VITTORIO FROSINI

LA CRIMINALITÀ INFORMATICA

SOMMARIO: 1. I tre aspetti del rapporto fra la criminalità e l'informatica. — 2. La creazione del bene informatico nella società tecnologica. — 3. Tipologia dei reati informatici. — 4. La nuova figura del criminale informatico. — 5. Vittimologia dei reati informatici. — 6. La criminalità organizzata: il modello mafioso. — 7. Caratteri tecnologico e transnazionale della criminalità organizzata. — 8. Differenze e somiglianze fra criminalità organizzata e terrorismo politico. —— 9. Strumenti giuridici della lotta contro la criminalità organizzata: il ricorso all'informatica. — 10. La repressione del riciclaggio del denaro di provenienza illecita. — 11. L'informatica e la lotta alla criminalità organizzata. — 12. Il diritto di libertà informatica.

1. I TRE ASPETTI DEL RAPPORTO FRA LA CRIMINALITÀ E L'INFORMATICA.

Il rapporto fra l'antico male della società umana, la criminalità, e la nuovissima conquista dell'intelligenza umana, l'informatica, va considerato sotto tre aspetti, collegati fra loro come i tre lati della figura di un triangolo. Il primo di essi è il rapporto esistente fra le nuove forme della criminalità comune, individuale o associata in piccoli gruppi, le quali generano le forme dei *computer crimes*, o reati informatici, che violano la legalità nei suoi termini già conosciuti, come il furto o la frode, o nei termini creati dalla civiltà tecnologica, come il danneggiamento di un sistema elettronico, inteso come bene informatico. Il secondo aspetto del rapporto è quello riferito alla criminalità organizzata, la quale opera seguendo i piani criminosi di una impresa collettiva, e dunque agisce in forma socializzata. Il terzo aspetto consiste nella applicazione dei metodi e degli strumenti informatici per la lotta alla criminalità informatica nel quadro della società tecnologica avanzata.

Per ognuno di questi tre aspetti, si possono elencare gli elementi costitutivi del rapporto ad un duplice livello: il primo è quello

* Conferenza tenuta il 17 maggio 1997 nello Instituto Andaluz Interuniversitario de Criminologia a Siviglia.

della strumentazione tecnica di cui si serve la criminalità e chi la combatte, cioè le forze dell'ordine; il secondo è quello rappresentato dalla configurazione giuridica dei reati e delle misure legali predisposte per la repressione dei reati informatici. In questa sede di trattazione, l'esame dei tre aspetti sopra enunciati del rapporto fra criminalità e informatica viene svolto al secondo livello, il giuridico.

Vi è infatti il riconoscimento, ormai acquisito in sede culturale, in sede scientifica e in sede accademica, di una nuova branca della dottrina giuridica, che è il diritto dell'informatica. Esso va distinto dall'informatica giuridica, la quale si occupa della funzionalità pratica attribuita all'informatica come strumento operante nel campo del diritto: come la ricerca automatica dei dati giuridici, legislativi o giurisprudenziali; l'automazione delle procedure giudiziarie e di quelle elettorali e parlamentari; la creazione di archivi bibliografici e infine la creazione di sistemi esperti in campo giuridico. Il diritto dell'informatica riguarda invece le questioni connesse all'impiego dell'informatica non come strumento ausiliario, ma come oggetto esso stesso di disposizioni normative e di indagini dottrinarie.

2. La creazione del bene informatico nella società tecnologica.

L'avvento dei sistemi di produzione e di trasmissione a distanza di informazioni automatizzate, che consentono di memorizzare, elaborare e diffondere i dati informatizzati con l'impiego di un linguaggio elettronico, ha creato nuovi tipi di valore aggiunto nel campo della produzione economica e dei servizi. Infatti il primo di essi consiste nella trasformazione del materiale originario, che potremmo dire ancora grezzo, dei dati inseriti come *input* in un computer fornito di apposito programma o *software*, in un prodotto finito diverso, che è il risultato del procedimento elettronico, con cui quei dati sono stati trattati. Un ulteriore valore aggiunto è poi quello conferito all'output così ottenuto dalla sua trasmissione o diffusione in tempo reale per mezzo delle operazioni della telematica, cioè del trasferimento della merce informatica. È stato così creato un quarto settore dell'attività economica, detto appunto quaternario, il quale si è distaccato dal settore terziario o dei servizi. Esso caratterizza ormai la nuova società dell'informazione, la quale non potrebbe sopravvivere se privata dei servizi automatizzati ; ma il nuovo settore è diventato il terreno di cultura di germi malefici, che hanno generato la criminalità informatica.

Il reato informatico colpisce un nuovo bene economico, che può essere definito come bene informatico, il quale, una volta che sia stato riconosciuto e protetto dalle leggi, diventa un nuovo bene giuridico. Esso è infatti l'oggetto di un nuovo diritto di carat-

tere reale, ossia di inerenza del diritto al bene che ne rappresenta l'oggetto, di *jus in re propria*, anche se si tratta di una *res* o cosa immateriale, come lo sono del resto anche i prodotti intellettuali, ma che è stata resa oggettiva, cioè misurabile in termini di valore economico e trasmissibile. Il bene informatico può essere venduto o ceduto in uso, ma può anche essere rubato, o danneggiato, o manomesso, o distrutto. Esso va dunque protetto, cioè difeso giuridicamente, oltre che per mezzo delle protezioni di carattere tecnico: quali sono la chiave elettronica, con la quale si limita la facoltà di accesso alla banca dati, per evitare la conoscenza non autorizzata, la riproduzione abusiva o la contraffazione di un programma; o il meccanismo logico di interruzione del procedimento; e altre.

3. Tipologia dei reati informatici.

Esaminiamo le nuove forme di reato attribuite alla criminalità informatica, collocandoci subito nel quadro della esperienza giuridica dell'Europa comunitaria, e trascurando perciò di compiere una ricognizione delle figure di reato informatico come esse sono apparse e sono state identificate nelle legislazioni dei singoli Stati europei e negli Stati Uniti d'America, dove ricordiamo che venne istituito, ad opera della giurisprudenza, il primo laboratorio giuridico di osservazione e di definizione dei nuovi reati. Tuttavia, per esigenze di economia della presente trattazione, prenderemo come punto di riferimento la Raccomandazione (N° R(89) 9) adottata dal Comitato dei ministri del Consiglio d'Europa il 13 settembre 1989, diretta agli Stati membri, sulla criminalità in rapporto con il computer. In essa si denunciava la « nuova sfida » lanciata dalla criminalità informatica, si sottolineava il suo carattere spesso transfrontaliero, dunque sovranazionale; si tracciava una direttiva per i legislatori nazionali, formulando due liste di infrazioni della legalità, che dovevano essere configurate come reati.

La prima lista, detta minimale, comprendeva l'elenco di quelle figure di criminalità informatica, per le quali appariva necessario ed urgente provvedere ad una serie di sanzioni giuridiche, in quanto si trattava di reati già conosciuti e diffusi.

Essi sono: 1) la frode informatica, intesa a servirsi di un trattamento informatico per ottenere un vantaggio economico a danno altrui; 2) il falso informatico, che consiste in una alterazione o soppressione dei dati informatici (esso corrisponde alla già nota falsità in atti); 3) il danneggiamento dei dati di programmi informatici; 4) il sabotaggio informatico, diretto ad ostacolare il funzionamento di un sistema informatico o telematico; 5) l'accesso non autorizzato in un sistema informatico, vale a dire l'intrusione in un « domicilio informatico » altrui; 6) l'intercettazione non autorizzata di comunicazioni telematiche; 7) la riproduzione abusiva

di un programma informatico protetto; 8) la riproduzione abusiva di una topografia di semiconduttore.

La seconda lista, detta facoltativa perché il perseguimento dei reati è lasciato a discrezione del governo nazionale, comprende: 1) l'alterazione dei dati o dei programmi informatici; questo reato è distinto dal falso informatico, perché connesso alla introduzione di un *virus* in un programma; 2) lo spionaggio informatico; 3) l'utilizzazione abusiva di un elaboratore, di un sistema informatico o di una rete telematica (questa è una figura di reato controversa: si pensi all'uso personale di un computer da ufficio); 4) l'utilizzazione abusiva di un programma informatico protetto.

4. La nuova figura del criminale informatico.

La rassegna delle definizioni giuridiche dei reati informatici ci introduce ad un altro argomento, di carattere non oggettivo ma soggettivo, rispetto al reato, di carattere non giuridico ma antropologico: la figura del nuovo tipo di criminale, prodotto dalla stessa società tecnologica, e cioè il criminale informatico. Bisogna però distinguere il criminale occasionale dal criminale professionista. Il primo tipo designa la persona che si rende responsabile di un reato per fini di profitto economico o di vendetta (per esempio un tecnico licenziato da una azienda) ma che delinque per un scopo limitato e che si serve dello strumento elettronico per conseguire una finalità non tecnologica: per esempio l'impiegato infedele di una banca che si appropria del denaro dei clienti stornando la destinazione di un contocorrente. Il secondo tipo rappresenta invece il criminale informatico, che si avvale della sua competenza specifica in materia elettronica al fine determinato di recare danno ad un sistema informatico, anche senza trarre vantaggio economico. È la categoria dei così detti *hackers*, chiamati anche « pirati informatici ».

Al termine *hacker* è stata attribuita una origine dalla lingua tedesca, in cui esso significa « zappatore »: in questo caso si tratta di colui che zappa e rovista il terreno dei programmi informatici, per aprirli come si apre una cassaforte. Va notato, che proprio in Germania esiste il Chaos Computer Club, che riunisce ogni anno ad Amburgo in un convegno gli specialisti di ogni Paese, che siano esperti in « scassinamento elettronico » per escogitare nuovi metodi tecnologici capaci di infrangere i dispositivi di sicurezza elettronica. Non si tratta però di una organizzazione criminale perché i suoi aderenti ritengono di contribuire in tal modo al progresso tecnico, obbligando le case produttrici di programmi informatici ad escogitare metodi più avanzati per garantire la sicurezza dei sistemi al riparo delle incursioni degli *hackers*; perciò i convegni vengono tollerati dalla polizia tedesca. Un *hacker* può però diventare un *cracker*, ossia un vero criminale informa-

tico, come è colui che introduce nelle reti di sistemi informatici un *virus*, ossia un'alterazione del programma, capace di infettare ogni altro programma con cui comunica; e perciò diventare causa di gravissimi danni economici, al punto da riuscire a mettere intere aziende finanziarie fuori servizio.

5. Vittimologia dei reati informatici.

Vale la pena di soffermarsi, sia pure brevemente, « sulla controfigura » del criminale informatico, e cioè sulla sua vittima. Lasciamo da parte quei casi, pure così frequenti, in cui l'aggredito il cui domicilio informatico viene violato (e infatti l'operazione condotta da un pirata informatico viene equiparata all'effrazione di una serratura ed all'invasione di un locale privato), sia un aggredito in quanto gestore di un ente con funzioni non economiche: per esempio i servizi informatici di interesse militare o scientifico. Consideriamo il caso di una azienda di credito, o di una compagnia di assicurazione, o di una rete di servizi commerciali: in questi casi il danno economico cagionato da sottrazione di dati o da immissione di un *virus* che rende inservibili i programmi può essere rilevante. Eppure si verifica, nella generalità dei casi, una complicità passiva, indiretta, clandestina del danneggiato: il quale preferisce occultare il danno ricevuto, pur di non esporsi ad una pubblicità negativa, per non aver saputo proteggere il denaro dei soci o dei clienti, e magari per aver mantenuto e per così dire nutrito nel suo seno il criminale informatico, se questi è un dipendente dell'azienda. Si verifica anzi talvolta, e non di rado, che scoperto il responsabile dell'atto criminoso, se questi è un dipendente dell'azienda egli venga promosso al rango di custode dei segreti elettronici contro le invasioni.

Sia consentito qui di fare riferimento ad un significativo episodio nella legislazione britannica. In preparazione della legge repressiva dei reati informatici, che poi fu il *Computer Misuse Act* 1990 approvato il 29 giugno 1990, il parlamento aveva nominato due distinte commissioni per una indagine ed una proposta di legge in materia: la *Scottish Law Commission*, che presentò il suo *Report* nel 1987 nel quale si raccomandava di *non* fare obbligo di denuncia dei reati subiti da parte delle aziende danneggiate; e la *Law Commission* per l'Inghilterrra ed il Galles, la quale invece dichiarò nel suo *Report* di volersi astenere da una pronuncia sul merito; sicché nella legge citata non fu fatta menzione del problema. Eppure, la denuncia obbligatoria servirebbe ad accrescere la vigilanza delle aziende, esposte ad una responsabilità penale di occultamento del reato, ed a rendere possibile la conoscenza della tipologia, della espansione e della frequenza dei reati. La trasparenza dell'informazione è infatti la principale tutela della libertà esercitata sotto la garanzia della legge.

6. La criminalità organizzata: il modello mafioso.

Dalla criminalità comune informatica va distinta la nuova criminalità organizzata, che si vale dei mezzi e dei metodi forniti dal progresso tecnologico per svolgere la sua opera malefica di corruzione, di ricatto e di violenza, che grazie alla potenzialità accresciuta degli strumenti di cui si serve, accrescono la sua pericolosità sociale, fino al limite di costituire quasi uno Stato dell'antidiritto nello Stato di diritto. L'esempio più probante di questa situazione patologica è quello che viene dato, per quanto riguarda l'Italia, dalla così detta mafia siciliana, organizzazione criminosa collegata ad altre associazioni similari, come la mafia statunitense e quella colombiana, da quando i suoi interessi economici si sono concentrati sul commercio e lo spaccio della droga. Prima di tratteggiare i caratteri della nuova criminalità organizzata nella società tecnologica, è opportuno procedere a qualche precisazione.

La mafia siciliana, che viene considerata un fenomeno caratteristico della Sicilia per tradizione e per mentalità, ha le sue radici storiche nella composizione della società civile siciliana, quale essa si formò con la presenza di una corte viceregale a Palermo, con l'assenza della nobiltà siciliana dalla campagna, preferendo la residenza presso la corte e trascurando gli impegni di governo locale; onde la formazione della categoria sociale dei « campieri » armati, che vigilavano le campagne e fungevano da mediatori fra la classe dominante e la classe dei governati. Tale condizione si prolungò anche sotto il governo dei borboni di Napoli.

Lo sfruttamento del contadino siciliano nella zona occidentale dell'isola, caratterizzata ancora dai feudi medievali, mentre nella zona orientale vi era una più estesa piccola proprietà, generò la mafia agraria che viveva in forma parassitaria sul lavoro altrui, e la mentalità tipicamente mafiosa del farsi giustizia da sé, senza far ricorso ai tribunali. Con l'unione della Sicilia al resto dell'Italia, e con il rifiorire dei commerci e delle attività produttive, che la Sicilia aveva conosciuto all'epoca del dominio normanno, con la sua nobiltà rurale e guerriera, alla mafia agraria successe la mafia urbana, che si insediò nella vita cittadina, prosperando con le estorsioni ai negozianti e con la speculazione edilizia. Ma nel corso degli ultimi decenni la mafia è venuta cambiando fisionomia: essa è diventata, da un insieme di famiglie legate ciascuna da vincoli di sangue, una società composita di vecchi e di nuovi criminali, una società di servizi (si intende, al servizio del male), un elemento rilevante del settore terziario dell'economia, che gestisce il traffico di armi e di droga, che impiega ingenti capitali, e che si è inserita nella logica economica della società tecnologica, in quanto svolge la sua attività illecita muovendosi sul terreno del trasferimento elettronico dei fondi, del commercio di valute, del gioco coi titoli delle borse azionarie.

7. Caratteri tecnologico e trasnazionale della criminalità.

Si è fatto riferimento alla mafia siciliana giacché essa costituisce una specie di modello, per delineare i nuovi parametri della criminalità organizzata nel quadro della civiltà tecnologica. Ma la mafia non è soltanto siciliana: questo non è che un episodio al quale vengono attribuiti certi caratteri folcloristici, dell'attività di una categoria criminosa presente anche in altri Paesi: come negli Stati Uniti, in cui alla mafia di origine siciliana si affiancano quella irlandese, quella cinese, e quella sudamericana; come nel pur ordinato Giappone, in cui la potente organizzazione degli Yakuze svolge una funzione di corrosione sociale non diversa. Ma vi è oggi una caratteristica delle grandi organizzazioni criminali, che le accomuna: esse sono ormai ramificate in una dimensione transnazionale, si sono dotate di strutture di supporto e di collegamento con l'impiego di sistemi elettronici e di reti di trasmissione telematica, che consentono collegamenti e solidarietà fra i raggruppamenti criminali dei diversi Paesi. Vi è infatti una nuova forma di criminalità organizzata, che consiste precisamente in una rete di traffico internazionale, con scambi di informazioni, di merci e di denaro: basti pensare alle procedura di raccolta del materiale grezzo della droga, di spedizione della stessa, di raffinamento in località anche assai lontane da quella di origine, di distribuzione clandestina e di spaccio al minuto della droga.

Questa complessità di rapporti è consentita solo dai mezzi odierni e di comunicazione di massa, e poiché parliamo della droga come di un fenomeno indicativo in forma specifica e rappresentativa dell'attività illecita delle organizzazioni criminali, va anche precisato che la diffusione della droga è essa pure un prodotto, sia pure malefico della civiltà tecnologica: basti pensare all'uso delle siringhe, che consentono una rapida assuefazione; per cui in certi Paesi, come la Svezia, la lotta alla droga si esplica con un controllo rigoroso della importazione e della vendita delle siringhe. La droga è però in se stessa un effetto della nuova civiltà dei consumi, in quanto essa rappresenta una controcultura, un tunnel per l'evasione dal conformismo o dalla solitudine nella società di massa, è una forma di protesta psicologica, magari a livello inconscio, contro l'alienazione della persona umana in una crisi di trasformazione del mondo dei valori morali.

8. Differenze e somiglianze fra criminalità organizzata e terrorismo politico.

È certamente discutibile l'affermazione, che il terrorismo, come viene designata l'attività politica dedita alla violenza e alla sovversione sociale, debba considerarsi come pertinente o affine alla cri-

minalità organizzata. Essa non lo è infatti per quanto attiene alla intenzione soggettiva ed al comportamento dei suoi partecipanti, che anzi sono spesso uomini o donne di assoluta probità ed abnegazione dei propri interessi individuali, e nemmeno lo è per quanto attiene alle sue finalità ultime, che possono essere collegate ad una rivendicazione di libertà, anche se attribuita ad una minoranza, tuttavia, da un punto di vista e di osservazione puramente fenomenico, queste differenze sostanziali vengono messe tra parentesi nell'opera di prevenzione e repressione, che viene compiuta dalle forze dell'ordine, le quali sono tenute a difendere gli interessi della società politica governante e ad assicurare la normalità della vita civile della popolazione governata.

Occorre perciò fare qualche riflessione in merito, per comprendere anche il fenomeno del terrorismo politico collocandolo nel quadro della civiltà tecnologica, nella quale è diventato possibile, anche a gruppi estranei alle forze armate legalmente riconosciute, di disporre di armi micidiali, quali le bombe ad orologeria o con comando a distanza, i missili con testata esplosiva, le armi da guerra automatiche; per non parlare di altre armi di natura psicologica, come i messaggi lanciati con trasmissioni televisive. Il terrorismo politico contemporaneo si differenzia da quello dei secoli precedenti, che hanno conosciuto attentatori con pugnali e con bombe a mano, non soltanto per i mezzi di cui si serve, ma perché esso è un terrorismo di tipo tecnologico.

Il terrorismo tecnologico considera la violenza armata non come uno strumento provvisorio, ma come un fine esso stesso, come dimostrazione di un potere, che è destinato ad essere propagandato attraverso i mezzi di comunicazione di massa, giornali, radio e televisione; senza questa risonanza nella pubblica opinione, essa fallirebbe il suo scopo. La violenza esercitata dalle organizzazioni terroristiche, spesso a danno di folle inermi e inconsapevoli, come quelle che popolano le stazioni ferroviarie e i supermercati, è una violenza concepita come tecnica del terrore, e che perciò fa ricorso a preferenza agli strumenti di morte più sofisticati, ai piani di guerriglia urbana preparati a tavolino come un meccanismo da montare e smontare, alla razionalità fredda e cinica della strage come esecuzione capitale istantanea di massa. Considerato come una forma di criminalità organizzata, un accordo per la repressione del terrorismo venne infatti stipulato fra gli Stati membri del Consiglio d'Europa il 27 gennaio 1977.

9. Strumenti giuridici della lotta contro la criminalità organizzata: il ricorso all'informatica.

Il rapporto, che si è venuto a costituire, sia pure in modi diversi come si è indicato, fra la criminalità e l'informatica, trova riscon-

tro nel rapporto tra le forze dell'ordine e l'informatica, che è necessario per contrastare adeguatamente le nuove forme di reato. Poiché non è possibile contenere, in uno spazio ideale limitato come questo, una rassegna analitica delle iniziative, delle procedure, delle normative giuridiche, che sono state attuate al fine sopra menzionato nei Paesi appartenenti all'area della civiltà tecnologica, sarà dato particolare rilievo, in questa sede, all'esperienza giuridica italiana, con gli opportuni riferimenti agli sviluppi, che si sono verificati in sede comunitaria europea.

Il punto di avvio della nuova dimensione informatica, a cui il legislatore italiano ha indirizzato l'opera delle forze di polizia, può essere identificato nella legge del 1 aprile 1981, n. 121, sul « nuovo ordinamento dell'Amministrazione della pubblica sicurezza ». In essa veniva infatti istituito un « Centro di elaborazione dati » presso il ministero dell'interno (art. 8) e veniva fatto obbligo di notificare, entro la fine di ogni anno, l'esistenza di archivi magnetici (banche dati personali) detenuti da enti o anche da singoli privati al ministero. Veniva disciplinato, nella stessa legge, l'accesso ai dati e informazioni, e l'uso che poteva farsene. Per curiosità storica, riportiamo l'elenco delle notifiche presentate entro il 31 dicembre 1981, l'anno dell'emanazione della legge. Furono 61.717 notifiche, comprensive di 105.739 banche dati personali: fra le quali, 74 con dati attinenti all'attività politica; 453 con dati di natura sindacale; 15 con dati di natura religiosa; e persino 29 con dati di appartenenza razziale. S'intende che il numero si accrebbe negli anni successivi, sicché apparve evidente che buona parte della popolazione italiana era stata schedata ad opera di privati, a dimostrazione della esistenza di un nuovo potere sociale, il potere informatico che consente a chi lo detiene di conoscere, sorvegliare, ed all'occorrenza di suggestionare, con la pubblicità, i comportamenti altrui.

La lotta contro la criminalità organizzata, identificata genericamente con il termine « mafia », ebbe inizio in termini giuridici con il decreto legge del 13 settembre 1982, n. 846, che conteneva prescrizioni per la repressione dei reati di stampo mafioso (comuni anche ad altre associazioni criminose come la camorra napoletana e la 'ndrangheta calabrese); veniva altresì istituita una Commissione parlamentare di indagine, e con decreto legge del 6 settembre 1972 era già stato nominato un Alto Commissario con poteri speciali per la Sicilia.

10. La repressione del riciclaggio del denaro di provenienza illecita.

Altre leggi seguirono, che qui non elenchiamo; ma va ricordato il decreto legge del 29 giugno 1990, poi convertito in legge del 4 agosto 1990, n. 227, con cui veniva delineata la nuova fisionomia

della criminalità organizzata come società di servizi finanziari illeciti, e veniva imposta la rilevazione dei trasferimenti elettronici dei fondi (denaro, titoli e valori) da e per l'estero; anche a questa legge altre ne seguirono per la lotta al riciclaggio del cosiddetto « denaro sporco », cioè di provenienza illecita.

Per rendersi conto dell'incidenza sui mercati finanziari del cosiddetto « denaro sporco » accumulato con i proventi del *racket* o taglieggiamento dei privati, del prelievo di « tangenti », ossia di somme per mediazione forzosa negli appalti anche di opere pubbliche, del traffico d'armi e degli enormi guadagni ricavati dallo spaccio di droga, basterà citare un episodio. Il 20 febbraio 1995 a Catania gli agenti della Guardia di Finanza arrestavano, mentre stava per imbarcarsi sull'aereo diretto a Lugano (Svizzera), un distinto signore, incensurato, di professione dichiarata imprenditore edile, tale G.C., come venne riportato sui giornali. Il personaggio intratteneva rapporti di affari con istituti finanziari del più alto livello, e all'atto dell'arresto si preparava a trasferire, con una sola operazione di trasferimento elettronico di fondi, la cifra di 1.600 miliardi di lire. Com'è evidente, il potere di corruzione di una organizzazione criminale che disponga di mezzi tali, le consente di superare molti ostacoli ed anche forti scrupoli.

Va ricordato, che ancor prima di una legislazione statale repressiva del riciclaggio del denaro di provenienza illecita, quando si cominciarono a delineare le conseguenze di natura penale assunte dal fenomeno, come le imputazioni di connivenza nelle operazioni di illecito arricchimento, il 12 dicembre 1968 venne sottoscritto un accordo dal Comitato per le regolamentazioni bancarie e le pratiche di vigilanza di Basilea, in cui sono rappresentate le Banche Centrali e con esse gli organi di vigilanza bancaria di nove Paesi europei, più gli Stati Uniti e il Giappone: nell'accordo stipulato non si faceva però ancora menzione dei sistemi informatici. Lo strumento giuridico decisivo per una cooperazione fra gli Stati della Comunità Europea su questa linea direttiva fu dato dalla convenzione firmata a Strasburgo l'8 novembre 1990, « sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato », alla quale aderì anche l'Italia con legge del 3 agosto 1993, n. 328, che introdusse nel codice penale l'art. 648-*ter* con la sanzione prevista di una reclusione da quattro a dodici anni e con la multa da due a trenta milioni di lire. Seguì il decreto legge del 17 settembre 1993, n. 369, nel quale venne prevista per gli imputati di associazione a delinquere di stampo mafioso « i quali, anche per interposta persona, fisica o giuridica, risultano essere titolari o avere la disponibilità a qualsiasi titolo di denaro, beni o altre utilità di valore sproporzionato al proprio reddito, o alla propria attività economica, e dei quali non possono giustificare la legittima provenienza », la pena di una reclusione da due a cinque anni e la confisca dei beni.

11. L'INFORMATICA E LA LOTTA ALLA CRIMINALITÀ ORGANIZZATA.

I tempi erano ormai maturi per l'avvento dell'informatica e della telematica nel rapporto fra le forze dell'ordine e la criminalità organizzata sul piano degli accordi internazionali.

L'evento più significativo al riguardo fu la sottoscrizione dell'accordo di Schengen del 14 giugno 1985 relativo all'eliminazione graduale dei controlli alle frontiere comuni, stipulato fra i governi del Benelux, della Germania e della Francia: successivamente altri Stati aderirono, come l'Italia con protocollo del 27 novembre 1990 e la Spagna con protocollo del 25 giugno 1991.

L'interesse presentato dall'accordo di Schengen non è però limitato all'indicazione, contenuta nel titolo, dell'apertura delle frontiere, benché questo sia stato un passo in avanti decisivo nella storia del cammino verso una Unione Europea: passo in avanti, che ha fatto procedere verso il Trattato di Maastricht del 7 febbraio 1992. Infatti, nell'accordo di Schengen venne programmato un sistema informativo automatizzato per lo scambio rapido di informazioni su persone e cose per la salvaguardia comune dell'ordine e della sicurezza pubblica e per il controllo sull'ingresso negli spazi comunitari dei cittadini di Stati terzi, cioè extraeuropei. Nel 1988 venne istituito, sulla base dell'accordo, un gruppo di lavoro permanente, che ha predisposto la creazione di una struttura stellare articolata in un sistema centrale (C.SIS) con sede in Francia e sistemi nazionali (N.SIS) ad esso collegati, e una struttura di comando e di controllo denominata SIRENE (*Supplementary Information Request at the Nation Entry*) per valutare le richieste dei Paesi aderenti e assistere gli operatori di Polizia.

L'accordo di Schengen è ormai operante da tempo, sebbene abbia talvolta incontrato ritardi nella sua piena applicazione, come nei riguardi dell'Italia, finché questa è stata priva di una legislazione sulla protezione dei dati personali. Alla iniziativa pubblica di livello internazionale ed alle iniziative di livello nazionale, si è affiancata talora anche l'iniziativa privata nel ricorso ai mezzi e ai metodi informatici. Infatti l'associazione Bancaria Italiana (ABI) ha promosso il progetto « Gianos », diventato operativo dal 3 gennaio 1995, che coordina 319 banche, ed è diretto a individuare i comportamenti sospetti della clientela. Una legge del 1991 (N. 197) aveva resa obbligatoria l'istituzione di un archivio unico centralizzato delle operazioni bancarie: con le indagini ed analisi informatiche condotte secondo il progetto Gianos, su 3.500.000 operazioni bancarie superiori ai 20 milioni di lire, si è giunti nel 1995 a identificare i soggetti che avevano operato per conto proprio o in conto terzi con versamenti in denaro contante di tale entità da richiedere una giustificazione.

12. Il diritto di libertà informatica.

L'apporto, che si può considerare per il momento conclusivo del cammino percorso nella lotta alla criminalità informatica nell'esperienza giuridica italiana, è quello fornito dalla legge del 23 dicembre 1993, n. 547, che si intitola precisamente: « Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica ». Essa venne preparata da una Commissione ministeriale nominata dal ministro di grazia e giustizia Giuliano Vassalli il 4 gennaio 1991, composta da magistrati, professori universitari (fra i quali anche l'estensore delle presenti note) e da un esperto di informatica e venne presieduta dal magistrato dr. Piero Callà, direttore degli affari penali del ministero.

Va precisato, che la Commissione si trovò a dover scegliere fra due metodi di tecnica legislativa per la stesura del progetto di legge: l'uno, il metodo organico, consistente nella predisposizione di una legge che prevede diverse forme di reati connessi allo stesso bene giuridico, che si provvede a riunire in un solo *corpus* legislativo; come si era fatto in Francia con la legge del 5 gennaio 1988, che inserì un nuovo titolo, il terzo, composto di otto articoli, nel libro terzo del codice penale; l'altro, il metodo evolutivo, che consiste invece nell'apportare modifiche ed aggiunte alle norme già esistenti nel codice penale, come era stato fatto nella Repubblica Federale Tedesca con la legge del 5 maggio 1986. La Commissione scelse a maggioranza di seguire il metodo evolutivo, e ne risultò la legge citata, nella quale sono state previste sanzioni penali, detentive e pecuniarie, per quei reati informatici elencati nella Raccomandazione del Consiglio d'Europa, su cui abbiamo già riferito.

Va però ricordato, per completezza dell'argomento trattato, che nella recente legislazione italiana sono state emanate altre due importanti leggi, in materia di repressione della criminalità informatica. La prima è il decreto legislativo del 29 dicembre 1992, n. 518, relativo alla tutela giuridica dei programmi per elaboratore, le cui norme sono state adattate alla precedente legge sul diritto d'autore del 22 aprile 1941, N. 633: la nuova legge prevede sanzioni per chi abusivamente duplica a fini di lucro programmi per elaboratore, ovvero importa, distribuisce, vende, detiene o concede in locazione senza essere autorizzato tali programmi. Anche per questa legge si è preferito il metodo evolutivo al metodo organico, equiparando i programmi informatici ai prodotti intellettuali di carattere letterario e artistico, malgrado le palesi differenze, trascurando il carattere innovativo del linguaggio elettronico.

La seconda legge è quella del 31 dicembre 1996, n. 675, con la quale l'Italia ha finalmente provveduto a garantire la protezione dei dati personali, la cosiddetta privacy o riservatezza, ovvero,

come ebbe a definirlo la dottrina fin dal 1981, il « diritto personale di libertà informatica »: dunque il diritto di tutelare non solo gli interessi economici, ma anche e soprattutto gli interessi morali della persona umana, come era stato fatto dalla Spagna con l'art. 18 della sua Costituzione, del 23 dicembre 1978, alto esempio di civiltà giuridica.