

FERMIN MORALES PRATS

PRESUPPOSTI POLITICO-CRIMINALI PER UNA TUTELA PENALE DELLA RISERVATEZZA INFORMATICA (CON PARTICOLARE RIGUARDO ALL'ORDINAMENTO SPAGNOLO)

SOMMARIO

1. Premessa. Informatizzazione della società e libertà tecnologiche: la sfida informatica. — 2. Il codice vigente: privacy e riforma penale in Spagna. — 3. Direttrici e presupposti politico-criminali all'intervento penale nella sfera degli abusi informatici contro la privacy. — 4. La « proposta Ledesma » di riforma del codice penale.

1. PREMESSA. INFORMATIZZAZIONE DELLA SOCIETÀ E LIBERTÀ TECNOLOGICHE: LA SFIDA INFORMATICA.

La rivoluzione cibernetica, come ogni rivoluzione tecnologica, sta causando una profonda riorganizzazione economica, politica e sociale. Il *boom* informatico ha provocato la formazione, in primo luogo, di una *nuova forma di produzione*; il settore dell'informazione costituisce ormai il settore quaternario dell'economia, in quanto l'informatica non è più un fenomeno di élites tecnocratiche ma è diventata un fenomeno di massa (per esempio la massiva commercializzazione di micro-computer). Inoltre, l'informazione, in quanto a valore di mercato, ha moltiplicato la sua importanza, frutto dell'applicazione delle telecomunicazioni al *computer*. La cosiddetta *telematica* che rende possibile l'accesso a distanza e in « tempo reale » (*time sharing*) alle banche dati elettroniche attraverso sofisticate reti di terminali, fornisce attualmente una nuova fonte d'energia. Ma, come segnalano Simon Nora e Alan Minc nella loro famosa relazione sugli effetti dell'informatizzazione, la telematica, a differenza dell'elettri-

cià, non trasmette una corrente inerte, ma informazione, cioè potere¹.

Precisamente su questo punto conviene fare una riflessione di grande portata; l'informatizzazione della società postindustriale sta operando in un determinato contesto sociale, senza una previa ridefinizione dell'accesso individuale e collettivo alle fonti d'informazione. Da questa prospettiva, lo sviluppo informatico si erige come nuovo pericolo per la libertà dell'individuo. Assistiamo, attualmente, ad un nuovo incontro dell'individuo con l'intimità in un disperato tentativo di trovare l'identità e la sicurezza esistenziali che gli sono negate nella sfera pubblica e sociale di una società massificata e corporativizzata a tutti i livelli². Il suddetto ritorno al privato si traduce, come conflitto politico-istituzionale, in conflitto *privacy-informatica*³. Il nuovo anelito alla *privacy* si è cimentato nell'individuo in un momento in cui è possibile un nuovo tipo di controllo sociale autentico e invisibile che rende possibile la memorizzazione dei dati personali. Si tratta, come ha segnalato Foucault, di un *controllo virtuale*, cioè preventivo e pertanto generalizzatore, che può materializzarsi in qualsiasi istante e che prescinde dal rapporto personale diretto fra chi controlla e chi è controllato⁴. Insomma, il terrificante « campo di concentramento mondiale » descritto dalla penna di Orwell nel suo « 1984 » può diventare realtà, se nel seno delle società postindustriali non si apre un profondo dibattito sul controllo dell'uso dell'informatica.

Di fronte alle minacce dello sviluppo tecnologico, le risposte che sono state offerte da diversi campi del sapere (giuridico, economico, sociologico...) sono state molteplici. Da alcuni settori dell'opinione è stato propugnato il rifiuto frontale dell'universo tecnologico⁵, in quanto costituisce un mero tentativo razionalizzante delle strutture socio-economiche del tardo capitalismo; entrare nell'ambito di discussione sul possibile uso sociale e democratico del *computer*, cioè sul controllo democratico delle fonti d'informazione postindustriali, costituirebbe (per quelli che la pensano così) un contributo alla coesione di un nuovo *umanesimo di classe*⁶. Dalla parte opposta si sono costituite delle teorizzazioni su un futuro tecnologico senza conflitti nella società cibernetica; si tratta delle cosiddette « computopías »

¹ NORA S.-MINC A., *Informe Nora-Minc (La informatización de la sociedad)*, México, 1980 (traduzione castigliana), pp. 18 e ss.

² FLAQUER L., *De la vida privada*, Barcelona, 1982, p. 61 e ss. e p. 151. Dello stesso autore v. anche *Vers una sociología de la privacidad*, en *Rev. PAPERS*, 17, pp. 109 e ss.

MATTEUCCI N., *Introduzione pubblico e privato*, in *Privacy e Banche dei dati (Aspetti giuridici e sociali)*, autori vari, Bologna, 1981, pp. 15 e 16.

³ Cfr. MORALES-PRATS F., *La tutela penal de la intimidad: privacy e informati-*

ca, Barcelona, 1984, pp. 16 e ss., e 24 e ss.

⁴ FOUCAULT M., *Nuevo orden interior y control social*, nella rivista *El viejo Topo*, n. 7, pp. 5 e ss.

⁵ Vid. per tutti MARCUSE H., *El hombre unidimensional (Ensayo sobre la ideología de la sociedad industrial avanzada)*, Barcelona, 1981, pp. 39-40.

⁶ Da questa posizione: JANCO M., e FURJOT D., *Informatique et Capitalisme*, Paris, 1972, pp. 100 e ss.; MANACORDA P.M., *El ordenador del capital (Razón y mito de la informática)*, Madrid, 1982, pp. 37 e ss. e 205 e ss.

(utopie del *computer*) sostenitrici di un mondo felice sotto l'egida dell'informatica.

Infine, la terza posizione si intravede nelle risposte sopra citate. Davanti ai presagi « paleontomarxisti » che propugnano una posizione di « chi va là! » metafisico in attesa di una nuova società che superi il capitalismo, e di fronte all'autocompiacimento di un superficiale postmodernismo, si deve postulare l'« esorcismo » dei miti positivi e negativi del *computer* attraverso un'analisi dei nuovi conflitti che la società postindustriale propone⁷. Paradossalmente, l'informatica può essere utilizzata come una nuova forma di *totalitarismo virtuale* oppure come un nuovissimo *fattore di coesione della società civile e delle sue libertà*. Quest'ultima opzione deve stimolare ad affrontare lo studio dello sviluppo informatico allo scopo di chiarire quali sono le *libertà tecnologiche* dell'individuo e quali le condizioni che ne possano permettere l'uso. In questo senso bisogna sottolineare che il diritto alla *privacy* appare ai nostri giorni come il nuovo « *habeas* » del cittadino, pilastro basilare di altre libertà politiche e partecipative. La *privacy* è, infatti, un *presupposto di esercizio virtuale* di altri diritti individuali e collettivi. Qui non si tratta di sostenere una concettualizzazione liberale dell'intimità in quanto appendice complementare della libertà⁸. La *privacy* non può restare delimitata come sfera asociale, dato che un'interpretazione garante della stessa deve demarcarla come una libertà tecnologica, in definitiva, come un *diritto al controllo sui dati personali* che circolano nella società cibernetica. È su questo piano che il diritto all'intimità acquisisce il suo significato democratico. Questa concezione funzionale della *privacy* permette di fissare in se stessa le facoltà di controllo dell'identità informatica dell'individuo. Si tratta pertanto di organizzare un *ambito legale* che permetta l'accesso alle banche dati personali informatizzate (diritto di correzione, di cancellazione). Insieme ad esso sarà necessario circoscrivere quali informazioni si debbano catalogare come non memorizzabili perché vi si annidano gravi pericoli di discriminazione (dati sul comportamento sessuale, informazioni su appartenenze a gruppi politici, fede religiosa...). Infine questa nuova legislazione dovrà essere accompagnata da misure istituzionali, in quanto queste costituiscono le condizioni o le premesse minime di esercizio delle facoltà dell'individuo e, di conseguenza, è opportuna la creazione di Registri attraverso i quali si possa controllare la costituzione di banche dati, la registrazione delle acquisizioni di informazioni personali... Nello stesso modo la supervisione di questa attività di registrazioni e del funzionamento operativo delle banche dati deve ricadere

⁷ Nella letteratura spagnola, partendo da questa posizione cfr. GARZON GLARIANA G., *La protección jurídica de datos de carácter personal*, in *Rev. 1ª Instancia*, n. 1, 1982, p. 10; MORALES PRATS F., *La tutela...*, op. cit., pp. 34-35.

⁸ BALDASSARRE A., *Privacy e Costituzione*

ne (L'esperienza Statunitense), Roma, 1974, pp. 288 e ss., 397 e ss., e 468 e ss.; FROSINI V., *La protezione della riservatezza nella società informatica*, in *Privacy e banche dei dati*, op. cit., pp. 39 e ss.; MATTEUCCI N., *Introduzione*, op. cit., p. 22.

su una Ispezione pubblica di dati, che in altri paesi viene chiamata « Magistratura informatica »⁹.

Comunque, queste misure sul piano interno degli Stati, poco o nulla apporteranno in difesa della *privacy* se la cooperazione internazionale in questa materia (attualmente in una prima fase) non darà frutto rapidamente. Altrimenti, la propagazione dei cosiddetti *paradisi informatici nei paesi del terzo mondo* (carenti di regolamentazione), fornirà un esempio storico di ciò che si chiama *frode di legge internazionale*. È ineluttabile, quindi, una armonizzazione legislativa fra gli stati.

In questo contesto, la pretesa contrapposizione « *privacy* - libertà informatica » non è altro che un'errore. Il controllo democratico sui centri informatici non solo permetterà la salvaguardia dell'intimità, ma inoltre renderà possibili nuove vie di esercizio del diritto di accesso all'informazione di contenuto non personale. Di conseguenza, la ridefinizione della libertà informatica nel suo *sensu attivo* per il cittadino, deve portare con sé il riconoscimento del diritto di accesso ai dati informatizzati di carattere sociale, economico e culturale. Il diritto all'informazione costituisce in questa maniera, un'altra delle nuove libertà tecnologiche che si allinea nell'ordine di necessità postindustriali dell'individuo insieme al diritto alla *privacy*.

D'altra parte il *boom* del fenomeno informatico ha generato anche nuove forme di *pirateria industriale*, che meritano un breve commento. Gli strumenti giuridici orientati verso la protezione delle invenzioni e, in generale, dei segni distintivi e della concorrenza nel traffico mercantile, hanno manifestato la loro obsolescenza di fronte alla proliferazione di mercati paralleli di *programmi informatici* « *software* »¹⁰. L'ordinamento legale dei brevetti e dei diritti d'autore (*copyright*) e della classica tutela dei segreti industriali si

⁹ Per tutti, vedi FROSINI V., *Banche dati e tutela della persona*, nel volume dallo stesso titolo della Camera dei Deputati italiana (Servizio per la documentazione automatica; quaderni di documentazione n. 4, Roma, 1981, pp. 7 e ss.; SIMITIS S., *Chancen und Gefahren der elektronischen datenverarbeitung*, in *Neue Juristische Wochenschrift (NJW)*, 197, pp. 675 e ss.; RODOTÀ S., *La protección de la vida privada y control de la información (dos temas de preocupación creciente para la opinión pública)*, in *Novatca*, 1978, pp. 14 e ss.; PEREZ LUÑO A.E., *Derechos humanos y constitución*, Madrid, 1984, pp. 345 e ss.

¹⁰ TIEDEMANN K., *Poder económico y delito*, Barcelona, 1985, pp. 121 e ss.

FROSINI V., *Cibernética, derecho y sociedad* (Ed. española-Apéndice, pp. 184 e ss.), Madrid, 1982.

KIRBY M.D., *Aspects Juridiques de la Technologie de l'information*, en *Une analyti*

preliminaire des problèmes juridiques dans l'informatique e les communications. Politiques d'Information, d'informatique et de communications, OCD., Paris, 1983, pp. 45 e ss.; BRIAT M., *La fraude informatique: une approche de Droit Comparé*, en *Revue du Droit Penal et de Criminologie* (Numéro spécial: Informatique et delinquance), n. 4, 1985, pp. 287 e ss.; PARKER D.B., NYCUM S., OURA S.A., *Computer abuse*, Contemporary Criminology, New York, John Wiley & Sons, 1982, pp. 35 e ss.; SIEBER V., *Computerkriminalität und Strafrecht*, 2^a ed., Köln., 1980; ID., *Urheberrechtliche und wettbewerbsrechtliche Erfassung der unbefugten Softwarenutzung*, in *Betriebs-Berater*, 1981, pp. 1547 e ss.; ID., *Gefahr und Abwehr der Computerkriminalität*, in *Betriebs-Berater*, 1982, pp. 1433 e ss.; ID., *Der urheberrechtliche Schutz von Computerprogrammen*, *Betriebs-Berater*, 1983, pp. 977 e ss.

vede nella necessità di nuovi rimedi giuridici tendenti alla protezione dei beni informatici. Ebbene, la salvaguardia giuridica del *software* a livello statale ed internazionale (mediante un sistema di registro e un ordinamento legale speciale) non devono comportare il rinforzamento del potere tecnocratico. Il riconoscimento legale del diritto all'integrità delle manifestazioni tecnologiche, prodotto dell'intelligenza umana, deve articolarsi come il diritto al controllo collettivo d'informazione rilevanti nell'ordine socio-economico e culturale prima accennato.

Insomma, siamo di fronte ad un elenco di problemi propri di ciò che si è chiamato « bivio postmoderno » che, se non si affronta con lucidità e prontezza, chiuderanno la strada a un auspicato patto o formula di compromesso fra tecnologia e libertà.

2. IL CODICE VIGENTE: PRIVACY E RIFORMA PENALE IN SPAGNA.

Il « Código Penal » spagnolo (cod. pen.) si mostra particolarmente arcaico nella protezione di necessità umane che si sono manifestate allo stesso ritmo della società postindustriale. In ciò che riguarda la tutela dell'intimità, la legislazione penale vigente mostra notevoli lacune, ormai superate nella maggior parte dei codici europei. In questo senso il cod. pen. spagnolo è carente di una moderna disciplina penale del segreto professionale, delle riprese filmate e delle intercettazioni telefoniche clandestine, così come degli abusi informatici contro la *privacy*¹¹.

In questo campo, l'unico passo avanti positivo che si possa indicare, negli ultimi tempi, è la riforma del 15 ottobre 1984 (legge organica 7/1984) sulla tipizzazione penale dell'uso illecito di spie telefoniche (artt. 192-*bis* e 497-*bis* del cod. pen.).

Una volta paralizzato l'*iter* parlamentare del Progetto di codice del 1980 per mancanza di volontà politica da parte dei governi succeduti alla UCE (Unione di Centro Democratico), che introduceva la creazione del reato informatico contro l'intimità (art. 199 del Progetto)¹², le speranze di un cambio nella repressione dell'uso illecito dell'informatica si sono focalizzate sulla Riforma Parziale e Urgente del cod. pen. del 1983 (legge organica 8/1983, del 25 giugno), caldeggiata dal Governo socialista. Nonostante ciò la riforma del 1983 difficilmente poteva colmare le suddette lacune legali per diverse ragioni:

a) la riforma del cod. pen. era caratterizzata dalle note di *urgenza* e *parzialità*. Il legislatore ha preteso di risolvere una serie di problemi

¹¹ Su questi problemi vedi MORALES PRATS, *La tutela...*, op. cit., pp. 159 e ss.

¹² L'art. 199 del Progetto del C.P. del 1980 affermava quanto segue: « Colui che, mancando alle prescrizioni legali sull'uso dell'informatica, registrasse dati relativi all'onore o all'intimità personale o familiare di terzi,

o a danno degli stessi manipolasse l'intervento legittimo o illegittimo processato, sarà punito con la pena dell'arresto da due a ventiquattro fine di settimana e multa da sei a dodici mesi, sempre che il fatto non costituisca resto più grave. Saranno inflitte pene superiori in grado se si divulgasse l'informazione ottenuta ».

esistenti nella realtà penale e penitenziaria spagnola, la cui trascendenza era talmente grande che la loro soluzione non ammetteva ulteriori dilazioni, e supposeva né più né meno che la necessità di soddisfare le esigenze di un Diritto penale nell'ambito dello Stato di Diritto: affermazione stabile del principio di colpevolezza e di quello della tipicità del fatto di reato; regolamentazione del c.d. « agire per un altro » nel seno delle persone giuridiche; introduzione delle regole relative al reato continuato e al reato associativo, soppressione degli effetti aggravanti della recidiva reiterata; regolamentazione dell'errore; riforma della tutela della libertà religiosa e della libertà di coscienza; nuova protezione della sicurezza nel lavoro ecc.¹³.

b) La mancanza di una tradizione e di una cultura giuridica riguardo al bene giuridico della riservatezza in Spagna, presenta la necessità che la tutela penale dello stesso si produca nel contesto di un nuovo Codice penale, che comporti una profonda riformulazione dell'attuale selezione e sistematizzazione del quadro dei beni giuridici protetti nel testo vigente.

c) La difficoltà di tipizzare penalmente fattispecie di reato così complesse come quelle perpetrate con il *computer*.

d) La necessaria cautela e ponderazione di valori che deve presiedere alla creazione di reati informatici, in modo che la nuova sfera di controllo penale non trasgredisca altri interessi legittimi che possano entrare in conflitto con la *privacy* informatica (per esempio, la libertà d'informazione, il diritto di accesso collettivo ai dati informatici, ecc.).

Attualmente, l'attenzione della dottrina nell'ambito che studiamo si proietta sulla « *Propuesta de Anteproyecto del Nuevo Código Penal del 1983* », presentata dal Ministero di Grazia e Giustizia del Governo Socialista; proposta di riforma globale che sarà oggetto delle nostre attenzioni nei seguenti paragrafi.

3. DIRETTRICI E PRESUPPOSTI POLITICO-CRIMINALI DELL'INTERVENTO PENALE NELLA SFERA DEGLI ABUSI INFORMATICI CONTRO LA PRIVACY.

La *privacy* informatica si può inquadrare nella categoria dei cosiddetti « interessi diffusi »; cioè, fra quell'elenco di necessità tangibili per la maggior parte della popolazione che si sono create negli ultimi decenni (l'ambiente, determinati aspetti dell'ordine socio-economico, patrimonio artistico...). Su questi interessi si fondano la maggior parte delle proposte politico-criminali di riforma, tendenti alla creazione di nuove figure tipiche, tendenza più accen-

¹³ Per uno studio della Riforma penale del 1983, vedi QUINTERO OLIVARES G. y

MUÑOZ CONDE F., *La reforma penal de 1983*, Barcelona, 1983.

tuata in paesi che presentano Codici palesemente sfasati nella loro Parte Speciale, come è il caso del cod. pen. spagnolo.

Le linee di riforma, orientate verso la criminalizzazione di nuove condotte, hanno un fondamento socio-politico. In questo senso, se il concetto materiale di bene giuridico svolge il ruolo del limite dello *jus puniendi*¹⁴, ciò non deve implicare l'inserimento delle garanzie politico-criminali che da esso stesso derivano nelle coordinate inibitorie dello Stato liberale. Di conseguenza, il processo di criminalizzazione-depenalizzazione deve essere interpretato in tutta la sua complessità¹⁵, a partire dal modello di Stato sociale e democratico di Diritto (art. 1.1. della Costituzione spagnola).

Questo processo acquisisce particolare rilievo quando fra il testo costituzionale e l'ordine punitivo, regna una *profonda divergenza* quanto ai postulati politici originari di configurazione di ognuno degli stessi¹⁶, come succede rispetto al bene giuridico della riservatezza. Per questo, il fatto che tale bene giuridico abbia le sue *radici nella Costituzione* (art. 18 della Costituzione spagnola) costituisce un punto di riferimento e una direttrice imprescindibile per le proposte politico-criminali in questo campo¹⁷. Riassumendo, si può dire che suddetto « radicamento costituzionale del diritto alla *privacy* (art. 18 Cost.), nei suoi aspetti preinformatici e informatici, si erige come *premessa politico-criminale*.

Ma non basta la giustificazione giuridico-politica per una proposta di riforma penale orientata verso la criminalizzazione *ex novo*. Ogni proposta di riforma nell'ambito penale punitivo deve orientarsi verso i principi che reggono la politica criminale, perché in questa istanza si esprimono i fini del sistema penale ed i limiti dell'intervento punitivo e, in definitiva, le condizioni in cui può essere efficace il diritto penale¹⁸. Di conseguenza, l'incriminazione per uso illecito degli schedari elettronici dovrà rispondere a dei principi politico-criminali che evidenzino la *necessità e adeguatezza* dell'intervento penale.

¹⁴ Per tutti, RUDOLPHI J., *Los diferentes aspectos del concepto del bien jurídico*, in *Revista Nuevo Pensamiento Penal*, 1973, p. 333; MIR PUIG S., *Introducción a las bases del Derecho Penal*, Barcelona, 1976, pp. 128 e ss.

¹⁵ TERRADILLOS BASOCO J., *La satisfacción de necesidades como criterio de determinación del objeto de tutela jurídico-penal*, in *Revista de la Facultad de Derecho de la Universidad Complutense*, n. 63, 1982, p. 144.

¹⁶ Cfr. ESCRIBA GREGORI J., *Algunas consideraciones sobre Derecho Penal y Constitución*, in *Revista Papers*, n. 13, 1980, pp. 146 e ss.

¹⁷ Sul concetto di bene giuridico « costituzionalmente orientato » (Costituzione come istanza di valutazione per la selezione di beni giuridici da proteggere penalmente), SAX V., *Grundsätze der Strafrechtspflege*, in Bettermann-Nipperday-Scheuner, *Die Grundrechte*, BD, III-2, Halbland, 1959, pp. 909 e ss., oppure anche RUDOLPHI J.J., *Los diferentes...*, *op. cit.*, pp. 345-347.

¹⁸ HASSEMBER W., *Strafrechtsdogmatik und Kriminalpolitik*, Hamburgo, Rowolth, 1973, p. 55; ROXIN C., *Política criminal y sistema de Derecho Penal*, Barcelona, 1972 (traducción de MUÑOZ CONDE F.), pp. 8 e ss.

3.1. *Premesse esterne: presupposti politici ed amministrativi alla luce del principio del minimo intervento.*

Per affrontare l'analisi dei presupposti politici ed amministrativi, è opportuno stabilire i seguenti postulati di partenza:

a) non basta evidenziare la gravità delle azioni discriminatorie a cui può dar luogo la manipolazione del *computer*.

b) Non è sufficiente neanche mettere in risalto l'importanza della *privacy* informatica (*habeas data* o *scriptum*) nella società informatica, in quanto garanzia di esercizio virtuale di altri diritti fondamentali.

c) La gravità dell'offesa (*principio di offesa*) e la qualità del bene giuridico messo in pericolo o distrutto, delineano i presupposti definienti la missione del diritto penale nelle società democratiche: ma la giustificazione di nuove incriminazioni esige, insieme all'osservanza dei limiti derivati dal carattere frammentario e di esclusiva protezione di beni giuridici, proprio dell'intervento penale, la conservazione del senso di *ultima ratio* del diritto penale¹⁹.

In questa misura l'intervento e la sanzione penale sono inadeguati, sempre che altri strumenti giuridici extrapenalici, meno traumatici e meno stigmatizzanti, garantiscano una tutela sufficiente. Il principio di *ultima ratio* acquisisce speciale significato nell'ambito degli « interessi diffusi ». In caso contrario, il Diritto penale si vede strumentalizzato e la sua funzione sviata, come alibi con funzione di insabbiare le contraddizioni della tutela dei beni giuridici che possono risultare antagonistici nella struttura del sistema socio-economico. La mancanza di funzionalità di fondo determina la non applicazione dei tipi penali che rimangono ridotti al ruolo di precetti sulla carta: chiaro esempio quello che ROXIN ha denominato « fughe verso il diritto penale »²⁰.

Secondo quanto si è detto, la creazione di delitti informatici contro la *privacy*-informatica sarà adeguata politico-criminalmente se previamente si costituiranno i *meccanismi di prevenzione e polizia amministrativa* (licenze per la costituzione di banche dati, Registro pubblico di banche dati, ordinamento di contravvenzioni e sanzioni amministrative) sulle banche dati, così come l'*ordinamento legale extra-penale* dei sistemi informatici. Questo ambito legale dovrà disciplinare ognuna delle fasi del ciclo operativo del *computer* e programmazione, trasmissione dell'informazione.

La definizione giuridica di questa intelaiatura preventiva espressa in una legge di base di protezione dei dati personali insieme ad altre leggi settoriali, costituisce il requisito *sine qua non* per valutare « come » e « fino a che punto » è necessario e razionale l'intervento legale nel settore informatico.

¹⁹ Cfr. MUÑOZ CONDE F., *Introducción al Derecho Penal*, Barcelona, 1975, pp. 59 e ss.

²⁰ ROXIN C., *Franz Von Liszt und die Kriminalpolitische Konzeption des AE*, in *Franz V. Liszt zum Gedächtnis*, 1969, pp. 77 e ss.

È ovvio sottolineare che la conservazione del carattere di *ultima ratio* non implica l'affermazione della natura secondaria (meramente sanzionatoria) e non autonoma delle norme penali; il diritto penale è *autonomo* nel creare e interpretare le sue istituzioni e nell'effettuare proposte normativo-valutative dalle quali derivano mandati o regole di determinazione²¹. Tutto ciò non si contraddice con il fatto che il legislatore penale per preservare beni giuridici tanto valorizzati nella società postindustriale (come la riservatezza, l'ambiente...) ha bisogno di presupposti di fatto del reato a partire da concetti extrapenali, oppure rimanda per le sue verifiche ad altre branche dell'ordinamento giuridico in cui sono definiti e valutati questi elementi. Di conseguenza, la necessità dell'elaborazione di uno statuto giuridico per la protezione di banche dati informatiche personali diventa più perentoria come premessa politico-criminale.

D'altra parte, la futura criminalizzazione dell'uso illecito del *computer* non deve pregiudicare né eliminare l'esistenza di contravvenzioni amministrative nello statuto giuridico dell'informatica. A questo riguardo è opportuno che l'applicazione delle sanzioni amministrative e penali non si produca con sistema accumulativo, e nello stesso tempo bisognerà evitare la sovrapposizione delle sfere dell'illecito penale a quello amministrativo allo scopo di preservare il postulato del *ne bis in idem*²². Insieme a questo, la sfera dell'illecito amministrativo dovrebbe essere coperta dalle garanzie processuali, giurisdizionali ed interpretative, tradizionali del diritto penale; questo procedimento di « *trasferimento di garanzie* » dal penale all'amministrativo è stato applicato in questi ultimi tempi in altri ambiti dell'illecito amministrativo, per esempio in quello delle infrazioni tributarie.

A sua volta, il regime giuridico di protezione dei dati personali dovrà tenere in considerazione altri provvedimenti che riguardano l'infrastruttura dell'amministrazione. In concreto la istituzione di *organismi pubblici indipendenti* che svolgano le funzioni di controllo sulle banche dati pubbliche e private e di controllo dei dati memorizzati, si basa su un altro presupposto politico-criminale di tipo politico-amministrativo; gli organi specializzati e indipendenti del potere esecutivo suppongono una garanzia per esercitare un autentico *controllo preventivo* della costituzione di banche dati attraverso il sistema di preve autorizzazioni (licenze e verifica del registro). Inoltre, gli organi di « *Pubblica Ispezione di Dati* » come la « Commissione Nazionale di Informatica e libertà » in Francia e la « *Datainspektionen* » della Svezia²³ dimostrano come la cosiddetta « Magistratura Informatica » svolge anche la funzione di *agente coadiuvante* per l'ammi-

²¹ Vedi COBO DEL ROSAL M.-VIVES ANTON T.S., *Derecho Penal. Parte General*, Valencia, 1984, pp. 33-34.

²² MORALES PRATS F., *La tutela...*, op. cit., pp. 328 e ss.

²³ Cfr. arts. 15 e ss. Ley de Datos Sueca (Datalagen) de 1973, parzialmente riveduta nel 1979 e arts. 6 e ss., della legge francese riguardante « Informatica, schedari e libertà » del 1978.

nistrazione della giustizia, concretamente in campo penale, sgravandola della ricezione di denunce e richieste, come pure di altre attività istruttorie. Con tutto ciò non si vuole creare una giurisdizione speciale dell'informatica, poiché, come indica JOINET, la magistratura informatica « può solo esercitare funzioni di controllo e, di conseguenza, non può far altro che formulare ammonizioni o citazioni. In caso di infrazioni deve lasciare il posto a organi giurisdizionali ordinari »²⁴.

I *fattori politici, giuridici ed amministrativi* sopra citati devono strutturare l'« ambito di intervento » diritto penale nel settore dell'informatica relativo ai dati personali. Attualmente la Spagna è priva di uno statuto giuridico sulla protezione dei dati personali e di un organismo politico-istituzionale che svolga i compiti di ispezione e controllo delle banche dati. La norma costituzionale contenuta nell'art. 18.4 Cost. (« La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos ») ancora non è stata attuata. Il Governo spagnolo ha ratificato nel 1984 l'Accordo del Consiglio d'Europa circa la protezione delle persone rispetto all'uso automatizzato dei dati di tipo personale del 17 settembre 1980 (aperto alla firma degli Stati il 28 gennaio 1981)²⁵; tuttavia il citato testo internazionale non può colmare la lacuna della legislazione spagnola sulla tutela dei dati, visto che l'Accordo non è concepito secondo la tecnica del *self-executing*, in quanto l'art. 4 del suddetto Accordo condiziona l'entrata in vigore dello stesso all'adozione delle opportune misure istituzionali da parte dello Stato firmatario, che rendano possibile la reale applicazione dei principi del trattato. Questa condizione ancora non è stata osservata dai poteri pubblici in Spagna. Si potrebbe pensare solo ad una ipotetica situazione in cui il « Defensor del Pueblo » (Difensore del Popolo) assumesse le funzioni di controllo di dati personali rispetto alle banche dati gestite dalla P.A. e protetti dal diritto costituzionale dell'intimità (art. 18 Cost.). Ma tale possibilità sembra remota, data la carenza di mezzi economici e tecnici della figura del « Defensor del Pueblo ».

3.2. *Premesse interne; praticabilità ed effettività dei provvedimenti penali.*

Una volta chiarito il primo livello di premesse politico-criminali di natura politica ed amministrativa, ci dobbiamo porre degli interrogativi sulle *condizioni interne* alle quali deve adempiere una futura ti-

²⁴ JOINET J.L., *Orientaciones principales de la ley francesa relativa a la informática, los ficheros y libertades*, in *Revista de Documentación Administrativa*, 1978 (abril-junio), p. 98.

²⁵ Per tutti SARZANA C., *L'attività delle istituzioni internazionali in materia di tutela*

della privacy, in *Banche dei dati*, op. cit., pp. 412 e ss.; GARZON CLARIANA G., *La protección de los datos personales y la función normativa del Consejo de Europa*, separata de la *Revista de Instituciones Europeas*, Madrid, 1981 (n. 1), in particolare pp. 144 e ss.

pizzazione penale degli abusi dell'informatica contro la *privacy-habeas data*. In questo modo, partendo dai principi di *razionalità, praticabilità ed effettività* delle norme penali²⁶, riteniamo opportuno affrontare la problematica della tecnica legale da usare, i *requisiti interni* della formulazione tipica e, in terzo luogo, il *raggiungimento* e momento della tutela del bene giuridico intimità.

3.2.1. *Il principio di razionalità dell'intervento penale.*

La *razionalità* della norma penale è intimamente legata alla *tecnica legislativa* adottata. Nel raggiungimento della menzionata razionalità si mette in gioco né più né meno che la legittimazione della sanzione penale, secondo il grado di adeguatezza della configurazione tipica specifica relativamente alla necessità e allo scopo della protezione penale. La mancata realizzazione di questo rapporto di razionalità mediante la comminatoria penale determina la frustrazione sia della funzione di protezione del bene giuridico sia di quella di motivazione propria delle norme penali²⁷, in quanto dette funzioni si verificano a partire dalla selezione del bene giuridico da proteggere in modo preciso e meditato; in caso contrario, come sostiene QUINTERO, la determinazione dell'oggetto giuridico di protezione e dell'entità degli attacchi penalmente sanzionabili, non potrà realizzarsi secondo i postulati politico-criminali (principio di intervento minimo, principio di offesa, ecc. ...)²⁸.

I suddetti problemi di tecnica legislativa si aggravano quando i presupposti di fatto del reato si proiettano su sfere di attività altamente tecnicizzate e pericolose²⁹. In questi caso il legislatore penale suole ricorrere alla tecnica delle cosiddette *leggi penali in bianco*, formula lecita sempre che concorrano ragioni tecniche e politico criminali precise ed evidenti³⁰. Questo è quanto si verifica nei reati informatici, secondo quanto ci dimostra la legislazione comparata; in queste infrazioni penali si constata un legame dei presupposti di fatto del reato con altre branche dell'ordinamento giuridico. Di conseguenza, esiste una impossibilità tecnica di configurazione di tipi penali chiusi e rigidi. La descrizione di azioni come « raccolta abusiva di dati », « manipolazioni nel trattamento elettronico dei dati e nel *software* », « fughe di informazioni... », dipendono da concetti tecnici e giuridici propri dell'informatica (es. « raccolta di dati », *software*, « dati automatizzati », *habeas data*, « telematica »...).

Nella misura in cui l'ordinamento giuridico spagnolo presenta un chiaro *vuoto legale extrapenale* in materia di dati personali compute-

²⁶ Cfr. ZIFF H., *Kriminalpolitisch (Eine Einführung in die Grundlagen)*, Karlsruhe, 1973, pp. 30-31.

²⁷ ZIFF H., *op. loc. ult. cit.*

²⁸ QUINTERO OLIVARES G., *Introducción al Derecho Penal*, Barcelona, 1981, pp. 48-49 e pp. 83 e ss.

²⁹ Su questi problemi, vedi HAFT, *Zur Situation des Datenschütz strafrechts*, NIW, 1979, pp. 1194 e ss.; MORALES PRATS, *La Tutela...*, pp. 330 e ss.

³⁰ MUÑOZ CONDE F., *Introducción...*, *op. cit.*, p. 22.

rizzati, e non essendo applicabile la Convenzione del Consiglio d'Europa per le ragioni precedentemente esposte, il legislatore penale al momento di affrontare la prossima riforma penale può trovarsi di fronte alla seguente alternativa:

a) rinviare la configurazione reati contro la riservatezza informatica in attesa della approvazione del regime giuridico dei dati personali informatici, in modo tale che le condotte delittuose vengano comprese in quest'ultimo e non nel Codice penale;

b) procedere alla tipizzazione di questi reati nel nuovo cod. pen., conoscendo tuttavia la sua non funzionalità politico-criminale data la mancanza di presupposti politici, amministrativi e tecnico-legali nella pianificazione informatica e telematica.

Secondo noi, sembra preferibile la prima opzione, in quanto altrimenti la norma penale in bianco non troverebbe definizioni per assenza di un inquadramento legale metapenale: lo stesso succedrebbe nel caso in cui si optasse per l'impiego di tipi formalmente chiusi che però contengano termini normativi in attesa di valutazione in altre branche dell'ordinamento.

Nel caso in cui il legislatore si dichiarasse a favore della seconda opzione (cioè creazione di reati informatici senza la previa esistenza di una legge di tutela dei dati personali) sarebbe necessario stabilire che la Convenzione del Consiglio d'Europa, nonostante non sia esecutiva, abbia almeno valore interpretativo.

Dalla buona scelta della tecnica giuridica utilizzata dipende il rispetto del *principio di legalità penale* e dell'obiettivo da esso perseguito, il raggiungimento della sicurezza giuridica, il cui fallimento determina il perversimento del significato garantista della *tipicità penale*³¹.

La legislazione comparata europea nella maggior parte dei casi si è dichiarata a favore del non inserimento nel codice penale degli abusi informatici che attentano alla riservatezza. In questo modo le leggi di tutela dei dati personali informatizzati contengono capitoli dedicati alle infrazioni penali, allo scopo di evitare che nei codici penali comuni si accumulino concetti tecnici complicati che si devono interpretare in ottemperanza alla legislazione extra-penale sulle banche dati³².

3.2.2. *Sintesi delle prospettive di riforma.*

La futura riforma penale spagnola dovrà tener conto di queste esperienze per chiarire quale strumento giuridico si adatti meglio alle esigenze politico-criminali.

³¹ Come segnalano COBO DEL ROSAL y VIVES ANTON: « El injusto penal es injusto "tipificando", y no cabe hablar de tipicidad allí donde una defectuosa técnica legislativa o una manipulación más o menos enmascarada dejan al arbitrio del intérprete y, en su caso, del juzgador, la determinación del contenido de las proposiciones legales. Procede re-

cordar que la idea de la tipicidad se origina en el derecho penal para dar concreción a las declaraciones constitucionales en las que se proclama el principio de legalidad » (COBO DEL ROSAL, M. VIVES ANTON T.S., *Derecho penal...*, op. cit., p. 291).

³² Cfr. MORALES PRATS F., *La tutela...*, op. cit., p. 333.

Vediamo schematicamente i modelli tipici offerti al legislatore penale:

a) la tipizzazione del codice penale dei reati informatici mediante *clausole di rinvio* alla legge di tutela di dati personali che costituirebbe la base su cui saranno configurati materialmente i presupposti del reato. Dunque, le formule di rinvio possono essere di ambito diverso. È quindi opportuno parlare di rinvio *in totum* e di rinvio a « precetti precisi » della normativa extra-penale. Il rinvio *in totum* era quello contemplato dal Progetto di Codice penale spagnolo del 1980 (art. 199) « El que faltando a las prescripciones legales sobre el uso de la informática... »³³.

b) La tipizzazione nella legge penale delle infrazioni analizzate mediante concetti normativi, evitando un rinvio esplicito, ma implicitamente richiamando una valutazione dei termini stessi già esposti in altre parti dell'ordinamento giuridico.

c) La creazione di un *diritto penale speciale nell'uso illecito dell'informatica*, nella stessa legge di protezione di dati automatizzati. Questa tecnica è la più adottata in Europa. Le leggi della Svezia (Datalagen dell'11 maggio 1973, riveduta nel 1979, artt. 20 e ss.), della Repubblica Federale Tedesca (Bundesdatenschutzgesetz, BDGS, del 27 gennaio 1977, art. 41), e della Francia (legge sull'informatica, schedati, e libertà, del 6 gennaio 1978, artt. 41 e ss.), tra le altre, contengono norme sanzionatrici di carattere penale, la cui struttura è incompleta, nel senso che esprimono clausole o regole interpretative contestuali di concetti informatici o telematici.

Una volta esposti i diversi modelli, è d'obbligo la valutazione *de lege ferenda* di ognuno di essi.

La configurazione *ex novo* di un *diritto penale speciale informatico* fornisce l'interpretazione e la determinazione della sfera di ciò che è punibile riguardo alla realizzazione delle garanzie del principio di legalità su un piano politico-criminale, come pure del concetto di tipicità penale nell'ordine sistematico. Ma la dispersione delle norme penali, attraverso le leggi penali accessorie o complementari, comporta la *perdita dell'efficacia preventiva generale*.

D'altro canto, l'inserimento degli abusi informatici nei codici comuni obbliga a ricorrere a *formule di rinvio* a precetti non penali, necessariamente aumentando i pericoli di *indeterminatezza di ciò che è punibile e di violazione del principio di certezza del diritto*. Questi pericoli si aggravano senza necessità quando il rinvio è *in totum* al regime giuridico informatico. Questi sarebbero in definitiva i costi del mantenimento della funzione di prevenzione generale della norma penale.

³³ Art. 199 PrCP 1980, vedi *supra* nota 12.

3.2.3. *Impostazioni de lege ferenda sull'illecito tipico nei reati contro la riservatezza informatica: aspetti soggettivi e aspetti oggettivi.*

L'alto grado di dipendenza delle proposte politico-criminali dell'ambito legale extrapenale, rispetto alla creazione di reati informativi si manifesta anche nella definizione del raggio di estensione oggettivo e soggettivo dell'illecito (*disvalore di azione e disvalore di risultato*)³⁴.

La configurazione tipica delle condotte lesive di beni giuridici personalissimi ed immateriali (per esempio l'onore), ha seguito i modelli dei reati di *mera attività*. In essi l'offesa si consuma con il verificarsi dell'azione dell'agente proiettata verso uno scopo il cui conseguimento è penalmente irrilevante; il contenuto tipico si completa attraverso l'indagine e la constatazione del concorso del dolo e dell'intenzione offensiva della volontà dell'agente. Su questo punto è opportuno un chiarimento: il fatto che reati formali prescindano dall'evento materiale non equivale a dire che non si produce un evento giuridico, cioè un'offesa rilevante ad un bene giuridico (c.d. principio di offensività)³⁵.

Dunque, la legislazione comparata e la realtà criminologica nell'ambito informatico, dimostrano come nella creazione di reati contro la *privacy* informatica si verifica un'*espansione della sfera tipica del disvalore di azione*, in rapporto agli attentati classici contro l'onore e la riservatezza preinformatica (segreti di documenti, segreto professionale, ecc.). I fattori di ampliamento della sfera tipica soggettiva dell'illecito, a nostro giudizio, sono i seguenti:

1. Si tratta di un ambito di attività altamente tecniche e sofisticate (banche dati, sistemi di programmazione, circuiti di trasmissione e circolazione telematica di dati, ecc.).

2. Quanto detto prima determina la diminuzione del livello di « rischio permesso » e la conseguente crescita delle esigenze di attenzione per la tutela del bene giuridico riservatezza. Tutto ciò, dal punto di vista penale si traduce nella creazione di doveri di custodia, diligenza e segretezza, prima sconosciuti nel diritto penale, nella sfera dei beni giuridici personalissimi ed immateriali.

In base a quanto esposto *de lege ferenda* non sembra sconsigliabile la creazione di *reati colposi* per l'infrazione di norme di attenzione, dettagliate nella legislazione protettrice di dati personali oppure nei codici di deontologia informatica. In tal modo ci si muoverebbe, per necessità politico-criminali, in senso difforme dalla linea tradizionale che ha configurato i reati contro l'onore e di scoperta

³⁴ Sul tema vedi MORALES PRATS F., *La tutela...*, op. cit., pp. 343 e ss.

³⁵ QUINTERO OLIVARES G., *Introducción...*, op. cit., pp. 107 e 108.

e rivelazione di segreti di documenti come fattispecie eminentemente dolose³⁶.

Se questa *espansione dell'illecito tipico* si proietta, a sua volta, sul disvalore di risultato, cioè sulla linea obiettiva che configura l'ambito nel quale si considera leso o messo in pericolo il bene giuridico, si infrange il principio di lesività o offensività delle norme penali. In questo difetto incorreva l'art. 199 del Progetto del cod. pen. del 1980, che tipizzava condotte come la registrazione di dati personali e la manipolazione di informazioni, venendo meno ai precetti legali sull'uso dell'informatica. Il progetto del 1980 finiva così per creare un *reato formale o di mera disobbedienza*, che insieme alla già citata tecnica della norma penale in bianco come « rinvio *in totum* » alla normativa extrapenale, apriva la strada all'incriminazione di semplici illeciti amministrativi.

Quanto affermato non impedisce che nelle future figure tipiche ci siano tipi di *pericolo concreto* chiaramente differenziati dalle mere infrazioni di polizia amministrativa. Per la definizione del giudizio di pericolo *ex ante* in un ambito di beni giuridici immateriali come la riservatezza ci viene in mente di ricorrere allo *scaglionamento di facoltà dell'habeas data o scriptum* durante l'iter del ciclo operativo delle banche dati. Quest'ambito referenziale facilita la valutazione dell'entità del pericolo e la constatazione del pericolo concreto ed effettivo. In questo modo, come criterio generale, si può affermare che a cominciare dalla fase di raccolta di dati personali è possibile che si crei il pericolo concreto e rilevante penalmente dell'*habeas data*. Anteriormente alla raccolta di dati personali dovranno agire le sanzioni amministrative (per esempio, per mancanza di autorizzazione o licenza), in quanto l'anticipo della tutela penale al di là del momento indicato può condurre all'incriminazione di meri illeciti amministrativi.

3.2.4. *I postulati della praticabilità ed effettività.*

Come indica MUNOZ CONDE; il principio di effettività si riscontra in una norma penale quando questa svolge la funzione di protezione di un determinato bene giuridico attraverso una funzione motivante della condotta dei cittadini affinché si astengano dal lederlo o metterlo in pericolo³⁷. Una tutela penale efficace della riservatezza rispetto all'informatica esige non solo dei presupposti politici e tecnici che do-

³⁶ In Svezia la « Datalagen » contiene soltanto reati colposi per infrazione di doveri di diligenza professionale, quando la norma di attenzione prescrive gli obblighi del responsabile della banca dati rispetto agli organi di ispezione; se i doveri di diligenza riguardano obblighi di garanzia rispetto a privati, la condotta si pone in contravvenzioni amministrative; in ogni caso l'imprudenza, perché costituisca reato, dovrà es-

sere grave (artt. 20 e ss. della « Datalagen »).

Nella Repubblica Federale Tedesca, la BDGS del 1977, stabilisce un ambito punitivo più ristretto e di conseguenza il campo delle contravvenzioni amministrative è più ampio (artt. 41 e ss. della BDGS).

³⁷ MUÑOZ CONDE F., *Función de la norma penal y reforma del Derecho penal*, en *Revista Nuevo Pensamiento Penal* (año 2, n. 4), 1974, pp. 400 e ss.

tino di razionalità le proposte di incriminazione, ma anche che la sanzione sia adeguata quantitativamente e qualitativamente. Rispetto alla tutela dell'*habeas data* si ripresenta la polemica sulla validità e legittimazione politico-criminale delle pene detentive brevi. Per parte della dottrina le pene pecuniarie non bastano poiché possono finire per diventare una voce di spesa ordinaria da parte di chi gestisce la banca dati. Da questa posizione si difende la esistenza di pene detentive brevi in quest'ambito delittuoso, per la loro *effettività intimidatoria* o da *shock*, sempre che superino i limiti temporali di sei mesi³⁸.

Per altri autori le pene detentive brevi sono carenti di legittimità politico-criminale dal punto di vista della prevenzione speciale, dato che l'imposizione di pene pecuniarie in un processo penale è già qualitativamente diversa da qualsiasi altro tipo di sanzione, dati gli effetti stigmatizzanti del processo e della condanna penale. In questo provvedimento, il ricorso alla breve pena privativa della libertà comporterebbe una sofferenza inutile e non necessaria³⁹.

Infine, la *praticabilità* dei provvedimenti penali esige delle condizioni processuali idonee, data la corresponsabilità politico-criminale del diritto processuale penale. Sotto questo profilo acquisterebbe una grande importanza il « grado di collaborazione » tra gli organi di controllo e l'amministrazione della giustizia penale. Parimenti la privatizzazione dello *ius puniendi* può essere uno strumento politico-criminale idoneo in alcune ipotesi delittuose.

4. LA « PROPOSTA LEDESMA » DI RIFORMA DEL CODICE PENALE (PANCP 1983).

4.1. *Introduzione.*

Una volta frustrate le aspettative di riforma con il progetto UCD del 1980, la Propuesta de Anteproyecto de nuevo Código penal (PANCP) presentata dal Ministro di Grazia e Giustizia Fernando Ledesma nel 1983, costituisce il progetto più serio della storia moderna del diritto penale spagnolo nell'affrontare la problematica penale del bene giuridico riservatezza (nei suoi aspetti preinformatici e informatici).

L'elaborazione della PANCP è preceduta da una lodevole volontà politica di modernizzare e umanizzare l'ordinamento punitivo. A tale

³⁸ LOSANO M., *La legislazione Tedesca nella protezione dei dati individuali*, in *Banche dei dati*, op. cit., pp. 174-175. Sull'effetto intimidatorio delle brevi pene detentive in delinquenti appartenenti a strati sociali medi o alti, vedere in generale TIEDEMANN K., *Die Bekämpfung der Wirtschafts-Kriminalität als Aufgabe der Gesetzgebung am Beispiel der Steuer- und Subventionsdelinquenz*, in *Goldammer's Archiv für Strafrecht*, 1974, p. 12; dello stesso autore:

Wirtschaftsstrafrecht und Wirtschaftskriminalität, Bd. 1 (Allg. Teil), Hamburg, 1976, pp. 73 e ss.

³⁹ Per tutti vedere: ROXIN, *El desarrollo de la política criminal desde el Proyecto Alternativo*, in la *Reforma del Derecho Penal*, ediz. a cura di S. MIR PUIG, Barcelona, 1980, pp. 94 e ss. In Spagna, a partire da queste premesse, LUZON PENA D.M., *Medición de la pena y sustitutivos penales*, Madrid, 1979, pp. 69 e ss.

scopo il Ministro di Grazia e Giustizia nominò nel gennaio del 1983 una Commissione di esperti composta dai professori Cobo del Rosal, Gimbernat Ordeig, Luzón Peña, Muñoz Conde e Quintero Olivares, e dal Magistrato della Suprema Corte di Cassazione García Miguel.

4.2. L'art. 189 della PANCP (1983).

Sebbene la PANCP abbia tenuto conto delle gravi lacune nella tutela penale attualmente offerta alla riservatezza indicando diversi rimedi (segreto professionale, divieto di controlli audiovisivi clandestini, sanzioni contro gli abusi informatici...), (il che la rende meritevole di valutazione positiva) a un secondo livello di analisi, la tipizzazione del delitto informatico contro la *privacy* (art. 189) deve essere oggetto di alcune riflessioni critiche di carattere politico-criminale e tecnico-giuridico. A nostro avviso, il testo deve essere migliorato e chiarito nel procedimento parlamentare di formazione legislativa.

L'art. 189 della PANCP afferma quanto segue: « 1. Colui che, infrangendo le prescrizioni legali sull'uso dell'informatica, registra dati relativi all'onore e all'intimità personale o familiare di terzi o, a danni degli stessi, manipola l'informazione legittima o illegittima ottenuta, sarà punito con la pena d'arresto da dodici a ventiquattro fine di settimana e multa da sei a dodici mesi — sempre che il fatto non costituisca reato più grave.

2. Si infliggeranno pene più gravi in caso di divulgazione dell'informazione ottenuta »⁴⁰.

Il progetto opta per l'inclusione nella proposta del codice di un reato contro la riservatezza informatica. Il precetto è strutturato attraverso una norma penale in bianco che non trova un ambito legale extrapenale nell'ordinamento spagnolo⁴¹.

Un altro aspetto criticabile è la formula con la quale si allude al futuro ordinamento giuridico sull'informatica. Nella norma si fanno dipendere le infrazioni alle « *prescripciones legales sobre el uso de la informatica* », espressione adottata pure dal Progetto del 1980. A nostro avviso deve essere richiamata unicamente la futura legge organica sull'uso dell'informatica, dato che solo questo e nessun altro può essere lo strumento legale adeguato in grado di sviluppare l'art. 18.4 della Costituzione Spagnola⁴². Perciò ciò che si richiede è il *rispetto del rango formale della legge organica*, dato che si tratta di stabilire il regime giuridico dell'esercizio di un diritto fondamentale (*privacy* in-

⁴⁰ L'« arresto fine di settimana » costituisce, nel PANCP una misura sostitutiva per pene non superiori a due anni (artt. 52 e 82), mentre la multa è calcolata con il sistema dei tassi giornalieri (art. 45).

⁴¹ Su questo aspetto vedi MORALES PRATS F., *Privacy y reforma penal: la Propuesta de Anteproyecto de nuevo Código pe-*

nal de 1983, in *Documentación Jurídica*, numero monografico dedicato alla Propuesta de Anteproyecto de nuevo Código Penal, Vol. I, Secretaría General Técnica del Ministerio de Justicia, Madrid, 1984, pp. 625 e 626.

⁴² MORALES PRATS F., *Privacy y reforma penal...*, op. cit., p. 626.

formatica). Se non si rispetta questa esigenza, la tipizzazione del reato informatico contro l'*habeas data* in forma così vaga può perfino trasgredire il principio di legalità e la riserva di legge in materia penale.

D'altro canto, l'art. 189 PANCP contiene una piccola appendice che dichiara la sussidiarietà del precetto (« ... sempre che il fatto non costituisca reato più grave »)⁴³. Si tratta di una clausola oscura, suscettibile di due interpretazioni:

a) la PANCP pretende di creare una *norma incriminatrice sussidiaria sulla « raccolta dei dati »* per la sussunzione degli abusi informatici contro la riservatezza che non trovino esplicita accoglienza in altri reati del testo di legge. Questa soluzione interpretativa non sembra percorribile in quanto l'art. 189 della PANCP non trova un ambito tipico di operatività quale norma residuale, per l'assenza di altri reati informatici nelle Proposte del nuovo codice.

b) Il progetto intende configurare un *tipo sussidiario* rispetto alle *altre infrazioni* penali di tipo informatico più gravi presenti nella legge di protezione di dati personali automatizzati. Questa seconda interpretazione è più coerente allo spirito globale ispirato dalla Proposta del 1983, ma è ancora in attesa della futura elaborazione della legge di dati informatici.

Arrivati a questo punto, riteniamo pertinente formulare le seguenti puntualizzazioni politico-criminali:

1. Se si propone di inserire nel nuovo codice la tutela degli aspetti informatici della *privacy*, i tipi penali dovranno contenere un rinvio preciso a precetti specifici della futura legge sulla raccolta ed elaborazione di dati.

2. Si dovrà evitare la sovrapposizione di tipi penali che possano dar luogo alla già menzionata regola di sussidiarietà.

3. La tutela della *privacy* informatica offerta dalla PANCP, si limita a descrivere infrazioni commesse da privati. A questo proposito è imprescindibile che nella discussione parlamentare del testo si prenda in considerazione la necessità di differenziare due livelli diversi di rapporti nei quali possa essere violato questo bene giuridico. In questo modo è necessario includere attentati contro la *privacy* informatica in quanto garanzia giuridico-politica rispetto allo Stato, istanza sulla quale si basa l'autentico *habeas data* del cittadino; con ciò si prenderebbe in considerazione il piano dei rapporti cittadino-Stato. In secondo luogo bisogna includere nella PANCP, anche gli attacchi alla *privacy* che possano prodursi sul piano dei rapporti di servizio tra la P.A. e gli amministrati (per esempio dati relativi alla previdenza sociale); si configurerebbe così un reato informatico contemplante abusi per mezzo del *computer*, nell'esercizio della pubblica funzione. La PANCP, in definitiva, appare come un testo insufficiente sotto questo aspetto, dato che contempla solamente i rapporti informatici tra privati in seno alla società civile⁴⁴.

⁴³ *Ibidem*, pp. 626-627.

⁴⁴ *Ibidem*, p. 627.