fuori. Il gruppo di lavoro ritiene che una situazione del genere crei un'incertezza giuridica (in particolare per quanto riguarda lo scambio di informazioni all'interno di un'organizzazione) e richieda il chiarimento della nozione di "attività".

Eccezioni ed esenzioni

Il gruppo di lavoro ribadisce la sua preoccupazione che l'adesione ai principi possa essere limitata da un'eventuale "legge, regolamento governativo o giurisprudenza" (paragrafo 5 lettera b) dei principi) senza ulteriore qualifica. Questo sembra applicarsi alle leggi di Stato come pure alle leggi federali, al presente o in futuro. Per garantire la certezza del diritto e la non discriminazione rispetto ad altre constatazioni di adeguatezza, il gruppo di lavoro raccomanda che siano fissati criteri più precisi per tali eccezioni e limitazioni, illustrati da esempi concreti, e che il loro effetto sia adeguatamente preso in considerazione. Per quanto riguarda l'esigenza di criteri più precisi, il gruppo di lavoro raccomanda di effettuare una chiara distinzione tra le opzioni e gli obblighi: l'adesione ai principi dovrebbe essere limitata soltanto nella misura in cui ciò è necessario per adempiere agli obblighi di legge o normativi (che comunque prevarrebbero sui principi) ma non a seguito di opzioni concesse dalla legislazione degli Stati Uniti, poiché questo causerebbe un serio indebolimento dei principi.

Per ragioni di trasparenza e di certezza del diritto, il gruppo di lavoro ritiene essenziale che la Commissione sia informata di ogni statuto o decreto legge che possa influire sull'adesione ai principi.

Per quanto riguarda il paragrafo 5, lettera c), il gruppo di lavoro raccomanda che ci si limiti alle eccezioni permesse dalla direttiva, che copre tutte le eccezioni ammesse dalla legge degli Stati membri. Il gruppo di lavoro ritiene che nessuna eccezione possa essere invocata al di fuori del suo contesto specifico, e che ogni eccezione può essere fatta valere soltanto per conseguire un fine specifico.

Il gruppo di lavoro esprime preoccupazione per il fatto che, oltre alle eccezioni già esposte, le FAQ contemplano un lungo elenco di ulteriori eccezioni, che portano in alcuni casi all'esenzione di intere categorie di dati: questo è vero, in particolare, per la vasta categoria dei "dati disponibili pubblicamente", che possono essere in effetti "disponibili pubblicamente" indipendentemente da qualsiasi considerazione di legittimità di elaborazione o di precisione dei dati. Il gruppo di lavoro sottolinea che tale esenzione non è contemplata dagli orientamenti OCSE e ritiene che accettarla significherebbe creare una comoda scappatoia alla tutela dei dati.

Notifica

Il gruppo di lavoro ribadisce la posizione, reiterata in tutti i suoi pareri precedenti, secondo la quale l'"approdo sicuro" (e di fatto ogni constatazione di adeguatezza) può soltanto interessare il trattamento dei dati trasferiti da un dispositivo di controllo dei dati dell'UE ad un paese terzo: i dispositivi di controllo dei dati dell'UE sono soggetti alle disposizioni nazionali che applicano la direttiva; lo stesso dicasi per i casi in cui i dati personali sono raccolti direttamente da singoli nell'UE da un'organizzazione statunitense che utilizza strutture situate sul territorio di uno Stato membro (articolo 4 della direttiva).

Tutto questo è ora riconosciuto dagli Stati Uniti al punto D1 delle FAQ n.14 sui prodotti farmaceutici e medicinali, ed nelle FAQ 9 sui dati riguardanti le risorse umane. Tuttavia, il principio della notifica afferma che:

" L'avviso dev'essere formulato (...) quando gli individui vengono invitati per la prima volta a fornire informazioni personali alle organizzazioni, oppure non appena possibile".

La frase sopra citata sembra implicare che la raccolta dei dati da singoli nell'UE da parte di organizzazioni statunitensi sarebbe regolata dai principi dell'"approdo sicuro", e non dalle disposizioni nazionali di applicazione della direttiva. Le sue conseguenze andrebbero quindi al di là del principio di notifica.

Il gruppo di lavoro ritiene che ciò non sia conforme all'articolo 4 della direttiva e raccomanda che la frase succitata sia omessa e sostituita dalla chiara indicazione che:

- qualora un'organizzazione USA intenda rilevare dati personali direttamente dai singoli cittadini nell'UE, essa deve conformarsi alle disposizioni nazionali in materia ai sensi della direttiva (ad esempio: articoli 6, 7, 10, 14 e, se del caso, articolo 8);
- qualora i dati personali vengano trasferiti all'organizzazione USA da un responsabile del controllo dei dati riconosciuto nell'UE, l'organizzazione dovrà richiedere a quest'ultimo di indicare a quale scopo i dati erano stati originariamente raccolti (questo è essenziale per determinare se un cambiamento di finalità si è verificato dopo il trasferimento, rendendo operativi i principi di avviso e di scelta; inoltre, la precisazione contribuirebbe alla ripartizione del rischio e della responsabilità).

Il gruppo di lavoro suggerisce che i punti di cui sopra siano oggetto di un nuovo documento FAQ volto a chiarire il principio di notifica.

Il gruppo di lavoro inoltre raccomanda di modificare il principio di notifica in modo da garantire che sia data notifica nel caso in cui i dati siano usati da un'organizzazione diversa.

Per quanto riguarda le FAQ 4, il gruppo di lavoro nota che nulla giustifica l'elaborazione di dati personali senza il consenso o la conoscenza degli interessati. Inoltre, lo stesso documento fa riferimento ad "altre circostanze in cui l'applicazione dei suddetti principi pregiudicherebbe gli interessi legittimi dell'organizzazione stessa" che il gruppo di lavoro considera una scappatoia troppo evidente.

Il gruppo di lavoro fa notare che il documento FAQ 14 sui prodotti farmaceutici e medicinali è recente e che il testo nella sua forma attuale pone diversi interrogativi, in particolare l'utilizzazione di dati per scopi incompatibili con quelli relativi alla ricerca scientifica.

Scelta

Il gruppo di lavoro ribadisce il parere espresso nel suo documento di lavoro del 7 luglio 1999: poiché i principi non includono alcun criterio di "legittimazione del trattamento", è auspicabile un rafforzamento del principio di scelta. Nella sua attuale versione, la combinazione dei principi di notifica e di scelta risulta nella possibilità di utilizzare i dati per scopi diversi da quelli notificati senza dovere offrire la possibilità di scegliere (a meno che lo scopo sia incompatibile o si tratti di informazioni a carattere delicato); questo contravviene agli orientamenti dell'OCSE ("Principio della limitazione dell'utilizzazione")[9]. Il gruppo di lavoro sostiene il principio che la possibilità di scegliere debba essere offerta quando i dati sono utilizzati per uno scopo compatibile ma diverso.

Il gruppo di lavoro condivide la posizione della Commissione espressa nella nota a piè di pagina al paragrafo relativo al principio di scelta, raccomanda che la definizione di dati delicati sia conforme all'articolo 8 della direttiva e ritiene che la scelta possa soltanto essere una base per l'elaborazione legittima solo se è basata su un'informazione adeguata.

Trasferimento successivo

Il gruppo di lavoro constata con preoccupazione l'aggiunta a questo principio dell'ultima frase, che solleva completamente le organizzazioni dalle loro responsabilità nel caso in cui le informazioni siano trasferite a terzi. Il singolo può non disporre di alcun ricorso legale eccetto contro l'organizzazione che ha operato il trasferimento e che può avere effettivamente agito avventatamente nel trasferire le informazioni. Il gruppo di lavoro raccomanda che la limitazione della responsabilità sia riconsiderata per mantenere la responsabilità dell'organizzazione che opera il trasferimento nei casi di negligenza e di comportamento incauto ed affinché l'organizzazione che opera il trasferimento sia tenuta ad assistere il singolo in caso di ricorso.

---

[9] "I dati personali non dovrebbero essere rivelati, resi disponibili o altrimenti utilizzati a scopi diversi da quelli precisati ai sensi del paragrafo 9 (Specificazione degli scopi) tranne che:
a) con il consenso dell'interessato
b) in forza di legge."

Sicurezza

Il gruppo di lavoro raccomanda che il testo della FAQ n. 10 sia modificato togliendo l'affermazione che all'interno del contratto non sono necessarie disposizioni riguardanti la sicurezza, poiché la legge di diversi Stati membri richiede tali disposizioni anche nei contratti per l'elaborazione dei dati presso lo Stato membro stesso.

Integrità dei dati

Il gruppo di lavoro ricorda che al paragrafo 8 degli orientamenti OCSE "i dati devono essere attinenti all'uso cui sono destinati e, nella misura in cui è necessario per l'uso suddetto, devono essere attendibili, completi ed aggiornati". Il principio dell'"approdo sicuro" dovrebbe riflettere questa posizione.

Accesso

Il gruppo di lavoro ricorda che il principio dell'accesso è di fondamentale importanza per ogni efficace regime di protezione dei dati, in quanto è il punto dal quale si dipartono tutti i diritti delle persone interessate. Il gruppo di lavoro insiste sul fatto che le eccezioni a questo principio fondamentale sono permesse soltanto in circostanze eccezionali e ribadisce la preoccupazione espressa in tutte le prese di posizione precedenti per quanto riguarda la portata e il carattere vago delle eccezioni e delle condizioni che gli Stati Uniti prevedono in relazione all'esercizio di questo diritto fondamentale.

Il gruppo di lavoro ribadisce il punto di vista che le considerazioni di costo sono necessarie per determinare le condizioni alle quali il diritto può essere esercitato, ma non possono essere una condizione al diritto stesso.

A differenza degli orientamenti[10] dell'OCSE, i principi dell'"approdo sicuro" non riconoscono il diritto individuale di ricevere le informazioni "in forma facilmente comprensibile". Inoltre, il principio dell'accesso limita il diritto di cancellare i dati ai casi in cui questi sono inesatti (il che è ovvio); nel suo parere 2/99 il gruppo di lavoro ha già espresso l'opinione che, per avere un senso, il diritto della persona interessata alla cancellazione dei dati deve applicarsi a tutti i casi in cui il relativo trattamento è illegale; ciò dovrebbe essere specificato nel principio e non nel testo delle FAQ.

La FAQ 8 elenca numerose eccezioni al principio di accesso; il gruppo di lavoro accoglie favorevolmente il fatto che alcune di queste eccezioni, rispetto al testo precedente, sono state limitate o chiarite. Tuttavia, il quadro globale dà ancora l'impressione che l'enunciato di questa FAQ indebolisca il principio anziché fornire indicazioni sulla sua applicazione. In particolare, il gruppo di lavoro ripete le sue obiezioni in merito ai punti D2 (nozione poco chiara), e D7. Per quanto riguarda il punto D5, il gruppo di lavoro ribadisce il suo punto di vista che i casi in cui l'accesso deve essere negato sono troppo ampi e vaghi e che la formulazione implica che tali considerazioni automaticamente scavalcano il diritto di accesso. Il gruppo di lavoro esprime preoccupazione per il fatto che ciò potrebbe provocare un serio indebolimento del livello globale di protezione dei dati.

Per quanto riguarda il punto D6, il gruppo di lavoro ritiene inadeguata la formulazione del secondo paragrafo e raccomanda o la sua soppressione o una formulazione più restrittiva, in modo da limitarlo all'esclusione degli abusi del diritto d'accesso.

Il gruppo di lavoro ribadisce altresì la sua opposizione al punto D8, per le ragioni già esposte nel documento di lavoro del 7 settembre 1999; inoltre, il fatto che le informazioni siano pubblicamente disponibili non priva gli interessati del loro diritto di accesso.

Applicazione

Il gruppo di lavoro accoglie favorevolmente le informazioni dettagliate fornite dagli Stati Uniti nelle ultime settimane di colloqui (in particolare: lettera della FTC, raffronto dei meccanismi del settore privato americano per il componimento delle controversie in materia di privacy, la FAQ 11, il memorandum sul Fair Credit Reporting Act).Tali informazioni sono preziose ed hanno per-

[10] "Principio della partecipazione individuale", punto a) iv.

messo al gruppo di lavoro di disporre di un quadro più chiaro delle strutture di applicazione che possono essere messe a disposizione degli interessati. Avendo esaminato i documenti succitati, il gruppo di lavoro esprime il timore che:

1. I meccanismi del settore privato esistenti si occupino esclusivamente delle attività on-line: BBB On-line; Web Trust; TRUSTe: (sottolineatura aggiunta)[11] ;
2. Lo stesso si constata nella lettera del Presidente FTC dell'1 novembre 1999 (paragrafo 2: "online privacy", "Internet environment"; paragrafo 3: online marketplace, survey of web sites; paragrafo 4: "online privacy policies"" e così via; sottolineatura aggiunta)[12] .
3. Ai sensi del paragrafo 4 dei principi, possono godere dei vantaggi dell'"approdo sicuro" le organizzazioni soggette a *"norme statutarie, di regolamentazione, amministrative o d'altro tipo (o a norme stabilite da borse valori nazionali, associazioni registrate di agenti di borsa, agenzie di compensazione registrate, ovvero enti normativi in materia di titoli municipali) che tutelino efficacemente la riservatezza dei dati personali"*. Tuttavia, nessun'informazione è stata fornita sugli enti pubblici che assicurerebbero l'applicazione di una così vasta gamma di regolamentazioni.

In queste circostanze, il gruppo di lavoro esprime il parere che il campo d'applicazione di ogni constatazione di adeguatezza debba essere espressamente limitato ai settori per i quali informazioni sufficienti ed inequivocabili sono state raccolte e per i quali è stata accertata l'esistenza di meccanismi di applicazione. In effetti, l'estensione del campo d'applicazione di una constatazione di adeguatezza oltre questo limite esporrebbe la decisione alla contestazione e questo non è auspicabile per nessuna delle parti interessate.

Per quanto riguarda il principio di applicazione, il gruppo di lavoro ritiene che, per avere un significato, il principio debba comprendere il risarcimento di ogni danno subito dall'individuo in seguito alla violazione dei principi: questo è un parere generale del gruppo di lavoro e si applica ad ogni paese terzo (documento di lavoro sul trasferimento dei dati personali verso paesi terzi: WP 12 del 24 luglio 1998, pagina 14: "riparazione adeguata". Nei casi in cui la riparazione dei danni non è contemplata nella normativa americana esistente, l'organizzazione privata dovrebbe poter offrire questa possibilità come condizione per qualificarsi per l'"approdo sicuro".

Per quanto riguarda le FAQ 11 (Risoluzione delle controversie e applicazione), il gruppo di lavoro rileva che questo testo esamina una serie di aspetti relativi all'applicazione l'importanza dei quali è tale che dovrebbero essere inclusi nel principio di applicazione stesso. Per il collegamento tra i diversi livelli d'applicazione è particolarmente importante che gli organismi preposti alla composizione delle controversie adottino la prassi di riferire i casi irrisolti alla FTC. I requisiti di trasparenza e rapidità del meccanismo di composizione delle controversie dovrebbero inoltre essere integrati nel principio.

In base alle FAQ 11, gli organismi preposti alla composizione delle controversie possono richiedere requisiti di ammissibilità per l'accettazione dei reclami. Il gruppo di lavoro ritiene che requisiti di questo tipo debbano essere espliciti, oggettivi e ragionevoli. Inoltre, il rifiuto di dare seguito ai reclami dovrebbe essere debitamente motivato.

In generale, il gruppo di lavoro nota che le disposizioni di applicazione negli Stati Uniti presentano un quadro piuttosto confuso nel quale non è possibile identificare con facilità quali siano i diritti del cittadino in caso di violazione dei principi. Le FAQ 11 offrono semplicemente una serie di raccomandazioni che possono condurre ad un'esecuzione frammentata ed irregolare.

FAQ 5 - Ruolo delle autorità di protezione dei dati

Il gruppo di lavoro ha discusso il testo della FAQ 5 proposto dagli USA e conclude che il

---

[11] Come già detto, le attività on line possono essere soggette alla legislazione UE nei casi in cui esse riguardano la raccolta di dati personali direttamente da singoli nell'UE (cfr. I capitoli Campo di applicazione e struttura e Notifica).

[12] V. Nota 6.

ruolo delle autorità di protezione dei dati previsto in questo testo non è legalmente o praticamente realizzabile. In particolare, il gruppo di lavoro nota che la legislazione nazionale non conferisce alle autorità nazionali la competenza di trattare i reclami concernenti le violazioni delle norme di protezione dei dati al di fuori della loro giurisdizione.

Il gruppo di lavoro prende atto d'altra parte della disponibilità delle autorità nazionali ad offrire la loro cooperazione sotto forma di informazioni e di consulenza, se questo può essere utile nel contesto dell'"approdo sicuro". Il gruppo di lavoro constata che la cooperazione è stata promossa dagli Stati Uniti per un periodo limitato successivo al lancio dell'"approdo sicuro".

In questo contesto, il gruppo di lavoro invita la Commissione a considerare se l'offerta di fornire informazioni e consulenza, combinata con l'impegno unilaterale da parte dell'organizzazione americana interessata di adeguarsi al parere delle autorità nazionali - un impegno che, se non rispettato, avrebbe come conseguenza un'azione per frode da parte della FTC - potrebbe contribuire al rispetto dei requisiti di cui alla parte (a) del principio di applicazione dell'"approdo sicuro". In caso affermativo, il gruppo di lavoro fa notare che le autorità nazionali potrebbero essere disposte a cooperare in questo modo per un periodo iniziale di 3 anni. Il gruppo di lavoro rileva inoltre che le autorità nazionali potranno voler rivedere l'accordo entro la fine di quel periodo se il numero di organizzazioni americane che si valgono di questa possibilità fosse tale da poter affermare che, in luogo di essere un accordo provvisorio per colmare una lacuna limitata, esso viene a sostituirsi negli Stati Uniti agli accordi di applicazione veri e propri.[13]

Il gruppo di lavoro invita inoltre la Commissione a studiare in che modo potrebbe essere utile un meccanismo a livello europeo, che potrebbe *inter alia* fornire una tribuna per contribuire ad assicurare un'impostazione coordinata ed armonizzata.

Proposta di decisione della Commissione del 24 novembre 1999

Il gruppo di lavoro desidera attirare l'attenzione della Commissione su quanto segue:

1. La proposta non fa alcun riferimento al lavoro effettuato dal gruppo di lavoro per stabilire i criteri di valutazione dell'adeguatezza nei paesi terzi (WP 12). Il gruppo di lavoro ritiene che la valutazione dell'adeguatezza debba essere effettuata sulla base di tali criteri per garantire un'impostazione equilibrata ed imparziale a tutti i paesi terzi, indipendentemente dal modo scelto - norme di legge o autodisciplina - per garantire la protezione dei dati. Dovrebbe inoltre essere fatto riferimento specifico ai pareri già espressi dal gruppo di lavoro sull'"approdo sicuro", indicando dove sono stati pubblicati.

2. Sulla sostanza della decisione, il gruppo di lavoro osserva che i criteri per l'adesione all"approdo sicuro" non sono gli stessi nei testi americani e nella proposta di decisione. Ai sensi dei paragrafi introduttivi 3 e 4 dei principi degli Stati Uniti, le organizzazioni possono qualificarsi per l'"approdo sicuro" in uno dei seguenti modi:

"a) aderendo a un programma di autodisciplina in materia di riservatezza che ottemperi ai principi,

b) sviluppando proprie politiche in materia di riservatezza, purché conformi ai principi,

c) essendo soggette a normative statutarie, di regolamentazione, amministrative o altre che tutelino efficacemente la riservatezza"

Secondo l'articolo 1 della proposta di decisione della Commissione, si considera che aderiscono all'"approdo sicuro", le organizzazioni che:

" dichiarano pubblicamente di conformarsi ai principi e sono soggette ai poteri statutari di un ente pubblico indipendente autorizzato ad esaminare qualsiasi reclamo e ad ottenere provvedimenti inibitori contro prassi sleali o ingannevoli."

I principi devono conformarsi alla decisione.

3. Il gruppo di lavoro osserva inoltre che il considerando 8 afferma che la legge contempla diverse eccezioni alla giurisdizione della Federal Trade Commission, senza peraltro indica-

[13] Alcune delegazioni riservano la propria posizione su questo paragrafo.

re in modo specifico i settori esclusi o se tutti i settori esclusi sono soggetti alla giurisdizione di un altro organismo pubblico. Analogamente, si dovrebbe fare riferimento alle disposizioni che conferiscono ai pochi enti pubblici citati il potere di agire contro le pratiche ingannevoli o le dichiarazioni false.

Poiché l'essere soggette alla giurisdizione di un organismo pubblico abilitato ad agire contro le pratiche sleali o ingannevoli è una *conditio sine qua non* per le organizzazioni che desiderano aderire all'"approdo sicuro", il gruppo di lavoro ritiene fondamentale chiedere che vengano forniti chiarimenti su questo punto e che il campo d'applicazione dell'"approdo sicuro" sia limitato ai settori soggetti alla giurisdizione di un organismo pubblico di questo tipo.

4. La proposta di decisione della Commissione non fa menzione del modo in cui le organizzazioni possono perdere i vantaggi dell'"approdo sicuro" - o, per dirlo in parole più semplici, quali siano le procedure per l'esclusione dall'elenco del Ministero del commercio.

Il solo impegno che figura nei testi statunitensi è quello di inserire nell'elenco *"qualsiasi notifica ricevuta da organismi di risoluzione delle controversie, di autoregolamentazione e/o governativi riguardante casi in cui organizzazioni che aderiscono all'"approdo sicuro" continuano a non conformarsi ai suoi principi o eventuali decisioni dei suddetti organismi. Ciò avverrà però solo dopo aver fornito all'organizzazione in questione la possibilità di replicare entro trenta giorni."*. (FAQ 11)

In base alla proposta di decisione, un'indicazione negativa può solo dare origine alla sospensione del trasferimento dei dati, ai sensi dell'articolo 2.2.(a). Nella situazione attuale, l'eventuale sospensione ai sensi dell'articolo 2.2.(a) non comparirebbe nell'elenco, in quanto questo non fa menzione di constatazioni negative effettuate nell'Unione europea.

Inoltre, il gruppo di lavoro è dell'avviso che le condizioni previste dall'articolo 2.2[14] per la sospensione del trasferimento dei dati rischia di dimostrarsi di difficile applicazione pratica, cosa inaccettabile nel caso in cui ci sia violazione dei diritti individuali. Nel testo dell'articolo 2.2, pertanto, le parole "danno irreparabile" andrebbero sostituite con "danno grave e imminente".

5. Il gruppo di lavoro rileva che l'articolo 1, paragrafo 3, riporta un testo proposto dagli Stati Uniti che recita: *" Si presume che il rispetto delle leggi statunitensi Fair Credit Reporting Act o Financial Modernization Act garantisca un livello adeguato di protezione per quanto riguarda le attività di un'organizzazione che rientrano nel campo d'applicazione di tali leggi."*. Per quanto riguarda queste leggi degli Stati Uniti, il gruppo di lavoro attira l'attenzione della Commissione sul fatto che un'analisi della FCRA era all'ordine del giorno della 17ª riunione del 7 giugno, ma né la legge né la valutazione di adeguatezza erano state discusse per mancanza di tempo e, per quanto riguarda la legge Financial Modernization Act, il gruppo di lavoro ha soltanto di recente preso visione del testo.

Alla luce di quanto sopra, il gruppo di lavoro può esprimere un parere sul livello di adeguatezza di queste due leggi soltanto dopo una discussione approfondita. Qualora dall'esame delle due leggi non emergesse alcuna constatazione di adeguatezza, ogni riferimento ad esse dovrà essere tolto dalla decisione.

---

[14] Articolo 2.2: "Le autorità competenti degli Stati membri possono altresì avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per sospendere flussi di dati diretti a un'organizzazione che rispetta i principi nei casi in cui:

a) gli organismi pubblici statunitensi di cui all'articolo 1, paragrafo 1, lettera b), o un meccanismo indipendente di ricorso degli Stati Uniti nell'ambito di quanto esposto alla lettera a) del "principio di applicazione" abbiano rilevato violazioni dei principi, oppure

b) vi siano sufficienti motivi per ritenere che il meccanismo di attuazione negli Stati Uniti non stia adottando o non adotterà misure adeguate e tempestive volte a risolvere il caso in questione, che sia sostanzialmente probabile che una violazione dei principi sia stata commessa e le autorità competenti dello Stato membro abbiano fatto il possibile per informare l'organizzazione dandole l'opportunità di reagire e che la continuazione del trasferimento dei dati potrebbe provocare danni irreparabili agli interessati.

I flussi di dati devono riprendere non appena sia garantito il rispetto dei principi."

6. Il gruppo di lavoro è inoltre dell'avviso che l'articolo 2.1 debba essere modificato come segue:

"L'articolo 1 non pregiudica il potere delle autorità competenti degli Stati membri di intervenire per garantire la conformità con le disposizioni nazionali approvate conformemente a disposizioni diverse da quelle previste agli articoli 25 e 26 della direttiva"

Scambio di lettere

(non datate ma pubblicate sul sito web il 15 novembre)

Il gruppo di lavoro desidera attirare l'attenzione della Commissione sui seguenti punti:

- ***Il cosiddetto "periodo di grazia", ovvero data di entrata in vigore:*** sia nel progetto di lettera degli Stati Uniti che nel progetto di risposta della Commissione si fa cenno al fatto che la Commissione e gli Stati membri faranno uso della flessibilità offerta dall'articolo 26 per evitare di interrompere i flussi di dati verso le organizzazioni statunitensi per un determinato periodo successivo alla decisione di cui all'articolo 25.6 dell'"approdo sicuro". In tal modo le organizzazioni statunitensi avranno l'opportunità di decidere se partecipare o meno all'"approdo sicuro" e, se necessario, di adeguare le loro prassi nell'ambito dell'informazione.

Considerando che, ai sensi della direttiva, la Commissione può agire in materia di trasferimenti a paesi terzi soltanto quando: a) un paese terzo non garantisce un livello di protezione adeguato e la Commissione avvia negoziati per porre rimedio alla situazione (articolo 25, paragrafi 4, 5 e 6) oppure b) qualora la Commissione decida che alcune clausole contrattuali tipo offrono le garanzie sufficienti (articolo 26.4), il gruppo di lavoro si domanda su quale base la Commissione intende utilizzare la flessibilità consentita dall'articolo 26 della direttiva per dare alle organizzazioni statunitensi tempo sufficiente per decidere se aderire o meno all'"approdo sicuro".

- ***Uso dei contratti - articolo 26 della decisione:*** Nel progetto di lettera dell'UE si afferma che *"la Commissione e gli Stati membri sono del parere che i principi (dell'"approdo" sicuro US) possono essere utilizzati in tali accordi come disposizioni fondamentali in materia di tutela dei dati. La Commissione ha avviato colloqui con gli Stati membri in seno al comitato di cui all'articolo 31 riguardo a tali disposizioni, in vista dell'adozione di una decisione in virtù dell'articolo 26.4 per autorizzare clausole tipo..."*

Considerando che il gruppo di lavoro è sempre stato del parere che l'analisi dell'adeguatezza delle soluzioni contrattuali richiede la considerazione di un'insieme di questioni più complesse di quelle prese in considerazione nell'ambito di soluzioni quadro, un impegno del genere appare prematuro. Va da sé che i principi dell'"approdo sicuro" devono essere migliorati e risultare adeguati prima che si possano prendere in considerazione come parte del contenuto di clausole tipo.

Conclusioni

Il gruppo di lavoro conclude, alla luce delle osservazioni e raccomandazioni fin qui esposte, che gli accordi per l'"approdo sicuro" come risultano nelle versioni attuali dei diversi documenti restano insoddisfacenti. Il gruppo di lavoro invita la Commissione a sollecitare la controparte statunitense ad apportare una serie di miglioramenti sostanziali, volti in particolare a:

- chiarire il campo d'applicazione dell'"approdo sicuro" e soprattutto ad eliminare ogni possibile malinteso sulla facoltà delle organizzazioni Statunitensi di scegliere di seguire i principi dell'"approdo sicuro" nei casi per i quali si applica la direttiva;
- stabilire disposizioni più affidabili che consentano di identificare con certezza gli aderenti all'"approdo sicuro" e che evitino il rischio che i vantaggi dell'"approdo sicuro" continuino ad essere accordati anche dopo che l'adesione all'approdo sicuro, per una ragione o un'altra, è stata ritirata;
- stabilire in modo inequivocabile che la giurisdizione di un organismo pubblico adeguatamente autorizzato è valida per tutti i partecipanti all'"approdo sicuro";
- far sì che gli organismi del settore privato preposti alla composizione delle controversie siano tenuti a riferire i casi di reclami non risolti ad un organismo pubblico del tipo di cui sopra;

- rendere le eccezioni e le esenzioni ammesse meno generiche e meno vaghe, in modo che le eccezioni siano effettivamente tali, ossia si applichino solo quando necessario e nella misura del necessario e non siano un invito generalizzato a scavalcare i principi; questo punto è particolarmente importante per quanto riguarda il diritto di accesso;
- rinforzare il principio della scelta, che è la chiave di volta dell'impostazione degli Stati Uniti.

Questi punti sono stati sviluppati in modo particolareggiato nelle sezioni precedenti di questo parere; il gruppo di lavoro auspica che si tenga conto delle considerazioni esposte.

Il gruppo di lavoro invita inoltre la Commissione a rivedere l'articolo 2 del progetto di decisione affinché sia chiaro che la decisione non pregiudica il potere delle autorità nazionali competenti per quanto riguarda le leggi nazionali per l'applicazione di disposizioni della direttiva diverse dagli articoli 25 e 26 e affinché sia possibile intervenire, ai sensi dell'articolo 2, paragrafo 2, nei casi in cui il trasferimento dei dati potrebbe provocare "danni irreparabili" agli interessati.

Il gruppo di lavoro sottolinea infine l'importanza di continuare e addirittura accelerare i lavori sulle clausole contrattuali tipo, in vista di una decisione o delle decisioni ai sensi dell'articolo 26 paragrafo 4, che è una parte importante del lavoro per semplificare e rendere più trasparenti le misure di sicurezza richieste per i trasferimenti ai settori nei quali una protezione adeguata non è altrimenti garantita.

Fatto a Bruxelles, il 3 dicembre 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

6.3.3. Internet

Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware

5093/98/IT/def.
WP 17

Gruppo di lavoro per la tutela delle persone
con riguardo al trattamento dei dati personali

Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware

Adottato dal gruppo di lavoro il 23 febbraio 1999

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE
CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

Visti gli articoli 29 e 30, paragrafo 3 della direttiva,

Viste le sue regole di procedura e in particolare gli articoli 12 e 14,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

1. Il gruppo di lavoro incoraggia l'industria del software e dell'hardware a lavorare su prodotti Internet rispettosi della privacy, fornendo i necessari strumenti per conformarsi alla normativa europea sulla protezione dei dati.

Una condizione per rendere legittimo il trattamento lecito dei dati personali è che il soggetto dei dati sia informato e sia messo al corrente del trattamento in questione. Il gruppo di lavoro è quindi particolarmente interessato a tutti i tipi di operazioni di trattamento attualmente effettuate da software ed hardware su Internet senza che la persona interessata ne sia a conoscenza e che quindi sono per lei "invisibili".

Esempi tipici di questo trattamento invisibile sono il "chattering" a livello HTTP[15], "hyperlink" automatici a terzi, il contenuto attivo (come Java, ActiveX o altre tecniche di scrittura basate sull'utente) e il meccanismo dei "cookies", così come attualmente applicato nei comuni browser.

2. I prodotti Internet di software ed hardware dovrebbero mettere a disposizione degli utenti Internet informazioni sui dati che si intendono raccogliere, memorizzare o trasmettere e lo scopo per cui ciò viene fatto.

I prodotti Internet di software ed hardware dovrebbero anche permettere all'utente dei dati di avere facilmente accesso, in qualsiasi momento, ai dati raccolti che lo riguardano.

Ciò significa ad esempio:

[15] Ciò significa che nella richiesta http sono trasmesse informazioni che oltrepassano quelle necessarie per contattare il server.

- nel caso di un browser software, che, al momento di stabilire un collegamento con un web server (spedendo una richiesta o ricevendo una pagina web), l'utente debba essere informato di quale informazione s'intende trasferire e a quale fine;
- nel caso di hyperlink spediti da un sito web ad un utente mediante qualsiasi mezzo, che il browser dell'utente dovrebbe indicarli tutti all'utente;
- nel caso di cookies, che l'utente dovrà essere informato quando un cookie dovrebbe essere ricevuto, memorizzato o spedito dal software Internet. Il messaggio dovrebbe specificare, in un linguaggio generalmente comprensibile, quali informazioni s'intendono memorizzare nel cookie, ed a quale fine, nonché il periodo di validità del cookie stesso.

3. La configurazione dei prodotti hardware e software non dovrebbero, per default, consentire la raccolta, la memorizzazione o la trasmissione d'informazioni persistenti sul cliente[16]. Ad esempio:

- il browser software dovrebbe, per default, essere configurato in modo tale da trattare solamente la quantità minima di informazioni necessarie per stabilire un collegamento Internet. I cookies, per default, non dovrebbero essere né spediti, né memorizzati.
- durante la sua installazione, una funzione browser destinata a memorizzare e a trasmettere i dati sull'identità dell'utente o sul suo comportamento riguardo le comunicazioni (profilo) non dovrebbe essere completata automaticamente con dati preventivamente memorizzati sull'attrezzatura dell'utente.

4. I prodotti Internet di hardware e software dovrebbero permettere al soggetto dei dati di decidere liberamente sul trattamento dei propri dati personali, mettendo a disposizione strumenti di facile utilizzazione per filtrare (cioè respingere o modificare) la ricezione, la memorizzazione o la trasmissione di informazioni persistenti sul cliente seguendo alcuni criteri (compresi i profili, il campo o l'identità del server Internet, il tipo e la durata delle informazioni raccolte, memorizzate o spedite e così via). L'utente dovrebbe poter disporre di chiare istruzioni sull'impiego del software e dell'hardware per l'applicazione di queste opzioni e strumenti. Ad esempio:

- ciò significa che il browser software dovrebbe fornire opzioni in modo che l'utente possa configurare il browser, specificando quali informazioni quest'ultimo potrà o meno raccogliere e trasmettere;
- ciò significa per i cookies che l'utente potrà sempre scegliere se accettare o respingere la trasmissione o la memorizzazione di un cookie nel suo insieme. L'utente potrà anche scegliere di decidere quali elementi dell'informazione andranno conservati o eliminati da un cookie, a seconda, ad esempio, del periodo di validità dello stesso o della spedizione e ricezione di siti web.

5. I prodotti Internet di software ed hardware dovrebbero permettere all'utente di eliminare le informazioni persistenti sul cliente in modo semplice e senza partecipazione del mittente. Dovranno essere fornite all'utente chiare informazioni sulle modalità d'esecuzione. Se le informazioni non possono essere tolte dovrà esistere un modo affidabile per prevenirne il trasferimento e la lettura.

- I cookies e le altre informazioni persistenti sul cliente vanno memorizzati in un modo standardizzato e devono essere facilmente e selettivamente cancellabili sul computer del cliente.

Contesto generale

Attualmente è quasi impossibile utilizzare Internet senza essere confrontati a elementi che invadono la privacy e a operazioni di trattamento dei dati personali effettuate in un modo che resta

---

16 Informazioni persistenti sul cliente è un termine tecnico (non giuridico) con il quale s'intendono le informazioni comunicate al cliente (il PC dell'utente) e che rimangono più a lungo di una sessione sul computer. Una sessione inizia quando il cliente chiede una pagina di un particolare sito web e finisce quando decide di chiudere il programma browsing o il computer, oppure quando chiede una pagina di un altro sito web. I cookies sono informazioni persistenti tipiche del cliente, lo stesso dicasi per le preferenze riguardanti la privacy.

invisibile al soggetto dei dati. In altre parole, l'utente Internet non sa che i suoi dati personali sono stati raccolti, successivamente elaborati, e che potrebbero essere utilizzati a fini a lui sconosciuti. Il soggetto dei dati non sa nulla del trattamento e non ha la libertà di prendere decisioni al riguardo.

Un esempio di questo tipo di tecnica è costituito dal cosiddetto cookie, che può essere definito come una registrazione informatica d'informazioni trasmessa da un web server ad un computer dell'utente per la futura identificazione di tale computer al momento di future visite allo stesso sito web.

I browser sono programmi di software progettati, tra l'altro, per visualizzare graficamente il materiale disponibile su Internet. I browser comunicano tra il computer dell'utente (cliente) ed il computer a distanza in cui sono memorizzate le informazioni (web server). I browser spesso trasmettono al web server più informazioni di quelle strettamente necessarie per stabilire la comunicazione. I browser classici trasmetteranno automaticamente al web server visitato il tipo ed il linguaggio del browser, il nome degli altri programmi software installati sul PC dell'utente ed il sistema operativo, la pagina di riferimento, i cookies, ecc. Tali dati possono anche essere trasmessi sistematicamente a terzi dal browser software in modo invisibile.

Queste tecniche permettono di creare "clicktrails" riguardanti l'utente Internet. I clicktrails sono costituiti da informazioni su comportamento, identità, strade seguite o scelte effettuate da questi durante la visita di un sito web. Essi contengono i collegamenti che un utente ha seguito e sono registrati nel web server.

Le direttive europee 95/46/CE e 97/66/CE sulla protezione dei dati contengono disposizioni particolareggiate per la tutela delle persone con riguardo al trattamento dei dati personali. Entrambe le direttive sono pertinenti alle situazioni di cui trattasi nella presente raccomandazione, in quanto i dati personali relativi agli utenti Internet sono trattati in tale contesto.

I cookies o i browser possono contenere o trattare successivamente dati che consentono l'identificazione diretta e indiretta di un singolo utente Internet.

L'applicazione delle disposizioni sul corretto trattamento, le basi legittime del trattamento ed il diritto del soggetto dei dati di decidere sul trattamento dei propri dati portano alla raccomandazione di cui sopra.

Il gruppo di lavoro è particolarmente preoccupato dei rischi inerenti al trattamento dei dati personali riguardanti soggetti di dati che sono completamente all'oscuro di tale trattamento. I progettisti del software e dell'hardware sono quindi invitati a prendere in considerazione e a rispettare i principi di queste direttive al fine di rafforzare la privacy degli utenti Internet.

Fatto a Bruxelles, il 23 febbraio 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

Raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni

5005/99/def.
WP 18

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni

Adottata il 3 maggio 1999

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Istituito dalla Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995[17],

Considerando gli artt. 29 e 30, paragrafi 1 e 3, della suddetta direttiva[18],

Considerando il suo regolamento interno, in particolare gli artt. 12 e 14 di quest'ultimo,

Ha adottato la presente raccomandazione:

L'obiettivo della raccomandazione è di ricordare l'applicazione alle misure adottate a livello europeo in materia di intercettazione delle telecomunicazioni dei principi di tutela dei diritti e delle libertà fondamentali delle persone fisiche, e in particolare della loro vita privata e della riservatezza della corrispondenza.

Il campo d'applicazione della presente raccomandazione copre le intercettazioni in senso lato, vale a dire l'intercettazione del contenuto delle telecomunicazioni ma anche i dati attinenti alle telecomunicazioni, e in particolare eventuali misure preparatorie (quali il "monitoring" e il "data-mining" dei dati sul traffico) di cui si terrà conto per decidere l'opportunità dell'intercettazione del contenuto della telecomunicazione[19].

1. Portata delle disposizioni adottate a livello europeo in materia di intercettazione delle telecomunicazioni

a. La risoluzione del Consiglio del 17 gennaio 1995 relativa all'intercettazione legale delle telecomunicazioni[20] specifica le condizioni tecniche necessarie per l'intercettazione delle telecomunicazioni, senza affrontare la questione delle condizioni in cui simili intercettazioni devono aver

---

[17] Direttiva del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, G.U. L 281 del 23.11.1995, pag. 31.

[18] I tre membri che rappresentano rispettivamente il Registertilsynet (Danimarca), la Commission Nationale de l'Informatique et des Libertés (CNIL, Francia) e il Data Protection Registrar (Regno Unito), non hanno partecipato al voto di questa raccomandazione, ritenendo che il soggetto trattato non fosse di competenza del gruppo. Essi sostengono tuttavia in linea di massima la raccomandazione.

[19] Questo caratterere esteso della nozione di intercettazione delle telecomunicazioni corrisponde al campo di applicazione della risoluzione del Consiglio del 17 gennaio 1995 relativa all'intercettazione legale delle telecomunicazioni, citata in appresso (Capitolo A.1.), e al quadro generale delle disposizioni giuridiche applicabili in materia (si veda in appresso il Capitolo B.).
La raccommandazione si applica all'intercettazione delle telecomunicazioni non pubbliche su Internet. Un'attenzione particolare è dedicata alla problematica generale del trattamento dei dati personali legati allo sviluppo della rete Internet dal gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, nel quadro dei lavori svolti parallelamente dalla "task force internet" del gruppo.

[20] G.U. C329 del 14.11.1996.

luogo. Il testo della Risoluzione stabilisce che gli operatori delle reti e i fornitori di servizi sono tenuti a consegnare ai «servizi autorizzati» i dati intercettati non codificati.

Quanto detto vale per le telefonate sulla rete fissa o tramite cellulare, la posta elettronica, le telecopiatrici e i messaggi telex, il flusso di dati Internet, sia per quanto riguarda la conoscenza del contenuto delle telecomunicazioni che i dati relativi alle telecomunicazioni (questi si riferiscono in particolare ai dati sul traffico, ma anche a qualsiasi altro segnale emesso dalla persona oggetto della sorveglianza - punto 1.4.4. della risoluzione).

I dati riguardano la persona sorvegliata nonché le persone che chiamano o sono chiamate da questa persona[21].

La risoluzione prevede anche che la localizzazione geografica dell'utilizzatore mobile costituisce un dato al quale i servizi autorizzati devono avere accesso[22].

Questa risoluzione del 18 gennaio 1995 forma attualmente l'oggetto di una revisione, e uno dei principali obiettivi è l'adeguamento alle nuove tecnologie di comunicazione. Il progetto di testo specifica in particolare l'applicazione delle misure di intercettazione alle telecomunicazioni via satellite[23].

b. Le riflessioni del gruppo di lavoro hanno per oggetto il campo d'applicazione delle misure previste dalla risoluzione del Consiglio del 17 gennaio 1995. Una versione non pubblicata del documento suddetto e posteriore a questo («dichiarazione d'intenzioni» in data 25 ottobre 1995), prevede che i firmatari del testo potranno mettersi in contatto per quanto concerne le specifiche in materia di intercettazione delle telecomunicazioni con il direttore del «Federal Bureau of Investigation» degli Stati Uniti. Il testo prevede inoltre che, previo consenso dei «partecipanti», altri Stati membri possono partecipare allo scambio di informazioni, alla revisione e all'aggiornamento delle specifiche.

Il gruppo fa osservare, da un lato, che lo statuto giuridico di questo testo - in particolare la sua firma effettiva da parte dei paesi interessati - non è chiaro e che esso non è, ai sensi della giurisprudenza della Corte europea dei diritti dell'uomo citata in appresso, accessibile ai cittadini dato che non forma l'oggetto di alcuna pubblicazione. D'altra parte, da questo testo emerge la volontà di mettere a punto misure tecniche di intercettazione delle telecomunicazioni in concertazione con Sstati non soggetti alla convenzione europea dei diritti dell'uomo e alle direttive 95/46/CE e 97/66/CE.

c. Il gruppo di lavoro constata che il testo della risoluzione del Consiglio pretende di disciplinare aspetti tecnici relativi alle modalità di intercettazione delle comunicazioni senza mettere in discussione le disposizioni nazionali che regolamentano le intercettazioni da un punto di vista giuridico. Tuttavia, talune misure previste dalla risoluzione intese ad estendere le possibilità di intercettazione delle comunicazioni sono in contraddizione con le disposizioni nazionali, più protettrici, di taluni paesi dell'Unione europea (in particolare: punto 1.4, comunicazione dei dati relativi alle chiamate, inclusi quelli relativi alla telefonia mobile, senza tener conto dei servizi anonimi e prepagati attualmente disponibili; punto 1.5, localizzazione geografica degli utenti mobili; punto 5.1,

[21] Art. 1.4 dell'allegato della risoluzione del Consiglio del 17 gennaio 1995.

[22] Art. 1.5, op. cit.

[23] Documento 10951/1/98, Enfopol 98 Rev 1 (http://www.heise.de/tp/deutsch/special/enfo/6332/1.htm). Una versione ancora più recente sembra essere stata approvata dal gruppo di lavoro "cooperazione di polizia" del Consiglio ed essere stata trasmessa al Parlamento europeo affinché questo possa adottarla o modificarla. La nuova risoluzione dovrebbe essere adottata dal Consiglio il 27-28 maggio 1999 (si veda il "Datenschutz-Berater, 15.02.99, pag. 5, che menziona una versione non pubblicata del 20.01.99). La commissione giuridica e dei diritti dei cittadini del Parlamento europeo ha raccomandato alla commissione per le libertà pubbliche e gli affari interni (capofila) di respingere il progetto di revisione della raccomandazione del Consiglio nella versione proposta in ENFOPOL 98, fra l'altro per motivi di tutela della vita privata e l'imminente entrata in vigore del Trattato di Amsterdam (si veda la relazione del sig. Florio). La commissione per le libertà pubbliche non ha accolto questa raccomandazione e proporrà quindi in seduta plenaria di approvare ENFOPOL 98 sulla base della relazione del sig. Schmid. Il Parlamento europeo adotterà una decisione all'inizio di maggio.

divieto agli operatori di rivelare a posteriori le intercettazioni realizzate).

d. Anche se la risoluzione del Consiglio persegue l'obiettivo della «tutela degli interessi nazionali, della sicurezza nazionale e di indagine sulla criminalità grave», il gruppo attira l'attenzione sui rischi dovuti ad un'estensione ad un numero crescente di paesi - in parte paesi terzi - delle tecniche di intercettazione e di decifrazione delle telecomunicazioni.

Une dichiarazione ufficiale del Parlamento europeo del 16 settembre 1998 relativa alle relazioni transatlantiche[24], «ritiene che l'importanza crescente della rete Internet, e più in generale, delle telecomunicazioni a livello mondiale e in particolare il sistema Echelon, nonché i rischi di una loro utilizzazione abusiva, richiedono l'adozione di misure di protezione delle informazioni economiche e di una crittografia efficace.»

Queste considerazioni evidenziano i rischi legati ad un'intercettazione delle telecomunicazioni che non sono limitati solo a questioni di sicurezza nazionale e non riguardano unicamente l'Unione europea. Esse mettono in dubbio la loro legittimità, in particolare alla luce degli obblighi derivanti dal diritto comunitario in materia di tutela dei diritti e delle libertà fondamentali delle persone fisiche, e soprattutto della loro vita privata.

e. Il gruppo sottolinea infine che l'entrata in vigore del trattato di Amsterdam comporterà un cambiamento della base giuridica a livello europeo per quanto riguarda le misure di intercettazione delle telecomunicazioni. La competenza attuale del Consiglio per elaborare il testo della risoluzione, basata sugli artt. K.1, paragrafo 9, e K.3, paragrafo 2, del trattato relativi alla cooperazione di polizia e giudiziaria, sarà sostituita da un competenza d'iniziativa della Commissione europea basata sul nuovo art. K.6, paragrafo 2.

2. Quadro giuridico generale

f. Il gruppo ricorda che ogni intercettazione delle telecomuncazioni, intesa come la presa di conoscenza da parte di un terzo del contenuto e/o dei dati riguardanti le telecomunicazioni private tra due o più corrispondenti, in particolare i dati del traffico legati all'utilizzazione dei servizi di telecomunicazione, costituisce una violazione del diritto alla vita privata degli individui e della riservatezza della corrispondenza. Un'intercettazione è ammissibile solamente se soddisfa tre esigenze fondamentali, in conformità all'art. 8, paragrafo 2, della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950[25] e all'interpretazione di questa disposizione da parte della Corte europea dei diritti dell'uomo: una base giuridica, la necessità della misura in una società democratica e la conformità ad uno degli obiettivi legittimi enumerati nella convenzione[26].

La base giuridica dovrà definire con precisione i limiti e le modalità del suo esercizio, grazie a norme chiare e dettagliate, che sono necessarie se si tiene conto del perfezionamento continuo dei mezzi tecnici disponibili[27]. Il testo della legge dev'essere accessibile al pubblico affinché i cittadini possano conoscere le conseguenze del loro comportamento[28].

In un simile contesto giuridico dev'essere vietata una sorveglianza generale o a campione

---

[24] Sessione plenaria, processo verbale parte II, B4-0803, 0805, 0806 e 0809/98.

[25] Va sottolineato che le garanzie fondamentali riconosciute dal Consiglio d'Europa in materia d'intercettazione delle comunicazioni comportano alcuni obblighi per gli Stati, indipendentemente dalle distinzioni esistenti a livello dell'Unione europea in funzione del carattere comunitario o intergovernativo delle questioni affrontate.

[26] La Convenzione n°108 del Consiglio d'Europa prevede anche che un'ingerenza è tollerata unicamente se si tratta di una misura necessaria in una società democratica alla tutela degli interessi nazionali enumerati al suo art. 9, paragrafo 2 (si osservi che gli interessi nazionali enumerati nella convenzione 108 e nella convenzione per la tutela dei diritti dell'uomo non sono esattamente gli stessi), e se essa si limita unicamente al perseguimento di questo obiettivo.

[27] Si vedano in appresso gli obblighi previsti dall'art. 4 della raccomandazione n° 4 del Consiglio d'Europa del 7 febbraio 1995 sulla tutela dei dati personali nelle telecomunicazioni, e in particolare nei servizi telefonici.

[28] Sentenze Huvig e Kruslin contro la Francia del 25 aprile 1990, serie A n° 176 A e B, pag. 15 e segg.

delle telecomunicazioni[29].

g. Nell'Unione Europea, la direttiva 95/46/CE[30] sancisce il principio della tutela del diritto alla vita previsto dalla legislazione degli Stati membri. Questa direttiva precisa i principi contenuti nella convenzione europea per la tutela dei diritti dell'uomo del 4 novembre 1950 e nella convenzione del 28 gennaio 1981 del Consiglio d'Europa per la tutela delle persone con riguardo all'elaborazione automatica dei dati personali. La direttiva 97/66/CE[31] concretizza le disposizioni di tale direttiva precisando l'obbligo che incombe agli Stati membri di garantire la riservatezza delle comunicazioni tramite leggi nazionali che assicurino la riservatezza delle comunicazioni efettuate tramite una rete pubblica di telecomunicazioni o di servizi di telecomunicazioni accessibili al pubblico.

Ai sensi dell'art. 13, paragrafo 1, della direttiva 95/46/CE, uno Stato membro può adottare misure legislative intese a limitare la portata di taluni obblighi (ad esempio, relativi alla raccolta dei dati) e di taluni diritti (ad esempio, il diritto di essere informati in merito ad una raccolta di dati) previsti dalla direttiva[32]. Tali eccezioni sono dettagliatamente enumerate: la limitazione deve costituire una misura necessaria per tutelare gli interessi pubblici enumerati in modo esaustivo nei paragrafi da a) a g) di tale articolo, quali la sicurezza dello Stato, la difesa, la pubblica sicurezza, per la prevenzione, l'indagine, individuazione e le procedure contro i reati.

Anche la direttiva 97/66/CE stabilisce all'art. 14, paragrafo 1, che gli Stati membri possono limitare l'obbligo della riservatezza delle comunicazioni sulle reti pubbliche unicamente se questa misura è necessaria per tutelare la sicurezza dello Stato, la difesa, la pubblica sicurezza, la prevenzione, l'indagine, l'individuazione e le procedure contro i reati.

3. Obblighi degli operatori e dei fornitori dei servizi di telecomunicazione

h. È opportuno osservare che gli obblighi relativi alla sicurezza e alla riservatezza dei dati cui sono soggetti gli operatori e i fornitori di telecomunicazioni - nonché gli Stati membri - rispettivamente sulla base degli artt. 17, paragrafi 1 e 2, della direttiva 95/46 e sulla base degli artt. 4, 5 e 6 della direttiva 97/66/CE, costituiscono il principio e non l'eccezione.

---

[29] Si vedano in particolare le sentenze Klass, del 6 settembre 1978, serie A n°28, pag. 23 e segg., e Malone, del 2 agosto 1984, serie A n°82, pag. 30 e segg.

Sia la sentenza Klass che la sentenza Leander del 25 febbraio 1987 ribadiscono la necessità di "garanzie sufficienti contro gli abusi dato che un sistema di sorveglianza segreto inteso a proteggere la sicurezza nazionale comporta il rischio di indebolire o anche distruggere la democrazia col pretesto di difenderla" (Sentenza Leander, serie A n°116, pag. 14 e segg.).

Nella sentenza Klass, la Corte osserva (paragrafi 50 e segg.) che la valutazione dell'esistenza di garanzie adeguate e sufficienti contro gli abusi dipende dalle circostanze del caso. Nella sentenza in questione essa ritiene che le misure di sorveglianza previste dalla legislazione tedesca non autorizzano la sorveglianza generale o per campione e non trasgrediscono l'art. 8 della Convenzione europea per la tutela dei diritti dell'uomo. Le garanzie previste dalla legge tedesca sono le seguenti: le misure di sorveglianza sono consentite solamente se alcuni indizi consentono di sospettare che qualcuno progetta, compie o ha compiuto taluni reati gravi; esse sono consentite solo se non è possibile stabilire i fatti in altro modo o con un onere considerevolmente superiore; anche in tal caso, la sorveglianza può riguardare unicamente la persona sospetta o le persone che si ritiene possano avere contatti con tale sospetto.

[30] L'art. 3 della direttiva 95/46/CE esclude dal suo campo d'applicazione il trattamento di dati personali per l'esercizio di attività che non rientrano nel campo d'applicazione del diritto comunitario, nonché il trattamento dei dati ai fini della sicurezza pubblica, della difesa, della sicurezza dello Stato e le attività dello Stato nel campo del diritto penale. La maggior parte delle leggi nazionali per il recepimento di questa direttiva valgono anche per attività non coperte dal diritto comunitario.

A partire dal momento in cui un trattamento dei dati è realizzato nel quadro della direttiva (ad esempio, elenco delle chiamate registrate da un operatore ai fini della fatturazione), ma forma in un secondo tempo l'oggetto di un trattamento consistente in una intercettazione di tali dati, devono essere applicate le disposizioni del diritto comunitario. La direttiva 95/46/CE prevede a tal fine una serie di garanzie che devono essere rispettate nel quadro di tali intercettazioni, che saranno illustrate in appresso.

[31] Direttiva del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, G.U. L 24 del 30 gennaio 1998, pag.1.

[32] PreVisto all'art. 6, paragrafo 1 - principi relativi alla qualità dei dati, all'art. 10, all'art. 11, paragrafo 1, - informazione delle persone interessate, e agli artt. 12 - diritto d'accesso e 21 - pubblicità dei trattamenti.

Il gruppo ricorda che tali obblighi valgono in modo generale anche per gli operatori in virtù dell'art. 7 della convenzione del Consiglio d'Europa n°108 relativa alla tutela delle persone con riguardo al trattamento dei dati personali del 28 gennaio 1981, e dell'art. 4 della raccomandazione del Consiglio d'Europa n°4 sulla tutela dei dati personali nei servizi di telecomunicazione, in particolare per quanto riguarda i servizi telefonici, del 7 febbraio 1995[33].

i. Questi obblighi comportano che gli operatori delle telecomunicazioni e i fornitori di servizi possono trattare i dati relativi al traffico e alla fatturazione delle telecomunicazioni unicamente se sono soddisfatte talune condizioni: partendo dal principio che i dati relativi al traffico concernente gli abbonati e utilizzatori devono essere cancellati o resi anonimi subito dopo la fine della comunicazione, ne segue che gli scopi per cui i dati possono essere trattati, la durata della loro eventuale conservazione nonché l'accesso a tali dati sono rigorosamente limitati[34].

j. Inoltre, gli operatori delle telecomunicazioni e i fornitori di servizi di telecomunicazione devono prendere le misure necessarie per rendere tecnicamente difficile o impossibile, tenuto conto dello stato attuale della tecnica, l'intercettazione delle telecomunicazioni da parte di chi non è autorizzato dalla legge.

Il gruppo sottolinea a tale proposito che la realizzazione di strumenti efficaci per l'intercettazione delle comunicazioni per scopi legittimi, che utilizzano le tecniche più avanzate, non deve comportare un abbassamento del livello generale della riservatezza delle comunicazioni e della tutela della vita privata delle persone fisiche.

Questi obblighi assumono un significato particolare nel caso in cui le telecomunicazioni tra persone situate sul territorio degli Stati membri transitano o possono transitare all'esterno del territorio europeo, in particolare nel caso dell'utilizzazione di satelliti o di Internet.

k. Ai sensi della direttiva 95/46/CE, il fatto di rendere accessibili tali telecomunicazioni all'esterno dell'Unione europea potrebbe inoltre costituire una violazione dell'art. 25 della direttiva, dato che le autorità straniere che le intercettano potrebbero non essere in grado di assicurare un adeguato livello di protezione dei dati.

4. Rispetto delle libertà fondamentali da parte delle pubbliche autorità nel quadro delle intercettazioni

l. È importante che il diritto nazionale precisi in modo rigoroso e nel rispetto di tutte le disposizioni summenzionate:

---

[33] "4.1. I dati personali raccolti e trattati dagli operatori delle reti o dai fornitori di servizi non devono essere divulgati, a meno che l'abbonato in questione non abbia espressamente acconsentito per iscritto e l'informazione divulgata non consenta l'identificazione dell'abbonato.
L'abbonato può ritirare il suo consenso in qualsiasi momento, ma non retroattivamente.
4.2. I dati personali raccolti e trattati dai gestori della rete o dai fornitori di servizi possono essere comunicati alle pubbliche autorità se tale comunicazione è prevista dalla legge e costituisce una misura necessaria in una società democratica:
a.per tutelare la sicurezza dello Stato, la pubblica sicurezza, gli interessi monetari dello Stato o nell'ambito di un procedimento contro un reato;
b.per la tutela della persona interessata e dei diritti e delle libertà altrui.
4.3. Nel caso di una comunicazione di dati personali alle pubbliche autorità, il diritto interno dovrebbe regolamentare:
a. l'esercizio dei diritti di accesso e di rettifica da parte della persona interessata;
b. le condizioni alle quali le pubbliche autorità competenti potranno negare le informazioni alla persona interessata o rinviarne la consegna;
c. la conservazione o la distruzione di tali dati."

[34] Si vedano in particolare gli obblighi previsti dall'art. 6 della direttiva 97/66/CE.
Tali obblighi fanno sorgere dei dubbi per quanto riguarda le pratiche diffuse presso i gestori dei servizi di telecomunicazione che consentono un esame generale e preliminare dei dati del traffico degli abbonati, al fine di individuare il comportamento sospetto di taluni abbonati - ed eventualmente consentire l'intercettazione mirata del contenuto di talune telecomunicazioni.