DIRITTO DEL COMMERCIO INTERNAZIONALE
Anno XXII Fasc. 2 - 2008

Lauso Zagato

IL TRASFERIMENTO DI DATI PERSONALI VERSO STATI TERZI: ESITI (IN PARTE SORPRENDENTI) DELL'UNILATERALISMO GIURIDICO CE

Estratto

MVLTA PAVCIS AG

Milano • Giuffrè Editore

LAUSO ZAGATO

IL TRASFERIMENTO DI DATI PERSONALI VERSO STATI TERZI: ESITI (IN PARTE SORPRENDENTI) DELL'UNILATERALISMO GIURIDICO CE

I. Premessa. — II. Inseguendo il flusso di dati in uscita dalla CE: volontà di applicazione extraterritoriale della disciplina comunitaria. — III. Reazioni all'unilateralismo CE.

I. *Premessa.*

1. Oggetto del presente lavoro è uno specifico aspetto del sistema di protezione giuridica dei dati personali (1) elaborato dalla Comunità europea (CE) nel corso dell'ultimo decennio: la disciplina del trasferimento di tali dati verso Paesi terzi. L'attenzione sarà centrata sull'atteggiarsi della Comunità in quanto soggetto dell'ordinamento internazionale, piuttosto che sulle reciproche relazioni nella materia in esame fra ordinamenti interni

(1) Sull'evoluzione della nozione di riservatezza da diritto dell'individuo ad essere lasciato solo all'attuale diritto all'autodeterminazione informativa, e sulle tappe che la scandiscono, v.: G. Busia, *Riservatezza (diritto alla)*, in *Dig. Pubbl.*, Agg. I, Torino, 2000, pp. 476-510; A. Cerri, *Riservatezza (diritto alla).* II) *Diritto comparato e straniero*, in *Enc. giur.*, XXVII, Roma, 1991, pp. 1-9; S. Faro, *Trattamento dei dati personali e tutela delle persone*, in *Dig. Pubbl.*, Agg. I, Torino, 2000, pp. 543-573; V. Frosini, *Tecnologie e libertà costituzionali*, in *Dir. inf.*, 2003, pp. 487-491; A. Mantelero, Digital Privacy: *tecnologie conformate e regole giuridiche*, in F. Bergadano, A. Mantelero, G. Ruffo e G. Sartor, Privacy *digitale. Giuristi e informatici a confronto*, Torino, 2005, p. 18 ss. (in particolare le pagine iniziali); P. Pallaro, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, 2002, pp. 1-48; S. Rodotà, *Intervista su* privacy *e libertà*, Bari, 2005, pp. 1-153, *passim*; Id., *Tecnologie e diritti*, Bologna, 1995, pp. 1-122; G. Santaniello, *Il sistema delle garanzie della* privacy *(profili introduttivi)*, in A. Loiodice e G. Santaniello, *La tutela della riservatezza*, in *Trattato di diritto amministrativo*, diretto da Giuseppe Santaniello (in seguito *Tratt. Santaniello*), vol. XXVI, Padova, 2000, pp. 3-31 ; G. Sartor, Privacy, *reputazione, affidamento: dialettica e implicazioni per il trattamento dei dati personali*, in F. Bergadano, A. Mantelero, G. Ruffo e G. Sartor, Privacy *digitale*, cit., pp. 81-97; G. Sbrana, *I diritti alla riservatezza, origini e prospettive*, in AA.VV., *Il rispetto delle regole. Scritti degli allievi in onore di Alessandro Pizzorusso*, Torino, 2005, p. 105 ss.; R. Zaccaria, *Diritto dell'informazione e della comunicazione*, Padova, 2007, p. 34 ss.; V. Zeno-Zencovich, *Il «diritto di essere informati» quale elemento del diritto di cittadinanza*, in *Dir. inf.*, 2006, pp. 1-10.

diversi: quello della CE, quello dei singoli Stati membri (SM) e quello di Stati terzi (2). Ne uscirà confermato come la società della globalizzazione costituisca il terreno dello scontro per l'egemonia tra diversi ordinamenti giuridici, con le relative, inevitabili forzature unilateralistiche che ne conseguono. Proprio il tentativo della CE di imporre agli altri soggetti internazionali l'adeguamento dei rispettivi ordinamenti interni al regime di protezione dei dati contenuto nella Direttiva 95/46, e le reazioni nei confronti di tale tentativo costituiscono l'oggetto del presente lavoro.

Vanno, in proposito, tenute in conto le conseguenze che l'acquiescenza da parte dell'Unione europea (UE) verso la politica di sicurezza inaugurata dalla superpotenza USA dopo l'11 settembre esercita anche sulla disciplina del flusso transnazionale dei dati personali. La scelta operata nel 2006 dalla Corte di Giustizia (3), con l'annullamento degli atti emanati dalle istituzioni comunitarie in relazione all'accordo tra Comunità e Stati Uniti che va sotto il nome di *Passenger Name Record* (PNR) (4), fornisce al riguardo un apprezzabile contributo di chiarezza. La pronuncia (5) riconsegna infatti all'interprete la possibilità di analizzare la disciplina CE del trasferimento dei dati verso l'esterno senza l'assillo e le

(2) Sul rapporto tra ordinamento interno degli SM e ordinamento interno della Comunità europea — ben distinti tra loro, anche se entrambi «contrapposti» all'ordinamento internazionale — v. in particolare L. Picchio Forlati, *Il fondamento giuridico dell'Unione europea: Trattato o Costituzione?*, in *Scritti di diritto internazionale in onore di Gaetano Arangio-Ruiz*, vol. II, Napoli, 2004, pp. 1377-1386. Cfr. anche A. Tizzano, *Capacità privatistica e competenza contrattuale delle Comunità europee*, in *RDIPP*, 1978, p. 17 ss., e L. Zagato, *La politica di ricerca delle Comunità europee*, Padova, 1993, pp. 85-87.

(3) CGCE 30 maggio 2006, C-317/04 e 318/04, *Parlamento europeo c. Consiglio e Commissione*, in *Racc.*, I-4795 ss. Primi commenti in V. Michel, *La dimension externe de la protection des données à caractère personnel: acquiescement, perplexité et frustration*, in *RTDE*, 2006, pp. 549-559 e A. Montelero, *Note minime in margine alla pronuncia della Corte di Giustizia delle Comunità europee sul trasferimento dei dati personali dei passeggeri dei vettori aerei verso gli Stati Uniti*, in *Contr. impr./Eur.*, 2006, pp. 1075-1081.

(4) V. Decisione del Consiglio 2004/496/CE del 17 maggio 2004 relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (*Passenger Name Record*, PNR) da parte dei vettori aerei all'ufficio doganale di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti, in *G.U.* L 183 del 20 maggio 2004, e Decisione della Commissione 2004/535/CE del 14 maggio 2004 relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti (*United States Bureau of Customs and Border Protection*) in *G.U.* L 235 del 6 luglio 2004. Per prime considerazioni G. Buttarelli, *Il trasferimento all'estero dei dati personali*, in G. Santaniello (a cura di), *La protezione dei dati personali* (*Tratt. Santaniello*, vol. XXXVI, 2005), pp. 263-279.

(5) Vero è che i giudici di Lussemburgo hanno fondato la loro decisione sull'errata scelta della base giuridica di tali atti, tralasciando di conseguenza gli altri motivi di impugnazione fatti valere dal Parlamento europeo (PE). L'argomento non verrà approfondito in questa sede (v. comunque oltre, nota successiva). Piuttosto, il nuovo Trattato firmato a Lisbona dai Capi di Stato e di governo il 13 dicembre 2007 (c.d. Trattato di Lisbona) trae le conclusioni dalla pronuncia in esame, distinguendo tra un regime ordinario di tutela (art. 16 Trattato sul funzionamento dell'Unione europea) e un regime speciale (art. 39 TUE) da applicare al trattamento dei dati in materia di Politica estera e di sicurezza comune. V. anche oltre, nota successiva.

distorsioni introdotte dalla pressione dell'obiettivo predominante della sicurezza: obiettivo il cui perseguimento, come i giudici di Lussemburgo hanno sottolineato, piuttosto che venire ascritto alla Direttiva 95/46 ed all'art. 95 del Trattato CE (TCE), è proprio della disciplina di cui al Titolo VI Trattato UE (TUE) (6).

All'indagine che segue rimarrà estraneo il tema della disciplina dei dati personali nel *Web*. La Corte ha infatti stabilito, nella sentenza *Lindqvist* (7), che il capo IV della Direttiva 95/46 predispone un regime speciale (punto 63), implicante norme specifiche, e non contenente disposizioni relative alla rete Internet. Qualora si attribuisse al «legislatore comunitario l'intenzione di includere prospettivamente nella nozione di trasferimento verso un paese terzo l'inserimento [...] di dati su una pagina Internet» (punto 67), ne conseguirebbe che ogni operazione di caricamento di dati personali su una pagina Internet costituisce «necessariamente un trasferimento verso tutti i paesi terzi in cui esistono i mezzi tecnici necessari per accedere ad Internet». Il regime speciale di cui al capo IV della Direttiva verrebbe così a costituire, per quanto riguarda le operazioni su Internet, il regime generale di protezione dei dati sulla rete (punto 69); e ciò in contrasto con la volontà del «legislatore» comunitario (8).

II. *Inseguendo il flusso di dati in uscita dalla UE: volontà di applicazione extraterritoriale della disciplina comunitaria.*

2. La tutela dei dati personali è disciplinata dalla Direttiva 95/46/CE (9), come integrata dalla Direttiva 2002/58/CE (10) relativa alla vita

(6) La scelta operata dalla Corte non entra dunque nel merito di quel drammatico processo di «mitridatizzazione» dei diritti che incombe come un convitato di pietra sullo sviluppo del lavoro che segue (v. oltre, par. 16). L'espressione è usata da S. Rodotà, *Intervista...*, cit., pp. 94-95: un processo di mitridatizzazione, a piccole e progressive dosi, fa abbassare la soglia di percezione della libertà. V. anche M. Simoncini, *Legislazione antiterrorismo e tutela della* privacy, in *RTDP*, 2007, pp. 959-1000.

(7) CGCE, 6 novembre 2003, C-101/01, *Bodil Lindqvist*, in *Racc.*, I-12971 ss.

(8) Sull'argomento L. Zagato, *Il trasferimento dei dati personali all'esterno della UE nella Rete: rivincita del multilateralismo?*, in B. Cortese (a cura di), E-commerce *in Europa*, Padova (di prossima pubblicazione).

(9) Direttiva 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 di tali dati, in *G.U.* L 281 del 23 novembre 1995. Per prime informazioni: R. Delfino, *La direttiva comunitaria 46/95 «sulla protezione dei dati personali e sulla libera circolazione di tali dati»*, in *Contr. impr./Eur.*, 1996, pp. 888-895; R. Imperiali D'Affitto, *La direttiva comunitaria sulla* privacy *informatica*, in *DCSI*, 1995, pp. 569-588; L. Zagato, *Il trattamento dei dati personali, tra libertà di circolazione e tutela delle persone fisiche*, in *NLCC*, 1998, pp. 195-202. La Direttiva 46/95 ha avuto applicazione in Italia con l. n. 675 del 31 dicembre 1996, Tutela delle persone e altri soggetti rispetto al trattamento dei dati personali, in *G.U.* n. 5 suppl. ord. 3 dell'8 gennaio 1997, più volte modificata e integrata (da ultimo con d.lgs. n. 135 dell'8 maggio 1998). Successivamente il regime del trattamento dei dati è stato innovato dal d.lgs. n. 196 del 30 giugno 2003 (codice in materia di protezione dei dati personali), in *G.U.* n. 174 (s.o. 123/L) del 29 luglio 2003, entrato in vigore il 1°

privata e alle comunicazioni elettroniche (modificata dalla *Retention Directive* dell'aprile 2006) (11); non invece dalla Direttiva sul commercio elettronico (12), il cui art. 1, par. 5, lett. *b*) esclude dal campo d'applicazione della medesima «le questioni relative alla società dell'informazione» oggetto della disciplina di cui alla Direttiva 95/46/CE in esame.

Sembra qui necessario un richiamo alle nozioni essenziali contenute nella Direttiva 95/46. Secondo l'art. 2, lett. *b*) di questa, si intende per trattamento dei dati personali (13) l'insieme delle operazioni condotte con o senza ausilio di processi automatizzati e applicate a dati personali, quali «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 successivo art. 3, nello stabilire il campo d'applicazione *ratione materiae* della Direttiva, stabilisce al par. 2 (14) che questa non si applica al trattamento dei dati personali finalizzato ad attività «che non rientrano nel campo di applicazione del diritto comunitario» quali quelle previste dai Titoli V (Disposizioni sulla politica estera e di sicurezza comune) e VI (Disposizioni sulla cooperazione giudiziaria e di polizia in materia penale) del TUE, e comunque ai trattamenti aventi ad oggetto pubblica sicurezza, difesa, sicurezza dello Stato e attività in materia penale. Ancora, la Direttiva non si applica in caso di trattamento di dati personali effettuato «da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico».

Alla stregua del successivo art. 4, par. 1, lett. *c*), gli SM sono tenuti ad applicare le disposizioni nazionali di attuazione dello strumento anche (15) al trattamento di dati personali nel caso in cui il responsabile di tale trattamento non sia stabilito nel territorio di uno SM, ma utilizzi a fini del trattamento «strumenti, automatizzati o non automatizzati», situati nel territorio di tale Stato membro (16). Il trattamento dei dati personali può anche essere effettuato (art. 7) quando vi sia stato esplicito consenso dell'interessato, oppure risulti necessario all'esecuzione di un contratto (o di misure pre-contrattuali) con tale persona, per la salvaguardia di un suo interesse vitale, oppure per adempiere ad un obbligo legale cui è tenuto il responsabile del trattamento o un compito connesso all'esercizio di pubblici poteri di cui questi sia investito (17).

Richiamato l'art. 8, che individua al par. 1 quelle categorie particolari di dati (i c.d. dati sensibili) per le quali il trattamento è vietato (18) salvo si rientri in una delle ipotesi di deroga indicate dai successivi paragrafi (19), vengono ancora in rilievo ai fini del presente lavoro l'art. 10, relativo alle informazioni minime che il responsabile del trattamento deve fornire alla persona interessata (20), e l'art. 13. Quest'ultimo disciplina i limiti che gli Stati possono imprimere alla protezione garantita dalla Direttiva (21).

---

gennaio 2004. Sulla l. n. 675 del 1996 v.: G. Alpa, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. inf.*, 1997, pp. 703-734; C. Bianca e F. Busnelli (a cura di), *Tutela della* privacy, in *NLCC*, 1999, pp. 219-875 (di seguito *Commentario Bianca/Busnelli*); V. Franceschelli (a cura di), *La tutela della* privacy *informatica*, Milano, 1998, pp. 1-281; E. Giannantonio, M. Losano e V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l. n. 675 del 1996*, Padova, 2ª ed., 1999, pp. 1-745 (di seguito *Commentario Gianantonio/Losano/Zeno-Zencovich*). Sul codice del 2004 G. Cirillo, *Il codice sulla protezione dei dati personali*, Milano, 2004, pp. 1-713 (di seguito *Commentario Cirillo*).

(10) 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, in *G.U.* L 201 del 31 luglio 2002. La Direttiva 2002/58 abroga la Direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, in *G.U.* L 24 del 30 gennaio 1998. Per prime considerazioni: G. Cassano e M. Aquino, *Il trattamento dei dati personali alla luce della Direttiva 2002/58*, in *Contr.*, 2003, pp. 402-412; S. Vigliar, Privacy *e comunicazioni elettroniche: la Direttiva 2002/58/CE*, in *Dir. inf.*, 2003, pp. 401-424.

(11) Direttiva 2006/24 del PE e del Consiglio del 15 marzo 2004 riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la Direttiva 2002/58, in *G.U.* L 105 del 13 aprile 2006.

(12) Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, in *G.U.* L 178 del 17 luglio 2000.

(13) Per dati personali si intende invece — lett. *a*) — «qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale».

(14) Alla stregua del par. 1, le disposizioni della direttiva si applicano al trattamento «di dati personali interamente o parzialmente automatizzato», nonché a quello non automatizzato di dati «contenuti o destinati a figurare negli archivi».

(15) Le altre due ipotesi disciplinate dall'art. 4, par. 1, rispettivamente alle lett. *a*) e *b*), riguardano il responsabile del trattamento stabilito in più SM (in tal caso lo SM deve adottare le misure necessarie ad assicurare l'osservanza, da parte di ciascuno stabilimento, degli «obblighi stabiliti dal diritto nazionale applicabile») e il responsabile stabilito in un luogo in cui si applica la legislazione di uno SM, pur essendo a questo esterno.

(16) In tale ipotesi il responsabile deve designare, in base al par. 2, un rappresentante stabilito nel territorio dello SM.

(17) Infine, il trattamento può ancora essere effettuato quando sia necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento o dei terzi cui i dati vengono comunicati, a condizione che non prevalgano invece l'interesse o i diritti e le libertà fondamentali della persona interessata (di cui all'art. 1, par. 1).

(18) È vietato il trattamento dei dati personali «che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale» nonché dei dati relativi alla salute ed alla vita sessuale.

(19) Tra queste deroghe: consenso esplicito dell'interessato, salvaguardia di interessi vitali della persona interessata, necessità a fini di prevenzione o diagnostica medica. La lista fornita dai parr. 2 e 3 non è comunque esaustiva, dal momento che il successivo par. 4 autorizza gli Stati membri «purché siano previste le opportune garanzie», a stabilire ulteriori deroghe per motivi di interesse pubblico rilevante.

(20) Informazioni da fornire comunque sono quelle relative ad identità del responsabile (o del suo rappresentante) e finalità del trattamento; ulteriori informazioni riguardanti destinatari dei dati, esistenza del diritto di accesso e possibilità di rettifica dei dati possono risultare necessarie ai fini di un trattamento «leale» nei confronti della persona interessata.

(21) Si tratta di misure aventi ad oggetto: salvaguardia della sicurezza dello Stato,

3. La disciplina del trasferimento di dati verso Paesi terzi è contenuta nel capo IV (artt. 25-26) della Direttiva 95/46. Prima di esaminare tali disposizioni giova occuparsi degli aspetti istituzionali (capo VI: Autorità di controllo e Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, artt. 28-30) e procedurali (capo VII: misure comunitarie d'esecuzione, art. 31).

La Commissione adotta le misure indicate dagli artt. 25 e 26, operando secondo la procedura di cui all'art. 31 par. 2 (comitato di gestione), ed avvalendosi della collaborazione fornitale (art. 29, par. 1) dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali (*Gruppo* ex *art. 29*), composto dai rappresentanti delle autorità di controllo nazionale incaricate di sorvegliare, nel territorio dello SM, l'applicazione delle disposizioni di attuazione della Direttiva ([22]). A tali autorità nazionali di controllo spetta la designazione del membro che le rappresenta nel Gruppo, ai cui lavori partecipa, senza diritto di voto, la stessa Commissione. Il Gruppo si avvale inoltre della presenza attiva (con diritto di voto, cioè) del Supervisore europeo per la protezione dei dati ([23]).

Il ruolo del Gruppo, malgrado i pareri da esso forniti rivestano carattere consultivo ([24]), non tollera fraintendimenti: è composto infatti di soggetti che esercitano, Stato per Stato, una autorità indipendente di controllo sull'applicazione della normativa nazionale (come armonizzata dalla Direttiva) godendo di poteri investigativi, di intervento, di promozione di azioni giudiziarie in caso di violazione di norme nazionali. Di conseguenza esso si trova «in una posizione di osservatorio privilegiato di tutte le pertinenti normative, europee e nazionali»; di più, il *Gruppo* ex *art. 29* viene maturando un'esperienza «su scala internazionale circa leggi, prassi e problemi inerenti alla protezione dell'autodeterminazione informativa» ([25]). Le indicazioni contenute nei suoi pareri assumono anzi, alla luce della natura fondamentale del diritto da proteggere, «un valore aggiunto rispetto al disposto della direttiva», incidendo sulla corretta interpretazione da dare a tale disposto ([26]).

Va sottolineata la forza del blocco istituzionale creatosi tra Commissione, *Gruppo* ex *art. 29* (con le sue puntuali articolazioni a livello di singoli Stati membri), Comitato di gestione di cui all'art. 31, Supervisore. Nella UE emerge insomma una originale struttura integrata che si occupa tendenzialmente di tutto ciò che riguarda la tutela dei dati, inseguendone gli aspetti salienti lungo i diversi aspetti della società della Rete, scomponendoli e ricostruendoli in un quadro unitario: svolgendo così un ruolo di «attrattore» che la porta, inevitabilmente, ad ampliare progressivamente l'ambito del proprio intervento.

4. Il trasferimento dei dati ([27]) verso uno Stato terzo, da parte di soggetti stabiliti nella Unione, è possibile quando (art. 25, par. 1) lo Stato terzo in questione garantisca un livello di protezione adeguato. Tale valutazione (par. 2) risulta da una serie di parametri — tra i quali natura dei dati ([28]), finalità (soprattutto nel caso in cui i dati abbiano rilievo a fini occupazionali), Paese d'origine o di destinazione finale — la cui sussistenza o meno può essere rilevata vuoi dalle autorità garanti nazionali, vuoi dalla Commissione, che si scambiano i rispettivi pareri in proposito. Data la

---

difesa, pubblica sicurezza, misure di accertamento e perseguimento di infrazioni penali e violazioni della deontologia professionale, interessi economici e finanziari rilevanti (sia dello SM che della UE), protezione della persona interessata o dei diritti e delle libertà altrui. A determinate condizioni, deroghe possono essere applicate anche per motivi di ricerca scientifica ed elaborazione di statistiche.

([22]) Art. 28, par. 1. Si tratta di autorità indipendenti nell'esercizio delle funzioni loro attribuite, autorità che dispongono (art. 28, par. 3) di *poteri investigativi* (diritto di accesso ai dati oggetto di trattamento e di raccolta di ogni informazione necessaria all'adempimento della funzione), di *poteri effettivi d'intervento* (tra cui, oltre alla formulazione dei pareri *ex* art. 20, quello di ordinare congelamento, cancellazione o distruzione dei dati, oppure di vietare un trattamento, di rivolgere un avvertimento al responsabile del trattamento, nonché di adire le istituzioni politiche nazionali, *in primis* il Parlamento) e di *promuovere azioni giudiziarie* in caso di violazione delle disposizioni nazionali. Sull'Istituto del Garante per la *privacy* nell'ordinamento interno italiano v. A. Simoncini, *Autorità indipendenti e «costruzione» dell'ordinamento giuridico: il caso del Garante per la protezione dei dati personali*, in *Dir. pubbl.*, 1999, p. 851 ss.

([23]) Istituito — *ex* art. 286, par. 2 del Trattato CE — dal Reg. 45/2001 del PE e del Consiglio del 18 dicembre 2000 sulla protezione degli individui con riguardo al trattamento dei dati personali da parte delle istituzioni della Comunità e sulla libera circolazione di tali dati, in *G.U.* L 8 del 12 gennaio 2001. L'art. 46, lett. *f*) e *g*) del Reg. 45/2001 stabilisce in capo al Supervisore l'obbligo di cooperare con il *Gruppo* ex *art. 29*. Per una disamina approfondita del ruolo del Supervisore si rimanda a H. Hijmans, *The European Data Protection Supervisor: The Institutions of the EEC Controlled by an Independent Authority*, in *CMLR*, 2006, pp. 1313-1342. Sull'art. 286 quale «espressione di un principio di importanza costituzionale dell'ordinamento comunitario», v. B. Cortese, *Commento all'art. 286 Trattato CE*, in A. Tizzano (a cura di), *Trattato sull'Unione europea*, Milano, 2004, pp. 1284-1287. V. anche E. Lucchini Guastalla, *Il diritto alla* privacy *nella prospettiva europea*, in G. Iudica e G. Alpa, *Costituzione europea e interpretazione della Costituzione italiana*, Roma, 2006, pp. 183-197.

([24]) In particolare il *Gruppo* ex *art. 29* deve (art. 30, par. 1) esaminare — lett. *a*) — le questioni attinenti all'applicazione delle norme nazionali di attuazione della Direttiva, formulare pareri — lett. *b*) — «sul livello di tutela nella Comunità e nei paesi terzi», consigliare la Commissione — lett. *c*) — circa i progetti di modifica della stessa, e — lett. *d*) — sui codici di condotta elaborati a livello comunitario e previsti dall'art. 27, par. 3 (capo V, codici di condotta) in attuazione della previsione di cui al par. 1 di tale articolo. Alla stregua di quest'ultimo, SM e Commissione «incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione» della direttiva, ad opera degli SM.

([25]) P. Pallaro, *op. cit.*, p. 147.

([26]) *Id.*, p. 153.

([27]) La Direttiva non fa cenno al mezzo di trasmissione utilizzato: in relazione allo stato di avanzamento tecnologico, si può distinguere a seconda del modo di presentazione (testo in chiaro o criptato), al supporto (cartaceo, banda magnetica o perforata, disco), al mezzo di trasporto (fisico, posta, telecomunicazione commutata per circuiti o per pacchetti), all'interfaccia (terminale, ovvero da *computer* a *computer*), al tipo di circuito (direttamente nel paese di destinazione o con transito intermedio attraverso un altro Paese), alle relazioni tra trasmittente e ricevente: v. C. Amato, *Art. 28*, in *Commentario Bianca/Busnelli*, cit., p. 650.

([28]) Da porre in relazione al divieto di trattamento di categorie particolari di dati sensibili: v. *supra*, nota 18.

genericità della disposizione, non può stupire che uno dei primi interventi del *Gruppo* ex *art. 29* abbia riguardato proprio l'elaborazione dei principi che l'ordinamento del Paese terzo deve contemplare nella propria legislazione interna onde essere individuato come capace di «protezione adeguata» ([29]).

Nel caso in cui la Commissione intervenga constatando la sussistenza (par. 6) o l'assenza (par. 4) di un livello di protezione adeguato garantito dallo Stato terzo, i singoli SM si devono conformare a tale decisione. Il parallelismo si interrompe insomma nel momento della constatazione, ad opera della Commissione, che lo Stato terzo non garantisce un livello di protezione adeguato (par. 4): si parla quindi di un parallelismo provvisorio di competenze, applicabile anche alle ipotesi di negoziazione con i Paesi terzi. Dal momento della constatazione negativa solo la Commissione potrà avviare negoziati con lo Stato terzo per giungere alla modifica della situazione risultante dalla constatazione.

In deroga all'art. 25, gli SM possono disporre il trasferimento di dati verso Paesi terzi che non garantiscono una tutela adeguata dei dati (art. 26, par. 1) in caso di consenso manifestato in maniera inequivocabile dell'interessato, oppure quando il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato ed il responsabile del trattamento (o tra questo ed un terzo nell'interesse della persona interessata), o per l'attuazione di misure pre-contrattuali ([30]).

5. I parr. 4 e 6 dell'art. 25 prevedono dunque il potere della Commissione di adottare decisioni secondo la procedura del comitato di gestione (art. 31) previa consultazione — *ex* art. 30, par. 1, lett. *b*) — del *Gruppo* ex *art. 29* ([31]). Orbene, nessuna decisione è stata presa fino ad oggi

([29]) Parere 12/98 del 24 luglio 1998 sul *trasferimento di dati personali verso Paesi terzi: applicazione degli artt. 25 e 26 della direttiva europea sulla tutela dei dati (WP 12)*, consultabile al sito: *www.ec.europa.eu/justice#home/fsi/privacy/docs/wpdocs/1998/wp12#it.pdf*. A giudizio del Gruppo, perché vi sia protezione adeguata il trattamento deve avere le seguenti caratteristiche: finalità limitata (utilizzo dei dati solo per scopi chiari, prefissati, comunicati ai titolari, ed utilizzati in modi non incompatibili con tale finalità); qualità e proporzionalità dei dati trattati (adeguatezza, pertinenza, non eccedenza); trasparenza e diritto di accesso (principi questi derogabili dalla legislazione dello Stato terzo solo nei limiti indicati dagli artt. 11 e 13 Direttiva); sicurezza (misure da adottare contro i rischi di accesso non autorizzato o di modifiche e cancellazione dei dati); restrizioni ai successivi trasferimenti a terzi (onde controllare che garantiscano a propria volta un adeguato livello di tutela); consenso esplicito al trattamento (nel caso di dati sensibili).

([30]) Il trasferimento può essere altresì disposto dagli SM per interesse pubblico rilevante o per motivi giudiziari, oppure per la salvaguardia dell'interesse vitale della persona interessata. La deroga è infine concessa — art. 26, par. 1, lett. *f*) — nel caso di trasferimento a partire da un registro aperto alla consultazione del pubblico «nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione».

([31]) V. i seguenti pareri del *Gruppo di lavoro* ex *art. 29* in tema di protezione dei dati (consultabili al sito *www.ec.europa.eu/justice#home/fsi/privacydocs*): 4/2002 sul livello di tutela dei dati personali in Argentina, adottato il 3 ottobre 2002; 2/2001 sul livello di tutela dei dati personali in Canada, adottato il 26 gennaio 2001; 5/99 sul livello di tutela dei dati personali in Svizzera, adottato il 7 giugno 1999; 6/2003 sul livello di tutela dei dati personali

sulla base del par. 4; al contrario, la Commissione ha emanato un certo numero di decisioni *ex* par. 6, nei confronti di: Argentina, Canada, Svizzera, Stati Uniti, ed inoltre Isola di Man e Isole del Canale (Bailato di Guernsey) ([32]).

Tralasciando per il momento il rapporto con gli USA, negli altri casi significativi indicati ([33]) ci si trova in presenza di normative introdotte negli ordinamenti federali rispettivamente di Argentina, Canada e Svizzera, a coronamento dello sforzo compiuto dai legislatori di tali Stati per consentire che tali ordinamenti siano giudicati idonei a fornire una protezione adeguata alla stregua dei parametri UE. In tutti e tre i casi la Commissione, seguendo il parere del Gruppo *ex* art. 29, verifica la sostanziale corrispondenza del livello di tutela della *privacy* garantito dalla nuova legge con quello in vigore nella UE. Unico punto di preoccupazione è il fatto che, trattandosi di Stati federali, la nuova legge possa non trovare applicazione a livello locale.

Per quanto in particolare riguarda il Canada, la legge federale — c.d.

nell'isola di Man, adottato il 21 novembre 2003; 5/2003 sul livello di tutela dei dati personali a Guernsey, adottato il 13 giugno 2003. La complessità dei rapporti con gli SU ha dal canto suo richiesto una intensa attività di produzione di pareri da parte del *Gruppo*; ciò suggerisce di elencare a parte la successione di tali pareri: v. oltre, nota 44.

([32]) Rispettivamente: Decisione della Commissione 2003/490/CE del 30 giugno 2003 conforme alla Direttiva 95/46/CE del PE e del Consiglio e riguardante l'adeguatezza della tutela dei dati personali fornita in Argentina, in *G.U.* L 168 del 5 luglio 2003; Decisione della Commissione 2002/2/CE del 20 dicembre 2001 conforme alla Direttiva 95/46/CE del PE e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (*Canadian Personal Information Protection and Electronic Document Act*), in *G.U.* L 2 del 4 gennaio 2002; Decisione della Commissione 2000/518/CE del 26 luglio 2000 riguardante l'adeguatezza della tutela dei dati personali in Svizzera a norma della Direttiva 95/46/CE, in *G.U.* L 215 del 25 agosto 2000; Decisione della Commissione 2000/520/CE del 26 luglio 2000 a norma della Direttiva 95/46/CE del PE e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e delle relative «domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del Commercio degli Stati Uniti, in *G.U.* L 215 del 25 agosto 2000; Decisione della Commissione 2004/411/CE del 28 aprile 2004 riguardante l'adeguatezza della tutela dei dati personali nell'isola di Man, in *G.U.* L 151 del 30 aprile 2004; Decisione della Commissione 2003/821/CE del 21 novembre 2003 riguardante l'adeguatezza della tutela dei dati personali in Guernsey, in *G.U.* L 308 del 25 novembre 2003. Una decisione emanata a suo tempo nei riguardi dell'Ungheria è stata invece travolta dagli sviluppi del processo di allargamento: v. Decisione della Commissione 2000/519/CE del 26 luglio 2000 riguardante l'adeguatezza della tutela dei dati personali in Ungheria a norma della Direttiva 95/46/CE, in *G.U.* L 215 del 25 agosto 2000.

([33]) Scarso interesse presentano ai fini del presente lavoro le decisioni relative all'isola di Man ed al Bailato di Guernsey. Trattasi di possedimenti della Corona britannica del tutto indipendenti tranne che per la difesa e le relazioni internazionali, di cui è responsabile il governo britannico. In base al Protocollo n. 3 dell'Atto di adesione del RU del 1972, a tali territori si applicano solo le misure doganali dei trattati CE, mentre per ogni altro aspetto rappresentano Stati terzi. La vigenza di tale regime è ribadita dall'art. 299, par. 6, lett. *c*) del TCE. Con la *Data Protection (Bailiwick of Guernsey) Law 2001* e, rispettivamente, con il *Data Protection Act 2002*, è stata estesa al bailato ed all'isola di Man la normativa che ha dato applicazione nell'ordinamento interno del RU alla Direttiva 95/46.

PIPED Act (o *Canadian Act*) del 13 aprile 2000 ([34]), entrato in vigore all'inizio del 2001 e rivolto alle organizzazioni del settore privato che «rilevano, usano o comunicano informazioni personali nell'ambito di attività commerciali» — si applica dal 1° gennaio 2001 alle informazioni personali rilevate o comunicate da organizzazioni quali imprese, stabilimenti o aziende operanti a livello federale ([35]). Solo dal 2004 il *PIPED Act* viene applicato a qualsiasi organizzazione, federale o meno, che utilizzi nel territorio canadese dati personali nell'ambito di attività commerciali ([36]). L'art. 26, par. 2 della legge canadese prevede che, ove le province si dotino di normative giudicate dai competenti organi centrali «adeguate» alla stregua della legge federale, alla trasmissione di dati relativa a transazioni interne alla provincia sia applicata tale normativa. Il *PIPED Act* continuerà invece ad applicarsi alle attività di rilevazione, utilizzo e comunicazione dei dati fra province, nonché nei casi non coperti dalla legislazione provinciale ([37]).

Venendo all'Argentina, l'art. 43, par. 3 della Costituzione del '94 prevede un ricorso giurisdizionale chiamato *habeas data* ([38]). La decisione di adeguatezza della Commissione CE, non diversamente dal precedente parere favorevole espresso dal *Gruppo* ex *art. 29*, si fonda sul lavoro di consulenza svolto a stretto contatto con le autorità argentine incaricate di

([34]) Consultabile al sito *www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6#4/C-6#cover-F.html*.

([35]) Con esclusione dei dati sanitari personali; per questi ultimi la legge si applica a partire dal 1° gennaio 2002.

([36]) Ciò ad esclusione delle organizzazioni governative soggette al *Federal Privacy Act*, a quelle regolate dal settore pubblico a carattere provinciale, alle organizzazioni senza scopo di lucro; il *PIPED Act* non si applica neppure a quei dati sui lavoratori dipendenti che siano usati per scopi non commerciali.

([37]) Nel marzo 2002 la Commissione CE ha emanato delle *Frequently Asked Questions* (FAQ) «*on the Commission's adequacy finding on the Canadian Personal Information Protection and Electronic Documents*» per agevolare i privati che debbano conformarsi alle norme del *PIPED Act*. Alla penultima *Question*, relativa al rapporto tra *PIPED Act* e normativa provinciale, la Commissione risponde che, secondo le previsioni, via via che il governo canadese riconoscerà «*a provincial law as being substantially similar to PIPED Act then the Commission Decision will be adapted to reflect this*». Nel successivo Commission Staff Working Document, *The Application of Commission decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the PE and of the Council on the adequate protection of personal data provided by the Canadian PIPED Act*, Bruxelles, 20 November 2006 (SEC (2006) 1520), viene confermato il giudizio di adeguatezza del PIPED Act canadese alla luce, anche, dei primi positivi risultati ottenuti a livello di «*provincial legislation*» (Quebec, Alberta, British Columbia).

([38]) Si tratta di un'azione concessa a chiunque per «venire a conoscenza di tutti i dati che lo riguardano presenti presso registri o banche dati pubblici oppure banche dati private aventi finalità informative». Alla norma è stata riconosciuta dalla giurisprudenza la diretta applicabilità. Il principio di habeas data costituzionale si sta peraltro affermando nei principali ordinamenti giuridici sudamericani. Sull'argomento: T. Frosini, *Tecnologie e libertà costituzionali...*, cit., p. 493 ss. e E. Rozo Acuña, Habeas *data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*, in *Dir. pubbl. comp. eur.*, 2002, p. 1923 ss.

promulgare la normativa applicativa della disposizione costituzionale ([39]). Il giudizio positivo sulla legislazione emanata a livello centrale si accompagna anche in questo caso a preoccupazioni relative all'applicazione della stessa a livello provinciale.

Nel caso della Svizzera, la Decisione della Commissione che definiva adeguato il livello di protezione offerto dal *Swiss Federal Act on Data Protection* (SFADP) è stata presa malgrado le preoccupazioni espresse dal *Gruppo* ex *art. 29 ([40])* circa l'adeguatezza della legislazione cantonale. Essendosi negli anni successivi avuto, dietro pressione degli organi comunitari, l'inserimento di clausole sulla tutela dei dati nelle Costituzioni di 16 su 26 cantoni (ma alcune altre sono in corso), il Documento di lavoro dei servizi della Commissione dell'autunno 2004 ([41]) prende atto con soddisfazione di tale positiva evoluzione.

6. Quanto agli Stati Uniti, l'evidente impossibilità da parte UE di imporre la propria disciplina alla superpotenza americana risalta alla luce della diversità tra i due ambienti giuridici in materia di *privacy* ([42]). La Decisione 2000/520 ([43]) è stata emanata a conclusione di un lungo nego-

([39]) Legge 25.326 sulla tutela dei dati personali del 4 ottobre 2000 (consultabile al sito *www.protecciondedatos.com.arg*) e Regolamento approvato con decreto 1558/2001 del 3 dicembre 2001: mancavano peraltro, al momento della Decisione 2003/490 della Commissione CE, casi pratici di applicazione della normativa nazionale argentina in esame.

([40]) Piuttosto, nel suo parere il Gruppo ha valutato il fatto che la Svizzera è parte, dal 1999, della Convenzione (ETS n. 108) del Consiglio d'Europa sulla protezione delle persone con rispetto al trattamento dei dati a carattere personale, aperta alla firma a Strasburgo il 28 gennaio 1981 ed entrata in vigore a livello internazionale il 1° ottobre 1985 (protocollo addizionale entrato in vigore il 1° luglio 2004; per prime informazioni V. Frosini, *La Convenzione europea sulla protezione dei dati*, in *RDE*, 1984, pp. 3-18). Il Gruppo richiama quanto già affermato nel citato *WP 12*: per quanto l'adesione della Svizzera alla Convenzione n. 108 sia importante, il conseguimento degli obiettivi di questa non è tale da garantire automaticamente l'esistenza di un livello sufficiente di tutela ai fini dell'applicazione della Direttiva 95/46. Ciò a causa di alcuni limiti, tra i quali: mancanza di restrizioni al trasferimento dei dati verso Stati terzi non parte alla Convenzione; mancanza di obbligo per i responsabili del trattamento di fornire informazioni all'interessato prima del trattamento; assenza di previsioni in materia di pubblicità commerciale e di decisioni individuali automatizzate; mancata previsione di istanze *ad hoc* per svolgere indagini indipendenti e risolvere controversie. Sul punto v. (pp. 766-767) P. Pallaro, *Rapporti commerciali tra UE e Stati terzi e la questione della tutela dei dati personali. Il difficile confronto UE-USA*, in questa *Rivista*, 2000, pp. 753-788.

([41]) Commission Staff Working Document, *The Application of Commission Decision 2000/518/EC of 26 July 2000 Pursuant to Directive 95/46/EC of European Parliament and of the Council on the Adequate Protection of Personal Data Provided in Switzerland*, Bruxelles, 20 ottobre 2004 (SEC (2004) 1322). I servizi della Commissione svolgono la loro valutazione sulla base di quanto previsto dall'art. 4, par. 1 cpv. della Decisione 2000/518, che chiama la Commissione a valutarne l'applicazione «sulla base delle informazioni disponibili, tre anni dopo la sua notifica agli Stati membri».

([42]) V. oltre, par. 12.

([43]) Preceduta da ripetuti pareri del *Gruppo* ex *art. 29*: trattasi dei seguenti pareri: 1/99 del 26 gennaio 1999 concernente il livello di protezione dei dati negli SU e le discussioni in corso fra Commissione europea e SU; 2/99 del 3 maggio 1999 sull'adeguatezza dei principi internazionali dell'approdo sicuro pubblicati dal Dipartimento del commercio degli SU il 19 aprile 1999; 4/99 del 7 giugno 1999 sulle domande più frequenti (FAQ) che devono essere

ziato con le autorità di quello Stato, in specifico Commissione federale per il Commercio (FTC) e Dipartimento dei trasporti (DOT). Con tale atto la Commissione stabilisce l'adeguatezza della protezione fornita dai Principi dell'approdo sicuro (*Safe Harbour Privacy Principles*) e dalle relative Domande più frequenti (FAQ) pubblicate dal Dipartimento del Commercio degli Stati Uniti; entrambi i documenti sono allegati alla Decisione ([44]). La Decisione è seguita da due Documenti di lavoro dei servizi della Commissione rispettivamente del 2002 ([45]) e del 2004 ([46]).

7. Alla stregua dell'art. 26, par. 2 della Direttiva 95/46, uno SM può autorizzare, anche al di là delle ipotesi di cui al par. 1 ([47]), un trasferimento o una categoria di trasferimenti di dati verso un Paese terzo che non garantisca un livello di protezione adeguato secondo lo schema comunitario, «qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone», nonché per l'esercizio dei diritti connessi. Tali garanzie devono risultare in particolare da adeguate clausole contrattuali. Sullo SM grava l'onere di informare gli altri Stati membri e la Commissione. In caso di opposizione notificata da parte di uno SM o dalla Commissione «debitamente motivata sotto l'aspetto della vita privata e dei diritti e delle libertà fondamentali delle persone» (par. 3 cpv.) la Commissione adotterà le misure appropriate secondo le procedure di cui all'art. 31, par. 2 (comitato di gestione).

---

pubblicate dal Dipartimento del commercio degli SU in relazione ai proposti principi dell'approdo sicuro sull'adeguatezza dei principi internazionali dell'approdo sicuro; 7/99 del 3 dicembre 1999 sul livello della protezione dei dati fornito dai principi dell'approdo sicuro pubblicati unitamente alle domande più frequenti (FAQ) e agli altri documenti relativi il 15 e 16 novembre 1999 dal Dipartimento del commercio degli SU; 3/2000 del 16 marzo 2000 sul dialogo UE/USA concernente l'accordo (*Arrangement*) sull'approdo sicuro; 4/2000 del 16 maggio 2000 sul livello di protezione fornito dai principi dell'approdo sicuro.

([44]) Insieme ad un riepilogo sulle modalità di esecuzione dei principi (All. III), ad un *memorandum* su tutela della riservatezza e risarcimento dei danni nella legislazione degli SU (All. IV), a due lettere — a nome rispettivamente della *Federal Trade Commission* e del *Department of Transportation* (All. V e VI) — inviate alla Commissione europea in risposta a richieste di chiarimento sulle rispettive funzioni e «filosofie» amministrative inoltrate da quest'ultima. Ancora agli Enti governativi americani (FTC e DOT), autorizzati a svolgere istruttorie oltre che ad ottenere riparazioni in relazione ai *principi dell'approdo sicuro*, ed alle basi giuridiche delle rispettive competenze nella materia alla stregua dell'ordinamento statunitense è dedicato il VII e ultimo allegato.

([45]) Documento di lavoro dei servizi della Commissione sull'applicazione della Decisione 520/2000/CE della Commissione, del 26 luglio 2000, a norma della Direttiva 95/46 del PE 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, Bruxelles 13 febbraio 2002, SEC (2002) 196.

([46]) Documento di lavoro dei servizi della Commissione sull'applicazione della Decisione 520/2000/CE sull'adeguatezza della protezione dei dati personali offerta dai principi di approdo sicuro e dalle relative «domande più frequenti» pubblicate dal Dipartimento del commercio degli Stati Uniti, Bruxelles 20 ottobre 2004, SEC (2004) 1323.

([47]) V. *supra*, par. 4 (e nota 30).

Con le due Decisioni 2001/497 e 2002/16 ([48]), la Commissione ha individuato distinti insiemi di clausole tipo per quanto riguarda il trasferimento di dati personali a responsabili e, rispettivamente, ad incaricati del trattamento ubicati all'esterno dell'Unione. In entrambi le ipotesi le clausole sono stipulate tra un esportatore di dati, situato in un Paese UE, ed un importatore — responsabile o rispettivamente incaricato del trattamento — situato in un Paese terzo che non prevede una tutela adeguata. Nel primo caso, il responsabile deve obbligarsi a rispettare quei principi elencati all'appendice 2 della Decisione 2001/497, che costituiscono «il nucleo di riferimento della valutazione [...] del livello di tutela degli ordinamenti dei paesi extracomunitari» ([49]). Si tratta degli stessi principi che la Commissione usa per verificare *ex* art. 25 l'adeguatezza o meno della tutela dei dati garantita da ordinamenti giuridici di Stati terzi: finalità limitata, qualità e proporzionalità dei dati, trasparenza, accesso, limiti al trasferimento successivo.

Le decisioni in esame tolgono agli SM la facoltà di giudicare garanzie non adeguate le clausole contrattuali previste da tali insiemi; non impediscono però agli stessi di avvalersi dei poteri loro attribuiti dalla Direttiva 95/46 per proibire o sospendere il flusso di dati verso specifici Stati terzi (art. 4 di entrambe le decisioni) in determinati casi, informandone la Commissione che a sua volta avvisa gli altri SM. Ciò in particolare ([50]) quando risulti che la legislazione dello Stato terzo obbliga l'importatore ad applicare ai principi di tutela dei dati deroghe «eccedenti quelle ritenute necessarie in una società democratica» ([51]).

8. I due strumenti disciplinati dagli artt. 25 e 26 della Direttiva

---

([48]) Decisione 2001/497/CE della Commissione del 15 giugno 2001 relativa alle clausole contrattuali tipo per il trasferimento dei dati a carattere personale verso paesi terzi a norma della Direttiva 95/46/CE, in *G.U.* L 181 del 4 luglio 2001, cui fa seguito la Decisione della Commissione 2004/915/CE del 27 dicembre 2004 che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi, in *G.U.* L 385 del 29 dicembre 2004, e Decisione 2002/16/CE della Commissione del 27 dicembre 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento residenti in paesi terzi, a norma della Direttiva 95/46/CE, in *G.U.* L 6 del 10 gennaio 2002.

([49]) A. GIANNACCARI, *L'ambito di applicazione della legge, l'importazione e l'esportazione di dati personali*, in PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, I, Milano, 2003, pp. 294-295. Nel caso invece sia l'incaricato di trattamento ad aver sede fuori dalla UE, la clausola 5 della Decisione 2002/12 pone solo l'obbligo di garantire l'applicazione di una serie di norme tecniche e di sicurezza.

([50]) Le altre due ipotesi prese in considerazione dall'art. 4 delle Decisioni 2001/497/CE e 2002/16/CE sono: accertamento da parte di un'autorità competente che l'importatore dei dati non ha rispettato le clausole contrattuali, o probabilità di mancato rispetto delle clausole contrattuali tipo, di talché «la prosecuzione del trasferimento comporterebbe un rischio imminente di grave pregiudizio alle persone interessate ai dati».

([51]) La disposizione si riferisce a quegli Stati in cui i poteri della pubblica autorità di agire in deroga alle norme poste a tutela della *privacy* si estendono al di là di quanto prevede l'art. 13 della Direttiva (v. *supra*, par. 2), relativo alle deroghe ed eccezioni al regime garantito dalla Direttiva all'interno del territorio della UE.

95/46 individuano, soprattutto se considerati congiuntamente, una puntuale volontà di applicazione extraterritoriale della disciplina CE. Tale volontà risulta invero non frenata, ma piuttosto esaltata dalla predisposizione di clausole-tipo: consapevole della relativa rarità delle ipotesi di applicazione dell'art. 25, la Commissione affida alle imprese il compito di garantire la corretta applicazione della normativa CE nei rapporti con l'esterno. Che questa sia l'ambizione della normativa in discorso è stato d'altro canto affermato a chiare lettere a suo tempo dallo stesso garante italiano, che ha parlato ripetutamente di un modello europeo che «si pone come punto di paragone fuori dall'Europa», onde contribuire ad una decisiva evoluzione della difesa della sfera privata «nella partita planetaria in corso» ([52]).

Di per sé non vi è nulla di inaudito o di sorprendente in tale manifestazione di unilateralismo: per non andare distanti nel tempo, risale a pochi anni prima, al periodo cioè precedente l'accordo di Marrakesh sull'OMC, la pretesa degli Stati Uniti di applicazione da parte degli Stati dell'Asia orientale degli *standard* di tutela della proprietà intellettuale vigenti nell'ordinamento giuridico interno della superpotenza, pretesa accompagnata dalla minaccia di ricorso a (e talora dall'applicazione di) sanzioni commerciali unilaterali ([53]). La novità significativa sta piuttosto nel «chi», l'Unione europea cioè, pretende di ergersi a protagonista della stagione dell'unilateralismo nel campo della protezione dei dati. Se era tradizionalmente la posizione di egemonia economica americana a creare «esternalità» che richiedevano agli altri Stati risposte politiche per difendersi dall'impatto extraterritoriale degli strumenti di politica interna USA, ora «*the reversal of this pattern has not gone unnoticed*» ([54]).

Il tentativo europeo di esportare i propri *standard* di tutela dei dati ha causato un ampio dibattito tra gli studiosi americani. Certo, in dottrina è prevalsa, soprattutto in una prima fase, una certa irritazione nei confronti della pretesa CE, giudicata irrealistica ([55]). Non mancano peraltro posizioni differenti. In particolare vi è chi ha plaudito all'iniziativa comunitaria:

([52]) Nel discorso di presentazione della Relazione per l'anno 2000 del garante per la *privacy* (consultabile *on-line* al sito *www.privacy.it*) si legge testualmente: «Il modello europeo di protezione dei dati personali, infatti, ha ormai superato i confini dell'Unione e ispira le legislazioni dei Paesi più diversi [...]».

([53]) Su tale fase (che investe i rapporti degli SU con Corea del Sud, Repubblica popolare cinese, Taiwan, Thailandia) v. L. Zagato, *Sul trattamento dei PVS in materia di diritto d'autore*, in L. Forlati e L. Zagato (a cura di), *Cultura e innovazione*, Milano, 2000, pp. 51-60.

([54]) C.-J. Bennett, *Privacy Self-Regulation in a Global Economy: a Race to the Top, the Bottom or Somewhere else?* (Atti delle 22ª Conferenza internazionale sulla *privacy* e la protezione dei dati personali, Venezia, 28-30 settembre 2000).

([55]) Capace tuttavia di forzare lo Stato egemone a negoziare quanto meno un'interpretazione meno rigida di tali *standard*: v. J. Fromholz, *The European Union Data Protection Directive*, riportato, in A. Giannaccari, *L'ambito di applicazione...*, cit., p. 266. Per una riflessione sulla applicazione extraterritoriale del diritto europeo funzionale alla protezione

si tratta in modo particolare dei fautori di una normativa federale sulla *privacy*, che nella disciplina comunitaria hanno trovato un punto d'appoggio anche politico — opportunità di non lasciare il monopolio normativo alla UE in una materia tanto delicata — per le loro tesi ([56]).

9. È giunto il momento, prima di approfondire le successive vicende del tentativo di applicazione extraterritoriale della disciplina prevista dalla Direttiva 95/46, di analizzare più in profondità la natura dei due strumenti in discorso.

Sotto il profilo formale sembrerebbe non risultare alcuna differenza: in entrambi i casi — si tratti di misure prese *ex* art. 25, par. 6, come di misure *ex* art. 26, par. 2 — ci troviamo di fronte a decisioni della Commissione rivolte agli Stati membri, decisioni che pongono fine ad un parallelismo imperfetto delle competenze tra SM e istituzioni della Comunità. Qui però la corrispondenza si interrompe.

La decisione *ex* art. 26, par. 2 è effettivamente ciò che pretende di essere: una misura amministrativa interna a forte rilevanza internazionale, idonea, come tale, a consentire alla Comunità di aggirare ostacoli insormontabili posti dalla legislazione di determinati Stati terzi, contribuendo così a raffreddare eventuali rischi di confronto con tali Stati ([57]). Anche il ricorso da parte comunitaria a modelli contrattuali per lo svolgimento di politiche comunitarie è ben conosciuto, a partire da quel *Model Contract* (di ricerca) che ne è stato l'antesignano ([58]). La principale novità consiste in ciò che nel caso oggetto di questo studio il modello contrattualistico è proiettato all'esterno, è volto cioè a conseguire con strumenti privatistici quel farsi largo, non altrimenti conseguibile, di misure affermatesi in ambiente giuridico comunitario in ambienti giuridici affatto estranei. Due ulteriori considerazioni si impongono allora.

In primo luogo, l'art. 26, par. 2 lascia comunque aperta la possibilità per esportatore ed importatore dei dati di fissare autonomamente per

dei diritti umani, v. L. Picchio Forlati, *Critères de rattachement et règles d'applicabilité, à l'heure de la protection des droits de l'homme en Europe*, in *RDIPP*, 2005, p. 953 ss.

([56]) Per un qualificato esempio di tale posizione v. J. Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, in *EJIL*, 2000, p. 135 ss. A detta dell'autore l'unilateralismo, nell'attuale stadio del flusso di dati nelle relazioni transfrontaliere, è destinato a pagare comunque. L'esempio UE non ha comunque trovato seguito, per il momento, a livello federale, quanto piuttosto a livello di singoli Stati federati, più d'uno dei quali si è dotato negli ultimi anni di normative vincolanti in materia di protezione dei dati.

([57]) Trattasi di un ruolo a grandi linee simile a quello giocato dalle misure *antidumping*. Donde, in entrambi i casi, «la contiguità con la condotta delle relazioni esterne»: L. Zagato, *I diritti della difesa nei procedimenti comunitari* antidumping, in questa *Rivista*, 1999, pp. 727-755 (specie p. 728).

([58]) V. L. Zagato, *La politica di ricerca della Comunità europea*, Padova, 1993, p. 345 ss. D'altro canto, uno studio sulle clausole contrattuali che garantissero un livello di tutela equivalente a quello assicurato dalla Convenzione n. 108 del 1981 — studio non a caso recante la dicitura *Model Contract* — era già stato effettuato dal Consiglio d'Europa nel 1992: v. Coe, *Model Contract to Ensure Equivalent Protection in the Context of Transborder Data Flows with Explanatory Report*, Strasbourg, 2 novembre 1992.

contratto «adeguate garanzie per i diritti dell'interessato», autorizzabili da parte di uno Stato membro; le clausole contrattuali tipo elaborate dalla Commissione costituiscono quindi un modello di riferimento per la definizione contrattuale degli scambi di informazione a carattere transnazionale, che lascia all'autonomia dei privati uno spazio tanto più sfruttabile quanto più particolare od episodica sia la vicenda contrattuale soggiacente. Nel caso invece di applicazione continuativa e professionale dello scambio, gli operatori economici del settore troveranno conveniente ricorrere alle clausole tipo, onde avvalersi della non contestabilità (nei limiti sopra indicati) del contratto che le incorpori.

In secondo luogo, rigore formale e articolazione del corpo di disposizioni contenuto nello schema contrattuale stabilito dalla Commissione, inducono l'interprete a chiedersi se non si sia in presenza della tipicizzazione legislativa di una figura di contratto (transnazionale) di trasferimento di dati. Ad una tale constatazione non sarebbe certo opponibile la particolare e più limitata finalità dei due atti — le Decisioni 2001/497 e 2002/16 cioè — i cui allegati individuano le varianti di tale contratto tipico. Poiché invero «specifiche esigenze si rinvengono sempre [...] all'origine dei processi di tipicizzazione» (59), nulla osta, in principio, a che la tipicizzazione legale possa essere provocata dall'esigenza di assicurare un determinato livello di tutela nella trattazione dei dati all'esterno della CE (60). È quanto fornisce una conferma, quantomeno, della necessità di approfondire, negli studi sul diritto europeo dei contratti, il problema delle basi giuridiche di tale diritto nell'ordinamento interno della Comunità europea: argomento spesso sottovalutato, quasi tali basi giuridiche andassero senz'altro ricondotte alla sola direttiva d'armonizzazione *ex* art. 95 TCE, e non fossero invece rinvenibili in una ampia gamma di atti, vincolanti come di *soft law*, di cui le istituzioni comunitarie dispongono (61).

10. Con il procedimento *ex* art. 25, par. 6 siamo invece proiettati in un diverso scenario. In tutti i casi esaminati — Argentina, Canada, Svizzera, Stati Uniti — emerge un incontro tra le volontà dei soggetti internazionali interessati.

Nei primi tre casi, l'incontro di volontà si manifesta attraverso una articolazione di comportamenti: a monte vi è una revisione della legislazione (e della prassi amministrativa) interna da parte degli organi a ciò deputati degli Stati terzi, che prende a riferimento la Direttiva 95/46; al

(59) L. ZAGATO, *Il contratto comunitario di licenza di* know-how, Padova, 1996, p. 88.

(60) La particolare esigenza che spinge il legislatore «a predisporre una regolamentazione positiva di un dato contratto, sino a quel punto solo socialmente tipico, non è indice della angustia di valutazione, bensì spia dell'esigenza in contemplazione della quale la tipicizzazione legale è operata»: così U. PERFETTI, *La tipicità del contratto di* franchising, in *Quadr.*, 1991, p. 54.

(61) Per una prima indagine in tal senso, L. ZAGATO, *Il contratto comunitario...*, cit., *passim*.

momento conclusivo di tale revisione corrisponde l'emanazione, nell'ordinamento interno della Comunità, della Decisione di adeguatezza di tale legislazione da parte dell'organo amministrativo CE. Il parallelismo tra i comportamenti assunti nei rispettivi ordinamenti interni da CE e Stati terzi, parallelismo che si concreta nell'emanazione di atti normativi e provvedimenti amministrativi tra loro congrui — e al quale si affianca una fitta attività diplomatica, pur destinata a rimanere sullo sfondo — consente di individuare nel giudizio di adeguatezza *ex* art. 25, par. 6 il momento conclusivo di un accordo internazionale per comportamento concludente tra CE e Stati in esame (62). Tale accordo prevede il conformarsi, nella materia, dell'*environment* giuridico di detti Stati a quello comunitario, onde entrare a far parte del *continuum* di flusso di dati da e per la CE, potendo contare sulla non interruzione di tale flusso a causa di iniziative degli apparati statuali degli SM operanti *uti singuli* (63).

Considerazioni in larga misura convergenti vanno svolte per i principi dell'approdo sicuro. A tale riguardo la dottrina non ha mai messo seriamente in discussione la presenza di un accordo internazionale (64), aiutata in questo da un più esplicito manifestarsi del profilo sinallagmatico, oltre che dalla terminologia ondivaga cui ha fatto ricorso il *Gruppo* ex *art. 29*: in almeno un'occasione questo si è riferito ai risultati delle trattative CE/SU con il termine *Arrangement*, destinato a sparire nei successivi pareri (65). Non è naturalmente dato sapere se ci sia stato un momento in cui le due Parti — CE e SU — abbiano valutato l'eventualità che l'incontro delle rispettive volontà dovesse risultare da un Accordo scritto, con ogni probabilità in forma semplificata. Si è alla fine fatto ricorso allo stesso procedimento utilizzato nei casi dianzi analizzati: una serie di atti di approssimazione progressiva a quanto richiesto dalla CE posti in essere dalle autorità amministrative degli Stati Uniti, all'ultimo dei quali corrisponde, nell'ordinamento interno della UE, l'emanazione della Decisione 2000/520 (66).

Piuttosto, è il contenuto dell'accordo sull'approdo sicuro tra UE e SU a risultare diverso dai precedenti. Le autorità americane si impegnano solo a mettere gli operatori privati che lo vogliano in grado di ottemperare ad un complesso di regole e principi profondamente estranei all'ordinamento giuridico di quel Paese e ad esercitare un controllo assai *soft* sui compor-

(62) Ciò per la libertà della forma degli accordi consentita dal diritto internazionale. Sull'argomento: Lord MCNAIR, *The Law of Treaties*, Oxford, 1961, p. 6 ss.; R. QUADRI, *Diritto internazionale pubblico*, 5ª ed., Napoli, 1968, p. 162 ss.; L. ZAGATO, *Sul trattamento dei PVS...*, cit., pp. 53-54.

(63) Fatti salvi naturalmente i casi di applicazione dell'art. 13: v. *supra*, par. 2.

(64) Non senza cadere in qualche ingenuità: v. per tutti A. GIANNACCARI, *op. cit.*, p. 277: dopo aver parlato di «accordo noto con il nome di "*Safe Harbour*"», l'autore specifica in nota: «l'accordo è stato ratificato (*!*) con la decisione della Commissione del 26 luglio 2000».

(65) V. parere 3/2000 (*supra*, nota 44).

(66) La corretta sequenza non sfugge a A. MANTELERO, *Attività di impresa in Internet e tutela della persona*, Padova, 2004, pp. 215-216.

tamenti di tali operatori. L'effettivo monitoraggio sulla prassi delle imprese che dichiarino di optare per l'applicazione dei principi dell'approdo sicuro è in pratica demandato alla CE. In cambio la stessa CE riconosce la rispondenza dei principi dell'approdo sicuro ai propri *standard* interni di protezione dei dati. Gli obblighi assunti dalla controparte nei confronti della CE con l'accordo in discorso sono assai meno penetranti, per concludere, di quanto siano stati invece per Argentina, Canada, Svizzera.

III. *Reazioni all'unilateralismo CE.*

11. L'iniziativa della CE volta ad assicurare l'applicazione extraterritoriale della propria normativa sulla *privacy* ha incontrato da subito gravi difficoltà: dovute, per un verso, alle resistenze che lo schema fondato sull'art. 25 incontra una volta giunto a contatto con l'ambiente giuridico USA, ed al tentativo di rigetto che quest'ultimo ambiente riproduce di continuo per forza naturale. Per l'altro verso, le clausole modello della direttiva hanno innescato una vera e propria sollevazione da parte di un blocco di soggetti transnazionali guidati dalla Camera di Commercio Internazionale (ICC) di Parigi, blocco che ha goduto inoltre dell'appoggio di alcuni importanti Stati membri della Comunità europea.

Cominciando dalle prime, l'adeguatezza del principio dell'approdo sicuro a garantire un trattamento di dati di cittadini CE in linea con la normativa vigente nel mercato interno è stata al centro di forti polemiche; ciò non solo nel periodo iniziale ([67]), a ridosso cioè dell'emanazione della Decisione 2000/520, ma anche in seguito. All'origine di tali polemiche troviamo la radicale divergenza della disciplina dei dati personali tra le due sponde dell'Atlantico ([68]), come pure il rigore insoddisfacente con cui, a giudizio della Commissione ([69]), le autorità americane avrebbero esercitato i loro obblighi di controllo.

Orbene: malgrado ciò, e ad onta di previsioni ampiamente negative, i principi dell'approdo sicuro stanno avendo successo. Se nel periodo immediatamente successivo alla Decisione 2000/520 erano stati infatti pochi gli operatori americani che si occupano del trattamento di dati ad aver autocertificato la conformità della propria politica di *privacy* ai *Safe Harbour Principles*, alla fine del 2003 il numero ha raggiunto la cifra di

([67]) V. Relazione per l'anno 2001 del Garante per la protezione dei dati personali, p. 93.

([68]) Su tali fenomeni non è possibile in questa sede soffermarsi. Per un quadro d'insieme v. A. ETZIONI, *The Limits of Privacy*, New York, 1999, pp. 1-288, e C. SHAPIRO e H.R. VARIAN, *US Government Information Policy*, Berkeley, 1997, *passim*.

([69]) V. il documento di lavoro dei servizi della Commissione dell'ottobre 2004, sottoposto al Comitato di cui all'art. 31 della Direttiva 95/46: *supra*, par. 3.

400, per superare ampiamente il migliaio all'inizio del 2008 ([70]). Non è un trionfo, ma si tratta di un numero significativo ([71]).

12. Veniamo a quella che si è definita una vera e propria «sollevazione» ([72]), formalmente in nome del rilancio di un modello di autoregolamentazione, contro le clausole contrattuali tipo elaborate sulla base dell'art. 26, par. 4 ([73]) dalla Commissione. Onde dare conto della intensità delle critiche, giova intanto inquadrare brevemente taluni profili del contenuto delle clausole in esame.

Il contratto tra esportatore ed importatore di dati nel Paese terzo deve in particolare contenere sempre — art. 3 delle Decisioni 2001/497 e 2002/16 — la clausola c.d. del *terzo beneficiario*. Ciò perché il soggetto interessato dal trattamento ([74]) è estraneo all'accordo tra i due operatori e «in quanto tale, in assenza dell'apposita disposizione non potrebbe far valere, anche per via giudiziale, il proprio diritto alla correttezza del trattamento» ([75]). In particolare l'interessato, come terzo beneficiario, può chiedere l'osservanza di una serie di obblighi che incombono sia sull'esportatore ([76]) che sull'importatore ([77]) e far valere la responsabilità che ricade sugli stessi, separatamente ed in solido, per violazione di qualsiasi obbligo

([70]) I dati al sito *www.export.gov/safeharbor*, consultato l'ultima volta il 10 luglio 2008. Il dato è reso più significativo dal fatto che, ad esempio, il gruppo *General Motors* con tutte le sue affiliate e filiali dentro e fuori gli SU (comprese Australia e Taiwan) conta per uno. La concentrazione delle adesioni in determinati Stati — California,, NY, Massachussets, Texas, Florida, Illinois, Pennsylvania, New Jersey, Washington, Virginia e Georgia — richiederebbe poi un approfondimento *ad hoc*.

([71]) Osservando la suddivisione per comparti produttivi, se i servizi fanno la parte del leone, i risultati forse più interessanti si hanno nel settore industriale: ad una pressocché totale assenza di autocertificazioni nei settori tradizionali (carbone, acciaio, macchine utensili) corrisponde una forte presenza nella lista dei settori informatico, biotecnologico e chimico-farmaceutico.

([72]) V. *supra*, par. 11.

([73]) Ancora *supra*, par. 7.

([74]) Rappresentato eventualmente da un'associazione, sempre che tale rappresentanza sia ammessa dalla legge nazionale dell'interessato.

([75]) A. MANTELERO, *I flussi transfrontalieri di dati personali: l'effetto delle politiche comunitarie*, in *Contr. impr./Eur.*, 2002, p. 1304.

([76]) V. clausola-tipo n. 4, *Obblighi dell'esportatore di dati*: tali obblighi hanno ad oggetto, oltre naturalmente al rispetto delle leggi dello Stato membro in cui l'esportatore ha sede, l'informazione dell'interessato (al più tardi al momento del trasferimento) circa l'eventualità che i dati sensibili vengano trasmessi in uno Stato terzo che non fornisce adeguata tutela, la «messa a disposizione, a richiesta delle persone interessate» di copia delle clausole, la risposta a qualsiasi richiesta dell'interessato — nonché delle autorità di controllo degli SM — circa il trattamento dei dati ad opera dell'importatore degli stessi.

([77]) V. clausola-tipo n. 5, *Obblighi dell'importatore di dati*: l'importatore deve garantire che la legge applicabile nel suo caso non gli impedisce di adempiere ad obblighi contrattuali (l'obbligo comprende quello di dare immediata notizia all'esportatore in caso di sopravvenuta modifica di legge), garantire che il trattamento avvenga in conformità agli *standard* applicabili nel Paese in cui l'esportatore dei dati ha sede, rispondere a tutte le richieste ragionevoli dell'interessato e dell'esportatore e collaborare con le competenti autorità di controllo nel caso di indagini, fornire su richiesta agli interessati copia delle clausole stipulate ed indicare la sede competente per eventuali reclami. L'importatore deve inoltre accettare di sottoporre a controllo i propri servizi di trattamento su richiesta dell'esportatore;

assunto nei suoi confronti (78); può inoltre, nel caso di controversia non passibile di soluzione amichevole, scegliere l'istanza cui demandare la soluzione (79), nonché avvalersi delle clausole relative alla scadenza (80) ed alla modifica del contratto. A chiusura del sistema, la clausola-tipo n. 10 della Decisione 2001/497 (clausola 9 della Decisione 2002/16) stabilisce che la legge applicabile sia sempre quella dello Stato in cui ha sede l'esportatore di dati.

13. Proprio la rigidità dei due insiemi di clausole-tipo offerti dalle Direttive 2001/497 e 2002/16 ha unito nello scontento imprese multinazionali statunitensi ed europee, organizzazioni economiche transnazionali e internazionali.

Tale sollevazione si è manifestata nelle dure critiche espresse dai Ministeri del Commercio e dei trasporti degli USA, così come dalla ICC (81) e dalla *Global Privacy Alliance* (GPA) (82), nonché da varie associazioni professionali su entrambe le sponde dell'Atlantico. Il momento in cui

---

tale controllo avverrà ad opera dell'esportatore, o di un ente ispettivo indipendente qualificato selezionato dall'esportatore e «ove necessario, di concerto con le autorità di controllo».

(78) V. Decisione 2001/497, clausola-tipo n. 6, *Responsabilità*: le parti convengono che le persone interessate che abbiano subito pregiudizio dalle operazioni di trattamento e trasferimento dei dati hanno diritto ad indennizzo (par. 1); esportatore ed importatore sono responsabili separatamente ed in solido, mentre la persona interessata può citare in giudizio anche uno solo di loro. Il par. 3, facoltativo, stabilisce che se una delle parti viene riconosciuta responsabile di una violazione commessa dall'altra, «la seconda delle parti indennizza la prima per ogni costo, onere, danno, spesa o perdita sostenuta dalla prima, nei limiti che le sono imputabili». Per il caso invece in cui il trattamento fuori dalla UE sia svolto da un semplice incaricato, la Decisione 2002/16 stabilisce che l'importatore divenga responsabile nel caso di sparizione dell'esportatore. L'esportatore può essere «scomparso di fatto» o avere cessato di esistere giuridicamente, o essere divenuto insolvente.

(79) V. clausola-tipo n. 7, *Mediazione e giurisdizione*: importatore ed esportatore si impegnano ad accettare la decisione delle persone interessate di avvalersi della mediazione di un terzo indipendente o dell'autorità di controllo, oppure di deferire la controversia all'autorità giudiziaria dello SM in cui ha sede l'esportatore. La risoluzione della controversia può anche essere deferita, di comune accordo tra la persona interessata e la sua controparte, ad un organo arbitrale avente sede in un Paese ratificante della Convenzione di NY sul riconoscimento e l'esecuzione dei lodi arbitrali.

(80) V. clausola-tipo n. 9, *Scadenza delle clausole*: «Le parti convengono che la scadenza delle presenti clausole, in qualsiasi circostanza e per qualsiasi motivo, non esonera le parti stesse dagli obblighi e/o condizioni di cui alle clausole stesse per quanto riguarda il trattamento dei dati trasferiti».

(81) In pressocché aperto contrasto con il testo della Direttiva 95/46 questa aveva elaborato già nel 1998 le *Model Clauses for Use in Contracts Involving Transborder Data Flows*, Parigi, 23 settembre 1998. Trattavasi peraltro di una rielaborazione, alla luce (e in polemica) con la Direttiva 95/46 del risalente *Model Contract* del Consiglio d'Europa. Il *Model Contract*, che si richiamava esplicitamente ai principi contenuti nella Direttiva 108/81 del COE, era stato infatti elaborato congiuntamente, nel 1992, da COE, Camera di Commercio internazionale di Parigi e Commissione delle Comunità europee. V. *supra*, nota 58.

(82) La GPA ha in particolare presentato un duro documento alla *Conference on the Implementation of Directive 95/46/CE*, tenutasi a Bruxelles nei giorni 30 settembre-1° ottobre 2002. Sull'attività lobbystica svolta dalla GPA per ottenere un abbassamento del livello di protezione dei dati anche *all'interno* della UE, e sul relativo dibattito, v. A. Mantelero, *Attività di impresa...*, cit., p. 219. Cfr anche i siti *http://news.zdnet.co.uk* e *www.reuters.co.uk* (in relazione alle notizie pubblicate nell'autunno 2002).

l'ondata di rigetto della normazione ha avuto maggior forza coincide con la presentazione, nel corso del 2002, della proposta di modifica alla Direttiva 95/46 da parte di quattro Stati membri: Austria, Finlandia, Regno Unito e Svezia. Elemento qualificante di detta proposta era l'inserzione, nell'art. 26, par. 4 della Direttiva, dell'espressione «o altri strumenti» per indicare la possibilità della Commissione di avvalersi, in alternativa alle clausole contrattuali tipo, di strumenti diversi per decidere dell'esistenza di garanzie adeguate per il trasferimento di dati verso l'esterno della UE (83). Ai sensi della nota esplicativa che accompagnava la proposta di modifica, per «altri strumenti» si dovevano intendere (punto 28) appositi codici di condotta introdotti dalle società che si occupano del trattamento di dati (84).

Nel corso del successivo dibattito i fautori di un ricorso più ampio all'autoregolamentazione da parte delle organizzazioni che trattano dati hanno richiamato, oltre alle difficoltà legate all'applicazione ad Internet della disciplina sul trasferimento transfrontaliero di dati, i problemi posti dal trasferimento dei dati all'esterno della UE quando lo stesso abbia luogo nell'ambito delle attività di imprese facenti parte dello stesso gruppo. Su quest'ultimo problema, in effetti, la Direttiva 95/46 è completamente silente.

All'offensiva in esame è stata opposta, da parte delle istituzioni comunitarie, così come della dottrina maggioritaria, la sostanziale inanità delle garanzie offerte dai codici di condotta, ove manchi il controllo di apposite autorità sul contenuto e, soprattutto, sull'applicazione delle misure di autoregolamentazione; donde il carattere solo integrativo di simili strumenti (85).

14. La ribellione contro le clausole tipo ha trovato soluzione, per un verso, con la Decisione 2004/915 del 27 dicembre 2004, relativa ad un insieme alternativo di clausole contrattuali tipo (86); per l'altro verso con l'individuazione, ad opera del *Gruppo* ex *art. 29*, dei criteri per l'applicazione della Direttiva 95/46 al trasferimento internazionale di dati all'interno di gruppi transnazionali (87).

---

(83) Ove la Commissione decida, secondo la procedura di cui all'art. 31, par. 2 della Direttiva, che, «*certain standard contractual clauses or other instruments offer sufficient adequate safeguards [...], Member States shall take the necessary measures to comply with the Commission's decision*».

(84) *Data Protection Directive (95/46/EC) Proposals for Amendment Made by Austria, Finland, Sweden and the United Kingdom Explanatory Note*, consultabile al sito *http://pi.gn.apc.org/intl#orgs/en*.

(85) V. per tutti S. Simitis, *Il contesto giuridico e politico della tutela della* privacy, in *Riv. cr. dr. priv.*, 1997, pp. 563-581, *passim*, in specie p. 570.

(86) V. *supra*, nota 48.

(87) *Gruppo di lavoro* ex *art. 29* in tema di protezione dei dati, *Working Documents: Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, adottato il 3 giugno 2003 (*WP 74*); *Establishing a Model Checklist Application for Approval of Binding Corporate Rules*, approvato il 14 aprile 2005; *Setting Forth a Co-Operation Procedure for*

Va esaminata dapprima la soluzione data a questo secondo problema. Già nel 2003 il Gruppo si esprimeva con favore circa la possibilità di consentire, accanto ad altri strumenti di cui agli artt. 25-26, l'emanazione da parte dei gruppi multinazionali di codici di condotta per il trasferimento internazionale dei dati tra tutte le imprese che ne facciano parte: il Gruppo dichiarava peraltro a tale riguardo di preferire l'espressione *Norme vincolanti d'impresa* (*Binding Corporate Rules*) a quella, meno puntuale, di *codici di condotta* (88). Tali norme sono da valutare alla stregua del criterio delle «garanzie sufficienti» di cui all'art. 26, par. 2 della Direttiva 95/46, fermo restando che non sussiste al riguardo quel parallelismo asimmetrico tra competenze degli SM e competenze della Commissione altrimenti caratterizzante gli artt. 25-26. La Commissione non può, cioè, emanare decisioni vincolanti, e le singole autorità nazionali di protezione dei dati restano libere di lasciare o meno operare nel loro territorio le *Norme vincolanti d'impresa*; donde un'accresciuta centralità del ruolo giocato dal *Gruppo* ex *art. 29* nella definizione di un atteggiamento omogeneo delle autorità degli SM. A parere del Gruppo è in particolare sotto il profilo dell'esecuzione che va operata una distinzione, all'interno di un sistema di regole applicabili per definizione su scala globale, tra le informazioni in genere e quelle aventi origini nella UE e da lì trasferite in un Paese terzo. L'attenzione del Gruppo si concentra di conseguenza sulla *legal enforceability* delle norme da parte dei soggetti interessati, individuando il contenuto necessario delle regole in esame (89) in una serie di previsioni a favore del terzo corrispondenti grosso modo a quelle presenti nella Decisione 2001/947, e nella presenza di impegni alla collaborazione con le autorità nazionali di protezione dei dati, oltre che nel rispetto dei principi generali di cui al *WP 12* (90).

15. La Decisione 2004/915 fa seguito, dal canto suo, ad un'iniziativa presa dalla ICC in collaborazione con una serie di organizzazioni imprenditoriali transnazionali; lasciata cadere la proposta di autoregolamentazione, queste presentavano nel corso del 2003 una proposta di clausole

Issuing Common Opinions on Adequate Safeguards Resulting from «Binding Corporate Rules», approvato il 14 aprile 2005.

(88) La nozione di *codice di condotta* nell'accezione in discorso differisce invero da quella, di cui all'art. 27 della Direttiva 95/46 (codici elaborati da organizzazioni professionali, ecc: v. *supra*, par. 2), con la quale spartirebbe peraltro — *WP 74* punto 4 — almeno una caratteristica: entrambe *«are supposed to overcome the level of abstraction of the legislation [...] the corporate rules should contain tailormade provisions as well as a reasonable level of detail in the description of the data flows, purposes of the processing, etc.»*. Sui codici di condotta nel diritto commerciale internazionale, v. per tutti F. Galgano e F. Marrella, *Diritto del commercio internazionale*, 2ª ed., Padova, 2007, p. 237 ss. (ampia bibliografia ivi).

(89) Il successivo strumento di lavoro dedicato alla procedura di cooperazione, del 18 aprile 2005, contiene le disposizioni cui l'impresa multinazionale deve sottostare per individuare l'autorità nazionale di protezione dei dati destinata a fungere da *leading authority* nella procedura di cooperazione richiesta per l'autorizzazione.

(90) A loro volta riprodotti all'Appendice 2 della decisione 2001/497 (v. *supra*, par. 7).

contrattuali alternative (91), profondamente modificato nel corso delle consultazioni, anche a seguito delle critiche apportate dal *Gruppo di lavoro* ex *art. 29* (92). Da queste ultime è opportuno prendere le mosse.

Nel suo parere il *Gruppo* ex *art. 29* aveva notato il persistere di tre gravi lacune nella proposta, pur modificata, che gli era stata presentata, lacune relative rispettivamente all'obbligo di cooperazione con le autorità per la tutela dei dati, alle restrizioni del diritto d'accesso e al sistema di responsabilità (93). Nel primo caso il Gruppo lamenta l'indebolimento degli obblighi di cooperazione dell'importatore dei dati con le autorità per la tutela dei dati nella UE (94): indebolimento netto, perché non sostenuto da alcuna proposta alternativa, ispirata — in ipotesi — alle insistite richieste di meccanismi flessibili di composizione delle controversie (95).

Quanto all'accesso, va premesso che, come per le clausole tipo, anche per l'insieme di clausole alternative valgono i principi vincolanti da leggere alla luce delle disposizioni della Direttiva 95/46; orbene, l'art. 12 di quest'ultima impone ai responsabili del trattamento la concessione di un ampio diritto di accesso (96). È ben vero che il successivo art. 13 autorizza gli SM ad emanare misure legislative limitative di un tale diritto nel caso in cui ciò risulti necessario, *inter alia*, ai fini «della protezione della persona interessata o dei diritti e delle proprietà altrui». Una simile decisione è rimessa peraltro al legislatore dello SM, non all'organizzazione che tratta i

(91) Tale insieme alternativo è «destinato ad offrire un livello di protezione di dati comparabile a quello offerto dall'insieme di clausole adottato dalla decisione 2001/497/CE»: così il considerando 2 della Decisione 2004/915. Il consorzio di imprese che segue l'iniziativa della ICC è composto da *Japan Business Council in Europe* (JBCE), *European Information and Communication Technology Association* (EICTA), *EU Committee of the American Chamber of Commerce in Belgium* (AMCHAM), *Confederation of British Industry* (CBI), *International Communication Round Table* (ICRT) e *Federation of European Direct Marketing Associations* (FEDMA).

(92) *Gruppo di lavoro* ex *art.* 29 per la tutela dei dati personali: Parere 8/2003 sul progetto di clausole contrattuali tipo presentato da un gruppo di organizzazioni commerciali («il contratto modello alternativo») del 17 dicembre 2003.

(93) Il Gruppo sottolinea come, malgrado le organizzazioni proponenti avessero a suo tempo giudicato impraticabili le clausole tipo della Commissione, l'insieme alternativo proposto non differisca molto dalle clausole tipo di cui alle Decisioni 2001/497 e 2002/16: è solo più impreciso dal punto di vista della terminologia giuridica. In ogni caso, visto che il risultato finale viene quasi a coincidere con le clausole tipo della Commissione, si può ben dare un parere favorevole [...] dopo che saranno stati modificati i tre punti che danno luogo ad insuperabile perplessità da parte del Gruppo stesso.

(94) Secondo la proposta di clausole alternative, le autorità di tutela sui dati degli SM possono aspettarsi al più «una collaborazione in buona fede nelle risposte alle indagini sul trattamento dei dati personali». Verrebbero meno gli obblighi (clausola 5 della Decisione 2001/497) di sottoporre a controllo i propri servizi di trattamento su richiesta dell'esportatore di dati e di attenersi al parere dell'autorità di controllo per quanto riguarda il trattamento dei dati.

(95) Sul genere di quelle avanzate dalla GPA. Da notare che lo stesso Gruppo propone invano che siano le organizzazioni commerciali interessate a svolgere il ruolo di arbitri qualificati «nell'individuazione delle misure disciplinari contro quelle società che non onorino i propri obblighi sulla tutela dei dati».

(96) V. *supra*, par. 2.

dati: tra i motivi che la giustificano non può certo essere fatto rientrare il pregiudizio degli interessi economici di quest'ultima.

Più cauto è l'approccio del Gruppo al terzo punto, quello del sistema di responsabilità; ciò perché lo stesso Gruppo conviene in questo caso sul carattere gravoso del sistema di responsabilità cumulativa stabilito dalle clausole tipo. Con alcuni accorgimenti, il sistema di responsabilità sussidiaria proposto potrebbe allora risultare funzionale ([97]): andrebbe tuttavia chiarito l'effettivo campo di applicazione della responsabilità sussidiaria dell'esportatore per le inadempienze dell'importatore di dati (*culpa in eligendo*). Le clausole alternative dovrebbero inoltre specificare che l'importatore accetta di essere citato in giudizio nella Comunità da parte della persona interessata nell'esercizio dei diritti di terzo beneficiario ([98]). Il rifiuto dell'importatore di ottemperare ai propri obblighi ai sensi del contratto ([99]) dovrebbe infine costituire prova di mancato rispetto dell'insieme di clausole alternativo, tale da giustificare la sospensione del trasferimento di dati ai Paesi terzi in discorso ad opera delle autorità nazionali di controllo.

La Decisione 2004/915 prende atto delle ulteriori modifiche introdotte nel testo dopo le critiche del Gruppo e conclude che le garanzie offerte sono sufficienti ai sensi dell'art. 26, par. 2. Ciò malgrado solo sul terzo punto, quello per cui la distanza iniziale tra le parti era minore, le modifiche introdotte appaiano effettivamente in linea con le richieste del *Gruppo* ex *art. 29*. Le disposizioni sul diritto di accesso in particolare sembrano ancora inadeguate, rispetto all'impianto della Direttiva 95/46 e nel confronto con le clausole tipo di cui alla Decisione 2001/497.

Resta in ogni caso che le soluzioni offerte dall'insieme alternativo, malgrado il clima polemico in cui l'iniziativa ha avuto origine, presentano in definitiva carattere integrativo, e non certo alternativo al *corpus* di regole elaborato dalla Comunità.

16. In conclusione. Né i principi dell'approdo sicuro né l'insieme alternativo costituiscono una battuta d'arresto della tendenza all'applicazione extraterritoriale della normativa comunitaria; testimoniano, al contrario, una sua effettiva capacità di imporsi. È quanto dire che gli operatori internazionali non comunitari che si occupano del trattamento dei dati personali, così come i rispettivi Stati di appartenenza, hanno preso estremamente sul serio la minaccia di bloccare l'esportazione dei dati dalla Comunità. L'unilateralismo perseguito dalla UE in materia di protezione dei dati sembra proseguire, fino a questo punto, il suo percorso vittorioso. L'impiego delle clausole tipo — particolarmente appetibile per quelle imprese aventi sede in Nordamerica e che trattano non occasionalmente dati provenienti dalla UE, ma con destinazione finale in Paesi diversi, in particolare dell'Asia orientale ([100]) — costituisce uno strumento ulteriore di affermazione del modello comunitario, affidato come questo è a strumenti privatistici.

Tale tendenza risulta rafforzata alla luce delle disposizioni contenute nel progetto di Trattato sul funzionamento dell'Unione europea: assegnando alla tutela dei dati nella UE carattere *lato sensu* costituzionale, questo contribuisce infatti ad irrigidire ulteriormente la pretesa delle norme poste a tutela della *privacy* di vedersi applicate in tutti i frangenti, indebolendo le pretese dell'industria di risolvere il problema tramite ricorso generalizzato a codici di autoregolamentazione.

Un breve sguardo sulle conseguenze dell'unilateralismo UE per l'ambiente giuridico dell'Estremo Oriente conforta le conclusioni raggiunte. Se la Corea del Sud pare tuttora prediligere un ambiente giuridico «americano» per la protezione dei dati ed il Giappone si è dato una normativa che intende collocarsi in una situazione intermedia tra i regimi esistenti sulle opposte sponde dell'Atlantico ([101]), da Hong Kong e da Singapore vengono indirizzi decisamente ispirati all'esperienza normativa comunitaria ([102]); orientamento evidente anche nel progetto malese ([103]). Da tutte le esperienze qui citate trapela la volontà di sfruttare la procedura *ex* art. 25, par. 6 della Direttiva 95/46.

Più in generale, la strategia di «esportazione» della propria legislazione da parte della UE ha in questi anni operato in profondità, non solo resistendo alle controffensive di cui è stata fatta oggetto, ma recuperando, anzi, peso ed importanza negli ambienti giuridici extraeuropei dopo il

([97]) L'esercizio dei diritti del terzo beneficiario da parte della persona interessata si esplicherebbe così in tre fasi: invito all'esportatore a far osservare il contratto all'importatore entro un mese; esecuzione forzata nei confronti dell'importatore di dati; azione sussidiaria nei confronti dell'esportatore per *culpa in eligendo*.

([98]) Di conseguenza una clausola dovrebbe prevedere l'obbligo dell'importatore di dati di dare la prova di possedere risorse finanziarie adeguate ad ottemperare alle proprie responsabilità (eventualmente tramite copertura assicurativa) nella CE.

([99]) Così come il rifiuto dell'esportatore di far osservare il contratto all'importatore entro un mese.

([100]) In tal senso già, alla fine del 2001, il *Memorandum* dal titolo *Implementing the U.S.-EU Data Privacy «Safe Harbour»* della Baker &McKenzie di Chicago, consultabile al sito *www.bakernt.com*.

([101]) Per prime informazioni sulla nuova *Personal Information Protection Law* giapponese, entrata in vigore il 1° aprile 2005, v. P. KALLENTER, *Japan Tightens Personal Data Protection*, consultabile al sito *www.infoworld.com/article/05/03/28/HPjapantightens personaldataprotection#1.html*.

([102]) V. V. LEHDONVIRTA, *European Union Data Protection Directive: Adequacy of Data Protection in Singapore*, in *Singapore Journal of Legal Studies*, 2004, pp. 511-546. L'autore richiama anche la situazione di Hong Kong, in particolare le prese di posizione delle autorità di quel territorio a regime speciale favorevoli ad un adeguamento ai parametri CE.

([103]) Per più aspetti proprio la *Proposal for a Personal Data Law* della Malesia (in *World data Protection Report*, November 2003) costituirebbe, anzi, il progetto più interessante e significativo. Resta che il progetto non ha fatto decisivi passi avanti nell'ultimo periodo; sull'argomento T. KHAW LAKE, *The Proposed Malaysian Personal Data Law. Some Salient Features, on line* al sito *www.ippp.um.edu.my/research*.

2002-2003: dal rilancio dei principi dell'approdo sicuro, al disinnesco dei profili più pericolosi insiti nella proposta dell'insieme alternativo, al rinnovato interesse di cui la disciplina comunitaria è fatta oggetto nell'ambiente giuridico dell'Estremo Oriente. Ciò, ben s'intende, senza sottovalutare i problemi e le ambiguità insite in un ipotetico adeguamento formale al quadro normativo comunitario da parte di regimi politici non sempre attenti alla tutela dei diritti umani ([104]).

È in un siffatto quadro giuridico d'insieme — quadro, si badi, non solo mantenutosi ma in larga misura rafforzatosi dopo l'11 settembre 2001 — che andranno allora approfondite le novità e le eventuali indicazioni in controtendenza, createsi con la scelta di privilegiare, su entrambe le sponde dell'Atlantico, quindi anche da parte della UE, le politiche di sicurezza ([105]) nella materia del controllo dei dati.

([104]) È infatti l'inserimento del diritto alla *privacy* (nel senso di autodeterminazione informativa: v. *supra*, nota 2) nel quadro dei diritti umani che sorregge teoricamente l'intero impianto, giustificando anche i costi imposti agli operatori.

([105]) Su come, con il *Programma dell'Aja* del 2004, gli SM abbiano estrapolato dal Titolo IV l'esistenza di un «autonomo principio di diritto collettivo alla sicurezza dei cittadini della UE, costruendovi attorno una specifica politica, invasiva e trasversale rispetto alle altre», v. L. Zagato, *Le competenze della UE in materia di asilo dopo i Trattati di Amsterdam e di Nizza, e nella prospettiva del Trattato su una Costituzione per l'Europa*, in Id. (a cura di), *Verso una disciplina comune europea del diritto d'asilo*, Padova, 2006, p. 198.