

alla riservatezza consisterebbe nel fare in modo che, quando ciò sia possibile, le tracce create dai dati nell'utilizzo di Internet non consentano l'identificazione dell'utilizzatore. Garantendo l'anonimato, i singoli potrebbero partecipare alla rivoluzione di Internet senza il timore che ogni loro mossa possa essere registrata consentendo di raccogliere informazioni su di loro, che potrebbero essere utilizzate successivamente contro la loro volontà.

La necessità dell'anonimato nelle comunicazioni in rete è già riconosciuta come assolutamente legittima in talune situazioni, ad esempio quando una vittima di un'aggressione sessuale o di una persona che soffre di dipendenza dall'alcol o dalle droghe desidera condividere le sue esperienze con altri, quando una persona che pensa al suicidio desidera consultare uno specialista sulla rete o quando qualcuno desidera denunciare un crimine senza timore di subire ritorsioni. In altre situazioni, l'anonimato garantito serve a proteggere non solo la riservatezza ma anche la libertà di espressione, come nei casi dei dissidenti politici soggetti a un regime politico totalitario che desiderano esprimere la loro opposizione al sistema politico in cui vivono e richiamare l'attenzione sulle violazioni dei diritti umani.

Ma la necessità di anonimato va molto oltre questi casi specifici. Infatti i dati transazionali, identificabili per il solo fatto di esistere, possono costituire uno strumento attraverso il quale il comportamento di una persona può essere seguito e controllato in una misura che non è mai stata possibile prima.

Conciliare la riservatezza con gli altri obiettivi politici

È chiaro quindi che il problema dell'anonimato su Internet è al centro di un dilemma per i governi e le organizzazioni internazionali. Da un lato la possibilità di conservare l'anonimato è essenziale se si vogliono mantenere nel ciberspazio i diritti fondamentali alla riservatezza e alla libertà di espressione. D'altro lato, la capacità di partecipare e comunicare in rete senza rivelare la propria identità contrasta con le iniziative che vengono attualmente sviluppate a sostegno di altri settori importanti come la lotta contro il contenuto illegale e nocivo, le frodi finanziarie o le violazioni al diritto d'autore.

Naturalmente questo apparente conflitto tra diversi obiettivi politici non è nuovo e, come sottolinea il Libro verde della Commissione sulla tutela dei minori e della dignità umana nei servizi audiovisivi e d'informazione, la Convenzione europea per la salvaguardia dei diritti dell'uomo già offre un quadro per la soluzione di tali conflitti: una serie di diritti fondamentali soggetti a talune restrizioni per ragioni specifiche, fra le quali la prevenzione del crimine.

Nell'esaminare tali restrizioni la giurisprudenza della Corte europea per i diritti dell'uomo ha sviluppato il principio di proporzionalità come criterio fondamentale per valutare la conformità di eventuali misure restrittive applicate ai diritti fondamentali garantiti dalla Convenzione.

Il fatto che si sia sviluppata tale giurisprudenza dimostra che è sempre stato necessario trovare un equilibrio fra obiettivi politici contrastanti. Nel contesto degli strumenti di comunicazione più tradizionali "fuori della rete" come lettere e plichi postali, telefono, giornali o trasmissioni radio-televisive, è stato possibile raggiungere un equilibrio fra questi obiettivi. La sfida che debbono affrontare oggi i politici consiste nell'assicurare che questa impostazione equilibrata, che garantisce i diritti fondamentali consentendo restrizioni proporzionate, in circostanze

limitate e specifiche, venga mantenuta nel nuovo contesto del ciber-spazio. Un elemento fondamentale ai fini di questo equilibrio sarà costituito dall'ampiezza e dai limiti stabiliti alle possibilità di una persona ad intervenire sulla rete mantenendo l'anonimato.

Imparando dal passato per trovare le soluzioni per il futuro

Sussiste un consenso generale sul fatto che l'attività su Internet non può sottrarsi ai principi giuridici fondamentali che vengono normalmente applicati. Internet non può costituire una zona franca dove le regole della società non vengono applicate. D'altronde, le possibilità degli Stati e delle autorità pubbliche di limitare i diritti degli individui e controllare comportamenti potenzialmente illegali non dovrebbero essere più ampie nel quadro di Internet di quanto possano esserlo nel mondo fuori della rete. L'esigenza che le limitazioni ai diritti e alle libertà fondamentali siano debitamente giustificate, necessarie e proporzionate alla luce degli altri pubblici obiettivi, deve valere anche nel ciber-spazio.

Il principio di trattare Internet esattamente come le altre tecnologie si rispecchia sia nell'introduzione alla Comunicazione della Commissione sul contenuto illegale e nocivo su Internet che stabilisce "che quello che è illegale fuori della rete rimane illegale anche sulla rete" e nella relazione del gruppo di lavoro sul contenuto illegale e nocivo su Internet che afferma nella sua seconda proposta di azione il principio che "l'informazione su Internet deve avere lo stesso libero flusso consentito all'informazione cartacea".

Sul problema fondamentale dell'anonimato bisogna seguire la stessa impostazione. Come dichiarato correttamente nella "Dichiarazione ministeriale di Bonn"³⁾, il principio da seguire deve essere che quando l'utilizzatore può scegliere di mantenere l'anonimato fuori della rete, tale possibilità deve sussistere anche sulla rete. I vari servizi e attività disponibili su Internet devono essere esaminati, e dove ciò sia possibile, debbono essere stabilite delle analogie con i servizi esistenti che utilizzano modalità di comunicazione e strumenti di consegna più tradizionali. Tali raffronti forniranno un quadro approfondito di quei settori dove è auspicabile la possibilità di mantenere l'anonimato e di quelli in cui non lo è.

Posta elettronica (corrispondenza da punto a punto attraverso Internet)

La maggior parte delle comunicazioni in posta elettronica identificano correntemente lo spediteur sia attraverso il suo indirizzo e-mail o attraverso l'indirizzo IP. Questa informazione è di solito disponibile sia per il destinatario della posta elettronica che per i fornitori di accesso e di servizi che partecipano alla prestazione del servizio posta elettronica. Vi sono tuttavia due tipi di soluzioni alternative che possono offrire un certo grado di anonimato:

1) servizi anonimi di ritrasmissione di posta elettronica - si tratta di un'opzione offerta dal fornitore di accesso o quando una persona si avvale di un servizio specifico "anonimizzante" al quale egli invia la propria posta elettronica. Il ritrasmettitore anonimo invierà il messaggio in forma anonima;

3) Dichiarazione della Conferenza ministeriale di Bonn sulle reti d'informazione globali, 6-8 luglio 1997.

2) accesso anonimo alla rete - in questo caso una persona può accedere a Internet mantenendo l'anonimato, ad esempio pagando in anticipo un certo importo di tempo in rete e ricevendo un indirizzo anonimo di posta elettronica o accedendo alla rete attraverso un chiosco pubblico di Internet.

I servizi di ritrasmissione anonima implicano la conservazione di un collegamento fra lo speditore del messaggio e il messaggio stesso che può essere ricostruito in una fase successiva, ad esempio nel quadro di un'indagine di polizia. Quindi esso non garantisce l'anonimato come permette invece la seconda alternativa e vi è la necessità di introdurre delle regole sull'uso fatto dal servizio di ritrasmissione dei dati identificabili che esso conserva. Tuttavia entrambe queste possibilità offrono importanti vantaggi ai fini della riservatezza degli individui e debbono essere salvaguardate e promosse.

L'esistenza di una possibilità di anonimato per la posta elettronica è particolarmente importante se si raffronta il servizio con altre tecnologie delle comunicazioni da punto a punto più tradizionali. Il vecchio servizio postale, ad esempio, è molto più favorevole alla riservatezza, in quanto la spedizione di una lettera normale può avvenire in un totale anonimato. Il servizio postale non è in grado di raccogliere dati transazionali identificabili circa il mittente della comunicazione (a meno che quest'ultimo scelga di rivelarsi sul lato esterno della busta). Il sistema di pagamento più comune (il francobollo postale) è anch'esso totalmente anonimo. È inoltre possibile per il mittente mantenere l'anonimato anche nei confronti del destinatario di una lettera.

I servizi di telefonia tradizionali offrono inoltre un maggior grado di anonimato rispetto alla posta elettronica. L'ampia disponibilità di chioschi pubblici consente un accesso anonimo alla rete e i servizi possono essere pagati con denaro liquido o con carte prepagate anonime. Le chiamate telefoniche eseguite in questo modo non creano dati transazionali identificabili. Quando un abbonato chiama utilizzando il proprio telefono, tuttavia, vengono prodotti dei dati transazionali ed è stato necessario introdurre delle regole sulla produzione di tali dati (attualmente è in atto un processo di armonizzazione a livello comunitario in conseguenza della direttiva "ISDN"⁴) allo scopo di limitare il periodo di conservazione di tali dati e le finalità per le quali essi possono essere utilizzati). Nondimeno, chi chiama resterà sconosciuto per il destinatario di una telefonata finché quest'ultimo non solleva il telefono, a meno che sia funzionante un sistema di identificazione delle chiamate, che consente di indicare il numero dell'apparecchio di chi chiama sull'apparecchio del destinatario prima che questi risponda. L'impatto di tale sistema sulla riservatezza delle parti nelle chiamate telefoniche è tale, tuttavia, che si è ritenuto necessario inserire un articolo specifico nella direttiva citata sopra, che assicuri la possibilità per l'utente di bloccare la trasmissione del proprio numero quando questi desidera farlo. Questa disposizione costituisce un precedente che può essere preso in considerazione nel campo della corrispondenza sulla rete da punto a punto.

4) Direttiva 97/66/CE del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla protezione della riservatezza nel settore delle telecomunicazioni, adottata, ma non ancora pubblicata.

Vi possono essere circostanze nelle quali si giustificano restrizioni alle comunicazioni anonime con la posta elettronica, ad esempio se vi è ragione di sospettare che una particolare comunicazione sia collegata alla preparazione di un atto di terrorismo o di altro grave atto criminale. Tali restrizioni possono comportare che un ritrasmettitore anonimo sia tenuto a fornire alla autorità di polizia la vera identità dei soggetti di una comunicazione. Tuttavia, tali restrizioni dovrebbero rispettare il criterio della proporzionalità ed essere rigidamente applicate in base ai casi individuali.

Newsgroups, Bulletin Boards, e altre sedi di dibattito pubblico

La comunicazione attraverso Internet non assume sempre la forma di corrispondenza privata da punto a punto. Le "newsgroups" e "chat rooms" dedicate ad argomenti particolari o a interessi comuni sono numerose e molto popolari. Qui le persone che contribuiscono con del materiale lo fanno sapendo che esso deve essere accessibile a un vasto pubblico che potrebbe includere bambini o altri soggetti vulnerabili. In tale situazione sussiste un'autentica preoccupazione per la natura dei contenuti che vengono offerti e la necessità di assicurare che contenuti non adeguati non possano essere resi disponibili in queste sedi aperte e/o che sussista una responsabilità qualora ne emerga l'illegalità.

Vi sono varie possibilità con le quali può essere esercitato un certo controllo su questi newsgroups. Un suggerimento è che tutti coloro che contribuiscono con del materiale possano essere identificati, e che venga tenuta traccia dei dati quando viene presentato del materiale. Tuttavia, ci si può chiedere se questa sia una soluzione proporzionata e praticabile al problema. Dopo tutto, nel mondo non virtuale, vi sono numerose bacheche collocate nei posti di lavoro, in scuole e università, sulle quali i singoli sono invitati ad apporre del materiale. Non è concepibile che l'accesso a tali bacheche possa essere rigidamente controllato in maniera analoga.

Tuttavia, esistono anche altre possibilità. Ad esempio, possono essere sviluppate soluzioni contrattuali atte a garantire un certo grado di "qualità del contenuto". Il fornitore del servizio di newsgroup potrebbe assicurare la partecipazione costante di un moderatore ai newsgroups, il cui ruolo sarebbe di controllare i contributi, per individuare un eventuale contenuto illegale e nocivo. Tale moderatore potrebbe assicurare che il contenuto non adeguato possa essere rapidamente eliminato e che le persone responsabili di tale materiale possano essere allontanate dal gruppo. Le chat line e party line telefoniche hanno sempre utilizzato tali meccanismi per controllare il comportamento dei partecipanti. È anche possibile attribuire ai fornitori di servizi un certo grado di responsabilità giuridica per il materiale che viene messo a disposizione, suscitando in tal modo in essi un interesse diretto ad esaminare tutto il materiale che entra e pubblicando solo quello che è considerato legale e accettabile per il consumo del pubblico. In questo scenario è possibile conservare l'anonimato dei contributori, mentre il fornitore di servizi assume un ruolo analogo a quello del direttore per la rubrica della posta di un quotidiano.

Questo potrebbe anche essere un settore dove le soluzioni tecnologiche potrebbero svolgere un ruolo importante. Se l'accesso completamente anonimo ad alcuni centri di discussione dovesse porre dei problemi, gli utilizzatori potrebbero essere autorizzati ad accedere sulla base di una "pseudoidentità" attribuita loro da un fornitore di servizi specializzato analogo ai ritrasmettitori anonimi di cui sopra. In tali

casi, mentre l'anonimato sarebbe normalmente rispettato, in caso di sospetta attività criminale, sarebbe possibile risalire alla vera identità dell'utilizzatore.

È chiaro che contributi interamente anonimi a questi centri di discussione sollevano difficoltà, che non sussistono nel caso della semplice comunicazione da punto a punto, e che debbono essere sviluppati meccanismi adeguati per impedire abusi. Tuttavia, i diritti fondamentali alla riservatezza e alla libertà di espressione non devono essere limitati in maniera sproporzionata da sistemi di identificazione obbligatori, in particolare quando sono disponibili altri strumenti più adeguati di controllo e moderazione del contenuto.

La navigazione passiva per i vari siti su Internet

La maggior parte dei siti di Internet esistono soprattutto per fornire informazioni al grande pubblico e milioni di individui trascorrono il loro tempo sulla rete navigando oziosamente per la miriade di diversi siti disponibili.

La più stretta analogia con questa pratica nel mondo non virtuale potrebbe essere quella del girare in una libreria o in una biblioteca o per i negozi in una città. Come per il navigare in rete, spesso non vi è l'intenzione di acquistare, ma semplicemente si è spinti dalla curiosità a vedere quello che è disponibile. Una differenza chiave, tuttavia, è che mentre il girare in una libreria o per negozi può essere fatto nell'anonimato pressoché completo, la stessa azione fatta sulla rete lascia invariabilmente una traccia digitale permanente e individuabile.

Non vi è una giustificazione dell'interesse generale o di ordine politico perché tali tracce possano essere identificabili, a meno che l'utilizzatore desidera che lo siano. Naturalmente la raccolta dei nomi e indirizzi di posta elettronica dei visitatori di un determinato sito commerciale costituiranno dei dati importanti per il proprietario del sito, che può voler usarlo a fini commerciali. Tuttavia, una simile raccolta di dati di individui che si limitano a navigare dev'essere totalmente trasparente e deve avvenire sulla base dell'autorizzazione dell'utilizzatore. Quanti desiderano navigare sulla rete anonimamente debbono essere liberi e in grado di farlo.

Acquisto di beni e servizi su Internet

Man mano che vengono sviluppati strumenti di pagamento sicuri, assieme a meccanismi relativi all'integrità dei dati e all'autenticazione delle operazioni (ad esempio firma digitale), Internet diventerà sempre di più un'area fondamentale di attività commerciale dove si va non solo per ottenere informazioni, ma anche per acquistare beni e servizi. In questo contesto sorge il problema se una persona per poter fare acquisti attraverso Internet debba poter essere identificabile o se debba sempre essere disponibile l'opzione dell'anonimato.

Nel mondo non virtuale i pagamenti anonimi effettuati con denaro liquido sono comuni e questa è considerata la modalità di pagamento più conveniente ed efficiente per beni e servizi, in particolare nel caso di somme relativamente modeste di denaro. Il venditore del negozietto all'angolo non è interessato tanto all'identità del cliente, quanto al fatto che il denaro che gli viene offerto sia moneta avente corso legale.

Per gli acquisti più importanti è spesso scomodo sia per l'acquirente che per il venditore utilizzare denaro liquido. Le banconote occupano molto spazio in un portafoglio o nella cassa. Tenere molto denaro liquido comporta poi il problema della sicurezza. Per queste ragioni i metodi di pagamento non anonimi come assegni o carte di credito tendono a essere preferiti quando l'importo dell'acquisto è importante.

Naturalmente quando il pagamento viene effettuato utilizzando il credito, l'anonimato non è più un'opzione. Quando si acquista a credito, l'individuo incorre in un debito per il quale è responsabile. E naturalmente ci dev'essere una registrazione che collega l'individuo al debito sorto. Quando viene utilizzata una carta di credito convenzionale la responsabilità della persona è nei confronti dell'emittente della carta piuttosto che direttamente nei confronti del venditore, tuttavia è necessaria una traccia identificabile dell'operazione.

Il commercio elettronico attraverso Internet in linea di principio dovrebbe seguire il modello che è stato stabilito per i pagamenti fuori della rete. I singoli dovrebbero poter scegliere attraverso una varietà di metodi di pagamento sicuri, fra i quali dovrebbe esserci la possibilità di un sistema anonimo. I pagamenti in moneta elettronica dovrebbero offrire decisamente vantaggi rispetto a quelli tradizionali effettuati con denaro liquido, in modo da renderli più attraenti. Anzitutto possono essere conservati importi illimitati, ad esempio, su una piccola carta. In secondo luogo, la carta, senza incidere sull'anonimato, potrebbe prevedere aspetti connessi alla sicurezza come un codice di accesso individuale noto solo all'acquirente, che ridurrebbe notevolmente i rischi nel caso di perdita della carta. Questi aspetti potrebbero fare della moneta elettronica anonima un'opzione attraente anche per i grandi acquisti effettuati sulla rete.

Un requisito fondamentale è che tale moneta elettronica sia "denaro effettivo" verificabile. Ciò implica l'inclusione di tecniche anticontraffazione che garantiscano l'autenticità della moneta elettronica, senza incidere sulla possibilità di utilizzarla in maniera anonima.

Tuttavia vi sono altre considerazioni che devono essere tenute presenti nel valutare la auspicabilità dei metodi di pagamento anonimi sulla rete. Principale fra esse è la lotta contro il riciclaggio del denaro sporco. Il riciclaggio di importanti somme di denaro ottenuto da attività illecite come il traffico di droga, sia in modo anonimo sia utilizzando un'identità fittizia, costituisce un grave problema. Per contribuire a combattere questa attività, nel 1991 è stata adottata una direttiva (91/308/CEE) che cerca di impedire l'uso del sistema finanziario a fini di riciclaggio. Le disposizioni chiave di questa direttiva impongono alle istituzioni finanziarie e creditizie di esigere l'identità dei loro clienti prima di entrare in rapporti d'affari con essi e mantenere delle registrazioni delle operazioni effettuate per almeno un periodo di cinque anni.

La direttiva in se stessa non è tuttavia incompatibile con i pagamenti anonimi. Essa si concentra anzitutto sulle operazioni effettuate con banche o altre istituzioni⁵⁾, mentre i sistemi di pagamento elettronico sarebbero utilizzati essenzialmente per operazioni fra soggetti e commercianti che non fanno parte del sistema finanziario. Sarebbe nor-

5) L'articolo 12 comprende una disposizione che nel suo campo di applicazione potrebbe venire estesa a settori come le case da gioco e i commercianti di oggetti di elevato valore (arte, antiquariato, proprietà immobiliare, metalli preziosi).

male per una persona dover dimostrare la propria identità prima di effettuare un prelievo elettronico da una banca, e magari al momento di depositare importanti somme di moneta elettronica. Ma una volta che il denaro gli viene accreditato, non vi è ragione perché esso non sia anonimo come avviene per il denaro tradizionale. Le esigenze delle autorità di polizia nella loro opera di individuazione dei responsabili dei reati di riciclaggio debbono quindi essere vagliate molto attentamente rispetto ai vantaggi per la riservatezza che i pagamenti anonimi offrono. Limiti all'uso del pagamento anonimo possono essere introdotti, ma solo quando vi è la prova evidente che l'anonimato di una operazione può pregiudicare l'individuazione di un fenomeno di riciclaggio. Le operazioni di valore modesto non dovrebbero porre un problema a questo riguardo e anche le operazioni più importanti (ad esempio l'acquisto di un software costoso sulla rete) non significano necessariamente forme di riciclaggio.

RIASSUNTO DELLE PRINCIPALI CONCLUSIONI

- La possibilità di scegliere di restare anonimi è essenziale ai fini della tutela, per i singoli, sulla rete dello stesso grado di riservatezza esistente attualmente fuori della rete.
- L'anonimato non è adatto in tutte le circostanze. Stabilire le circostanze in cui l'opzione dell'anonimato è opportuna e quelle in cui non lo è, comporta un attento confronto fra i diritti fondamentali, non solo nei confronti della riservatezza, ma anche della libertà di espressione, e altri importanti obiettivi politici come la prevenzione del crimine. Le limitazioni di ordine giuridico che possono essere imposte dai governi al diritto di restare anonimi, o sugli strumenti tecnici per farlo (ad esempio disponibilità di prodotti cifrati), dovrebbero essere sempre proporzionate e limitate a quello che è necessario per proteggere uno specifico interesse pubblico in una società democratica.
- Dove possibile, l'equilibrio che è stato raggiunto in relazione alle precedenti tecnologie dovrebbe essere mantenuto per quanto riguarda i servizi offerti attraverso Internet.
- L'invio di posta elettronica, il navigare fra i siti della rete e l'acquisto di merci e servizi attraverso Internet dovrebbero essere tutti possibili in via anonima.
- Alcuni controlli sui soggetti che contribuiscono con del materiale a centri di discussione sulla rete (news-group, ecc.) sono necessari, ma il requisito imposto ai soggetti di identificarsi, nella maggior parte dei casi è sproporzionato e impraticabile. Devono essere preferite altre soluzioni.
- Gli strumenti anonimi per accedere a Internet (ad esempio chioschi pubblici di Internet, carte di accesso prepagate) e gli strumenti anonimi di pagamento sono due elementi essenziali per un vero anonimato sulla rete.

Mettere in pratica le conclusioni - Raccomandazioni operative

Le conclusioni di cui sopra, che sono essenzialmente relative all'estensione del diritto legittimo di una persona all'anonimato nel contesto di Internet, illuminano la situazione che deve essere realizzata se non si

vuole erodere la riservatezza dell'individuo. La situazione attuale è molto diversa. L'accesso dell'utilizzatore e l'attività su Internet solo raramente sono anonime. Gli sforzi per fornire servizi semianonimi (ad esempio ritrasmettitori anonimi) hanno posto regolarmente dei problemi, in quanto la configurazione tecnica sui protocolli Internet non consente facilmente un vero anonimato e gli strumenti di pagamento più diffusi sulla rete restano le carte di credito, mentre esperimenti con la moneta elettronica anonima debbono ancora affermarsi sul mercato elettronico tradizionale.

Perché questa situazione cambi, bisogna trovare il modo di mettere in pratica queste conclusioni. Debbono essere intraprese delle iniziative a una serie di livelli diversi:

1) *Ambiente normativo*

Il principio che la raccolta di dati personali identificabili deve essere limitata al minimo necessario, dov'essere riconosciuto nelle legislazioni nazionali e internazionali che si occupano di Internet. Inoltre esso deve essere incluso nei codici di condotta, nelle linee guida degli altri strumenti di "soft law" che vengono sviluppati. Dove ciò sia appropriato, il principio deve specificare che ci deve sempre essere la possibilità di conservare l'anonimato.

2) *Contesto tecnologico*

Le discussioni nel quadro del consorzio della rete Internet dovrebbero essere intensificate al fine di sviluppare l'infrastruttura e i protocolli Internet che conducono all'attività dell'utilizzatore anonimo.

Il finanziamento della ricerca e dello sviluppo (come quella disponibile nel quadro del 5° programma quadro di ricerca e sviluppo tecnologico) dovrebbero essere mirate specificamente a progetti che cercano di sviluppare strumenti anonimi di pagamento attraverso Internet e strumenti di accesso anonimi (ad esempio, terminali pubblici Internet).

3) *Ambiente economico*

I governi dovrebbero esaminare le modalità per fornire un sostegno economico diretto a promuovere la diffusa adozione sul mercato di tecnologie che migliorano la riservatezza e consentono agli utilizzatori di restare anonimi. Ad esempio, un governo potrebbe utilizzare il proprio potere di mercato come cliente maggiore per prodotti e servizi della tecnologia delle informazioni e includere i requisiti sulla riservatezza e l'anonimato fra i criteri per il proprio appalto pubblico. Bisogna anche prendere in considerazione la necessità di prodotti e servizi che favoriscano la riservatezza attraverso sovvenzioni o agevolazioni fiscali, come avviene nel caso di prodotti ecologici come la benzina senza piombo.

4) *Accrescere la consapevolezza fra gli utilizzatori di Internet, i fornitori di accesso e di servizi e l'industria della tecnologia dell'informazione*

La maggior parte degli utilizzatori di Internet non si rende conto dei rischi che corre la loro riservatezza a causa dell'attività da essi svolta sulla rete. Vi è una necessità urgente di fornire consulenza e orientamenti a questo riguardo. Le autorità per la protezione dei dati in tutto il mondo hanno un importante ruolo da svolgere nel fornire tale consu-

lenza. Gli orientamenti prodotti dalla commissione spagnola per la protezione dei dati indicano la strada da seguire. Bisogna preoccuparsi di assicurare la diffusione più ampia possibile di tale consulenza alla comunità Internet.

Anche quelli che raccolgono ed elaborano i dati attraverso Internet (fornitori di accesso, fornitori di servizi, siti web) debbono essere coscienti che sono già soggetti alle legislazioni esistenti in materia di protezione dei dati che richiedono, fra l'altro, trasparenza e apertura nella raccolta dei dati e che limitano le finalità per cui i dati personali possono essere utilizzati e pubblicati.
