

JEAN P. SPREUTELS

LA RESPONSABILITÀ PENALE CONNESSA AD ABUSI NELLA APPLICAZIONE DELL'INFORMATICA

SOMMARIO

1. Premessa. La criminalità informatica. — 2. Le varie tecniche impiegate per la frode informatica. — 3. Alcuni casi celebri. — 4. Il diritto penale di fronte alla criminalità informatica: a) Il diritto vigente. Incriminazioni generiche. — 5. Difficoltà nell'applicazione delle figure classiche di reato contro il patrimonio alle ipotesi di « pirateria informatica ». — 6. I reati di falso. — 7. Altri reati classici: truffa, frode fiscale, danneggiamento. — 8. Incriminazioni specifiche. — 9. b) *De lege ferenda*. Progetti di riforma della codificazione penale nel quadro internazionale. — 10. In particolare, le incriminazioni specifiche contenute nel progetto di riforma del codice penale canadese. — 11. Il progetto di legge belga relativo alla protezione di certi aspetti della vita privata. — 12. Conclusioni.

1. Premessa. La criminalità informatica.

Il crimine informatico costituisce una realtà sociologica ben differenziata e tende a configurarsi come una categoria giuridica speciale¹, benché di frequente accada che il *computer* altro non sia che lo strumento per la consumazione di un reato classico: truffa, falso in scritture² o furto.

In genere, la criminalità informatica si sviluppa nell'ambito della criminalità economica, e ne diventa un aspetto rilevante ma difficile da scoprire e da reprimere³, specie sul piano internazionale⁴.

* Con il gentile consenso dell'Autore, si riproduce la traduzione dell'intervento su « *La responsabilité pénale découlant des atteintes aux applications de l'informatique* » svolto nel corso del colloquio internazionale tenutosi a Bruxelles nei giorni 14-16 giugno 1984 sul tema « *Informatique et Droit en Europe* ». A maggior comodità del lettore, nelle note sono stati eliminati alcuni riferimenti eccessivamente specifici all'ordinamento belga, e aggiunte invece alcune integrazioni volte a consentire la comparazione con il quadro normativo e istituzionale italiano.

Traduzione e adattamento di CARLO ROSELLLO.

¹ X. LINANT DE BELLEFONDS, *L'informatique et le droit*, Paris, 1981, p. 68.

² M. BELMAS-MARTY, *Droit pénal des affaires*, t. I, 2^e éd., Paris, 1981, p. 89.

³ I reati che ricadono nel campo dell'in-

formatica (ad es. furto di dati, violazione di segreti, manipolazione di dati informatizzati) fanno parte dell'elenco di reati ai quali si applica la raccomandazione n. (81) 12 sulla criminalità economica adottata dal Comitato dei Ministri del Consiglio d'Europa il 25 giugno 1981.

Il rapporto elaborato dal comitato ristretto di esperti sulla criminalità economica indica che in certi Stati le infrazioni relative agli elaboratori elettronici pongono delicati problemi, ad es. per la circostanza che non è possibile ingannare una macchina, e che pertanto non è configurabile un reato di truffa, o ancora che i dati registrati non possono essere considerati documenti in senso giuridico, e quindi non si può propriamente configurare la fattispecie di falso in documenti (*La criminalité des affaires*, Comité européen pour les problèmes criminels, Conseil de l'Europe, Strasbourg, 1981, p. 46).

⁴ V. J.P. SPREUTELS, *Vers un droit pé-*

Nella maggior parte delle nazioni evolute sono stati intrapresi studi e ricerche sulla frode informatica, alcuni dei quali sotto l'egida dell'O.C.D.E. e del Consiglio d'Europa.

Ancora non esiste una conoscenza adeguata del fenomeno della criminalità informatica, e spesso le stesse vittime contribuiscono a questa disinformazione con la volontà di non divulgare le frodi constatate, allo scopo di evitare una pubblicità che potrebbe creare proselitismo tra i potenziali criminali e panico tra i propri clienti⁵. Spesso poi accade addirittura che il colpevole, una volta scoperto, sia ingaggiato, vista l'ingegnosità di cui ha dato prova, con il compito di sorvegliare la sicurezza dei sistemi informatici dell'impresa danneggiata.

In Australia, un'inchiesta effettuata con l'aiuto di un questionario indirizzato a più di mille utilizzatori di sistemi di elaborazione elettronica ha rivelato tra il 1975 e il 1980 cinquantatre casi di uso abusivo ed illecito del *computer*, per un costo totale di 1,2 milioni di dollari. Gli illeciti commessi consistevano di volta in volta nell'uso non autorizzato dell'elaboratore, nel furto di una somma di denaro, nella manipolazione di fondi, nella manipolazione di programmi, appropriazione di dati, manipolazione delle parole chiave, manipolazione dei dati sottoposti a trattamento informatico, sviamento delle operazioni, furto dei programmi o dei risultati dell'elaborazione. Il settore bancario, non ha fatto denuncia di alcun illecito informatico di una qualche importanza⁶.

Un'altra inchiesta, effettuata in Belgio da ricercatori dell'Università cattolica di Louvain su un campione di duecento imprese informatizzate, rivela che tra di esse si sono constatati tre atti di vandalismo o di sabotaggio, una alterazione fraudolenta di dati o di programmi, tre furti o indebite appropriazioni di materiali, due di programmi, due di informazioni o dati e quattro di « tempo macchina », insieme a quattro occupazioni dei locali. L'ammontare complessivo dei danni raggiunge i 3.744.000 franchi belgi, importo che rappresenta circa il 5,4 del totale delle perdite dovute a rischi diversi. Gli autori di questo studio sostengono che « gli incidenti dolosi rimangono (...) un argomento tabù nel mondo dell'informatica belga », e secondo loro il volume reale dei danni subiti dalle imprese sarebbe notevolmente più elevato⁷.

Un recentissimo studio condotto dall'IBM-Giappone sulla criminalità informatica (spionaggio di dati, estrazione non autorizzata di dati, loro alterazione fraudolenta e utilizzazione abusiva del *softwa-*

nal international des affaires?, in *Journ. trib.*, 1981, p. 181.

⁵ M. MASSE, *L'application des incriminations traditionnelles à la délinquance informatique*, in *Informatique et droit pénal*, Travaux de l'Institut de sciences criminelles de Poitiers, 1981-4, Paris, 1983, p. 22.

⁶ *Computer abuse Case-Book and Analysis*, Computer Abuse Research Bureau,

Caulfield Institute of Technology, Victoria, 1980.

⁷ Y. CROMBE et L. WARTON, *La sécurité des systèmes informatiques*, Université Catholique de Louvain, Institut d'administration et de gestion, 1982, pp. 226-232. L. WARTON, *La sécurité informatique en Belgique*, in *Sécurité et protection en informatique*, Bruxelles, 1982, p. 255.

re) indica per parte sua che le perdite connesse a questo genere di illeciti oltrepassano per ammontare quelle relative alle rapine in banca. E si stimano fra 500.000 e 1.500.000 di marchi le somme illecitamente sottratte mediante manipolazioni informatiche nella Repubblica Federale Tedesca.

In assenza di una efficace tutela penale, o comunque di un rafforzamento di quest'ultima, le imprese ricorrono talvolta alla copertura assicurativa. Sistemi specifici di copertura a garanzia del rischio di frode informatica esistono e sono in avanzato corso di elaborazione in numerosi paesi, tra cui si segnalano soprattutto l'Australia, la Francia, il Regno Unito, la Svezia e il Belgio⁸.

2. *Le varie tecniche impiegate per la frode informatica.*

Un autore francese ha classificato le tecniche utilizzate per frodi informatiche in quattro categorie fondamentali: a) infrazioni commesse completamente al di fuori del funzionamento del sistema di elaborazione elettronica, e che mirano a impadronirsi di informazioni fornite alla macchina, di programmi o di dati; b) infrazioni che presuppongono il funzionamento normale dell'elaboratore, senza intervento sul programma o sui dati. Questi ultimi saranno quindi forniti dalla macchina stessa mediante una stampante, uno schermo catodico o un'altra struttura periferica, oppure saranno procurati mediante annotazione contabile o distribuzione automatica di biglietti; c) infrazioni consistenti in interventi di modifica dei dati (*inputs*) forniti all'elaboratore, senza modifica del programma. Si può trattare in questo caso di dati fittizi, ad esempio relativi a impiegati inesistenti a favore dei quali il *computer* accrediterà uno stipendio mensile, o di false fatture. O ancora può trattarsi di cancellature selettive o sostituzioni di dati, ad esempio su un bonifico bancario che venga intercettato e alterato e successivamente presentato per l'incasso, una sorta di « imboscata elettronica »; d) infine, altre infrazioni vengono commesse mediante un intervento sul programma, più frequentemente attraverso una sua alterazione. La macchina è allora programmata per consumare la frode. L'esempio più conosciuto è quello della grande compagnia di riassicurazioni americana che « creava », grazie al suo elaboratore, tutta una popolazione di assicurati fittizi, che cambiavano continuamente lavoro o indirizzo o si ammalavano. Per ciascuna di queste polizze, la società percepiva le provvigioni dalle compagnie assicuratrici del gruppo di cui essa teneva, con il proprio elaboratore, la contabilità. In questo modo, la compagnia di riassicurazioni fu in grado di lucrare cento milioni di dollari secondo una stima, addirittura un miliardo e mezzo di dollari secondo un'altra⁹.

⁸ Cfr. Ph. ULLMANN, *Les assurances de l'informatique*, in *Sécurité et protection en informatique*, cit., p. 235-238; H. GEVAERT, *Informatika en verzekering*, *ivi*, p. 113 ss.; specie, pp. 119-122; Ph. ULLMANN, *Les assurances de l'informatique*, in *Le droit des con-*

trats informatiques. Principes-Applications, Bruxelles-Namur, 1983, p. 445 ss., specie pp. 460-464.

⁹ M. MASSE, *L'application des incriminations traditionnelles à la délinquance informatique*, cit., pp. 24-26.

Tra le varie tecniche impiegate, se ne possono menzionare quattro dai nomi particolarmente evocativi: il *salame*, la *pattumiera*, la *fuga* e il *cavallo di Troia*.

Il programmatore di una banca immagina un calcolo degli interessi tale che tutti gli arrotondamenti siano effettuati per difetto, e la differenza tra il calcolo esatto degli interessi e l'arrotondamento venga accreditata su un proprio conto personale, che in tal modo aumenta lentamente ma inesorabilmente. Questo è il *salame*, vale a dire il prelievo di ridottissimi importi su un gran numero di conti a vantaggio di uno solo.

La *pattumiera* consiste nel prelevare negli archivi e nel leggere sistematicamente il contenuto delle bande magnetiche teoricamente cancellate dopo l'uso: trasposizione elettronica della raccolta dei rifiuti, che costituisce un metodo assai sperimentato di spionaggio industriale.

La *fuga* è la copiatura dei dati a distanza, effettuata grazie all'ausilio di emittenti radio clandestine.

Infine, il *cavallo di Troia* consiste nell'inserzione in un programma di istruzioni supplementari, accessibili al solo iniziato grazie ad un codice segreto, che gli danno, all'insaputa di tutti, accesso agli altri dati contenuti nell'elaboratore, malgrado le barriere esistenti tra i diversi schedari.

3. Alcuni casi celebri.

La stampa riferisce regolarmente di casi spettacolari di frode informatica.

È il caso di un economista di una quarantina d'anni che aveva lavorato per sette al *Federal Reserve Bureau*, e che aveva familiarizzato con gli elaboratori ivi in uso. Assunto successivamente da una società di investimenti di Wall Street, era stato incaricato di prevedere l'evoluzione della massa monetaria americana, compito che svolse brillantemente interrogando mediante il suo terminale l'elaboratore centrale della *Federal Reserve*, adoperando il codice di uno dei suoi ex colleghi di lavoro. L'F.B.I. scoprì la frode truccando gli archivi in modo da poter risalire all'intruso.

Altri casi celebri sono quelli di un impiegato delle poste della Germania Federale che di recente si è appropriato di cinque milioni di marchi mediante la sola manipolazione di un elaboratore, o quello di un truffatore che, grazie all'informatica, si è fatto pagare da una banca dell'isola di Man 260.000 sterline in due volte, a 72 ore di intervallo.

Anche la letteratura si è ormai impadronita del soggetto. Così, in *La nuit des enfants rois*, Bernard Lenteric racconta la storia di sette adolescenti di New York che rubano centinaia di milioni di dollari mediante una serie di crimini perfetti consumati mediante un potentissimo elaboratore; o ancora, il film *War games* descrive l'allarme

causato dall'inserimento di un video-gioco nell'elaboratore centrale del *North American Air Defense Command (NORAD)*, con la simulazione di un attacco nucleare dell'Unione Sovietica.

Ma talvolta la realtà va più lontano della finzione, e in effetti quest'ultimo film si ispira ad un episodio realmente accaduto negli Stati Uniti nel novembre del 1979: un nastro che simulava un attacco missilistico russo venne inavvertitamente lasciato inserito in un elaboratore; quando i tecnici lo attivarono, si credette, per sei tragici minuti, che i missili fossero veramente sulla rotta di attacco, e venne lanciato l'allarme. Oltre a ciò, sono stati scoperti numerosi casi di giovanissimi che sono riusciti a penetrare nei sistemi di elaborazione elettronica di università o di importanti imprese¹⁰.

Ed ha impiegato appena qualche mese un gruppo di giovani americani di età compresa tra i 15 e i 22 anni, prendendo spunto dal film menzionato, per riuscire, servendosi di un *home computer*, ad avere accesso alla memoria dell'elaboratore centrale di un centro di ricerche sulle armi nucleari, di quello della loro scuola, così come di una banca di Los Angeles, utilizzando i numeri telefonici della rete *Teletelnet*, alla quale gli apparecchi erano collegati. A questo proposito, l'inchiesta sopra menzionata condotta dall'IBM-Giappone rivela come la giovane generazione, i cosiddetti *micro-kids* fanatici dei *computers*, sia molto temuta dalle imprese informatizzate, e cita a titolo di esempio, fra gli altri, il caso di alcuni studenti che, connettendosi al suo centro di calcolo, hanno completamente distrutto i dati di una società canadese.

Si può quindi facilmente intuire l'inquietante dimensione di un fenomeno che trascorre dalla criminalità dei « colletti bianchi » a quella dei « pantaloni corti »...

4. *Il diritto penale di fronte alla criminalità informatica*¹¹.

a) *Il diritto vigente*. Incriminazioni generiche.

Un soggetto che si introduce senza esservi autorizzato in locali privati dove si trova un elaboratore elettronico di dati può essere perseguito per i reati di violazione di domicilio¹² o anche, se ne ricorrono gli elementi, di invasione di terreni o edifici¹³.

Se sottrae elementi del sistema di elaborazione o supporti dell'informazione come nastri o dischi magnetici, non vi sarà alcuna diffi-

¹⁰ *Le Monde* del 15 dicembre 1983.

¹¹ Nella descrizione dello stato del diritto comparato, ci si è basati soprattutto sul riassunto analitico delle risposte al questionario sulla repressione della frode informatica O.C.D.E., DSTI/ICCP/83.35, messo a punto il 1° settembre 1983 sulla base del contributo di 15 paesi membri (Australia, Austria, Belgio, Canada, Danimarca, Finlandia,

Francia, Germania, Italia, Islanda, Norvegia, Regno Unito, Stati Uniti, Svezia, Svizzera).

¹² Artt. 439 ss. del codice penale belga e artt. 614 e 615 cod. pen. italiano.

¹³ Artt. 545 e 563, 2° del codice penale belga. La norma del riferimento corrispondente nel nostro cod. pen. potrebbe essere l'art. 633 cod. pen.

coltà a ravvisare nella fattispecie un'ipotesi di furto, eventualmente con l'aggravante dell'effrazione o della violenza sulle cose¹⁴.

Allo stesso modo, potranno, con riguardo agli stessi beni, configurarsi le fattispecie generiche di truffa, appropriazione indebita, estorsione, ricettazione, bancarotta fraudolenta, e simili¹⁵.

L'utilizzazione abusiva di macchinari o di dati può essere considerata come furto di energia o quanto meno come furto d'uso¹⁶. Il « furto di tempo » dell'elaboratore è invece difficilmente inquadrabile in una fattispecie penale, anche se è noto come il tempo di un elaboratore possa risultare molto costoso¹⁷. Naturalmente, la parte offesa potrà chiedere la riparazione del danno patrimoniale se dimostra la ricorrenza di un reato come ad esempio il furto di energia o di impulsi elettronici.

È da aggiungere che la riproduzione di un documento contro la volontà e all'insaputa del suo proprietario può ugualmente integrare, secondo la giurisprudenza francese, un'ipotesi di furto¹⁸, e il discorso può essere esteso analogicamente alla riproduzione non autorizzata di dati.

In Svezia, in due casi che si sono verificati in due università, alcuni studenti hanno utilizzato illecitamente il sistema informatico dell'università stessa a scopi personali. In un'ipotesi, uno studente aveva addirittura cancellato delle registrazioni per far spazio a proprie operazioni personali. Sono stati condannati sotto il capo di imputazione di appropriazione indebita.

5. *Difficoltà nell'applicazione delle figure classiche di reato contro il patrimonio alle ipotesi di « pirateria informatica ».*

In genere, comunque, in un gran numero di ordinamenti, i giudici incontrano notevoli difficoltà ad applicare la nozione di furto alla sottrazione di dati di un elaboratore elettronico, in assenza del presupposto che questi ultimi siano classificabili come « beni materiali ».

Così, ad esempio, negli Stati Uniti si è deciso che il furto di un programma contenuto nella memoria di un elaboratore non possa essere considerato come furto di un « bene » ai sensi della definizione con-

¹⁴ Artt. 461 e 463 codice penale belga, e artt. 624 e 625, n. 2 cod. pen. italiano.

¹⁵ Artt. 496, 491, 470, 505, 489 codice penale belga e artt. 640, 646, 629, 648 cod. pen. e art. 216 l. fall.

¹⁶ Sul furto di energia cfr. per un primo inquadramento ANTOLISEI, *Manuale di diritto penale. Parte speciale*⁷, I, Milano, 1977, p. 232; sul furto d'uso di cui all'art. 626, n. 1 cod. pen. v. SEVERINO, *Il furto d'uso e delle energie e reati affini*, Milano, 1933; NEPI MODONA, *Cosa sottratta e restituita nel furto d'uso*, in *Riv. it. dir. pen.*, 1963, p. 1240 ss.

¹⁷ Il furto di « tempo maccina » non è passibile di sanzione penale in Austria e in Francia, mentre nel diritto svizzero tale comportamento potrebbe essere perseguito nell'ipotesi in cui cagioni un pregiudizio. Tale è il caso dell'installazione che funzioni già al massimo delle proprie capacità e che, in conseguenza della utilizzazione abusiva, non sia più disponibile al legittimo utilizzatore se non in misura parziale.

¹⁸ Cass., 8 Janvier 1979, D.S., 1979, J., p. 509 con *observation* di P. CORLAY.

tenuta nella legge¹⁹. Questo genere di problema si pone segnatamente in ordinamenti giuridici come quello australiano, austriaco, canadese, danese, italiano²⁰.

Negli U.S.A. il furto di beni immateriali consumato in relazione alla utilizzazione di sistemi informatici ha dato luogo a procedimenti penali, ma non senza suscitare sensibili difficoltà di ordine giuridico. Così, nel caso *Seidlitz* del 1978²¹, si trattava del furto di un programma, perpetrato mediante il terminale di un elaboratore utilizzato per accedere illecitamente ad un sistema informatico e riprodurre a distanza determinati programmi. I fatti erano stati commessi facendo oltrepassare le frontiere dello Stato ad impulsi elettromagnetici e riproducendo il programma che, di fatto, rimase intatto nell'elaboratore nel quale era registrato. I giudici ritennero che il fatto non ricadesse sotto la previsione della legge penale. La sola infrazione ravvisata fu quella di frode a mezzo di linee telefoniche, per la circostanza che l'accusato aveva utilizzato tali linee, ma solo in due dei quaranta casi di accesso illecito all'elaboratore a mezzo del suo terminale.

Un altro possibile capo d'accusa potrebbe essere la violazione di segreti industriali.

Per quanto concerne il furto, le difficoltà di inquadramento si manifestano in tutta la loro portata nelle ipotesi in cui non venga sottratto, in senso stretto, nessun bene materiale: tutti i casi in cui si verifica l'ascolto, la lettura su uno schermo catodico o, più frequentemente, la registrazione su un supporto di proprietà dello stesso « pirata informatico ». In fattispecie di questo genere, si può ancora parlare di sottrazione? E, in caso di risposta affermativa, si può configurare una sottrazione di cose ai sensi dell'art. 462 del codice penale belga²²?

In Francia, un tribunale ha condannato sotto il capo di imputazione di furto un imputato che aveva ricopiato su un disco magnetico una serie di programmi per elaboratore nella sede del suo *ex* datore di lavoro. Secondo tale decisione, « l'accusato si è in tal modo appropriato e ha detenuto, senza che gliene fosse rimesso il possesso, una serie di dati che, quale che fosse stata la sua partecipazione alla elaborazione delle informazioni che essi riguardavano, apparteneva al suo *ex* datore di lavoro, e si è reso in tal modo colpevole di furto²³ ».

¹⁹ *Ward v. Superior Court of California*, 3 CLSR 206 (Cal), 1972, citata da M.D. KIRBY, *Legal Aspects of Information Technology*, in *An exploration of Legal Issues in Information and Communication Technologies*, Paris, 1983, p. 28.

²⁰ La sent. Trib. Torino, 12 dicembre 1983 (*Basile e Bisio*), in *Giur. it.*, 1984, II, 351, con nota di FIGONE, *Sulla tutela penale del software*, ha recentemente esaminato una fattispecie concernente un programma redatto da un'impresa, sottratto da un dipendente di quest'ultima e riprodotto su di un altro

supporto. I giudici italiani hanno escluso che il fatto potesse essere perseguito come furto, non trattandosi di « cosa mobile » ai sensi dell'art. 624 cod. pen.

²¹ *United States of America v. Seidlitz*, 589 F2d 152 (4th Cir. 1978), appeal dismissed, 441 US 922 (1979).

²² Lo stesso problema si pone con riguardo all'art. 624 de. cod. pen. italiano.

²³ Corr. Montbéliard, 28 mai 1978, riprodotta in *Informatique et droit pénal*, cit., annexe III.

Si può pure pensare, a seconda dei casi, ad una violazione del segreto professionale o ad una rivelazione colposa o dolosa di segreti industriali²⁴, così come ad una violazione della legge sulle pratiche di commercio²⁵. In certi paesi, esistono disposizioni penali che sanzionano specificamente la violazione del segreto professionale al quale sono vincolati coloro che contribuiscono e partecipano al trattamento automatizzato di dati. È il caso, ad esempio, della Danimarca.

6. *I reati di falso.*

La falsificazione di programmi o di dati potrà, in certe ipotesi, essere considerata come falso in scritture²⁶. Il problema naturalmente è quello di stabilire se si può parlare a questo proposito di scritture in senso stretto. La dottrina più recente ritiene applicabile la nozione di scrittura alle schede perforate²⁷. Ma si può estendere l'analogia ai nastri o dischi magnetici? Sembra prender forma un'evoluzione della materia nel senso di estendere a queste fattispecie l'applicazione della sanzione per falso in scritture, specialmente in Svizzera²⁸, e alcuni autori hanno espresso l'opinione che la registrazione di un'informazione per mezzo di strumenti informatici costituisca in sé una forma di scrittura.

In Gran Bretagna, una persona è stata di recente perseguita sotto l'imputazione di falso in scritture per aver falsificato una serie di questionari conservati unicamente in veste informatizzata da una società commerciale.

7. *Altri reati classici: truffa, frode fiscale, danneggiamento.*

Grazie all'informatica, si possono poi commettere altri reati estremamente classici. I più frequenti e quelli che fanno più notizia sono le truffe. L'utilizzazione di un elaboratore può integrare gli artifici e raggiri richiesti per la consumazione del reato di truffa²⁹, anche se il risultato è semplicemente un pagamento a mezzo documenti o la materializzazione dell'operazione mediante un documento emesso dalla stampante dell'elaboratore³⁰. Ma è difficile assimilare alla truffa

²⁴ Art. 458 e 309 del code pénal belga e art. 623 del cod. pen. italiano.

²⁵ Art. 56 della legge belga sulle pratiche di commercio del 14 juillet 1971, su cui v. G. VANDERBERGHE, *Informatica en recht*, T. P.R., 1981, p. 285.

²⁶ Artt. 193 e ss. del code pénal belga e 476 ss. cod. pen. italiano.

²⁷ A. MARCHAL, *Faux commis dans les écritures et dans les dépêches télégraphiques*, *Novelles, Droit pénal*, t. II, 1967, p. 421.

²⁸ In una pronuncia resa nel 1970 (ATF 96 IV 185, *Journ. des Tribunaux* (Svizzera), *Droit pénal*, IV, 1972), il Tribunale federale svizzero ha ritenuto che dati informatizzati possano costituire scritture in senso proprio o

destinate a provare fatti aventi una rilevanza giuridica, e che è quindi possibile, nel manipolarli, commettere i reati previsti dagli artt. 251 ss. del codice penale svizzero.

²⁹ Si v. per es. Cass., 26 mars 1976, Bull., n. 97, p. 232, relativa a documenti di natura tale da far ipotizzare l'esistenza di un credito inesistente allorché siano emanazione di una procedura di elaborazione elettronica di calcolo e di gestione che conferisce loro credibilità ed efficacia.

³⁰ Si cfr. la giurisprudenza della Corte di Cassazione francese in materia di truffe alla T.V.A. cit. da M. MASSE, *op. cit.*, p. 29 e Cass., 16 mai 1979, pas., 1979, I, 1081; *Rev. trim. droit et proc. civ.*, 1979, p. 688;

l'ipotesi in cui l'inganno consista semplicemente nella apparizione di alcuni dati su uno schermo.

Certi elaboratori possono poi servire a commettere una frode fiscale, per esempio se si costituiscono degli archivi elettronici « a doppio fondo » in cui determinate informazioni non sono accessibili che mediante un codice segreto. Si può in tal modo ottenere una doppia contabilità, una « bianca », destinata al fisco, e l'altra « nera », che permette all'imprenditore di avere un'esatta rappresentazione dell'andamento dei suoi affari. Un elaboratore così programmato è praticamente uno strumento per la confezione di un falso in scritture contabili.

Il prelievo abusivo di denaro da un distributore automatico (il c.d. sportello elettronico delle banche) è stato qualificato dalla giurisprudenza belga come furto³¹, sia pure dopo qualche esitazione. Se la scheda magnetica è falsa o rubata, si può assimilare la fattispecie a un furto commesso con l'ausilio di una chiave falsa³², dato che la legge assimila alle chiavi false quelle smarrite, perdute o sottratte.

Per quanto concerne il danneggiamento, le disposizioni del codice penale relative alla distruzione, dispersione, deterioramento di cose altrui si possono applicare anche alla distruzione di installazioni per l'elaborazione di dati o dei supporti nei quali i dati sono immagazzinati.

Il problema si fa più delicato quando sono i dati stessi ad essere danneggiati o cancellati. Si tratterà infatti di stabilire se i dati possono essere considerati come « cose mobili ». È infatti noto come per rendere inutilizzabile un programma sia sufficiente talvolta un'anomalia minima inserita intenzionalmente nel programma, la scomparsa di una lista scelta a caso, un graffio di unghia su un disco, un po' di cenere di sigaretta su un nastro. Molto spesso, infatti, le informazioni immagazzinate in questi supporti materiali, come i programmi valutati per ore di programmazione impiegate, sono molto più costose e più difficili da rimpiazzare del materiale in se stesso.

8. Incriminazioni specifiche.

La maggior parte degli ordinamenti giuridici è priva di incriminazioni volte espressamente a sanzionare specificamente e in linea generale le frodi informatiche. Questo è il caso, ad esempio, dell'Australia, del Canada, della Finlandia, dell'Islanda, della Norvegia, della Svizzera e del Regno Unito.

Le disposizioni specifiche sono molto rare. Così, la legge svedese sulla protezione dei dati, che riguarda essenzialmente i dati a caratte-

R.C.J.B., 1984, p. 32 con *observation* di J.P. SPREUTELS, *Virement par erreur et cel frauduleux*.

³¹ Corr. Anvers. 29 avril 1971, *R.W.*, 1971-1972, col. 480, *observation* di J. LIEBAERT, Gand, 12 décembre 1981, *R.W.*, 1981-1982, col. 2562, *observation* di A. VANDEPLAS; corr. Liège, 22 mars 1982, *Jur. Liè-*

ge, 1982, p. 319 con *observation* di F. PIEDBOEUF. V. pure J.P. BUYLE, *Guichets automatiques: abus, fraude, erreur*, in *Rev. de la Banque*, 1983, pp. 495 ss.

³² Art. 467, comma 1, code pénal belge; Bruxelles, 22 mars 1973, *Journ. trib.*, 1974, p. 65 con *observation* di P. VANDERVEEREN.

re personale, contiene una disposizione un po' più estesa, che prevede la sanzione di un'ammenda o della reclusione per un periodo non superiore ai due anni per chiunque acceda con mezzi illeciti ad una registrazione destinata a trattamento automatizzato oppure alteri, cancelli o introduca illecitamente tale registrazione in una scheda, questo sempre che l'infrazione non ricada sotto la disciplina del codice penale (art. 21: « violazione di dati »).

Certi tipi di trattamento automatizzato dell'informazione beneficiano tuttavia di un regime di protezione particolare. È il caso, in Italia, dei dati amministrativi trattati dal Centro di elaborazione del Ministero degli Interni.

Ma è soprattutto nel campo della regolamentazione relativa al trattamento automatizzato di dati a carattere personale che si trova il maggior numero di disposizioni penali sanzionanti le violazioni commesse nell'applicazione dell'informatica³³.

In Belgio, alcune disposizioni sanzionatorie sono state introdotte in questa materia recentemente. La legge dell'8 agosto 1983 relativa alla organizzazione di un registro nazionale delle persone fisiche³⁴ definisce quest'ultimo come « un sistema di trattamento dell'informazione che assicura la registrazione, la memorizzazione e la comunicazione di informazioni relative alla identificazione delle persone fisiche » (art. 1).

A ciascuna persona è attribuito, al momento della prima iscrizione nel registro nazionale, un determinato numero (art. 2). L'utilizzazione di tale numero di identificazione senza autorizzazione o per scopi diversi da quelli per i quali è data l'autorizzazione è vietata (art. 9).

Tutte le persone iscritte al Registro nazionale o i loro legali rappresentanti hanno diritto: a) ad ottenere comunicazione delle informazioni che le riguardano e che sono archiviate nel Registro nazionale; b) ad ottenere la rettifica di quelle informazioni che non riproducano in maniera precisa, completa ed esatta i dati trasmessi dalle autorità addette alla tenuta dei registri della popolazione (art. 10). È previsto l'arresto da tre mesi a cinque anni e un'ammenda da mille a venticinquemila franchi per chi impedisca o si renda complice nell'impedire l'esercizio di tali diritti (art. 13, comma 2).

I soggetti che nell'esercizio delle loro funzioni intervengono nella raccolta, nel trattamento o nella trasmissione delle informazioni sono

³³ Cfr. soprattutto in proposito L. FOCANEAU, *La protection des données à caractère personnel contre l'utilisation abusive de l'informatique*, in *Journ. dr. int.*, 1982, p. 55; J. BARTHELEMY, *Les travaux de l'O.C.D.E., du Conseil de l'Europe et de la C.E.E.*, in *Banques de données, entreprises, vie privée*, Bruxelles, 1980, p. 107; E. PEETERS, *Actions en cours au niveau européen en matière de confidentialité et de protection des données*, *ivi*, p. 115; E. PEETERS, *Sécurité et confidentialité des données: actions communautaires*, in *Sécurité et protection en infor-*

matique, Bruxelles, 1982, p. 177; *La protection des données en Europe*, Conseil de l'Europe, Affaires juridiques, Strasbourg, 1975. Per la situazione francese v. in particolare P. SARGOS, *Les nouvelles incriminations directement liées à l'informatique*, in *Informatique et droit pénal*, *cit.*, p. 34 ss.

In lingua italiana cfr. G. ALPA e M. BESSONE, *Banche dati, telematica e diritti della persona*, Padova, 1984; nonché AA.VV., *Le banche dati in Italia*, Napoli, 1985.

³⁴ *Monit.* 21 avril 1984, p. 5247.

vincolati al segreto professionale. Essi devono inoltre esercitare la massima diligenza allo scopo di aggiornare le informazioni, di correggere quelle erronee e di cancellare quelle non più attuali oppure ottenute con mezzi illeciti o fraudolenti; devono prendere tutte le precauzioni utili al fine di assicurare e garantire la sicurezza delle informazioni registrate e di impedire che esse vengano alterate, danneggiate, o comunicate a persone che non abbiano ottenuto l'autorizzazione ad averne conoscenza; devono assicurarsi del carattere adeguato dei programmi destinati al trattamento automatizzato delle informazioni così come della regolarità della loro applicazione; devono infine sorvegliare sulla regolarità della trasmissione delle informazioni (art. 11). Sono ugualmente previste sanzioni penali per la contravvenzione a tali disposizioni (art. 13, comma 2).

Il decreto reale del 30 dicembre 1982³⁵ ha creato una banca dati relativa ai membri del personale del settore pubblico, che raccoglie i dati statistici relativi ai soggetti inquadrati nell'impiego pubblico. Tale provvedimento contiene disposizioni, munite di sanzioni penali, relative al diritto di accesso e di rettifica, e prevede obblighi a carico di coloro che, nell'esercizio delle proprie funzioni, intervengono nella raccolta, trattamento o trasmissione delle informazioni, sulla scorta di quanto già disposto dalla legge sul registro nazionale.

Tanto la legge 8 agosto 1983 quanto il decreto reale n. 141 del 30 dicembre 1982 istituiscono una Commissione consultiva con poteri di indagine, organi che di fatto sono stati fusi in una Commissione unica denominata *Commissione consultiva per la protezione della vita privata*³⁶, avente come funzione, in primo luogo, quella di fornire pareri, sia di propria iniziativa che su richiesta del Ministero di Giustizia, su tutte le questioni relative alla protezione della vita privata nel quadro dei provvedimenti legislativi appena menzionati e sull'evoluzione e l'applicazione pratica delle tecniche di gestione automatizzata dell'informazione. In secondo luogo la Commissione esamina, senza alcun pregiudizio per il ricorso all'Autorità Giudiziaria, i reclami che le vengono indirizzati con riguardo all'applicazione della legge e del decreto reale; e denuncia al Procuratore del Re le infrazioni di cui viene a conoscenza.

Infine, la legge 29 giugno 1981 contenente i principi generali in materia di sicurezza sociale dei lavoratori prevede l'istituzione di una banca dati pubblica relativa all'insieme delle informazioni concernenti il sistema di previdenza e sicurezza sociale, la cui utilizzazione attende ancora di venire disciplinata per legge.

9. b) De lege ferenda. *Progetti di riforma dei codici penali.*

La tendenza dei vari paesi evoluti a studiare ed approfondire i problemi connessi alla responsabilità penale degli utenti dell'informatica

³⁵ *Monit.*, 13 janvier 1983, n. 475.

³⁶ Arrêté royal du 20 avril 1984 relativo alla composizione e al funzionamento

della *Commission consultative de la protection de la vie privée* (*Monit.*, 26 avril 1984, p. 5483).

è assai marcata. A questo scopo in alcune nazioni sono state istituite dai poteri pubblici apposite commissioni, in particolare in Australia, tanto a livello federale che di singolo Stato, in Germania, in Norvegia e in Svezia. Talvolta detti studi vengono portati avanti nel quadro della riforma dei codici penali, come ad es. in Finlandia, in Francia e in Svizzera. In alcuni casi, poi, sono già stati elaborati alcuni progetti di legge. Così, negli Stati Uniti d'America, il Congresso è stato a più riprese investito di progetti di legge finalizzati a reprimere in maniera specifica i comportamenti delittuosi in materia informatica che involgano interessi federali. In Canada, sono state presentate varie proposte a iniziativa parlamentare e un progetto governativo. In Germania, il governo federale ha sottoposto al parlamento il progetto di una seconda legge volta a reprimere la criminalità economica, contenente alcune disposizioni finalizzate sia a sanzionare specificamente frodi informatiche quali la falsificazione di dati registrati e le manovre fraudolente commesse nell'ambito di operazioni giuridiche connesse con il trattamento di dati, sia ad adattare le norme esistenti alle esigenze del trattamento elettronico di dati: dolo in un'operazione giuridica, falsificazione nell'esercizio di pubbliche funzioni.

Anche altrove sono stati elaborati progetti concernenti la protezione specifica del trattamento automatizzato di dati a carattere personale: così in Belgio, Italia e Regno Unito.

Oltre a quelle il cui obiettivo è così limitato, si constata, fra le prospettive di riforma, una duplice linea di tendenza. Da un lato, vengono create incriminazioni specifiche, la cui portata è più o meno estesa, che mirano alla repressione delle frodi informatiche (Stati Uniti, Canada); dall'altro, si tenta di adattare allo scopo le disposizioni penali esistenti, estendendo la loro definizione o il loro campo di applicazione (ad es. in Finlandia, con riguardo alle nozioni di « bene », « frode », « falso in scrittura » e « spionaggio industriale »). Talvolta, si opera su entrambi i fronti, come ad esempio in Germania.

In Svizzera, la Commissione di esperti per la revisione del codice penale ha proposto di colmare certe lacune in materia di lotta contro la criminalità informatica mediante la creazione di una nuova incriminazione avente per oggetto la utilizzazione abusiva di dati, e consistente nell'accesso e nello sfruttamento intenzionali di questi ultimi in assenza di apposita autorizzazione.

Per consentire di combattere il sabotaggio informatico, i dati ed i programmi verranno assimilati ai beni protetti nell'ambito delle disposizioni riguardanti i delitti contro il patrimonio (art. 145 del codice penale svizzero). Integrerà tale fattispecie di rilevanza penalistica (perseguibile a querela di parte salvo che nel caso in cui abbia cagionato un pregiudizio considerevole) anche la cancellazione o l'alterazione dei dati o dei programmi. Infine, sarà egualmente perseguibile l'utilizzazione fraudolenta di un sistema di elaborazione dati, vale a dire la manipolazione a scopo di lucro di dati e di programmi con l'intento di trasferire ricchezza a danno di terzi.

10. *Le incriminazioni specifiche contenute nel progetto di riforma del codice penale canadese.*

In Canada, nel quadro della riforma del codice penale, un progetto governativo sottoposto alla Camera dei Comuni nel febbraio del 1984 tende ad introdurre numerose disposizioni penali finalizzate a reprimere comportamenti direttamente connessi con l'utilizzazione di sistemi di elaborazione elettronica dell'informazione³⁷. Secondo tali disposizioni, « chiunque dolosamente e senza averne diritto: a) direttamente o indirettamente ottiene le prestazioni di un sistema di elaborazione; b) mediante un dispositivo elettromagnetico, acustico o meccanico o di altra natura, direttamente o indirettamente, intercetta o fa intercettare le funzioni di un elaboratore; c) direttamente o indirettamente utilizza o fa utilizzare un elaboratore con l'intento di commettere un'infrazione prevista dalla lett. a) o b) o un'infrazione prevista dall'art. 387 concernente i dati o un sistema di elaborazione, è colpevole di un delitto punibile con la reclusione fino a dieci anni o di una contravvenzione punibile con procedimento sommario »³⁸. Secondo l'art. 387 (1.1) del codice penale canadese, commette un reato chiunque volontariamente: a) distrugge o altera i dati; b) priva i dati del loro significato, li rende inutili o inoperanti; c) impedisce, interrompe o crea difficoltà al legittimo impiego dei dati o d) impedisce, interrompe o crea difficoltà ad una persona nel legittimo impiego dei dati o rifiuta l'accesso ai dati ad un soggetto che ne abbia diritto. Tali reati sono punibili con pene che arrivano fino alla reclusione per un massimo di dieci anni.

11. *Il progetto di legge belga relativo alla protezione di certi aspetti della vita privata.*

Tra i numerosi altri ordinamenti che stanno progettando di dotarsi di una legislazione specifica a protezione del trattamento automatizzato dell'informazione, si segnalano in particolar modo l'Italia, il Re-

³⁷ Progetto di legge C-19 della Camera dei Comuni del Canada, seconda sessione, trentaduesima legislatura, 32-33 Elizabeth II, 1983-1984, *Loi modifiant le Code criminel*, e numerose leggi penali.

³⁸ Art. 301 (1). L'art. 301 (2) contiene le definizioni applicabili a tale disposizione. Per « dispositivi elettromagnetici, acustici, meccanici, e altro » si intendono tutti i dispositivi od apparecchi utilizzati o suscettibili di venir utilizzati per intercettare una funzione dell'elaboratore, ma la definizione non ricomprende gli apparecchi acustici adoperati per migliorare l'udito quando questo è inferiore al normale.

Per « dato » si intende la rappresentazione di informazioni o di concetti che sono o sono stati preparati in maniera tale da poter essere utilizzati da un elaboratore.

Per « funzione » si intendono soprattutto le funzioni logiche, aritmetiche, le funzioni di comando, di comunicazione così come le funzioni di memorizzazione e di archiviazione o di recupero dei dati.

« Intercettare » ha il senso attribuitogli dall'art. 178, 1.

« Ordinatore » va inteso come qualsiasi dispositivo o insieme di dispositivi connessi o collegati l'uno all'altro, che: a) contiene programmi per elaboratore o altri dati; b) conformemente alle istruzioni dei programmi esegua funzioni logiche o possa eseguire tutte le altre funzioni.

« Programma per elaboratore » va inteso come un insieme di dati che rappresentano istruzioni o rilevazioni e che, una volta trattati dall'elaboratore, gli fanno eseguire una determinata funzione.

gno Unito e il Belgio, dove il governo ha depositato nel novembre 1983 un progetto di legge relativo alla protezione di certi aspetti della vita privata il cui secondo capitolo è interamente consacrato al trattamento automatizzato di dati a carattere personale³⁹. La maggior parte delle disposizioni contenute in questo progetto è fornita di sanzione penale. Tale è il caso per quelle che riguardano la raccolta di dati (artt. 17, § 6 e 24), il divieto di trattare determinati dati (art. 21, § 7), l'informazione dell'interessato al momento della prima registrazione e il diritto di accesso (art. 22, § 7), l'indicazione dell'esistenza di una controversia giudiziaria relativa ai dati trattati (art. 24, § 2), gli obblighi che gravano su coloro che si occupano del trattamento automatizzato (art. 25, § 2), la dichiarazione preliminare e il registro pubblico (artt. 26, § 7 e 27, § 4), le interconnessioni, i raggruppamenti e il flusso transfrontaliero di dati (art. 30).

Per quanto concerne il diritto di accesso, è interessante segnalare una particolare fattispecie di rilevanza penalistica: il fatto di adoperare violenza o minacce nei confronti di una persona per costringerla a comunicare le informazioni ottenute mediante l'esercizio del diritto di accesso o a dare la sua autorizzazione alla registrazione di dati a carattere personale che la riguardano in un sistema di trattamento automatizzato, naturalmente senza pregiudizio dell'applicazione della disposizione del codice penale relativa all'estorsione (art. 22, § 7).

Nel motivare la *ratio* di tale disposizione, il Governo si dichiara particolarmente preoccupato del modo in cui potrebbe essere distorto lo scopo del diritto di accesso; infatti, i soggetti che entrano in rapporti contrattuali o in relazioni d'affari con il soggetto interessato (datori di lavoro, proprietari, locatori, ecc.) potrebbero arrivare a considerare del tutto normale e legittimo esigere la esibizione delle informazioni risultanti dal diritto di accesso come preliminari alla conclusione del contratto. Il progetto di legge sanziona penalmente tale comportamento.

Pene particolarmente severe sono poi previste a carico di colui che comunica ad un terzo un dato di carattere personale figurante in un sistema di trattamento automatizzato dell'informazione nella consapevolezza che si tratta di informazione non destinata ad essere comunicata a terzi (art. 31, § 1), e a carico di chi intenzionalmente abbia utilizzato un sistema di trattamento automatizzato di dati a carattere personale in modo non conforme alla finalità di tale trattamento (art. 31, § 2).

Tali disposizioni sono di particolare rilevanza non solo in quanto costituiscono le prime previsioni volte a sanzionare specificamente ed espressamente la responsabilità penale degli utilizzatori di siste-

³⁹ Progetto di legge relativo alla protezione di certi aspetti della vita privata, *doc. parl.* Chambre 1983-1984, 778, n. 1, su cui v. J.P. SPREUTELS, *Vie privée et informatique. La recherche d'un équilibre*, C.I.E.A.U.,

Bruxelles, 1983. Una prima versione dell'avan-progetto è stata oggetto di alcuni commenti: cfr. J. BERLEUR et Y. POULLET, *Le droit à la vie privée selon le projet Gol*, in *Journ. trib.*, 1982, p. 769.

mi di elaborazione automatizzata dell'informazione, ma anche nella misura in cui vietano il c.d. *detournement de finalit *, cos  come accade nella legge francese, in quella del Lussemburgo e in quella svedese.

Come indica nel suo primo rapporto la *Commission nationale de l'Informatique et des Libert s*, l'adeguamento dei dati registrati alle finalit  del trattamento   linea direttrice pi  feconda di quella del divieto aprioristico di raccolta, ed   contenuta in tutte le leggi « informatica e libert  ». La legge francese esige che le finalit  che giustificano la creazione di un sistema di raccolta e di trattamento dell'informazione vengano portate a conoscenza della Commissione, onde consentire un controllo sulla loro pertinenza⁴⁰. Allo stesso modo, il progetto belga cui si   fatto cenno prevede che debbano figurare nella dichiarazione preliminare e nel registro pubblico l'indicazione dello scopo perseguito con il trattamento automatizzato e quella relativa all'oggetto dei dati, e la giustificazione della scelta di certi dati con riguardo allo scopo perseguito (art. 27, §§ 1, 4 e 5). Inoltre, chi gestisce il sistema di elaborazione   tenuto ad adoperare la massima diligenza in modo da cancellare i dati estranei allo scopo della raccolta e del trattamento (art. 25, § 3).

Per la maggior parte delle infrazioni previste dal progetto, in aggiunta alla pena detentiva e pecuniaria, il Tribunale pu  ordinare la pubblicazione della sentenza, per intero o per estratto, in uno o pi  giornali, e la sua affissione a spese del condannato (art. 32). La pubblicazione della decisione di condanna   prevista anche dalla legge francese e da quella del Lussemburgo, assecondando la tendenza del diritto penale moderno a prevedere sanzioni ritagliate specificamente sul tipo di criminalit . Il giudice pu  inoltre disporre la confisca dei supporti materiali dei dati a carattere personale che formano l'oggetto dell'infrazione, cos  come i dischi e i nastri magnetici, con esclusione degli elaboratori o degli altri macchinari, o la cancellazione dei dati. La confisca o la cancellazione possono venire disposte anche nell'ipotesi in cui i supporti materiali dei dati a carattere personale non appartengano al condannato (art. 38, § 1). Infine, senza pregiudizio dei divieti disposti da norme particolari, il Tribunale pu , nei casi di condanna ad una pena detentiva di almeno tre mesi, proibire al condannato di gestire personalmente o per interposta persona un sistema di elaborazione automatizzata dei dati per un periodo fino a due anni (art. 33, § 2). Le violazioni di tali divieti sono sanzionate penalmente (art. 33, § 3).

Per quanto concerne la questione relativa alla individuazione del soggetto responsabile penalmente, nella relazione espositiva del progetto si legge che il Governo ha optato risolutamente per il sistema di imputabilit  giudiziaria in contrapposizione all'imputabilit  legale,

⁴⁰ Commission National Informatique et des Libert s, *Premier rapport au Pr sident de la R publique et au Parlement 1978-*

1980, Paris, La Documentation Fran aise, 1980, p. 27.

che conduce a svincolare la responsabilità penale dalla ricerca delle colpe autentiche. Di conseguenza, il progetto non fa riferimento alle nozioni astratte di padrone o di gestore del sistema di trattamento automatizzato dell'informazione, ma affida invece al giudice il compito di individuare concretamente in ciascun caso specifico i soggetti che, nella singola fattispecie, sono penalmente responsabili.

Un regime particolare è previsto per l'Amministrazione degli Interni, alla quale non sono applicabili per analogia le altre disposizioni del progetto (art. 16, § 3, comma 5). Per prima cosa, tale amministrazione non potrà gestire sistemi di elaborazione automatizzata dei dati a carattere personale che in vista della prevenzione di reati contro la sicurezza interna ed esterna dello Stato (art. 6, § 3, comma 1)⁴¹. Inoltre, la gestione di tali sistemi di elaborazione sarà controllata da due organismi appositamente creati dal progetto, il *Conseil de protection de la vie privée*, e la *Commission parlementaire pour la protection de la vie privée*.

Il Consiglio è composto da sei magistrati o magistrati emeriti o onorari, consiglieri della Corte di cassazione, consiglieri di Corte d'Appello o giudici di Tribunale, nominati per un periodo di cinque anni rinnovabile dal Senato a maggioranza di due terzi sulla base di una doppia lista fissata dall'assemblea generale della Corte di cassazione. La composizione del Consiglio ha come scopo quello di assicurare l'indipendenza, e la richiesta di una maggioranza qualificata per la nomina dei membri si propone di assicurare una partecipazione dei rappresentanti dell'opposizione nella nomina dei membri dell'organismo in questione⁴². Il *Conseil de protection de la vie privée* autorizza di volta in volta in relazione a ciascun caso il tipo di dati a carattere personale che possono essere inclusi nel trattamento automatizzato gestito dall'Amministrazione degli Interni⁴³; dispone inol-

⁴¹ Riferendosi al testo iniziale dell'avan-progetto, il *Conseil d'Etat* indicava come fosse fortemente auspicabile che la legge stessa precisasse i criteri sulla base dei quali il *Conseil de protection de la vie privée* dovrà rilasciare le proprie autorizzazioni. Il criterio che il testo del progetto propone « in vista dell'accertamento delle sanzioni penali menzionate al comma precedente » manca di precisione. Appare infatti evidente che il termine « accertamento » non può riferirsi alla scoperta degli autori delle infrazioni già consumate, dato che tale accertamento è di competenza dell'autorità giudiziaria. Allora, il riferimento alle infrazioni penali contro la sicurezza interna ed esterna dello Stato si presta ad equivoci. Sembra che non possa aver come obiettivo altro che la prevenzione a più o meno lungo termine di simili infrazioni. Su questo punto il testo dovrà essere precisato, dato che la fissazione di un criterio preciso riveste enorme importanza per accertare quali dati ricadano entro il regime di diritto comune previsto dal progetto.

⁴² Nella relazione espositiva che accom-

pagna il progetto si legge che l'ingerenza eccezionale del potere esecutivo nei diritti della personalità dei singoli individui sarà in tal modo sottoposta ad un controllo efficace e permanente da parte di organismi totalmente indipendenti dalle autorità che procedono alla sorveglianza e che sono investite di poteri e attribuzioni sufficienti per decidere in modo obiettivo.

Gli organismi di controllo, che provengono dal potere legislativo e giudiziario, possono coinvolgere la responsabilità politica del Governo così come la responsabilità penale di coloro che violino la legge o di quei ministri o funzionari che scientemente la facciano o la lascino violare.

⁴³ Il verbo « determina », utilizzato inizialmente dall'avan-progetto, poteva far credere che il *Conseil de protection de la vie privée* fosse investito di un potere regolamentare. Secondo le indicazioni del *Conseil d'Etat*, questo potere dovrà invece essere esercitato soltanto in via di autorizzazione e in rapporto a ciascun tipo di dati.

tre di un importante potere di sorveglianza, potendo verificare d'ufficio se il trattamento automatizzato gestito dall'Amministrazione degli Interni ricomprende altri dati a carattere personale diversi da quelli autorizzati (art. 16, § 3, comma 1). Il Consiglio può inoltre richiedere il concorso di esperti e può incaricare uno o più dei suoi membri, eventualmente assistiti da esperti, di procedere a ispezioni sul posto (art. 16, § 3, comma 2). Infine, l'operato del consiglio è fatto oggetto di pubblicità mediante la comunicazione annuale delle osservazioni del consiglio stesso alla commissione parlamentare sulla protezione della vita privata (art. 16, § 3, comma 4), il che consente un controllo politico del parlamento che può coinvolgere la responsabilità politica del governo.

12. Conclusioni.

L'informatizzazione sempre più accentuata della società moderna la rende particolarmente vulnerabile agli attacchi di una nuova criminalità. Di fronte all'inquietante sviluppo della criminalità informatica, il diritto penale risulta ancora fortemente sguarnito di rimedi specifici. E infatti, se certe fattispecie di rilevanza penalistica possono essere utilizzate per inquadrare comportamenti del tutto nuovi, ciò avviene spesso a costo di una interpretazione assai estensiva dei loro elementi costitutivi; e con un approccio che presenta limiti evidenti.

Sono pertanto necessarie riforme, che in certi ordinamenti giuridici sono già state avviate, volte a inserire nell'apparato normativo incriminazioni specifiche intese a fronteggiare le nuove fattispecie concrete, o quantomeno a modificare le disposizioni già esistenti in modo tale da renderle applicabili alla nuova realtà.

Fino a questo momento, tuttavia, gli sforzi del legislatore si sono concentrati soprattutto nel settore della protezione dei dati a carattere personale, dove è già possibile rintracciare i primi esempi di « reati informatici ». È auspicabile che, anche al di là di questo settore specifico, gli studi e le ricerche intrapresi, sia a livello nazionale che a livello internazionale, consentano al più presto di dotare l'autorità giudiziaria dei vari ordinamenti degli strumenti indispensabili allo scopo di combattere quello che, altrimenti, rischia di divenire un vero e proprio flagello sociale.