MARINO PETRONE

BANCHE DEI DATI E TUTELA DELLA « PRIVACY ». RIFLESSI PENALISTICI

SOMMARIO 1. Reati informatici e attentati alla privacy: particolarità. — 2. Potere informatico, offese alla riservatezza e libertà informatica. — 3. Le norme penali attualmente applicabili. — 4. La costruzione di un sistema specifico di tutela penale. Gli interessi confliggenti ed il loro bilanciamento. — 5. I tre possibili sistemi di valutazione legislativa dell'attività delle banche-dati. I criteri per la costruzione del sistema specifico di tutela penale. — 6. I progetti di legge pendenti alla Camera dei Deputati. Conclusioni.

1. Reati informatici e attentati alla privacy: particolarità.

Nell'ambito dell'ampia categoria dei cosiddetti *reati informatici*, quelli consistenti in una offesa alla sfera della riservatezza sono stati senza dubbio i primi a richiamare l'attenzione degli studiosi. E ciò a seguito della enorme diffusione delle banche di dati e della immediata constatazione dei rischi da esse derivanti.

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 fini in vista dei quali, appunto, sono stati pensati e realizzati, creino, nel contempo, nuovi pericoli, sia in sé, sia per l'uso distorto che può farsene.

L'atteggiamento di entusiastica ammirazione circa l'immensa potenzialità di un elaboratore elettronico — talora definito soltanto « protesi elettronica dell'intelligenza umana », ma, talaltra, elevato addirittura al rango di essere ragionante (« umanoide », ad esempio, lo si è pure definito) — ha condotto in breve ad una sorta di psicosi sociale, materiata di incondizionata fiducia nei poteri del nuovo « essere » (la cosiddetta « mistica del computer », condizione, tuttavia,

* Il presente scritto riproduce la relazione presentata al Convegno internazionale « La criminalità informatica: prevenzione e repressione » organizzato dal Centro Elettronico di Documentazione della Corte di Cassazione, a Roma i giorni 4-6 dicembre 1986.

essa stessa, per la commissione di tanti reati). Ma, nel contempo, sono emersi i rischi immanenti alla nuova tecnologia ed, in particolare, alla disponibilità, da parte dei gestori delle banche-dati, di una immensa quantità di informazioni sui singoli e sui gruppi sociali.

L'esigenza di tutelare la privacy dall'invadenza dei sistemi informatici si è, quindi, imposta in breve nello studio della complessa fenomenologia concernente la criminalità informatica.

È bene, tuttavia, avvertire che la tutela della riservatezza dall'uso distorto dei computer si colloca su di un piano particolare, nel quadro di quella fenomenologia. Non si tratta, qui, di proteggere beni patrimoniali, come, invece, accade in prevalenza negli altri settori individuabili nell'ambito predetto (ad esempio, le cosiddette truffe col computer o gli abusi del Bancomat ovvero quelli dell'EFT), bensì di salvaguardare un fondamentale diritto della persona umana che, come vedremo, riceve garanzia a livello costituzionale.

2. Potere informatico offese alla riservatezza e libertà informatica.

È innegabile che, tramite una banca di dati, si possano recare attentati alla riservatezza, intesa nel senso ristretto e, quindi, anche se non comprensiva dell'onore o del segreto. Le *forme di aggressione* a tale interesse, infatti, possono essere molteplici e vanno dalla tradizionale violazione di domicilio (art. 614 cod. pen.) alle interferenze illecite nella vita privata, vietate dal nostro codice penale tramite la previsione di cui all'art. 615-*bis*, introdotta dalla legge n. 98 del 1974 proprio per adeguare il sistema ai progressi della tecnologia. Ma un'ulteriore modalità della condotta offensiva, certamente più subdola per tutti i pericoli che racchiude, può individuarsi appunto nella raccolta di notizie concernenti i molteplici aspetti della personalità.

Non che i sistemi tradizionali di raccolta di dati non consentissero eguali attentati. È incontestabile, però, che l'elaboratore elettronico permette non soltanto di disporre dei dati stessi in tempi reali ma anche di aggregarli, elaborarli, per ottenere un prodotto nuovo che determina un vero salto di qualità. Integrando poi le notizie contenute in più banche di dati, attraverso un collegamento orizzontale, si potrebbe addirittura arrivare ad ottenere un *profilo completo* dell'identità e delle abitudini di vita di una persona.

Dalla conoscenza dei dati personali — specie di quelli c.d. *sensibili* — alla loro strumentalizzazione a fini di dominio, persecuzione o ricatto, il passo potrebbe essere assai breve.

La reazione contro i poteri del computer non ha tardato a manifestarsi. La gente invoca, quasi paradossalmente, un ritorno ai sistemi di documentazione tradizionale, anche perché essi, oltre a non consentire tali miracolose operazioni, finivano per proteggere con una invisibile pellicola — la polvere accumulatasi sui fascicoli — un altro innegabile interesse e cioè il cosiddetto *diritto all'oblio*.

All'elogio del computer è così seguita la sua demonizzazione. Ed, in verità, non può disconoscersi che, se il nuovo sofisticato strumento è veicolo di civiltà e di democrazia, tuttavia esso apre spaventose prospettive. Lo stesso possesso di dati personali da parte dei gestori dei grossi centri informatici è già di per sé un attentato alla privacy.

Guardato il problema in chiave giuridica, non si è tardato, così, ad individuare la nascita di un nuovo potere: il *potere informatico*. E, al tempo stesso, si è manifestata l'esigenza di contrapporre a quel potere una situazione soggettiva in funzione di tutela degli interessi compromessi dal suo esercizio, ossia la *libertà informatica*. Si è subito chiarito, poi, che essa ha non soltanto un contenuto *negativo*, come libertà, appunto, dalle arbitrarie ingerenze del potere informatico, ma anche un contenuto *positivo*, come diritto al controllo sui dati personali posseduti da terzi.

L'individuazione del punto di equilibrio tra le due situazioni confliggenti non è, peraltro, risultata agevole. E, del pari, complessa risulta la ricerca dei limiti in cui gli interessi coinvolti dall'uso del potere informatico possono essere tutelati tramite ricorso alla sanzione penale.

3. Le norme penali attualmente applicabili.

La ricognizione delle premesse sulla realtà del fenomeno e sull'impostazione generale datane sul piano giuridico, costituisce certo l'indispensabile quadro di riferimento per l'esame della sua rilevanza penale. Ma, fatte quelle premesse, la visuale penalistica si colloca su di un piano diverso, aprendo problemi nuovi. Si tratta, anzitutto, secondo un corretto metodo di indagine, di accertare se vi sono già nel sistema norme utilizzabili per la tutela di quegli interessi. Ed, in caso di esito negativo, di disegnare le linee del sistema da attuare.

Ora, quanto al primo momento, è bene ricordare che il divieto di analogia in campo penale non consente certo di forzare le figure criminose per adattarle, *per similitudinem*, alle nuove forme di attacco alla riservatezza.

E la ricerca sulla normativa penale applicabile alle offese alla cosiddetta riservatezza informatica non è, per la verità, molto produttiva. Prescindendo, ovviamente, dal considerare le norme a tutela dell'onore o del segreto (solo eventualmente applicabili, perché dotate di una diversa tipicità) occorre, così, prendere atto che le disposizioni poste a protezione di tale interesse non sono certo sufficienti a coprire le esigenze in questione. Se si eccettuano le poche, e di modesto valore sanzionatorio, norme penali dirette a garantire la riservatezza del lavoratore e contenute nello Statuto dei lavoratori (artt. 4, 5, 6 e, soprattutto, 8, in relazione alla disposizione sanzionatoria dell'art. 38), si deve rilevare come solo con la legge 1° aprile 1981, n. 121, si è realizzata una tutela specifica della riservatezza informatica.

La normativa penale, tuttavia, appare insufficiente anche in tale legge, per varie ragioni.

In primo luogo essa prevede come reato, nell'art. 12 (peraltro anche nella forma *colposa*) soltanto le condotte abusive di *comunicazione* o di *uso* dei dati, mentre non fa riferimento alla *raccolta* dei dati stessi. Non può, tuttavia, negarsi che gli abusi degli agenti pubblici, in tale fase, possano ricondursi a varie figure criminose tra quelle contenute nel Capo II del Titolo II del Libro II del cod. pen. ed, in particolare, alla fattispecie prevista dall'art. 323 (abuso d'ufficio).

In secondo luogo, la legge ha una portata del tutto settoriale, poiché riguarda solo il Centro elaborazione dati istituito presso il Ministero dell'interno. Esiste, è vero, in essa, una norma di carattere generale (art. 8, comma 4) con la quale si impone ad ogni amministratore, ente, impresa, associazione o privato che per qualsiasi scopo formi o detenga archivi magnetici nei quali vengano inseriti dati o informazioni di qualsivoglia natura concernenti cittadini italiani, di notificare l'esistenza dell'archivio al Ministero dell'interno. Ma si tratta solo di una disposizione posta a garanzia del controllo sull'*esistenza* delle banche-dati e non sulla loro *attività*. E, comunque, la norma si colloca ormai fuori dal sistema penale, poiché prevedeva la sola sanzione della multa, onde è rimasta travolta dalla depenalizzazione disposta con la legge n. 689 del 1981.

4. La costruzione di un sistema specifico di tutela penale. Gli interessi confliggenti ed il loro bilanciamento.

La costruzione di un sistema specifico di tutela della riservatezza informatica richiede, in primo luogo, l'individuazione degli interessi in gioco, e, quindi, la ricognizione della loro valenza, anzitutto sul piano costituzionale, al fine di operarne il bilanciamento.

Quanto al primo momento di indagine, è di immediata constatazione che il potere informatico può ricollegarsi sia ad interessi pubblici che ad interessi privati. La distinzione tra banche-dati *pubbliche* e *private* appare, in questo quadro, indispensabile per valutare la consistenza degli interessi confliggenti.

La raccolta ed elaborazione dei dati personali tramite banche-dati può, così, rispondere ad esigenze di interesse pubblico, come quelle di tutela dell'ordine pubblico o di giustizia (soprattutto penale) o di esercizio della libertà di comunicazione tramite la stampa o altri mezzi di comunicazione o di tutela della salute o di natura scientifica; ovvero ad interessi privati, in specie patrimoniali.

Sul versante opposto si colloca l'interesse dei singoli alla *disponibilità esclusiva dei dati personali*. Un interesse, questo, di natura *strumentale* poiché, a sua volta, è funzionalmente rivolto a garantire l'identità personale, l'intimità personale e familiare, la tranquillità. Tali situazioni soggettive, infatti, sono indubbiamente compromes-

se, quanto meno nella forma del *pericolo*, dall'esistenza di banche di dati personali, per l'*uso improprio* che di questi può farsi.

La consistenza di tali interessi e, quindi, la soluzione del conflitto che sorge fra di essi è, poi, diversa a seconda della natura del dato. Non vi è dubbio che, rispetto ai dati cosiddetti *neutri* (generalità, residenza, indirizzo, etc.) o, come pure li si è qualificati, *innocui*, l'interesse alla disponibilità esclusiva è meno intenso e, per ciò stesso, è più facile la prevalenza degli interessi contrapposti. Nei confronti dei dati cosiddetti *sensibili* (razza, religione, opinione politica, appartenenza a partiti o sindacati, condizioni di salute, etc.), invece, l'interesse alla disponibilità esclusiva è maggiore e, per ciò stesso, più facile è la sua prevalenza su quelli contrapposti. Anche se occorre riconoscere che un dato personale non può mai ritenersi innocuo, poiché anche da notizie in sé banali possono derivare strumentalizzazioni a danno del « titolare del dato ».

È indubbia, al tempo stesso, la rilevanza costituzionale di tutti questi interessi. Quelli sottesi al *potere informatico*, già ricordati, sono riconducibili, di volta in volta, agli artt. 21, 32, 33, 41, 112 Cost. Quelli sottesi alla *libertà informatica* si possono ricollegare fondamentalmente, salvo più specifiche sussunzioni (ad esempio, sotto gli artt. 14 e 15 Cost.), all'art. 2, comma 1, Cost., attenendo alla sfera inviolabile dell'uomo, come singolo o nei gruppi in cui si esprime la sua personalità.

Il loro bilanciamento appare, quindi, assai delicato e richiede, perciò, una attenta ed equilibrata ponderazione. Può qui già rilevarsi, tuttavia, che rispetto alla disponibilità esclusiva dei dati neutri si deve certamente considerare prevalente l'interesse alla tutela dell'ordine pubblico e della sicurezza pubblica o all'amministrazione della giustizia, mentre nessuna prevalenza potrebbe affermarsi rispetto all'interesse all'esclusiva disponibilità dei dati sensibili.

5. I TRE POSSIBILI SISTEMI DI VALUTAZIONE LEGISLATIVA DELL'ATTIVITÀ DELLE BANCHE-DATI. I CRITERI PER LA COSTRUZIONE DEL SISTEMA SPECIFICO DI TUTELA PENALE.

La reazione del legislatore alle nuove forme di attacco all'interesse all'esclusiva disponibilità dei dati personali (aggressioni che creano nuovi interessi strumentali) può determinarsi in modi diversi, riconducibili a tre distinti orientamenti.

1) Con l'indifferenza, lasciando quindi libera l'attività collegata alle nuove tecnologie (come accade attualmente, se pur in parte, in Italia). Si ha in tal caso una *liberalizzazione* dell'attività stessa.

2) Con l'opposto atteggiamento di divieto assoluto, ossia con la *criminalizzazione* (sia essa in termini di solo illecito extrapenale o anche penale).

3) Con una posizione intermedia, secondo la quale o tutto ciò che non è vietato è permesso, ovvero tutto ciò che non è permesso è vieta-

to. In tale ultimo caso, ovviamente, è necessaria una puntuale disciplina delle condizioni di liceità della condotta (*legalizzazione*).

Esclusa la praticabilità delle due soluzioni estreme, che, conducendo ad un sacrificio totale di una delle due sfere di interessi contrapposti, presupporrebbero una consistenza assolutamente e comunque prevalente dell'una sfera sull'altra (il che non può dirsi nel nostro caso), è evidente che la giusta soluzione sta nelle due posizioni intermedie. Gli Stati che hanno già assunto una posizione in materia si sono, seppur diversamente, orientati in tale direzione. Così, ad esempio, per quanto è dato sapere, negli Stati Uniti vige il principio secondo cui in materia di banche dei dati personali tutto ciò che non è vietato è permesso; nella Germania Federale, invece, ha prevalso il principio opposto, secondo cui tutto ciò che non è permesso è vietato.

La scelta della prima soluzione, peraltro, appare ispirata ad eccessiva larghezza verso il potere informatico e presuppone, comunque, un costume di prevalente autodisciplina che non può ritenersi raggiunto ovunque.

Appare, dunque, quasi obbligata, quale scelta ragionevole, quella verso una disciplina legislativa dell'attività in questione, con indicazione dei suoi presupposti e dei suoi limiti. Si tratterà di stabilire se la legalizzazione dell'attività richieda una *autorizzazione* — lasciandola così affidata al potere discrezionale pubblico — ovvero una mera *notificazione*. Ed è evidente che la scelta nel primo senso è indicativa di una maggiore cautela verso gli operatori del settore.

Quel che conta qui sottolineare, peraltro, è che, una volta imboccata tale strada, il ricorso alla sanzione penale risulta strettamente collegato alla maggiore gravità attribuita alla violazione di talune tra le diverse prescrizioni.

Nell'attribuzione della rilevanza penale a tali violazioni peraltro, il legislatore incontra, ovviamente, i consueti limiti costituzionali della riserva di legge, della sufficiente determinatezza e della offensività. Particolare attenzione, dunque, va rivolta, nella costruzione del corrispondente *sotto-sistema penale*, al pericolo di delegare a poteri non legislativi la descrizione della fattispecie ed a quello di costruire figure di pericolo presunto *iuris et de iure* che, invece, andrebbero confinate nel settore del mero illecito amministrativo. Né varrebbe, ad escludere tale scelta, la considerazione dello scarso valore dissuasivo della sanzione pecuniaria, a fronte dell'ostacolo costituzionale derivante dal principio di offensività (artt. 25, commi 2 e 3, 27, comma 3, Cost.).

A tali principi dovrebbe ispirarsi la disciplina penale delle offese agli interessi coinvolti nei tre fondamentali momenti in cui si snoda l'attività delle banche-dati, ossia quello della *raccolta*, del *trattamento*, e della *diffusione*. Prima ancora, peraltro, si pone una esigenza di *conoscenza* dell'esistenza delle varie banche-dati: ma è dubbio che alla violazione di tale interesse strumentale (es.: omessa notificazione) possa attribuirsi rilevanza penale, trattandosi di una tipica *infrazione ostacolo* che, sorreggendosi, sul piano lesivo, solo su di un pericolo presunto, andrebbe lasciata all'illecito amministrativo.

6. I progetti di legge pendenti alla Camera dei Deputati. Conclusioni.

La strada che sarà imboccata dall'ordinamento italiano non è ancora decisa. Pendono attualmente alla Camera dei Deputati due proposte di legge (n. 1144 e 1210) ed un disegno governativo (n. 1657), tutti presentati nel 1984 e basati sul sistema della notificazione.

Quanto alle sanzioni penali, solo una delle due proposte (la n. 1210) contiene previsioni penali, in un'unica disposizione che accomuna sotto una sola sanzione, peraltro assai lieve (multa da lire duecentomila a due milioni o reclusione da sei mesi ad un anno), condotte eterogenee sia quanto alla loro materialità, sia quanto alla loro offensività e all'elemento psicologico. Si tratta, infatti, di condotte, dolose o colpose, di omessa notifica o di abusiva diffusione di informazioni personali o di abusivo uso o acquisizione delle stesse.

Il disegno di legge governativo, invece, dedica ben otto articoli (dal 23 al 30) alla previsione di sanzioni penali, realizzando un quadro di tutela che risulta riferibile a ciascuna delle tre fasi sopra ricordate.

Il sistema che se ne ricava appare sufficientemente armonico e le critiche che gli sono state rivolte non sembrano decisive.

Non può farsi a meno di rilevare, tuttavia, che il meccanismo sanzionatorio relativo all'*ordine di cessazione* dell'attività, impartito dall'Ufficio di controllo nel caso di mancanza di notifica o di difformità rispetto al contenuto della stessa o in violazione delle disposizioni di legge, non risulta del tutto adeguato, dal momento che esso opera sul piano della mera *coercizione indiretta* (comminatoria della pena dell'arresto o dell'ammenda per il caso di inosservanza), mentre apparirebbe opportuno prendere anche sistemi di tipo *interdittivo* volti all'esecuzione coattiva dell'ordine, tramite *coercizione diretta*.

Ma non sembra neanche inopportuna, poi, la previsione di ulteriori figure criminose quali, ad esempio, l'*illegittimo accesso* ad una banca-dati o la *intercettazione abusiva* di una trasmissione di dati, almeno se riguardanti *dati sensibili*.

Per il resto, non v'è che da augurarsi che il progetto sia portato al più presto all'esame del Parlamento, onde anche il nostro Paese, così attento alla salvaguardia dei diritti individuali, possa allinearsi con quelli più progrediti nella tutela della riservatezza informatica.