

PRIVACY E DIRITTO PENALE

La perdita o, più realisticamente, la compressione della privacy rappresenta sicuramente la più grossa preoccupazione connessa alla diffusione delle tecnologie informatiche. In effetti, ci si trova al cospetto di prospettive di sviluppo e di innovazione tecnologica che, se sembrano da un lato allontanare (non fosse altro per il numero enorme di soggetti coinvolti) l'antico incubo Orwelliano, delineano dall'altro un modello di società profondamente diverso dai precedenti, i cui contorni appaiono in continuo divenire.

La realizzazione di tale modello, fondata sulla massima liberalizzazione e interconnessione dei servizi e delle infrastrutture di comunicazione, renderà già nel breve periodo realizzabili innovazioni che fino a poco tempo addietro apparivano per lo meno futuristiche.¹

Tuttavia, non poche delle attuali applicazioni di tali tecnologie generano, proprio rispetto alla privacy, grossi interrogativi.

¹ Basti pensare all'insegnamento a distanza, alla *web-tv*, al telelavoro, alla telemedicina, fino alle più svariate opportunità di sviluppo in tutti i settori chiave dell'economia (finanza, credito, produzione industriale, ricerca scientifica ecc.).

Società private, liberi professionisti e strutture statali raccolgono una quantità impressionante di dati su ogni singolo cittadino, e spesso non si ha la minima idea di come vengano utilizzati, o di quanto siano dettagliati. Archivi medici, automobilistici, scolastici, giudiziari, bancari, fiscali, profili lavorativi e rendiconti di carte di credito contribuiscono a delineare il profilo di ciascuno di noi.

Il fatto che le informazioni siano disseminate in luoghi diversi protegge in qualche modo la privacy, ma non appena la diffusione dei collegamenti fra le varie banche-dati sarà capillare -e la tendenza verso tale direzione sembra irreversibile- il computer potrà essere utilizzato per metterle in correlazione, raffrontarle ed elaborarle.² Se a ciò si aggiunge che l'attuale tecnologia su cui si basa il funzionamento della rete INTERNET - strumento principe per

² Ai sensi dell'art. 1 della legge 675/96, per banca-dati si intende qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento. È tuttavia evidente che una tale definizione ha una validità limitata al contesto cui si riferisce giacché le banche-dati sono deputate alla conservazione di qualsiasi genere di dati e non solo di quelli personali.

l'interconnessione fra i computer e, quindi, fra le banche dati - non è in grado di garantire la tutela della privacy degli utenti, si delinea un quadro davvero poco rassicurante.

Ogni utilizzatore della rete, infatti, lascia dietro di sé tutta una serie di informazioni idonee a identificarlo e a tracciarne un accurato profilo. Ha fatto, ad esempio, scalpore la notizia secondo cui un particolare software (un semplice javascript), necessario a consultare i dati reperibili sulla rete INTERNET, sarebbe in grado di registrare una serie di dati e informazioni relative agli utenti della rete.

Secondo alcune fonti, uno studente americano avrebbe sviluppato un software in grado di controllare, ogni secondo, in quale posizione della rete un determinato utente è situato, inviando successivamente ad un computer le risultanze da registrare. Altri hanno già sviluppato dei programmi, compilati con il linguaggio di programmazione Java, capaci di identificare e riportare nome, cognome ed indirizzo e-mail (o posta elettronica) dei singoli utenti che accedono ai siti INTERNET.

Sembra che la rilevazione di tali rischi abbia sollecitato le case sviluppatrici delle applicazioni Java a studiare nuovi sistemi di sicurezza capaci di neutralizzare le potenzialità indesiderate dei software stessi³.

Il problema è accentuato dal fatto che presto verranno collegati alla rete INTERNET, dal momento che l'accesso alle reti telematiche è possibile anche via etere, i network televisivi (c.d. Web-Tv), che potranno ampliare assai sensibilmente il numero degli utenti collegati e, quindi, il numero dei soggetti potenzialmente schedabili.

“Si è, così, verificato ancora una volta (ma il rilievo vale con riferimento a tutta la criminalità informatica e, quindi, anche fuori dal campo della riservatezza) quel fenomeno tipico di molte conquiste tecnologiche. Non è infrequente, infatti, che i nuovi mezzi resi disponibili dai progressi scientifici, nell'arrecare immediato vantaggio alla collettività per i fini in vista dei quali sono stati pensati

³ Detti avvenimenti sono ricordati da Riccardo Imperiali e Rosario Imperiali in *“La tutela dei dati personali”*, Milano, 1997, pagg. 19 e 20.

*e realizzati, creino, nel contempo nuovi pericoli, sia in sé, sia per l'uso distorto che può farsene.”*⁴

Non a caso la formulazione del concetto di privacy nacque come reazione al primo grande mutamento tecnologico che la storia ricordi: la rivoluzione industriale. Nella sua accezione originaria volle significare una difesa dall'intrusione della prima forma storica di mass-media, costituita dalla stampa, e si sostanziò nella breve ma incisiva frase: “*right to be let alone*” (letteralmente, diritto ad essere lasciati soli)⁵.

La trasformazione della moderna società, nella quale assume grande importanza l'informazione, oltre ad un'accresciuta attenzione per i diritti della personalità, ha comportato una progressiva rivisitazione del concetto di riservatezza, oggi inteso, più restrittivamente, come

⁴ M. Petrone in Relazione presentata al convegno internazionale “*La criminalità informatica: prevenzione e repressione*”, organizzata dal C.E.D. della Corte di Cassazione a Roma nei giorni 4-6 dicembre 1986.

⁵ Warren-Brandeis “*The right to privacy*” in Harvard Law Review 1881, 4, pag. 193.

interesse alla sottrazione di un irrinunciabile ambito vitale all'altrui conoscenza. Tale evoluzione è dovuta ad un duplice ordine di fattori: da un lato, la compressione del diritto di riservatezza è causata da confliggenti e irrinunciabili diritti, necessari per il corretto funzionamento del sistema democratico; dall'altro, dalla constatazione che le nuove possibili forme di aggressione alla privacy, attraverso l'elaborazione delle informazioni custodite nelle banche-dati, non hanno più una dimensione individuale bensì collettiva perché il trattamento automatizzato delle informazioni può ormai coinvolgere milioni di persone.

Un esempio, per quanto datato, può chiarire l'evoluzione in senso collettivo del fenomeno: nel 1972 la R.L. Polk and Company, società specializzata nelle ricerche di mercato, era riuscita a schedare le abitudini di circa 130 milioni di americani⁶. È quindi evidente come il rapporto fra soggetto titolare delle informazioni, potenziale vittima, e

⁶ Il caso è riportato da Westin-Baker "*Data-Banks in a free society*", New York, 1972, pag. 156.

gestore della banca-dati sia depersonalizzato, anzi le informazioni relative ad una singola persona acquistano valore se, e solo se, relazionate a tutte le altre. Da quanto detto discende chiaramente che ci si trova dinanzi ad un interesse collettivo alla corretta gestione dei dati personali, che è però suddivisibile in *“una serie di situazione soggettive singole.”*⁷

L'evoluzione in senso “dinamico” della privacy, da diritto personale al segreto ad interesse collettivo alla corretta gestione dei dati personali, si riflette sulla sua stessa protezione. Infatti, il controllo sulla gestione e sulla circolazione dei dati personali presuppone che la tutela spieghi i suoi effetti su più livelli: dalla possibilità di impedire che detti dati vengano raccolti, alla facoltà di aggiornarli o rettificarli, fino al diritto ad ottenerne la cancellazione o la trasformazione in forma anonima.

L'atteggiarsi della privacy ad interesse collettivo, o meglio a bene collettivo o superindividuale, pone in termini assai problematici il

⁷ A. Manna *“Beni della personalità e tutela penale”*, Bologna, 1993, pag. 339.

ruolo che è chiamato a svolgere il diritto penale (posto che il ricorso alla sanzione penale è giustificato dalla valenza costituzionale del diritto alla riservatezza -che trova fondamento negli articoli 2 e 3 della Costituzione- e dalla grande pericolosità che deriva dall'elaborazione informatica dei dati personali). Infatti, gli interessi diffusi o collettivi sono caratterizzati dal fatto di omologare una serie indeterminata di posizioni di vantaggio o di bisogno individuale, così che l'offesa all'interesse superindividuale si rivela capace di incidere su una pluralità di situazioni individuali. *“Se, dunque, gli interessi diffusi e collettivi sono caratterizzati dall'alto, e talvolta indeterminato, numero di posizioni mediatamente coinvolte, ciò significa che costituiscono di regola lo strumento concettuale per un'anticipazione della tutela.”*⁸

⁸ F. Palazzo *“I confini della tutela penale: selezione dei beni e criteri di criminalizzazione”*, in AA.VV. *op. cit.*, pag. 122.

La protezione di tali beni è quindi concretamente realizzabile solo con il ricorso allo schema del reato di pericolo astratto, con una conseguente anticipazione dell'area del penalmente rilevante al livello del semplice pericolo. Ciò non deve giustificare le preoccupazioni di quella parte della dottrina che teme un uso eccessivo dello strumento penale a discapito del diritto penale quale *extrema ratio* (c.d. tendenza alla panpenalizzazione)⁹. Infatti, il legislatore nella scelta delle condotte punibili incontra sempre i limiti imposti dalla riserva di legge, dalla sufficiente determinatezza delle fattispecie incriminatrici e dalla necessaria offensività della condotta, principi questi, idonei a restringere l'operatività del diritto penale unicamente a quei comportamenti rispetto ai quali le sanzioni extrapenali sarebbero insufficienti.

⁹ G. Pecorella "Aspetti penalistici della regolamentazione delle banche-dati", in AA.VV. "Le banche-dati in Italia", Napoli, 1985, pag. 150.