articolata, concepisce due forme di decisioni: una, indirizzata a destinatari ben determinati e coincidente alla precedente formulazione del previgente art. 249 TCE; la seconda, invece, di tipo indeterminato.

Questa duplice modalità di concepire e configurare le decisioni , incide sul loro contenuto, posto che l'art. 297 TFUE solo le decisioni che non designano i destinatari sono elevati a rango di atti legislativi; non anche quelle coi destinatari. Soltanto per i primi è prevista la pubblicazione sulla Gazzetta ufficiale europea, mentre le altre direttive e le decisioni che designano i destinatari sono notificate ai destinatari e hanno efficacia in virtù di tale notificazione.

Gli atti legislativi adottati secondo una procedura legislativa speciale sono firmati dal presidente dell'istituzione che li ha adottati.

Gli atti legislativi sono pubblicati nella Gazzetta ufficiale dell'Unione europea, ed entrano in vigore alla data da essi stabilita oppure, in mancanza di data, il ventesimo giorno successivo alla pubblicazione.

In ordine alla doppia natura delle decisioni, la decisione individuale costituisce l'atto giuridico tipico con cui le istituzioni dell'Unione europea regolano in modo vincolante le singole fattispecie, e si distingue per le seguenti caratteristiche: ha validità individuale, differenziandosi dal regolamento; è vincolante in tutti i suoi elementi, differenziandosi dalla direttiva; vincola direttamente i suoi destinatari. Una decisione destinata ad uno stato membro può, inoltre, nelle stesse condizioni di una direttiva, avere un effetto sui cittadini dell'Unione europea.[32]

La Corte di giustizia ha chiarito che: «Una decisione della Commissione [...] non è vincolante per soggetti diversi dalla persona o dalle persone che essa designa come destinatari».[33]

4.4 La posizione assunta dalla Corte di Giustizia

La Corte di Giustizia, nell'affrontare congiuntamente le questioni pregiudiziali, ha affermato che le disposizioni della direttiva 95/46 vanno interpretate alla luce dei diritti fondamentali garantiti dalla Carta.[34]

La Corte ha richiamato suoi precedenti nei quali si sofferma sull'importanza del diritto fondamentale al rispetto della vita privata di cui all'art. 7 e alla tutela dei dati personali di cui all'art. 8.[35]

Partendo dal presupposto che il trasferimento dei dati costituisce un trattamento dei dati personali, ai sensi dell'articolo 2, lettera b) della direttiva 95/46 effettuato nel territorio del Stato membro, configurandosi tale «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali", ciascuna autorità nazionale di controllo deve sorvegliare, ai sensi dell'art. 8, par. 3 della Carta e dell'art. 28 della direttiva 95/46, che vengano rispettate le norme dell'Unione sulla tutela delle persone fisiche.»

I soggetti deputati alla tutela della privacy hanno un potere di controllo e di sospensione del trasferimento dei dati nelle ipotesi in cui ritengano probabile la violazione dei princìpi che la loro attività mira a presidiare.

Nel dichiarare invalida la decisione 2000/520 della Commissione, la Corte di Giustizia ha affermato che l'art. 25 paragrafo 6 della direttiva 95/46/CE, letto in coerenza con gli artt. 7, 8 e 47 della Carta CEDU, vada interpretato nel senso che una decisione della Commissione, quale quella citata, con cui si è constatato un adeguato livello di protezione dei dati personali di un paese terzo, non impedisce che una autorità di controllo della privacy di uno Stato membro, possa esaminare la domanda di una persona in ordine all'accertamento di un adeguato livello di protezione da garantire durante il trattamento.

La Corte di Giustizia, nel riconoscere il potere della Commissione di adottare, sulla base dell'art. 25, paragrafo 6, della direttiva 95/46 una decisione con cui si constata che un paese terzo garantisce un adeguato

[32] L. Delpino, F. del Giudice, in Manuale di diritto amministrativo, Simone ed., 2015.

[33] Corte di Giustizia, Sentenza del 14 aprile 2011, causa C-327/09, Mensch und Natur AG)

[34] Corte di Giustizia, Google Spain e Google, C-131/12 EU :C:2014:317

[35] Corte di Giustizia, Google Spain e Google, C-131/12 EU :C:2014:317 punti 53,66, 74

livello di protezione, afferma che, essendo gli atti delle istituzioni europee, vincolanti per gli Stati membri, essa ha efficacia obbligatoria. In proposito, secondo l'art. 288 TFUE, le decisioni della Commissione hanno carattere vincolante per gli Stati membri destinatari. Ne consegue che, fino a quando la decisione non venga annullata dalla Corte, gli Stati membri e gli organi di controllo indipendenti non possono adottare misure contrarie a tale decisione.

Allo stesso tempo, ha rilevato la Corte, che non è pensabile che una siffatta decisione possa inibire i poteri riconosciuti alle autorità nazionali di controllo di fronte a fattispecie da valutare proprio ai sensi della direttiva 95/46.

Pertanto, rispetto alle questioni sollevate, la Corte di Giustizia ha risposto affermando che l'art. 25, paragrafo 6, alla luce degli artt. 7, 8, e 47 della Carta, vada inteso nel senso che una decisione adottata, quale la 2000/520, con cui la Commissione abbia constatato che un paese terzo garantisce un adeguato livello di protezione, non impedisce che la domanda di una persona volta ad accertare la adeguatezza del livello di protezione dei dati possa essere esaminata dall'autorità nazionale preposta a siffatto controllo.

Nel constatare che la direttiva non fornisce il concetto di «livello di protezione adeguato», è l'ordinamento giuridico del paese terzo interessato dalla decisione della Commissione che deve garantire siffatto livello, nel senso di saper assicurare, in considerazione della sua legislazione, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente analogo a quello garantito dall'Unione in forza della direttiva.

Pertanto, secondo la Corte, l'eventuale evoluzione del concetto di livello di protezione incombe alla Commissione, dopo aver assunto una decisione in forza dell'art. 25, paragrafo 6 della direttiva 95/46, verificare periodicamente se la situazione di fatto continui nel tempo ad essere compatibile con i princìpi da rispettare.

In sede di esame della validità di una decisione della Commissione, quale quella che ci occupa, vanno valutate anche le circostanze successive alla sua adozione, che potrebbero averne determinato l'inattualità o l'inadeguatezza rispetto al bene oggetto di tutela.

Per comprendere i passaggi logici ed argomentativi della Corte rispetto all'atto della Commissione 2000/520, appare utile soffermarsi su alcuni considerando: la Corte, nel considerando 94, afferma che «…si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata. Come garantito dall'articolo 7 della Carta (V., in tal senso, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 39».

Una normativa dell'Unione che ingeneri una invasione nei diritti fondamentali di cui agli artt. 7 e 8 della Carta deve prevedere regole chiare e precise che volte a normare le modalità e i limiti di applicazione della misura, nonché prevedano requisiti minimali da garantire agli interessati di tutelare in maniera efficace i loro dati difendendoli da abusi, accessi o usi illeciti.[36]

[36] Corte di Giustizia, Grande Sezione, 6 ottobre 2015, causa 362/14, considerando 91

Presupposto per una tutela giurisdizionale piena ed effettiva sancita dall'art. 47 della Carte europea dei diritti, è l'esistenza, all'interno della normativa, di strumenti giuridici di cui l'interessato possa avvalersi al fine di accedere a dati personali che lo riguardano, ovvero attraverso il diritto di ottenere la loro rettifica o distruzione.

In questo senso, la Corte ha assunto un atteggiamento a baluardo della privacy, aderendo ai fautori della difesa di questo diritto fondamentale[37] La Corte di Giustizia ha poi censurato l'art. 3, paragrafo 1, comma primo, della decisione 2000/520 nella misura in cui priva le Autorità nazionali di controllo, dei poteri ad esse riconosciuti dall'art. 28 della direttiva 95/46.

Deve ritenersi consentito, infatti, che qualora qualcuno adduca elementi idonei a far dubitare che uno Stato terzo garantisca un adeguato livello di protezione dei dati personali, quantunque questa circostanza sia stata constatata e riconosciuta da una precedente decisione della Commissione.

Alla luce dei considerando 102,103 e 104, infatti, la Corte ha negato che l'art. 25 paragrafo 6 della direttiva 95/46 attribuiscano alla Commissione il potere di limitare le prerogative delle autorità nazionali di controllo. Di tal chè appare evidente come la decisione abbia ecceduto la competenza attribuitale dall'articolo della direttiva sopra richiamato.

Non è mancato chi abbia sollevato delle perplessità sul contenuto della pronuncia, che, peraltro, sembra riaffermare la necessità di autonomia potestativa da ripartirsi tra gli Stati membri[38].

Secondo parte della dottrina, la Corte sarebbe andata oltre quanto richiesto da parte del giudice remittente, e cioè se le autorità preposte al controllo della tutela dei dati personali siano rigidamente vincolate ai termini dell'accordo o se possano decidere su eventuali violazioni in situazioni specifiche, riformulando, così la questione pregiudiziale al fine di esaminare la validità della decisione.[39]

L'accordo è il Safe Harbour, sottoscritto nel 2000 tra l'Unione europea e gli Stati Uniti d'America in ordine al libero trasferimento, a fini commerciali, dei dati di cittadini europei verso gli Stati Uniti da parte delle multinazionali UE. Tale accordo regola le modalità attraverso cui le società statunitensi possono esportare e gestire dati personali di cittadini europei.[40]

L'accordo prevede il rispetto di sette princìpi: 1) gli utenti vanno avvisati in ordine alla raccolta e all'utilizzo dei dati; 2) ognuno può rifiutare la raccolta dei dati e il loro trasferimento a terzi; 3) il trasferimento dei dati può avvenire solo a soggetti che rispettano princìpi adeguati di protezione; 4) le aziende devono fornire garanzie contro il rischio di smarrimento dei dati; 5) vanno raccolti solo i dati inerenti ai fini della rilevazione; 6) gli utenti hanno il diritto di accedere ai dati raccolti, nonché di correggerli e/o cancellarli se inesatti; 7) le suddette regole vanno attuate efficacemente. L'impresa che abbia aderito al programma, deve rinnovare la certificazione ogni dodici mesi.

---

[37] S. Rodotà, Internet e privacy, c'è un giudice in Europa che frena gli USA, in www.repubblica.it, 12 ottobre 2015

[38] In http://www.dimt.it/2015/12/02/il-caso-schrems-facebook-analisi-e-profili-di-collegamento-con-la-sentenza-google-spain/

[39] P. Falletta, La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande Sezione), 6 ottobre 2015, Schrems c Data Protection Commissioner, C-362/14), in www.federalismi.it

[40] EUR-Lex - 32000D0520 - EN, eur-lex.europa.eu.

Secondo alcuni autori, quanto alla paventata mancanza di misure di protezione che la Commissione avrebbe dovuto verificare nell'ambito del Safe Harbour, che dette misure di protezione sembrano comunque contemplate nell'ambito dei Safe Harbour Principles, e specificamente nella allegata FAQ 11, ove compaiono i meccanismi di ricorso a tutela dei consumatori, le riparazioni e le sanzioni, il ruolo di controllo e di risoluzione delle controversie affidato alla Federal Trade Commission.[41]

Né si comprende la reale utilità di aver invalidato la decisione della Commissione, una volta riconosciuto comunque, il potere – successivo alla stessa – delle autorità nazionali di controllo di vigilare sul trasferimento dei dati in caso di abusi anche solo potenziali.

Anche il Garante italiano per la protezione dei dati personali aveva preso atto dell'intesa tra Unione europea e USA autorizzando il trasferimento dei dati personali presso i server degli Stati Uniti, ma riservandosi di effettuare i controlli sui trasferimenti di dati e il loro trattamento, anche adottando, nell'eventualità, il blocco o il divieto di trattamento.

La sentenza della Corte ha, di fatto, dichiarato invalido l'accordo, imponendo, nuovamente, al Garante, di pronunciarsi di nuovo alla luce della pronuncia[42]

Vi è chi ha auspicato, anche alla luce della sentenza, una riforma ed un aggiornamento della normativa, utile anche per gli operatori del settore, dovendo attendersi novità soprattutto per quanto concerne la sorveglianza di massa.

Da rilevarsi, quale importante novità, la proposta del progetto di regolamento per la protezione dei dati personali all'attenzione delle istituzioni europee, contenente una sintesi di princìpi di difficile attuazione, ma utile ad attribuire affidabilità e fiducia alla normativa di settore.[43]

Alla forza propulsiva delle pronunce della Corte di Giustizia, hanno fatto seguito, il regolamento europeo in materia di protezione dei dati personali e la direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini, e la direttiva UE 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

[41] P. Falletta, La Corte di Giustizia, ancora una volta, conto le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande Sezione), 6 ottobre 2015, Schrems c Data Protection Commissioner, C-362/14), in www.federalismi.it

[42] Protezione dei dati personali: che cos'è il safe harbour in http://www.ilsole24ore.com/art/mondo/2015-10-06/protezione-dati-che-cos-e-safe-harbor-115055.shtml?uuid=ACeTQwAB

[43] In http://www.dimt.it/2015/12/02/il-caso-schrems-facebook-analisi-e-profili-di-collegamento-con-la-sentenza-google-spain/

CONCLUSIONI

Il lavoro, dopo essersi soffermato sul concetto di privacy, e sul rapporto che intercorre tra le potenzialità di Internet e la tutela dei dati personali, all'interno di un processo di liberalizzazione delle telecomunicazioni, ha affrontato il concetto di privacy nella sua accezione generica e nel diritto comune, ponendo in risalto le difficoltà di bilanciare la libera circolazione delle informazioni e la libertà di informazione e la tutela del diritto alla privacy.

Gli argomenti trattati, appaiono, infatti, fondamentali per affrontare e commentare le più significative pronunce della Corte di Giustizia che in questo ultimo periodo hanno caratterizzato e condizionato le prerogative e le potenzialità di Internet rispetto alla tutela dei dati personali.

La sentenza Schrems, nel dichiarare invalida la decisione del 26 luglio 2000 della Commissione europea, ha riconosciuto la piena indipendenza e autonomia delle autorità nazionali di controllo interne ad uno Stato, di decidere, in forza della direttiva 95/46/CE - relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati – se il trasferimento dei dati degli iscritti europei a facebook verso gli Stati Uniti possa essere bloccato laddove accerti che quel paese non offre un adeguato livello di protezione dei dati personali.

Prima ancora, con la sentenza nota come «Data Retention» ha dichiarato l'invalidità della direttiva 2006/24/CE sulla conservazione dei dati personali di traffico telefonico e telematico.

La sentenza «Google Spain contro AEPD» appare in linea con l'impostazione che, nell'ambito della tutela sovranazionale dei diritti fondamentali, riconosce l'esistenza nell'ordinamento comunitario del diritto all'oblio, che prevede la non diffondibilità, a meno che non sussistano particolari motivi, di notizie che siano di pregiudizio all'onore di una persona, per tali intendendosi principalmente i precedenti giudiziari di una persona; a meno che non si tratti di casi particolari ricollegabili a fatti di cronaca ed anche in tali casi la pubblicità del fatto deve essere proporzionata all'importanza dell'evento ed al tempo trascorso dall'accaduto. Bilanciamento è tra la privacy intesa come rispetto vita privata e diritto all'informazione.

Elemento comune alle pronunce è senz'altro la valorizzazione della Carta dei diritti fondamentali dell'Unione europea. L'art. 52 della Carta recita: "Ogni eventuale limitazione ai diritti fondamentali garantiti deve essere prevista dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

A distanza di anni rispetto all'epoca in cui il legislatore ha legiferato – chiaramente in relazione ai bisogni che si impongono in un determinato contesto sociale, quale quello degli attacchi terroristici di Londra e di Madrid – contesto che imponeva la necessità di adottare misure efficaci in materia di conservazione dei dati relativi alle comunicazioni, l'accertamento di attività segrete di monitoraggio delle comunicazioni private poste dalla National Security Agency, ha indotto la Corte di Giustizia ad avere un approccio differente

rispetto a quello avuto dal legislatore europeo fino a quel momento, mutando il bilanciamento tra il rispetto della privacy e delle libertà fondamentali e la sicurezza nazionale.

Va indubbiamente riconosciuto alle pronunce della Corte di Giustizia un ruolo anticipatorio all'interno di ambiti, quale quello di una efficace tutela dei dati personali e dei diritti fondamentali, in cui pare emergere un vuoto normativo, con evidenti responsabilità politiche, troppe volte colmato a livello giurisdizionale.

In questa prospettiva, allora, vanno letti i contenuti delle pronunce oggetto di commento, quali linee guida da prendere in considerazione, da parte del legislatore europeo in ordine alla predisposizione della futura riforma della direttiva sulla data retention. In primis, la necessità di un contenimento del periodo di conservazione (massimo sei mesi) e una chiara modalità di accesso ai dati di traffico da parte delle Autorità nazionali, conformi a requisiti di tracciabilità e di sicurezza.

Per garantire il rispetto di tali diritti fondamentali, la Commissione ha ritenuto necessario un intervento significativo sugli aspetti critici ed ha proposto di:

- restringere e armonizzare le finalità della data retention e le tipologie di reati in forza dei quali si può accedere e utilizzare i dati di traffico;

-assicurare una maggiore uniformità a livello europeo dei periodi di conservazione dei dati;

-limitare il numero dei soggetti autorizzati ad accedere a tali dati e ridurre le categorie di dati da conservare;

-supervisionare, attraverso un'autorità indipendente, le modalità di accesso ai dati applicate nei vari Stati membri;

-prevedere delle linee guida sulle misure tecniche e organizzative per l'accesso ai dati e l'utilizzo di tali dati.

Il 14 aprile 2016 il Parlamento europeo ha approvato definitivamente il Regolamento sulla protezione dei dati, sostitutivo della direttiva 95/46/CE e delle rispettive normative nazionali di recepimento[44].

Il 4 maggio 2016, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) il regolamento europeo in materia di protezione dei dati personali e la direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini, direttiva entrata in vigore 5 maggio 2016, da recepire, da parte degli Stati membri entro 2 anni.

Si tratta della direttiva UE 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

[44] Il pacchetto di riforma si compone di una Comunicazione della Commissione europea "Salvaguardare la privacy in un mondo interconnesso". Un quadro europeo della protezione dei dati per il XXI secolo, COM(2012) final; una Proposta di regolamento del Parlamento e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012)11 e infine una proposta di Direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di protezione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati, COM(2012)10.

Il 24 maggio 2016 è entrato ufficialmente in vigore il Regolamento sopra citato, n.2016/679, che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, e che, tra le novità principali:

-riconosce il «diritto all'oblio», ovvero la possibilità per l'interessato di decidere che siano cancellati e non sottoposti ulteriormente a trattamento i propri dati personali non più necessari per le finalità per le quali sono stati raccolti, nel caso di revoca del consenso o quando si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento;

-stabilisce il diritto alla "portabilità dei dati", in virtù del quale l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti, qualora l'interessato abbia fornito il proprio consenso al trattamento o se questo sia necessario per l'esecuzione di un contratto;

- sancisce il principio di *«accountability*», per cui il titolare dovrà dimostrare l'adozione di politiche privacy e misure adeguate in conformità al Regolamento;

- introduce il principio della «*privacy by design*» (che necessita di adeguate misure tecniche e organizzative sia nella fase della progettazione che della esecuzione del trattamento) e della «*privacy by default*» (che richiama il principio di necessità, disponendo che i dati siano trattati solamente per le finalità previste e per il periodo strettamente necessario a tali fini)[45].

Quanto alla trasmissibilità dei dati, nell'ambito dei rapporti con Stati terzi, il l2 febbraio 2016 è stato raggiunto un primo accordo politico e il 29 febbraio è stata data comunicata la presentazione dei testi giuridici dell'Usa-UE *Privacy Shield* da parte della Commissione europea[46].

[45] G. Scafati, S. Perelli Studio Legale – member of Brandi Partners in http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-05-16/la-privacy-europea-regolamento-ue-2016679-125453.php

[46] Il testo della Draft adequacy decision è consultabile in: http://europa.eu/rapid/press-release_IP-16-433_it.htm. (sito della Commissione)

BIBLIOGRAFIA

1. A. Westin, Privacy and freedom, The Bodley Head Ltd, 1970
2. M. Mensi e P. Falletta, Il Diritto del Web, Casi e materiali, ed. Cedam, Padova, 2015
3. O. Prevosti, 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, settembre 2014.
4. G. De Minico, La Privacy non è il diritto all'oblìo, in Europa, 11 novembre 2010
5. L. Delpino, F. del Giudice, in Manuale di diritto amministrativo, Simone ed., 2015

SITOGRAFIA

1. www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1663787

2. S. D. Warren e L. Brandeis The right to privacy, in http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

3. http://brunosaetta.it/privacy/privacy-o-diritto-alla-riservatezza-e-protezione-dei-dati-personali.html
4. http://brunosaetta.it/privacy/corte-europea-e-data-retention-no-alla-sorveglianza-digitale-di-massa.html
5. http://www.repubblica.it/tecnologia/2014/04/08/news/corte_giustizia_ue_conservazione_dati-83025720/
6. http://www.dirittoegiustizia.it/news/17/0000068206/Il_diritto_all_oblio_su_internet_in_Italia_prescrizioni_del_Garante_per_la_privacy.html
7. R. Cosa e L. Viola in http://sicurezzaegiustizia.com/diritto-all-oblio-il-caso-google-spain/
8. Comunicato stampa n. 70/14, Lussemburgo, 13 maggio 2014, in www.curiaeuropea.eu
9. S. Rodotà, Internet e privacy, c'è un giudice in Europa che frena gli USA, in www.repubblica.it, 12 ottobre 2015
10. http://www.dimt.it/2015/12/02/il-caso-schrems-facebook-analisi-e-profili-di-collegamento-con-la-sentenza-google-spain/
11. P. Falletta, La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande Sezione), 6 ottobre 2015, Schrems c Data Protection Commissioner, C-362/14), in www.federalismi.it
12. EUR-Lex - 32000D0520 - EN, eur-lex.europa.eu.
13. Protezione dei dati personali: che cos'è il safe harbour in http://www.ilsole24ore.com/art/mondo/2015-10-06/protezione-dati-che-cos-e-safe-harbor-115055.shtml?uuid=ACeTQwAB
14. http://www.dimt.it/2015/12/02/il-caso-schrems-facebook-analisi-e-profili-di-collegamento-con-la-sentenza-google-spain/
15. G. Scafati, S. Perelli Studio Legale – member of Brandi Partners in http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-05-16/la-privacy-europea-regolamento-ue-2016679-125453.php

ABSTRACT

The jurisprudence of the European Union Court on privacy: a front still open on the web giants

This paper examined the idea of privacy in its generic meaning and in the common legal framework by both emphasizing the difficulties in balancing both the free movement and freedom of information and protection of privacy rights. The aim of this paper is to show how the Internet realm has made necessary to attune legal interests and rights to safeguard, a harmonization not always easy to achieve.

Beside the undisputable difficulty to make this harmonization work, the multiple developments due to the political and social changes of our time must be acknowledged. Moreover, these changes force legislators to act differently, according to the incoming requirements.

After describing the idea of privacy in its generic meaning, retracing the evolution of the term in light of Warren and Brandeis statements, it was also analyzed in relation to its legal sphere: on one side the free movement of information and the freedom of information, facilitated by the huge prerogative of the Internet, as means of news and data potentially unlimited, on the other side the protection of privacy rights.

In 1890 Warren and Brandeis, two lawyers in Boston, foresaw the idea of privacy by shaping its legal coordinates. At the time, pictures of them attending private parties were publicly displayed on the local gossip newspapers. In order to safeguard their image, Warren and Brandeis wrote, in 1890, the famous paper, called "Privacy, right to be alone". In the pages of the "Harvard Law Review" they dealt with this concept as the universal right to be left alone: "*Later, there came a recognition of man's spiritual nature, of his feelings and his intellect...and now the right to life has come to mean the right to enjoy life-the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession-intangible, as well as tangible*"

This passage in particular highlights the most important principle, the right to be left alone. The most important value, requiring the creation of a system of protection and safeguard is strictly correlated to the own existence of the individual, which not only constitute damage to his or her won reputation but mainly an intrusion to someone's own privacy. Warren and Brandeis turned a legal right, already internalized in the judicial system, into a moral standard by also assigning an ethical profile to it. The definition initially succeeded, even though in almost fifty years of study its scope has been constantly extended and restricted. The terrorist attacks led legislators to adopt a normative, in a sense derogatory, with respect to the way of collection, procession and transfer of data. Obsolete legislations, established with the goal preserving national security, were updated by setting a system in which the man and its individuality became the focus of the new legal framework.

In no way the individual dimension and the heritage of data that distinguish someone can be sacrificed in name of a more general and indiscriminate control of data and information on behalf of a system of mass

surveillance, which is quite unacceptable. The European Court of Justice directly intervened, with three sentences not too remote from each other, and oriented the European legislator towards a strenuous defense of the right to privacy and guaranteed that the processing of personal data ought to be safeguarded through adequate forms of protection. Hence the debate over the idea of privacy, renewed by the decisions of the European Court of Justice and fostered by the complaints of Member States to censor the modalities of collection and procession of data, raised questions over the adequateness of the normative instruments and forced the European legislator to speak out loud, filling the void created by the declaratory of invalidity of the Directive 2006/24/CE.

The common element to all these sentences was the valorization of the EU Charter of Fundamental Rights. Article 52 of the abovementioned Charter states: "*Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others*"

The Schrems case, invalidating the 26 of July 2000 decision of the European Commission, recognized the full independence and autonomy of national authorities of internal control of a Member State to decide, thanks to Directive 95/46/CE – subject to the safeguard of the processing of personal data, and the free movement of such data – if the transfer of data of members of Facebook to the United States can be blocked wherever the country of destination would not guarantee an adequate level of protection of personal data.

The sentence known as "Data Retention" invalidated Directive 2006/24/CE, which concerned the preservation of personal data and management of phone and telematics records.

The "Google Spain v. AEPD" case aligns well with the introduction in the legislation, by safeguarding supranational fundamental rights, of the right to be forgotten. This right presupposes the non-disclosure of records, intending legal precedents, prejudicing the honor of an individual. This is always applied unless for exceptional cases related to newsworthy crimes; even in such cases the disclosure must be directly proportionate to the relevance of the event and to the time spent from the deed. Balance must be found between privacy perceived as respect for one's private life and right to inform.

The point of arrival for the European legislator is 2016/679 Regulation, inspired by the principles expressed by the ECJ receiving complaints from some Member States legislators, who pushed for a better set of policies regulating privacy and an equilibrium in the processing of personal data.

Stefano Rodotà is one of Italy's most prominent jurists and wrote the "Declaration of the Internet Rights", proposed by the European Commission in order to preserve rights and duties of the Internet and presented at November 2015 Internet Governance Forum in Brazil. This Declaration, although not legally binding, was meant to address the regularization of the rights of the Internet for Italian and European Institutions. Rodotà believed the reluctance of the public administration to regulate these mechanisms is mainly due to the fear of empowering the citizen too much. "*In the past, whoever referred to the public administration or to a private*

company and asked "Do you have data on me" would receive as an answer "We are not obliged to respond" and, in many cases it was legitimate to answer in that way. However, everyone now must be held accountable for and declare the information they possess on every individual and the use they are going to make of it. In this sense, the situation has therefore completely reversed".

Therefore, before the "Declaration of the Internet Rights", the owner of the data had absolute power to disclose or make use of the data of the individual, whereas now this power belongs to citizen too. Naturally, this leads to issues concerning the practical way the citizen is able to obtain his or her own data. The purpose of the regularization of these mechanisms was to have the citizen comprehend that any law on privacy is not a limitation, but rather an enlargement of his or her own freedom and power.

According to Rodotà, although the Internet is often perceived as a lawless place, evidence shows the contrary. "*We have plenty of regulations limiting true individual freedom. It is necessary to rebalance these rights. We must guarantee freedom rights, equality and dignity necessary to ensure the democratic functioning of the institutions and to avoid that mass surveillance, control and social selection will jeopardize public and private rights. The Internet turns into an increasingly important place for the organization of individuals and groups and remains an essential tool to promote individual and collective participation to stimulate democracy and equality. The principles regulating the Internet are also strongly affected by the economic developments that lead to innovation, fair competition and growth in a democratic context. A Declaration of the Internet Rights is an indispensible tool to set the constitutional foundations for supranational principles and rights*"

Years apart from the first legislation – up to date with the new social contexts and after the terrorist attacks in London and Madrid – requiring the adoption of efficient measures safeguarding data related to communications, the verification of secret activity of monitoring of the National Security Agency private communications forced the European Court of Justice to have a new, different approach involving a better balance between the respect for privacy and fundamental freedoms and national security.

The European Court of Justice sentences managed to foresee normative gaps, in areas such as the effectiveness over the safeguard of personal data and fundamental rights, remain unfilled by political and domestic interest of Member States' judicial systems.

The sentences containing the updated guidelines represented a starting point for the European legislator for future reform of the Directive on Data Retention. At first, the necessity of a restriction of the period of preservation (maximum six months) and a clear access for the traffic of data from national authorities, in compliance with security and traceability requisites.

In order to guarantee the observance of such fundamental rights, the European Commission deemed necessary to directly intervene with the critical aspects and proposed to:

- Restrict and harmonize the aims of Data Retention and the types of crime that lead to the access and utilization of data

- Ensure a greater European uniformity regarding the preservation of data

- Limit the number of members authorized to access such data and reduce the categories of preservation of data

- Supervise, through an independent authority, the modalities of access to data applied to different Member States

- Constitute technical and organizational guidelines in order to access and utilize data

On April 14, 2016 the European Parliament ultimately approved the Regulation on the protection of data, substituting Directive 95/46/CE and respective national normative of implementation.
On May 4, 2016 both the European Regulation on protection of personal data and the Directive regulating the treatment of personal data in the sectors of prevention, contrast and repression of crimes were published on the Official Journal of the European Union (OJ); the latter entered into force on May 5, 2016 and requiring all Member States to comply within two years.
EU Directive 2016/680 of the European Parliament and European Council, of April 27, 2016 related to the protection of people from the treatment of personal data from authorities to prevent, investigate, inspect and prosecute crimes or enforce criminal penalties, accompanied by a free circulation of such data.
Regulation 2016/679 officially came into force on May 24, 2016 and will become applicable directly in all EU Member States starting on May 25, 2018. Among the main amendments, this Regulation will:

- Recognize the “Right to be forgotten”, namely giving every citizen the possibility to decide to cancel or not process his or her own personal data. This right is applied in the occurrence that these data would be used for an objective that differs from the original one, in the occurrence of the suspension of the consent or when a citizen is opposed to the treatment of personal data and when the said treatment is not in compliance with the Regulation.

- Establish the right to the “Portability of data”, allowing every citizen to receive in a structured, public format (readable from every device) his or her own personal data. These data given to an appointed specialist of the treatment of data can be transmitted to another specialist with the permission of the

individual without impediments and with the consent of the individual for the signing of a new contract.

- Establish the principle of "accountability", forcing the owner of the data to provide the adoption of adequate policies and measures in the treatment of data and in compliance with the Regulation

- Introduce the principle of "privacy by design" (necessitating the implementation of technical and organizational measures in the processing and disclosure of data) and the "privacy by default" (recalling the principle of necessity by imposing that the data must be treated for the scope and length initially established)

On February 12, 2016 an agreement was signed concerning the transmission of data with non Member States and on February 29 the European Commission presented the USA-EU Privacy Shield regulation.

The sentences in this paper initiate a series of provision that enlarged and reinforced the idea of an individual from a judicial standpoint, adding value to his or her own moral and ethical freedom.