TRANSCRIME

WORKING PAPERS

research group on transnational crime, university of trento, school of law

via inama, 5 - 38100 - TRENTO - (Italy) tel. (+39) 0461 882304 fax (+39) 0461 882303 e-mail: transcrime@gelso.unitn.it

dicembre 1998

n. 29

PROCESSI DI GLOBALIZZAZIONE E CRIMINALITÀ ORGANIZZATA TRANSNAZIONALE

ernesto u. savona
in collaborazione con
federico lasco, andrea di nicola
e paola zoffi

relazione presentata al convegno:
"la questione criminale nella società globale "
napoli, italia,10 - 12 dicembre, 1998

INDICE

INTRODUZIONE

Questo saggio si propone di analizzare un problema di importanza crescente nella comunità internazionale, e cioè il rapporto che intercorre tra il processo di globalizzazione che sta investendo la nostra società e la criminalità organizzata transnazionale. La criminalità organizzata transnazionale si avvale di tutte le opportunità offerte dalla globalizzazione dei mercati e dalle nuove tecnologie di comunicazione e di gestione dell'informazione. La natura internazionale dell'attività di riciclaggio dei proventi di provenienza illecita, ad esempio, conferma che proprio questa attività criminale potrebbe risultare maggiormente avvantaggiata e rivoluzionata dallo sviluppo della tecnologia informatica e di comunicazione.

La criminalità organizzata transnazionale rappresenta una grave minaccia ai sistemi economici e finanziari di tutti gli stati e deve essere contrastata efficacemente a livello internazionale affinché il processo di globalizzazione possa procedere tranquillamente. I gruppi criminali che operano su mercati transnazionali, infatti, presentano delle caratteristiche peculiari quali la flessibilità e l'alto livello di organizzazione, che contribuiscono a complicare il lavoro delle autorità di investigazione e di tutti quegli organi e istituzioni che cercano di prevenire e contrastare le attività criminali.

I criminali tendono a massimizzare le opportunità offerte nei mercati nazionali o internazionali e a minimizzare il rischio di essere identificati, arrestati e condannati e avere sequestrati i proventi delle loro attività criminali. Unanime è la convinzione che il futuro terreno di scontro tra le agenzie di controllo ed il crimine organizzato sarà sempre più costituito dal mondo delle informazioni. Altrettanto importanti sono quindi quelle tecnologie che permettono di confrontarsi alla pari con le organizzazioni criminali operanti in contesti transnazionali. Considerando che la criminalità organizzata si è ramificata in una dimensione transnazionale, si comprende come sia necessario che la lotta per contrastare questo fenomeno assuma lo stesso carattere; ciò impone innanzitutto la circolazione delle informazioni ed una maggiore cooperazione tra le autorità investigative dei singoli paesi.

La preliminare definizione di alcuni termini è fondamentale al fine di procedere con la discussione dei temi trattati in questo saggio. La criminalità transnazionale è stata definita da alcuni autori come una serie di "attività criminali che si estendono in diversi paesi e che violano le leggi di diversi paesi" (Adler, Mueller, e Laufer, 1994, p.567). L'elemento che contribuisce a differenziare la criminalità transnazionale da quella nazionale risiede proprio nel fatto che la prima viola le leggi penali di diverse giurisdizioni mentre la seconda si limita a violare la legislazione penale di un singolo stato. Reati quali il riciclaggio di denaro sporco, il traffico illegale di armi e narcotici, la pirateria marina ed i reati ambientali costituiscono solo alcuni esempi di attività illecite poste in essere dai gruppi di criminalità transnazionale, mentre il furto e la rapina sono due esempi di reati compiuti da gruppi criminali che operano in un mercato nazionale.

Un'ulteriore distinzione deve essere evidenziata, ossia la differenza che intercorre tra il crimine internazionale e quello transnazionale. Mentre la caratteristica del primo è quella di violare leggi e regolamenti internazionali, la peculiarità della criminalità transnazionale è quella di violare leggi e regolamenti penali di diverse giurisdizioni nazionali. L'abbattimento intenzionale di un aereo civile effettuato da una unità militare è un esempio di reato internazionale mentre il dirottamento di un velivolo è un reato transnazionale. Può risultare utile evidenziare anche la differenza che intercorre tra la criminalità transnazionale e le imprese legittime. Il confine non sempre è certo poiché le attività che caratterizzano i gruppi di criminalità transnazionale sono in alcuni casi abbastanza simili a quelle che caratterizzano gli affari legittimi. Ad esempio, sia la *Federal Express* americana che il cartello colombiano di Medelin sono interessati a stimolare e sviluppare il commercio nei rispettivi paesi investendo risorse umane, capitali e sfruttando le economie di scala. La differenza fondamentale, tuttavia, sta nel giudizio sul modo di agire delle due diverse organizzazioni, poiché un giudizio di illegittimità accresce il rischio che i criminali siano interrotti nelle loro attività dalle operazioni di polizia. In poche parole, i gruppi che commettono dei reati transnazionali si configurano, sotto un certo punto di vista, semplicemente come delle organizzazioni che stanno dalla parte sbagliata della legge.

La maggior parte dei reati posti in essere dalle organizzazioni criminali transnazionali non rappresenta una novità; la novità risiede infatti negli aspetti di flessibilità organizzativa che caratterizzano le attività criminali. I reati rappresentano per le organizzazioni criminali quello che le attività legali rappresentano per le imprese legali. Questo saggio, piuttosto che considerare i singoli reati transnazionali, intende analizzare le due questioni che caratterizzano lo sviluppo ed il contrasto del crimine organizzato transnazionale: da una parte la globalizzazione dei mercati che induce delle facilitazioni nei fenomeni di migrazione e comunicazione e dall'altra la cooperazione internazionale nell'area della criminalità e della giustizia penale.

La definizione di criminalità transnazionale può essere analizzata evidenziando alcuni elementi centrali che la caratterizzano: le attività illecite poste in essere dai gruppi criminali transnazionali oltrepassano i confini nazionali e violano le leggi penali di almeno due giurisdizioni diverse. Proprio per questo motivo i termini "transnazionale" e "organizzato" vengono utilizzati in maniera intercambiabile per specificare la genericità della parola crimine. La terza caratteristica, forse la più importante, risiede nel forte elemento organizzativo della criminalità transnazionale. Per portare a termine delle operazioni che vadano al di là dei confini nazionali e per rendere minimo il rischio di essere catturati, i gruppi criminali transnazionali devono introdurre una disciplina strettissima, un elemento organizzativo flessibile e devono dotarsi di conoscenze tecnologiche avanzate. A questo proposito, l'Organizzazione delle Nazioni Unite (ONU) durante la Conferenza Mondiale sulla Criminalità Organizzata Transnazionale svoltasi a Napoli nel novembre del 1994, ha deciso di utilizzare il termine "crimine organizzato transnazionale" per sottolineare la sofisticazione di tipo organizzativo che caratterizza le attività criminali dei gruppi che operano in diversi paesi.

Il crimine transnazionale rappresenta un enorme problema che non deve in alcun modo essere sottovalutato. Una serie di effetti conseguenti allo sviluppo del Mercato Unico Europeo, ad esempio, in alcuni casi hanno determinato le precondizioni ideali per una forte espansione anche delle organizzazioni criminali transnazionali e delle loro attività.

La libertà di circolazione di persone, beni e capitali ed il conseguente abbassamento dei controlli sui movimenti degli stessi, l'apertura dei mercati dei paesi dell'est Europa ed i loro l'U.E. costituiscono gli elementi che facilitano lo sviluppo

Alcune cifre serviranno a comprendere la portata del problema qui in discussione. Secondo le stime effettuate dal Gruppo di Azione Finanziaria Internazionale sul Riciclaggio dei G7 (GAFI-FATF 1990, Annexes to the Report, p.12) il mercato della droga in Europa e negli Stati Uniti nel 1990 ammonta a più di 122 miliardi di dollari e il Fondo Monetario Internazionale ritiene che i profit ti accumulati annualmente dai gruppi criminali transnazionali a livello mondiale ammontino a 500 miliardi di dollari, il che equivale a circa il 2% del prodotto interno lordo (Tanzi e Quick, 1996). Nel 1996 le frodi e irregolarità al bilancio sono costate all'Unione Europea 1,3 miliardi di ECU (circa 1,4 miliardi di dollari), che rappresentano il 2% del bilancio di quell'anno (Commission des Communautes Europeennes, 1997, p.2).

L'obbiettivo di questo saggio è quello di dare alcune indicazioni sul problema emergente della criminalità transnazionale e questo obiettivo verrà perseguito cercando di rispondere ad alcune domande tra loro interrelate: perché il problema della criminalità transnazionale ha assunto un'importanza crescente ai giorni nostri? E, soprattutto, cosa si può fare per cercare di prevenire e contrastare questo fenomeno?

Nella prima parte verranno esaminati alcuni dati statistici riguardanti l'incidenza della criminalità transnazionale, al fine di fornire alcune indicazioni circa l'estensione del problema. Nella parte successiva si cercherà di evidenziare le relazioni che intercorrono tra la criminalità transnazionale ed il fenomeno di globalizzazione che sta caratterizzando la società in questi anni. Verranno quindi esplorati alcuni temi riguardanti la migrazione e la criminalità transnazionale, mettendo in luce alcune considerazioni riguardanti i c.d. *computer crimes o* reati informatici, che rappresentano uno dei maggiori, cruciali e recenti sviluppi della criminalità transnazionale. Infine alcune considerazioni conclusive riguardanti la cooperazione internazionale in materia di criminalità e di giustizia penale. La cooperazione internazionale costituisce il requisito necessario per un governo globale del problema "criminalità". Più i paesi diventeranno consapevoli delle difficoltà e dei costi di trattare individualmente problemi di giustizia penale, più guarderanno agli strumenti ed ai meccanismi della cooperazione internazionale come le soluzioni per i loro problemi.

1. L'INCIDENZA DELLA CRIMINALITÀ TRANSNAZIONALE.

I dati statistici riguardanti la criminalità transnazionale non sempre risultano chiari. Nonostante ci sia un urgente bisogno quantificare il fenomeno, ossia di sapere esattamente quanta criminalità transnazionale esista nel mondo e quanti individui siano coinvolti in questo tipo di attività criminale, una quantificazione di questo tipo che si avvicini alla realtà non è ancora stata effettuata in conseguenza dell'enorme difficoltà che si riscontra nel momento in cui si devono misurare delle attività che sono essenzialmente segrete. La presenza del c.d. "numero oscuro" vale anche per i fenomeni di criminalità

transnazionale, tuttavia alcune indicazioni riguardanti l'estensione del problema possono essere ricavate dall'esame dei seguenti dati:

- è stato stimato che l'industria mondiale della droga abbia una entrata annuale di circa 500 miliardi di dollari (UNDCP, 1994, p.1), il che rappresenta circa la metà dei 1000 miliardi di dollari spesi nel 1991 per la difesa a livello mondiale (SIPRI, 1992);

- le autorità di investigazione italiane hanno stimato che tre gruppi di criminalità organizzata operanti in Italia possono contare su più di 16.300 individui nelle loro fila, includendo 5.000 membri nella Mafia in Sicilia, 6.000 nella Camorra a Napoli e 5.300 nella N'drangheta in Calabria (Organizational Intelligence Unit, 1995, p.5);

- il Ministero dell'Interno della Federazione Russa ha evidenziato l'esistenza di più di 8.059 gruppi criminali operanti in Russia, con circa 35.000 membri ed un numero che varia da 70 ad 800 di *Vory v Zakone* (ladri nella legge, ossia membri che rispettano il codice di comportamento dell'organizzazione criminale). Il Ministero ha inoltre calcolato che circa 30 delle associazioni criminali eurasiatiche esistenti operano sul mercato internazionale (Organizational Intelligence Unit, 1995, p.3);

- è stato calcolato che circa 45 - 50 Triadi cinesi (le organizzazioni criminali che pongono le loro origini nelle società segrete presenti in Cina nel XVII secolo) pongono le loro basi organizzative ad Hong Kong e Taiwan, e si stanno espandendo in tutto il mondo (Organizational Intelligence Unit, 1995, p.6);

- l'Agenzia di Polizia Nazionale del Giappone ha rivelato che i gruppi criminali giapponesi denominati Yakuza o *Japanese Boryokudan* sono formati da circa 3.000 gruppi e sottogruppi per un totale che ammonta a circa 87.000 affiliati (Organizational Intelligence Unit, 1995, p.8);

- uno studio riguardante gli effetti del crimine organizzato sull'economia americana ha stimato che le organizzazioni criminali nel 1986 hanno ridotto la produzione americana di circa 17,4 miliardi di dollari ed hanno eliminato circa 400.000 posti di lavoro. Inoltre è stato stimato che nello stesso anno i prezzi al consumo sono aumentati dello 0,3% a causa delle attività della criminalità organizzata e che il reddito pro capite annuale si è abbassato per un valore pari a circa 73 dollari a testa (Wharton Econometrics, 1986, p.490).

2. IL PROCESSO DI GLOBALIZZAZIONE E LA CRIMINALITÀ ORGANIZZATA TRANSNAZIONALE.

Il processo di globalizzazione negli ultimi anni è divenuto una forza economica e sociale fondamentale a livello internazionale. Tuttavia se da una parte questo processo ha contribuito a potenziare le opportunità per le imprese legali, dall'altra ha facilitato lo sviluppo e la sofisticazione dei gruppi criminali che operano su mercati transnazionali.

Le operazioni criminali, infatti, sempre più frequentemente sono condotte su scala transnazionale. Questo processo è in parte dovuto alle stesse cause che hanno portato alla globalizzazione dei mercati convenzionali ma, in aggiunta, nel settore criminale esistono altri incentivi al proseguimento di questo trend. Operando in campo transnazionale si può approfittare delle disomogeneità legislative esistenti tra i diversi paesi così come dellInferiore capacità di controllo da parte delle agenzie di polizia nazionali.

Per questo motivo, ed al fine di sfruttare a pieno tutte le opportunità create dalla globalizzazione, è intuibile che specialmente nei gruppi criminali transnazionali si sia manifestata la necessità di una maggiore efficienza e flessibilità organizzativa. Le ultime operazioni di polizia internazionale sembrano confermare in pieno questo trend; testimoniano infatti come i gruppi criminali tradizionali siano in grado di legarsi, secondo le esigenze del momento, a diversi soggetti dellèconomia convenzionale o ad altri gruppi criminali, al fine di formare alleanze estemporanee in grado di meglio rispondere a particolari esigenze del mercato[1]. E proprio come le loro controparti nel mondo legale, le imprese criminali si sono dotate di un patrimonio logistico e tecnologico che comprende computers, fax, telefoni cellulari, in modo tale da trasformare queste opportunità in fiorenti

Il processo di globalizzazione è un processo dinamico. Alcuni dati forniti nel 1995 dallo *United Nations Development Program* (UNDP) indicano che il commercio internazionale delle merci è triplicato dal 1960 e che le transazioni internazionali sono cresciute di circa il 14%. LÕOrganizzazione Mondiale del Commercio (WTO*, World Trade Organizations*) ha stimato che nel 1995 il commercio mondiale di merci è stato valutato in circa 4300 miliardi di dollari**,** con una crescita pari a circa il 20% solo in quellànno (tabella 1). E'stato inoltre stimato che nel 1995 il commercio globale di servizi ha raggiunto un valore di poco al di sotto dei 1200 miliardi di dollari, con una crescita pari al 14% nello stesso anno.

[1] FATF-IX 1997-1998 Report on Money Laundering Typologies, 12 febbraio 1998.

Tabella 1

Crescita del commercio mondiale di merci 1990-1996
(in miliardi di dollari e in percentuale)

	Valore	Variazione annua %		
	1996	1990-1996	1995	1996
Mondo	**5100**	**7**	**19.5**	**4**
Nord America	826	8	14.5	6.5
America Latina	250	9.5	21.5	11.5
Messico	96	15	31	20.5
Altri paesi America Latina	154	6.5	17	6.5
Europa Occidentale	2271	5.5	22.5	3
Unione Europea (15)	2103	5.5	23	3
Economie in transizione	171	7	29	6
Europa Centrale ed Orientale	81	6.5	26.5	2
Africa	113	1.5	12.5	8.5
Sud Africa	28	3	10.5	2
Medio Oriente	160	3	13	12.5
Asia	1310	10	18	1
Giappone	413	6	11.5	-7
Cina	151	16	23	1.5
Sei paesi dell'Asia orientale*	131	12	23	3

* Hong Kong, Repubblica Coreana, Malaysia, Singapore, Taipei, Tailandia

Fonte: WTO 1997 p. 4

Il processo di globalizzazione ha allargato le opportunità non solo per le imprese legali ma anche per la criminalità transnazionale, creando nuovi affari e nuovi mercati nel mondo legale ma anche in quello criminale, e fornendo mezzi sempre più sofisticati e potenti con i quali le organizzazioni criminali possono essere più efficienti. Il processo di globalizzazione ha inoltre contribuito a sfumare i confini tra criminalità economica e criminalità organizzata. Criminalità organizzata e criminalità economica tendono progressivamente a sovrapporsi. La criminalità economica è cresciuta in maniera sempre più sofisticata ed organizzata, in conseguenza della maggiore complessità dei mercati economici nell'ambiente globale attuale, mentre i gruppi tradizionali di criminalità organizzata si sono diversificati, aggiungendo alle loro attività i reati economici più

lucrativi e meno rischiosi. Diversi tipi di frodi costituiscono il punto di saldatura tra il mercato legale e il mercato illegale. Le frodi al bilancio comunitario e, più in genere, le frodi sono reati di origine oppure strumentali ad altri reati come la corruzione o il riciclaggio. Diversificare le attività criminali in operazioni economiche in mercati legali assicura un profitto stabile che non crea sospetti, ma questo tipo di investimento è possibile solo se l'organizzazione criminale è in grado di trasformare la propria organizzazione in una struttura più flessibile ed efficiente.

Le organizzazioni criminali cercano di minimizzare i rischi di essere identificati, arrestati e condannati operando in quelle giurisdizioni ove vi è una carenza di strutture investigative e dove vi è la possibilità di utilizzare lo strumento della corruzione per portare a termine le attività criminali. Le ricerche sulla criminalità organizzata, infatti, concordano che i due strumenti tradizionali dell'azione delle organizzazioni criminali sono la violenza e la corruzione. I criminali utilizzano la corruzione per infiltrarsi nell'economia legale dove investono i proventi delle proprie attività illecite e usano la corruzione per garantirsi il controllo delle risorse disponibili (es. appalti, licenze, contributi).

L'influenza della globalizzazione sulla criminalità transnazionale può essere esaminata considerando la situazione di nazioni con un diverso livello di sviluppo. Per i paesi in via di sviluppo la globalizzazione ha portato ad una trasformazione da una economia locale verso mercati globali più aperti, ma ha anche portato ad una riduzione dei prezzi dei prodotti tradizionali, e quanto più questi mercati tradizionali diventano più competitivi e i profitti vengono ridotti, tanto più diventano appetibili i profitti illeciti. Un drastico declino dei prezzi dei beni di prima necessità in paesi come il Pakistan, dove il prodotto interno lordo si aggira sui 400 dollari ed un chilo di eroina base rappresenta per un fornitore un guadagno annuale che varia dai 750 ai 1000 dollari, rende inutile qualsiasi politica che si proponga di ridurre la produzione e il commercio di sostanze stupefacenti (UNDCP, 1994). Questo si capisce più chiaramente richiamando il fatto che la proporzione del debito esterno rispetto al prodotto interno lordo rimane molto alta nei paesi in via di sviluppo. Il rateo del debito del Pakistan, ad esempio, nel 1992 si aggirava intorno al 48%. Nonostante i paesi in via di sviluppo costituiscano un luogo di minori rischi per la criminalità transnazionale, la maggior parte degli introiti derivanti dalle attività criminali non rimane in questi paesi; infatti il denaro, una volta ripulito, confluisce nei conti correnti delle maggiori banche mondiali.

Gli effetti della globalizzazione sui paesi dell'ex Unione Sovietica e sui loro satelliti rappresentano in questo senso un fenomeno preoccupante. Il precedente sistema economico è stato distrutto e molti di questi paesi stanno cercando di combattere una crescita negativa e una forte inflazione. Per esempio in Georgia nel 1994 il prodotto interno lordo è diminuito del 28% ed il tasso di inflazione si aggirava attorno al 2000%. I fenomeni di transizione verso una economia di mercato globale e la privatizzazione che ha caratterizzato questa transizione hanno creato una serie di opportunità per la criminalità transnazionale, e solamente il basso tasso di guadagno degli investimenti effettuati nei paesi dell'ex Unione Sovietica sembra sia servito come barriera effettiva alle attività della criminalità transnazionale.

Se la situazione nei paesi in via di sviluppo desta preoccupazione, gli effetti della globalizzazione sulla criminalità organizzata nei paesi industrializzati non sono

assolutamente da trascurare. In primo luogo il processo di globalizzazione e la concorrenza che da questo ne deriva innestano una pressione economica sulle imprese marginali e creano un forte incentivo a queste stesse imprese a connettersi con il crimine transnazionale per sopravvivere. In secondo luogo una crescita del commercio mondiale comporta un conseguente aumento del numero delle transazioni finanziarie e contribuisce a diminuire il rischio che queste stesse transazioni vengano sottoposte a controlli da parte delle autorità investigative.

La prova di come la crescita del commercio mondiale e la liberalizzazione dei mercati hanno contribuito ad aumentare le opportunità per la criminalità transnazionale può essere rinvenuta in un esempio riguardante lUnione Europea. A partire dagli anni 80 in poi, anni in cui si è cominciato a costruire un mercato unico europeo, la confisca di sostanze stupefacenti è cresciuta in maniera esponenziale. I sequestri di eroina sono cresciuti di sette volte dal 1985 al 1994 mentre la confisca di cocaina è cresciuta del 42%, e questa crescita nellammontare delle confische non può essere certamente attribuita solo ad un rafforzamento delle forze di investigazione e di polizia. Che il numero annuale delle morti per droga sia inoltre cresciuto di 5 volte dal 1982 al 1991 suggerisce che lammontare globale di droga presente in Europa sia cresciuto, e questo costituisce una indicazione di come la riduzione delle barriere nei mercati economici possa essere un vantaggio per leconomia illegale.

3. MIGRAZIONE E CRIMINALITÀ ORGANIZZATA TRANSNAZIONALE.

Le differenze esistenti nelle condizioni di benessere dei cittadini nelle diverse nazioni sono uno dei fattori che maggiormente contribuisce alla migrazione. Sovrappopolazione, alti tassi di disoccupazione, disastri ecologici, privazione dei diritti civili, persecuzioni politiche e un basso tenore di vita sono tutti fattori che inducono molti individui a cercare una migliore qualità di vita da qualche altra parte, e tutto ciò contribuisce a creare un mercato di persone che richiedono di migrare e di organizzazioni criminali che sfruttano questa nuova domanda.

Le differenze nelle condizioni di benessere sono state catalogate dallo UNDP nel 1997; considerati questi fattori:

- circa l80% del prodotto interno lordo globale viene realizzato nei paesi industrializzati, nonostante la popolazione di questi paesi rappresenti solo il 20% rispetto alla popolazione mondiale;
- il divario tra il reddito pro capite nei paesi industrializzati e quello nei paesi in via di sviluppo si è triplicato dal 1960 al 1993, passando da 5.700 dollari a 15.400 dollari;
- i paesi industrializzati consumano la maggior parte della produzione annuale di energia, metallo e legno;
- più di 120 milioni di persone nellEuropa dellest guadagnano meno di 4 dollari al giorno;
- il tasso di crescita della popolazione è più alto nei paesi in via di sviluppo che nei paesi industrializzati e laspettativa di vita è più bassa nei primi che nei secondi;

- più di 30 paesi, la maggior parte dei quali situati in Africa, sono attualmente in stato di guerra.

Tenendo presente questi fattori e molti altri ancora, è logico pensare che migliaia di persone residenti nei paesi in via di sviluppo desiderino lasciare i loro paesi di origine per trasferirsi nei paesi industrializzati. Naturalmente, con un alto tasso di disoccupazione presente in tutta l'area europea, i singoli paesi europei hanno emanato delle leggi che prevedono delle misure restrittive sull'immigrazione, e queste legislazioni hanno in qualche modo frenato anche il flusso di immigrati legali e di coloro che chiedono asilo politico. Tuttavia poiché il desiderio di emigrare non è stato bloccato da queste leggi, si è creata una forte domanda di immigrazione illegale, e le organizzazioni criminali di tutto il mondo hanno cominciato a fornire i loro servizi offrendo la possibilità di migrare illegalmente.

Le opportunità di guadagni illeciti sono aumentate per le organizzazioni criminali rispetto al fenomeno della migrazione illegale, e deve essere inoltre evidenziato che il rischio associato a queste attività criminali è rimasto uniformemente basso. In molti paesi il traffico di immigrati non è ancora considerato un reato mentre in altri viene sanzionato in maniera lieve[2]. Ad esempio in America Centrale solamente Panama e Honduras hanno emanato una legislazione per combattere l'immigrazione clandestina (Winer, 1996, p.61). La situazione è la stessa nell'Europa centrale ed orientale. Anche nelle nazioni dell'Europa occidentale le sanzioni contro il traffico di immigrati clandestini spesso non superano i due anni di prigione e in molti casi si limitano ad una pena pecuniaria. A tutto ciò si deve aggiungere che in molti paesi gli standard che caratterizzano l'attività investigativa sono bassi e, combinati con gli alti livelli di corruzione, facilitano il fiorire dell'immigrazione illegale.

Ci sono alcuni aspetti tra loro correlati che coinvolgono le organizzazioni criminali che si occupano del mercato dell'immigrazione illegale. Alcuni gruppi criminali non si limitano al traffico di immigrati ma pongono in essere anche tutta una serie di attività collaterali quali la produzione di documenti falsi, e non si limitano al solo trasporto degli immigrati clandestini, ma spesso li sfruttano introducendoli nel mercato della droga e della prostituzione, con un meccanismo che li costringe a ripagare le organizzazioni criminali del costo dell'immigrazione clandestina. L'entrata nel mondo del crimine da parte degli immigrati clandestini spesso non è frutto di una libera scelta, ma deve ricondursi ad una sorta di circolo vizioso che si crea in queste situazioni (Transcrime, 1996, pp.53-72; Savona, Da Col e Di Nicola, 1997, pp. 191-207; Savona e Di Nicola, 1998).

La crescente esperienza maturata dalle organizzazioni criminali che si occupano del traffico di immigranti rappresenta probabilmente lo sviluppo più importante nell'immigrazione illegale. Le Triadi Cinesi, ad esempio, trafficano migliaia di cittadini cinesi in tutto il mondo, guadagnando annualmente una cifra che è stata stimata in circa 3,5 milioni di dollari (Smith 1994). Le Triadi rappresentano uno dei gruppi criminali più attivi sulla scena internazionale, e non si limitano al solo trasporto dei clandestini, ma una volta raggiunto il paese di destinazione, li costringono ad entrare nel mercato del lavoro

[2] Per ulteriori approfondimenti su questo tema si veda Belgium, Austria and ICMPD, 1995; Secretariat of the Inter-Governmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia, 1995a; e Siemens, 1996.

nero. La Mafia Russa è anchèssa coinvolta nel traffico di immigrati clandestini. Dopo il collasso dellUnione Sovietica, sono state aperte nuove rotte per il traffico di immigrati clandestini. Oggigiorno la Mafia Russa controlla la rotta Baltica che prende il via dai paesi asiatici ed attraverso gli stati Baltici giunge fino al cuore dellUnione Europea. (Ulrich, 1996, pp. 15-16; IOM - Migration Information Programme, 1997). Una stima degli introiti annuali derivanti dal traffico di immigrati clandestini per un singolo gruppo di Mafia Russa ammonta a circa 12 milioni di dollari (Savona, 1996, pp. 1-20).

I gruppi criminali appartenenti alla Yakuza giapponese si sono specializzati nel traffico di donne per lo sfruttamento sessuale. Questi gruppi stanno estendendo la loro presenza attraverso tutto il mercato del sud - est asiatico, importando in Giappone molte ragazze e giovani donne dai paesi vicini più poveri (Savona, Adamoli, Zoffi with the assistance of DeFeo, 1995, pp. 10-11). Naturalmente i gruppi Yakuza non sono i soli che si occupano di questo tipo di traffico. Le donne vengono trafficate in tutto il mondo a fini sessuali, dai mercati dellÆAsia, Sud America e Africa, e più recentemente dai paesi dellèx Unione Sovietica (IOM - Migration Information Programme, 1995). E le donne non sono il solo target di queste organizzazioni criminali, visto che anche i bambini vengono trafficati a scopi sessuali, per le adozioni illecite e per il traffico di organi umani.

Complessivamente i proventi del traffico mondiale di esseri umani è stato stimato in un importo che varia dai 5 ai 7 miliardi di dollari (Widgren, 1994, pp. 5-6); una stima più recente avvicina lÌmporto agli 8 miliardi di dollari (IOM, 1996, p. 3). Il costo della migrazione illegale naturalmente varia in ragione della distanza da percorrere e della difficoltà nellÀattraversare i confini. Ad esempio passare il confine tra il Messico e gli Stati Uniti costa al clandestino tra i 200 ed i 300 dollari, mentre passare il confine dalla Cina verso lEuropa o gli Stati Uniti costa tra i 35.000 ed i 40.000 dollari. Questi costi sono maggiori per gli individui che cercano di fuggire da una vita povera nel loro paese natale e spesso costringono gli individui ad entrare nel mondo del crimine nel nuovo paese al fine di pagare il viaggio.

Un dibattito è stato intrapreso a livello nazionale, regionale ed internazionale riguardo alle politiche da implementare nei vari paesi coinvolti da questo fenomeno al fine di trovare una soluzione ai crescenti problemi di immigrazione clandestina e di criminalità transnazionale. Cinque specifiche politiche attualmente in discussione sono solo alcune che, se attuate da tutti gli stati interessati a prevenire e reprimere il fenomeno dellÌmmigrazione clandestina, potrebbero portare ad un approccio integrato ed armonizzato del problema:

- la prima di queste politiche riguarda lo sviluppo prolungato sostenibile. LÌntenzione è quella di stabilizzare le economie dei paesi dai quali provengono la maggior parte degli immigrati clandestini, in modo tale che migliori condizioni di vita e opportunità di lavoro potrebbero costituire un incentivo a rimanere nei paesi nativi. Naturalmente questo scopo può essere raggiunto solo se i paesi industrializzati adottano un piano di lungo termine che riguardi lo sviluppo nei paesi più poveri. LÌntroduzione di politiche commerciali che incoraggino liberi scambi tra paesi poveri e paesi ricchi potrebbe aiutare a migliorare la situazione attuale. Risulterebbe inoltre utile un piano concertato di informazione che mettesse al corrente i potenziali migranti clandestini delle possibilità di immigrazione legale e dei pericoli associati allÌmmigrazione illegale;

- una seconda politica concerne l'armonizzazione delle politiche regolatorie dei paesi industrializzati. Raggiungere una migliore coordinazione a livello di paesi industrializzati per quel che riguarda le leggi sull'immigrazione potrebbe aiutare a creare un flusso stabile e programmato di migranti e ridurre la possibilità che questo flusso si stabilizzi in paesi impreparati a gestire l'arrivo di nuovi residenti;
- un altro set di politiche riguarda le misure di prevenzione e di controllo del crimine. I singoli stati devono arrivare a cooperare l'uno con l'altro con lo scambio di informazioni e tecnologie. Le attività di controllo sui confini dovrebbero essere migliorate e, ove manchino, dovrebbero essere emanate delle leggi che proibiscano il traffico di clandestini, e rafforzate quelle già esistenti qualora si dimostrassero troppo deboli per contrastare il fenomeno, il tutto accompagnato da una uniformità legislativa a livello regionale al fine di evitare disparità di trattamento. Gli stati dovrebbero inoltre essere pronti a darsi reciproca assistenza giudiziaria nei procedimenti contro i trafficanti di clandestini, includendo la possibilità di estradizione;
- ciascun stato dovrebbe implementare delle politiche atte a proteggere e reintegrare le vittime dello sfruttamento sessuale, come le donne ed i bambini. A queste vittime dovrebbe essere data la possibilità di rimanere nei paesi dove sono stati trafficati in base ad un programma di integrazione, e dovrebbero essere previsti dei meccanismi per rimpatriare coloro che desiderino ritornare nel loro paese di origine;
- altre politiche che abbiano come obiettivo l'integrazione dei migranti legali dovrebbero essere implementate. E' importante garantire a coloro che emigrano legalmente in un altro paese delle condizioni di vita confortevoli e rispettabili. Atti di discriminazione non dovrebbero essere tollerati e dovrebbe essere garantito l'accesso al sistema scolastico

4. I REATI INFORMATICI NEL "VILLAGGIO GLOBALE"

La globalizzazione sta cambiando il contesto nel quale operano sia le imprese legali che quelle illegali (Williams, 1994). Oggigiorno il crimine organizzato è una grande impresa, spesso a carattere internazionale o transnazionale, che sfrutta, ove sia possibile, le nuove tecnologie informatiche. Queste novità tecnologiche, soprattutto l'avvento di Internet, consentono delle comunicazioni immediate ed anonime tra lunghe distanze e consentono ai gruppi di criminalità organizzata di operare senza frontiere in modi finora sconosciuti. (Shelley, 1995, p. 465).

L'utilizzo dell'informatica in questo contesto si spiega con riferimento a molteplici fattori. Innanzitutto costituisce una struttura di supporto, fatta di computer e reti telematiche, utilizzata per la gestione dei proventi delle attività illecite. Alcune attività tipiche della criminalità transnazionale, come ad esempio il traffico di stupefacenti, il gioco d'azzardo, le scommesse illegali, i prestiti usurai, lo sfruttamento della prostituzione e l'immigrazione clandestina vengono ora controllate dai computer delle organizzazioni criminali con un'ottica manageriale simile, sotto certi aspetti, a quella di una holding non criminale.

L'ultimo decennio è stato testimone di un incremento sempre più forte nell'uso personale e commerciale di Internet. E'stato stimato che dai 15 ai 25 milioni di utenti utilizzino Internet

in 92 paesi, e il numero dei fruitori aumenta con una tasso che varia dal 5 all'8% ogni mese (Adams, 1996). Questo nuovo mezzo, che sembra non avere confini, è senza dubbio vulnerabile ad un utilizzo improprio, e non tutti gli ordinamenti giuridici prevedono come reati autonomi i "*computer crimes".* Un nuovo fenomeno di atti illeciti commessi con l'ausilio dei sistemi informatici o contro di essi è stato infatti identificato con il termine *computer crimes*, sulla base dell'esperienza degli Stati Uniti che per primi ne hanno sperimentato l'impatto dopo che, sempre per primi, hanno visto il diffondersi massiccio [3].

E' opportuno separare, innanzitutto, nell'ambito dei comportamenti di abuso dei mezzi informatici, i reati economici dalle violazioni della *privacy* individuale. La latitudine di certe definizioni del *computer crime* è infatti tale da abbracciare entrambi questi comportamenti, ma si tratta di fattispecie di natura diversa. L'indebita registrazione di dati personali pone problemi giuridici complessi sulla natura dei diritti violati e, generalmente, non viene posta in essere da soggetti isolati ma da organismi di strutture pubbliche o di aziende private. Altro è l'aspetto economico del *computer crime*, escludendo quindi l'analisi dei problemi relativi alla gestione delle banche dati.

In letteratura si ritrovano definizioni di *computer crime* assai numerose ed utilizzate per fini diversi. Un rapporto redatto dallo *U.S. Department of Justice, National Criminal Justice Information and Statistics Service* (1979) definisce il *computer crime* come "qualsiasi comportamento criminale o socialmente dannoso" che abbia avuto "per oggetto, ovvero per strumento un elaboratore di dati" e per la cui riuscita, scoperta ed accertamento sia "essenziale la conoscenza specifica della tecnologia elettronica"[4]. Al fine di una chiarificazione concettuale, il rapporto offre altre due disposizioni: una afferma che si tratta di "un tipo di reato non violento, compiuto all'interno di un sistema di computer", mentre l'altra specifica che un computer deve essere utilizzato "come strumento per commettere un reato di natura economica - finanziaria". Infatti lo stesso rapporto definisce l'utilizzo dell'elaboratore a scopo criminale come "un atto intenzionale compiuto con l'uso di un computer, per il quale uno o più agenti conseguono o potrebbero conseguire un illecito guadagno e una o più vittime subiscono o potrebbero subire una perdita".

Per quanto riguarda le principali tecniche impiegate nel *computer crime*, alcune sono esclusivamente informatiche mentre altre sono miste, ossia realizzate in parte attraverso la perpetrazione di un crimine di tipo convenzionale, si pensi ad esempio al furto di documenti cartacei per appropriarsi delle *passwords* ed al loro successivo utilizzo per ottenere l'accesso al sistema che altrimenti sarebbe negato.

Le tecnologie informatiche costituiscono dei formidabili strumenti per l'esercizio delle attività illecite, e nonostante il processo di globalizzazione e la proliferazione di Internet abbiano avuto un effetto apprezzabile su un gran numero attività criminali, solamente alcune di queste verranno analizzate, prima fra tutte il riciclaggio di denaro sporco. La ricerca di nuovi sistemi per inserire il denaro illecito nei canali legali dell'economia è andato di pari passo con il rafforzamento, da parte delle autorità di tutti i paesi del mondo, della legislazione per il controllo e la trasparenza dei movimenti di capitale. La ricerca di

[3] C. Triberti (a cura di), I reati informatici. Computer security, Gruppo Editoriale Fabbri, Bompiani, Sonzogno, Etas S.p.A., 1990, pp. 30 e ss.
[4] L. Picotti, Studi di diritto penale dell'informatica, Verona, 1992, p. 14.

nuovi metodi di riciclaggio da parte delle organizzazioni criminali è inoltre una conseguenza diretta dell'attività investigativa che in questo campo poteva e può contare su dei validi strumenti di investigazione e sull'appoggio di molti soggetti economici rilevanti, come gli istituti bancari e gli intermediari finanziari.

Le opportunità di riciclare proventi illeciti sono state favorite ed ingrandite dall'integrazione dei mercati finanziari, dalle innovazioni nei servizi finanziari e dall'esplosiva crescita di Internet utilizzata come mezzo di scambi finanziari. Queste transazioni finanziarie hanno luogo nel c.d. "cyberspazio" invece che in città come New York, Berlino o Tokyo, e di conseguenza la criminalità organizzata ha la possibilità di commettere dei reati transnazionali senza la necessità di oltrepassare confini geografici. Questa possibilità rappresenta un importante vantaggio a favore della criminalità transnazionale poiché il cyberspazio è ancora relativamente immune dalle forze di polizia.

Cyber-laundering o cyber-riciclaggio indica l'ultima tendenza in fatto di tecniche di riciclaggio. Le nuove frontiere dell'informazione, con in testa Internet, hanno contribuito a creare originali possibilità di occultamento, mascheramento e investimento dei proventi da attività illecite. L'uso di queste nuove tecnologie e la creazione di un mercato virtuale, basato sull'uso del denaro elettronico, rappresenterà molto probabilmente, il nuovo terreno di scontro tra agenzie di controllo e criminalità.

Il processo di globalizzazione sotto un certo punto di vista rappresenta una minaccia alla stabilità monetaria e ai sistemi di scambi finanziari. Negli ultimi anni, ad esempio, la criminalità organizzata russa ha infiltrato con successo i sistemi di trasferimento elettronico del denaro di alcune banche e società degli Stati Uniti. Queste organizzazioni criminali sono riuscite a portare a termine tutta una serie di operazioni assai complesse reclutando alcuni scienziati russi esperti di computer che un tempo erano membri privilegiati del mondo militare ed industriale sovietico. Questi esperti conosciuti come "*hacker*s" o "*crackers*" utilizzano programmi software chiamati "*sniffers*" o "cavalli di troia" per violare le barriere destinate a proteggere i sistemi informatici delle istituzioni americane. Una volta penetrato il sistema, i *crackers* possono accedere alle diverse filiali dell'istituzione, muovendo denaro all'interno dell'istituzione stessa prima di trasferirlo nei conti correnti di persone appartenenti alla criminalità organizzata. Questo genere di attacchi perpetrati dai *crackers* russi e da altri pirati informatici sono cresciuti drammaticamente da circa 200 all'anno a più di 1000 ogni mese, e causano dei danni altissimi alle società o istituzioni che ne sono vittime. Nel 1995 gli attacchi informatici sono costati ad alcune imprese e banche americane qualcosa come 300 milioni di dollari in due mesi (Alexander e Munro, 1996, p. 157).

Il processo di globalizzazione e la crescita di Internet hanno contribuito in maniera rilevante alla commissione di nuovi schemi di frode. Naturalmente non sono venute meno le frodi che esistevano prima dell'avvento di Internet, ma oggigiorno ci si trova sempre più spesso di fronte a nuovi e sempre più sofisticati tipi di frode, ed è notevolmente aumentata la possibilità di vedere rubato il proprio numero di carta di credito ogni volta che si effettua un acquisto in Internet.

Non tutti gli ordinamenti giuridici prevedono un reato autonomo di frode informatica, ma la ricomprendono nella fattispecie più ampia del reato informatico. In linea generale si può

prendere come punto di riferimento la definizione contenuta nella raccomandazione del Comitato dei Ministri del Consiglio dEuropa: per frode informatica si intende "lingresso, la cancellazione o la soppressione di dati o di programmi informatici, ovvero ogni altra ingerenza in un trattamento informatico che ne influenzi il risultato, causando in tal modo un pregiudizio economico o materiale ad unaltra persona, allo scopo di ottenere un vantaggio economico illegittimo per se stessa o per altri".

Le frodi compiute mediante lutilizzo di Internet e dei computers possono essere divise in tre diverse categorie. Si distinguono le *"input frauds"*, le *"output frauds"* e le *"throughput frauds",* ossia si può agire sui dati inseriti allinterno del computer, alterandoli (tramite cancellature selettive o sostituzione di dati) o immettendoli abusivamente (dati fittizi). Laalterazione è realizzabile su una struttura di dati già esistente. Ad esempio, prendendo in esame una ipotetica scheda elettronica composta da dati unitari che si riferiscono ad un certo elemento aggregante (per esempio una persona caratterizzata da cognome, nome e data di nascita), si potrà parlare di alterazione quando venga modificato abusivamente un singolo dato, definito nellInformatica come campo, ferma rimanendo la struttura della scheda. Si avrà invece immissione abusiva di dati se, allinterno di una struttura, si inseriscono dati fittizi senza che esista un precedente *record*.

Si può agire, oltre che sui dati, sul programma; quando questultimo, in base al quale il computer svolge la sua attività, viene alterato rispetto al suo funzionamento normale, può erogare elaborazioni diverse da quelle normali; la macchina è quindi programmata proprio per attuare le frodi. Un tale tipo di alterazione può essere compiuta solo da operatori molto esperti che conoscono molto bene le modalità di funzionamento sia degli aspetti informatici che dellorganizzazione. In tali casi per alterare il programma occorre essere in grado di procedere ad una modifica dello stesso dallinterno del sistema e tale operazione non è facilmente eseguibile senza lasciare tracce.

Più facilmente realizzabile è invece la creazione di un programma predisposto alla commissione delle frodi, come ad esempio le alterazioni (realizzate dallo stesso autore del programma commissionato da una banca) che permettono, in una contabilità bancaria, di accreditare su un unico conto (quello del programmatore - truffatore) piccolissime decurtazioni apportate sugli interessi (mediante arrotondamenti) di migliaia e migliaia di altri conti correnti di ignari clienti della banca. In questo ultimo caso il delitto di frode informatica si intende realizzato anche se laalterazione avviene ab origine e non si può distinguere tra un programma originale ed uno alterato.

La c.d. *input fraud* è probabilmente la più facile da realizzare poiché si tratta di manipolare o falsificare le informazioni contenute in un database. Gli esempi relativi a questo tipo di frodi sono innumerevoli. Ad esempio nel Regno Unito la *Audit Commission* ha reso noto un caso di frode in cui 68.000 sterline sono state accreditate sul conto corrente di un impiegato del governo centrale. Il frodatore ha semplicemente alterato un file, lasciando il nome e lindirizzo esatti del fornitore e cambiando i dettagli del conto bancario. I controlli interni mancarono di segnalare le nuove informazioni bancarie e conseguentemente la somma fu trasferita sul conto di colui che aveva iniziato la frode senza problemi. In un altro caso un giovane impiegato della *National Wastminster Bank* per un soffio non è riuscito a trasferire fraudolentemente una somma di denaro di circa 31 milioni di sterline su un conto corrente svizzero. Limpiegato fece il trasferimento con la

password di un'altra persona e fu scoperto solo perché l'ammontare del trasferimento eccedeva il limite di 30 milioni di sterline imposto sulla transazione (Backhouse, 1995, p. 57).

Appartengono alla seconda categoria di frodi le c.d. *"throughput fraud"*. Questo tipo di frode risulta più difficile da commettere perché richiede delle elevate conoscenze tecnologiche ed un accesso a database e software. Un esempio di questa frode venne alla luce quando un impiegato di banca, che lavorava nello sportello dei cambi di valuta, introdusse un tasso di cambio meno favorevole nel suo computer e si intascò la differenza. Appartengono alla terza categoria di frodi le c.d. *"output fraud"*. L'obbiettivo di questo tipo di frode è quello di nascondere o ritardare la scoperta dei dati fittizi inseriti in un computer al fine di porre in essere una *input fraud*. Si tratta di una frode che non presenta un alto grado di sofisticazione e non è comune poiché è molto vulnerabile e sono stati implementati diversi controlli al fine di evitare questo tipo di frode (Backhouse, 1995, p.57).

Come dimostrano gli esempi appena riportati, il processo di globalizzazione e la crescente importanza di Internet come mezzo di scambi economici hanno portato alla ribalta l'emergenza crimini informatici come un problema molto attuale ed importante. Ma in che cosa consistono esattamente i reati informatici? Il termine non è soggetto ad alcuna definizione precisa ed universale. Nonostante ciò, un punto di partenza può essere essere trovato evidenziando che i reati informatici coinvolgono l'utilizzo del computer e/o del software in uno di questi tre modi.

In primo luogo un computer può rappresentare il bersaglio di un reato, ed in questo caso l'obbiettivo del criminale è quello di ottenere delle informazioni dal computer o di distruggerle. Il computer può essere inoltre utilizzato come un mezzo nella commissione di altri reati. Questo è il caso in cui il criminale utilizzi il computer per facilitare alcuni reati tradizionali come le frodi o i furti, ad esempio quando un impiegato di banca utilizza un computer per prelevare una piccola somma da un grande numero di conti correnti per depositaria nel suo conto corrente. Infine il computer può essere utilizzato come elemento secondario nella commissione di alcuni reati; i trafficanti di droga, ad esempio, possono decidere di memorizzare le informazioni relative al traffico di stupefacenti in un personal computer. (Charney & Alexander, 1996). In questo caso il criminale utilizza il pc come uno strumento di tipo organizzativo per gestire gli affari di una impresa criminale, alla stregua di ciò che avviene nelle imprese legali.

Come già notato in precedenza, le innovazioni in campo tecnologico e comunicativo derivanti dal processo di globalizzazione della finanza e delle imprese, consentono al crimine in generale, ed alla criminalità organizzata in particolare, di diventare sempre più sofisticata e difficile da scoprire. Il volume, la velocità di spostamento elettronico del denaro e l'anonimato consentiti da Internet hanno aumentato le opportunità anche per le autorità di investigazione. Anche quando il computer viene utilizzato da un criminale ad esempio per registrare delle informazioni riguardanti il traffico di stupefacenti, questa situazione aumenta le possibilità per gli investigatori. Infatti i diversi modi in cui i criminali utilizzano i computers per le loro attività criminali hanno creato delle nuove opportunità, non solo per le autorità investigative, ma anche per i professionisti della sicurezza dei computer (Charney & Alexander, 1996).

Lo spostamento da un ambiente tangibile/corporale nel quale gli oggetti sono immagazzinati in una forma tangibile, verso un ambiente elettronico, intangibile, significa che i reati informatici e gli strumenti e metodi utilizzati per investigarli non sono più soggetti alle regole tradizionali e precostituite. Prima dell'avvento della rete dei *computers*, l'abilità di rubare informazioni o di danneggiare una proprietà erano rigidamente determinate da limitazioni fisiche. Nell'era dell'informatica tuttavia questi limiti non si applicano più. I criminali che rubano informazioni contenute in un network di computers possono ottenere una determinata informazione virtualmente da qualunque posto nel mondo. La quantità di informazioni che possono essere rubate e l'ammontare dei danni che possono essere causati da codici di programmazione alterati è limitata solo dalla velocità della rete e dall'equipaggiamento e dalla tecnologia sofisticata in possesso dei criminali. Poiché una attività del genere può facilmente essere portata a termine attraverso i confini sovranazionali, le autorità investigative devono coordinare attentamente tutte le investigazioni riguardanti i reati informatici. Ma una coordinazione domestica, ossia all'interno di una singolo stato, può risolvere solo una parte del problema poiché il crimine informatico, per essere contrastato efficacemente, necessita di una risposta internazionale organizzata (Charney & Alexander, 1996).

Poiché le materie legali e tecniche coinvolte nell'investigazione e prosecuzione del crimine informatico sono assai complesse ed abbastanza variabili, è necessaria una struttura flessibile e sofisticata che fornisca delle tecnologie avanzate oltre che una formazione scientifica e professionale alle autorità di investigazione. Inoltre, i corpi investigativi dovrebbero avere la possibilità di usare alcuni strumenti tipici delle investigazioni più complesse quali la sorveglianza elettronica e le operazioni sotto copertura. Infatti le risorse a disposizione di questi corpi dovrebbero essere così formidabili come quelle a disposizione dei criminali. Ma tutto ciò richiede una conoscenza approfondita dei computers, delle reti, delle tecnologie di decodificazione così come delle operazione e dello sviluppo dei mercati finanziari internazionali e dei loro prodotti. Inoltre è fondamentale che le informazioni ed i dati necessari per un'azione attiva delle autorità investigative si muovano oltre i confini nazionali con la stessa facilità con cui si muovono le informazioni che agevolano l'attività dei criminali. Proprio come il crimine organizzato e la criminalità dei colletti bianchi hanno oltrepassato i confini giurisdizionali degli stati, così dovrebbero fare le forze di polizia al fine di prevenire e combattere tali attività.

Risposte ai reati informatici

I reati informatici costituiscono un problema di crescente importanza all'interno della comunità internazionale e sono state ipotizzate diverse risposte a questo problema. Queste risposte possono essere classificate in base all'autorità o istituzione che intraprende l'azione di contrasto. In primo luogo un paese può decidere di procedere nel contrasto ai reati informatici con lo strumento legislativo, oppure le imprese possono sviluppare delle procedure per prevenire i reati informatici, infine gli individui possono intraprendere dei passi per assicurare loro stessi o le organizzazioni per le quali lavorano di non cadere vittime dei criminali e dei loro computers.

Prima di procedere ad analizzare le risposte ai crimini informatici, è necessario evidenziare alcuni aspetti inerenti al problema. La legge che governa il cyberspazio non è

sviluppata a sufficienza e la rete Internet si pone virtualmente al di là del controllo dei regolatori. Molti paesi non hanno una legislazione riguardante i crimini informatici mentre altri stati hanno emanato dei regolamenti insufficienti a contrastare efficacemente la criminalità informatica. Questa disattenzione ai reati informatici da parte delle singole nazioni rappresenta il maggior ostacolo alla cooperazione internazionale sull'argomento, poiché i paesi senza regolamentazione dei reati informatici sono spesso recalcitranti a devolvere risorse significative per cercare di arginare il problema a livello internazionale (Charney & Alexander, 1996). Ma la cooperazione internazionale rappresenta la giusta risposta al problema dei crimini informatici poiché tali reati coinvolgono attività che si estendono al di là dei confini nazionali. Un effettivo programma internazionale di prevenzione e repressione dei reati informatici potrà venire la luce solamente quando i singoli paesi riconosceranno che le attività criminali in questione rappresentano un pericolo domestico e che la cooperazione internazionale è necessaria per rispondere adeguatamente al problema.

La questione di base che concerne il problema dei reati informatici è questa: quale sistema giuridico dovrebbe avere giurisdizione su Internet? Come notato poc'anzi, le frodi informatiche sono diventate un problema a carattere internazionale ma, per portare solo un esempio, quali criteri dovrebbe applicare un tribunale per decidere la competenza giurisdizionale nel caso in cui una transazione finanziaria sia iniziata negli Stati Uniti, l'importo sia stato convertito in marchi tedeschi per il trasferimento elettronico e poi sia stato emesso da una banca francese? Inoltre, quale paese ha la responsabilità su di una banca che esiste solo nello spazio elettronico? Forse la competenza giurisdizionale dovrebbe essere quella del paese in cui è localizzato il computer coinvolto nel trasferimento elettronico di fondi. Ma anche in questo caso risulterebbe difficile individuare il *situs* di una transazione che coinvolge una vasta rete di apparecchiature di calcolo e comunicazione (Alexander & Munro, 1996, p.159).

Un ulteriore problema risiede nel fatto che la maggior parte delle vittime di reati informatici non riporta i casi, rendendo ancora più difficile quantificare precisamente l'ammontare dei danni provocati dai criminali che utilizzano la rete per le loro attività illecite. Le ragioni che stanno alla base della decisione di non denunciare i reati informatici variano da caso a caso. In alcuni casi si tratta semplicemente di una decisione d'affari. In altre parole, il danno può risultare di importanza secondaria, tale da non giustificare l'impiego di energie e risorse necessarie ad attivare una indagine. Un'altra ragione può risiedere nel fatto che l'effetto della notizia del reato informatico possa in qualche modo diminuire il valore dell'impresa che l'ha subito, e in questo caso si può decidere di gestire il problema internamente. Infine, alcune imprese sono consapevoli del fatto che una cattiva pubblicità potrebbe generare allarme nel pubblico e, soprattutto, che la notizia della vulnerabilità dei sistemi informatici potrebbe incoraggiare altri attacchi da parte dei pirati informatici (Charney & Alexander, 1996).

(a) Risposte legislative dei singoli stati[5]

[5] Le informazioni riguardanti la legislazione sui computer crimes sono basate su: paper relazione del Consiglio d'Europa intitolato "Committee of Experts on Crime and Cyberspace, Summary Report of the First

.

Nel dettare la disciplina sui *computer crimes* i legislatori dei diversi paesi hanno agito in modi differenti. In alcuni ordinamenti vi sono state leggi di modifica del codice che hanno inserito le nuove fattispecie come figure autonome a fianco di quelle tradizionali; questo è, ad esempio, il caso della legge di riforma della Repubblica Federale Tedesca o dell'Austria. Altri paesi hanno preferito operare attraverso l'estensione di definizioni normative già costitutive di fattispecie esistenti, lasciando inalterata la loro struttura (così la legge greca 26 agosto 1988, n. 1805) o hanno raggruppato le nuove norme in specifici titoli o capitoli, pur sempre inseriti nel codice, ma in posizione autonoma (questa è stata la scelta del legislatore francese, che ha introdotto nel titolo II del libro terzo del codice penale un nuovo capo III). In altri ordinamenti sono state emanate autonome e compiute discipline extracodicistiche della materia, con leggi speciali, le cui disposizioni sono applicabili solo in via sussidiaria (così l'articolo 1 della legge portoghese 17 agosto 1991, n. 109)[6].

Negli Stati Uniti i fenomeni di rilevanza penale connessi all'informatica si sono manifestati da tempo e sono stati oggetto d'indagine, analisi e classificazione quando ancora in altri paesi non si era sollevata alcuna questione in proposito. I reati informatici sono stati ricompresi all'interno di alcune leggi e regolamenti che originariamente non erano stati pensati ed emanati per trattare anche questo tipo di reati. Ad esempio l'*American Wire Fraud Statute* è stato esteso nella sua applicazione anche all'utilizzo dei computers[7] (Rosenoer, 1997, p.168). La prima legislazione federale creata per i reati informatici negli Stati Uniti è il *Computer Fraud and Abuse Act* del 1986, e l'ultimo aggiornamento della legislazione risale al 3 ottobre del 1996. Questa legge[8], emanata al fine di modificare parzialmente la precedente normativa, ha esteso la propria competenza prevedendo una disposizione penale relativa alle manipolazioni e al commercio di chiavi di accesso dei sistemi informatici illecitamente procuratesi, e si pone come obiettivo la protezione dei sistemi informatici del governo federale così come di quelli che vengono utilizzati dalle istituzioni finanziarie e dai centri ospedalieri; proibisce inoltre l'accesso non autorizzato a determinate informazioni come quelle riguardanti la difesa e le transazioni finanziarie (Rosenoer, 1997, p. 167).

A completare la legislazione federale negli Stati Uniti, nel 1986 è stato creato il *Federal Computer Investigation Committee* (FCIC) al fine di sviluppare e mantenere una rete di esperti di alto livello specializzati nei crimini informatici. Il FCIC è una associazione di investigatori, procuratori e altri professionisti che si occupano di prevenire, scoprire ed investigare i crimini informatici (Charney & Alexander, 1996). Le frodi informatiche sono reati in via di incremento, soprattutto negli Stati Uniti e per questo motivo

[6] L. Picotti, *op. cit*.

[7] Wire frauds are prohibited by 18 USC § 1343 and consist of (1) a scheme to defraud by means of false pretenses, (2) the defendant's knowing and wilful participation in the scheme with intent to defraud, and (3) the use of interstate wire communications in furtherance of the scheme. Furthermore, wire fraud is a predicate offence for a prosecution under the RICO (Racketeer Influenced and Corrupt Organizations) statute.

[8] The Computer Fraud and Abuse Act prohibits the transmission of "a program, information, code, or command to a computer or computer system, with intent to damage, or cause damage to, or to withhold or deny the use of, a computer, computer services or network, information, data, or programs." Such a transmission is also prohibited if undertaken with reckless disregard of a substantial and unjustifiable risk of the same effect. Trafficking in passwords for computers used by or for the US government is also barred (18 USC § 1030(a)(6)).

l'Amministrazione Clinton ha recentemente attribuito al *Federal Bureau of Investigation* (FBI) numerosi nuovi poteri, in osservanza ed esecuzione delle numerose leggi federali. All'interno dell'FBI è stata istituita un'apposita divisione strutturata in modo tale da contrastare a 360 gradi i reati informatici. Si tratta della *National Computer Crime Squad* (NCCS), un'unità il cui personale, specializzato in violazioni illecite dei sistemi informativi, lavora a stretto contatto con i Computer Emergency Response Teams (CERT) sparsi su tutto il territorio americano; per contrastare questi crimini spesso vengono effettuate anche speciali operazioni con l'ausilio di agenti infiltrati. In Europa due sono le polizie *computer crime*: quella belga e quella olandese. La prima contrasta principalmente il fenomeno della pedofilia su Internet, mentre la seconda si occupa sostanzialmente di contrastare l'*hacking*.

In Canada nel 1985 è stata emanata una legge sui reati informatici; il legislatore canadese infatti, mediante il *Canadian Criminal Law Amendment Act* del 1985, ha ritenuto opportuno creare la specifica fattispecie penale dell'accesso non autorizzato ed ha introdotto una nuova forma di reato per modifiche o cancellazioni non autorizzate di dati informatici. Il Canada ha inoltre espresso la volontà di supportare una iniziativa che si proponga la stipulazione di una convenzione internazionale sui reati informatici. In Giappone il reato di distruzione di registrazioni elettromagnetiche è stato penalizzato nel 1987, tuttavia il codice penale non è ancora stato riformato per quel che riguarda l'area dei reati informatici.

In Austria la legge n. 695 del 1987, entrata in vigore nel 1988, ha introdotto nel codice penale due nuovi articoli, il 126(b) intitolato "Danneggiamento di dati informatici," ed il 148(b) intitolato "Manipolazione abusiva di dati ai fini di frode." In Belgio la legislazione non è ancora completamente adeguata ai cambiamenti che intercorrono nelle tecnologie informatiche, nonostante che ci siano alcuni regolamenti che penalizzano specifici reati informatici, come il *computer hacking*. La Danimarca con la legge n. 229 del 6 giugno 1985 ha modificato alcuni articoli del suo codice penale, introducendo il reato di truffa informatica. Le altre ipotesi sanzionate sono l'impedimento al buon funzionamento degli elaboratori e l'accesso illegale ad informazioni o a programmi informatici altrui.

La Repubblica Ceca non ha una esperienza significativa nel campo dei reati informatici, ma alcuni casi recenti di danneggiamento di computers nel settore bancario dimostrano che questo tipo di reati non è sconosciuto. Il codice penale specifica tre tipi di reati informatici: (1) reati collegati all'abuso del computer; (2) reati legati alle informazioni e (3) reati che consistono nella commissione di reati tradizionali utilizzando i computers.

La Finlandia ha istituito una banca dati nazionale sui casi riguardanti i reati informatici, ed esiste una specifica unità di investigazione che si occupa di questi casi. Il Codice Penale è stato riformato in modo tale da prevedere anche alcuni reati informatici.

Il legislatore francese ha provveduto con la legge 88/19 del 5 gennaio 1988 a colmare il vuoto legislativo per contrastare la criminalità informatica. La legge ha introdotto nel codice penale vigente nuove ipotesi di reato poste a tutela del patrimonio e della fede pubblica contro le cosiddette manipolazioni informatiche. Il codice penale ora prevede alcune infrazioni in materia informatica quali l'accesso non autorizzato in un sistema informatico, l'alterazione o turbativa del suo funzionamento, il danneggiamento di dati, la

falsificazione di un documento informatico ed il suo uso, il tentativo e l'associazione finalizzata a perpetrare taluno di detti reati. Successivamente, nell'ambito della riforma del codice penale, sono state emanate due norme (legge n. 92/684 e 92/685 del 22 luglio 1992) che hanno modificato i precedenti testi normativi penalistici sia nel settore della protezione delle persone nei confronti delle banche dati che in tema di frode informatica.

In Germania la legge del 15 maggio 1986 ha introdotto nel codice penale tedesco quattro fondamentali specie di reato connesse con il mondo informatico: lo spionaggio informatico, la truffa informatica (nuovo paragrafo 263(a) StGb), le falsificazioni di dati rilevanti ai fini probatori unitamente all'inganno del traffico giuridico informatico ed infine i danneggiamenti mediante manomissione di dati e sabotaggi di impianti di elaborazione automatica o di supporto di dati. La giurisprudenza tedesca in qualche modo tenta di stare dietro alle innovazioni tecnologiche interpretando in maniera estensiva alcuni principi tradizionali di diritto penale per renderli applicabili alle nuove tecnologie elettroniche.

In Gran Bretagna il 20 giugno 1990 è entrato in vigore il *Computer Misuse Act* che ha introdotto i nuovi reati di accesso non autorizzato al materiale informatico, accesso abusivo aggravato dall'intenzione di manipolare i programmi a scopo di commettere un ulteriore reato e modifica non autorizzata di materiale computerizzato. La legge dispone nuove regole in base alle quali le Corti del Regno Unito avranno giurisdizione per le tre nuove fattispecie di reato in materia di *computer misuse*, nell'ipotesi in cui vi sia una connessione significativa con il Regno Unito. Tale connessione si viene a creare se il *computer misuse* ha origine nel Regno Unito o se è diretto contro un computer qui situato.

La Grecia con la legge n. 1805 del 26 agosto 1988 ha introdotto alcune modifiche al codice penale. La nuova legge ha previsto espressamente l'ipotesi della frode informatica, oltre ad aver equiparato i dati contenuti nell'elaboratore ai documenti scritti e ad averne

La normativa italiana in materia informatica ha raggiunto oggi un discreto livello di completezza, soprattutto grazie all'impulso comunitario. Il decreto legislativo n. 518/1992 e la legge 675/1996 tendono infatti verso l'allineamento del codice penale con alcune fattispecie criminose legate all'informatica e alla telematica. La legge 23 dicembre 1993, n. 574 ha emendato alcune disposizioni del codice penale ed ha introdotto nel nostro sistema una serie di crimini informatici, che comportano a carico del reo l'irrogazione di pene variabili fino a un massimo di cinque anni di reclusione. Tale legge non considera tutte le tipologie di aggressione ai dati e ai programmi informatici, ma soltanto alcune di esse; ad esempio il patrimonio informatico non è tutelato rispetto al furto, ma viene protetto verso il danneggiamento.

Con il decreto legislativo 29 dicembre 1992, n. 518 vengono definiti i limiti giuridici entro cui il software può essere considerato leale: a livello operativo l'utente non può utilizzare software copiato nella propria stazione di lavoro e deve prestare attenzione anche all'utilizzo delle risorse di rete per le quali vigono precise regole contrattuali. La legge 31 dicembre 1996, n. 675 contiene disposizioni alle quali dovranno conformarsi le aziende, sia per quanto riguarda l'organizzazione interna che la gestione dei sistemi di protezione dei dati soggetti alla tutela della norma stessa.

La legge portoghese 17 agosto 1991 n. 109 ha previsto una serie di nuove fattispecie di reati tra cui, ad esempio, il falso informatico, la truffa informatica, il sabotaggio informatico, l'accesso non autorizzato e l'intercettazione illegale delle comunicazioni nell'ambito di sistemi informatici. Anche la Svezia nel 1986 ha introdotto alcune modifiche al suo sistema penale allo scopo di assicurare una protezione contro atti rientranti nell'ambito della criminalità informatica. La legge è entrata in vigore il 10 luglio 1986 e con essa è stato modificato il codice penale, che adesso prevede il reato di frode informatica.

(b) Istituzioni finanziarie[9]

Le leggi emanate a livello nazionale ed internazionale non sono sufficienti a prevenire e combattere la criminalità informatica. Infatti questo tipo di legislazione potrebbe rivelarsi controproducente per le istituzioni e le società poiché potrebbe lasciare l'istituzione con un falso senso di sicurezza e tutto ciò potrebbe portare a misure di sicurezza interne deboli ed inadeguate (Mitchell, 1996, p. 262).

[9] Questa parte del saggio è basata principalmente sull'articolo di Daniel Martin intitolato "The Use of *Defense & Security*, n. 0, Novembre 1996.

Al fine di raggiungere un livello di sicurezza ottimale, le misure di sicurezza dovrebbero essere prese anche a livello di singole organizzazioni, imprese, istituzioni finanziarie. Ciò significa che le imprese e le istituzioni finanziarie dovrebbero implementare una propria salvaguardia delle strutture informatiche. Sarebbe infatti opportuno consentire alle istituzioni finanziarie un maggiore controllo sulle transazioni finanziarie. Alle banche, ad esempio, dovrebbe essere consentito di sviluppare dei mezzi più potenti per stabilire lldentità degli individui intestatari di conti correnti e migliori meccanismi per stabilire le fonti dei loro guadagni.

I singoli paesi, le banche e le altre istituzioni finanziarie devono sviluppare una nuova tecnologia per monitorare i flussi elettronici di denaro, poiché i programmi software e Internet hanno reso possibile agli individui e alle istituzioni di trasferire grosse somme di denaro al di fuori dei normali canali finanziari. Lo sviluppo di questo tipo di misure di sicurezza non può essere ritardata in quanto in assenza di una adeguata supervisione i criminali continueranno ad utilizzare le reti informatiche per trasferire i loro guadagni illeciti e questo porrà in serio pericolo il sistema finanziario internazionale (Alexander & Munro, 1996, p.160).

(c) Individui

Se la criminalità informatica presenta come caratteristica fondamentale quella di avere una vocazione internazionale, è altrettanto vero che le informazioni che devono essere protette sono essenzialmente nazionali o locali. Proprio per questo le misure di prevenzione al crimine informatico non dovrebbero essere limitate agli specialisti poiché ciascun individuo appartenente ad unlmpresa o istituzione finanziaria può contribuire alla difesa delle informazioni. Infatti la sicurezza informatica è un aspetto che riguarda tutti i componenti di unlstituzione o organizzazione, dai livelli più bassi a quelli più alti. Di conseguenza, forse uno dei migliori metodi di prevenzione rispetto ai crimini informatici è quello di insegnare agli individui che lavorano alllnterno di una struttura organizzativa a riconoscere le irregolarità presenti nel sistema informatico. Molte imprese tendono a proteggere ampiamente i livelli più alti dellbrganizzazione quando in realtà risultano molto più vulnerabili ai livelli più bassi, dove le pratiche sono variabili ed i controlli meno stretti. Poiché di solito la parte più debole si trova ai livelli più bassi dellbrganizzazione, ciascun individuo deve essere vigile ed essere consapevole della propria responsabilità per una

5. RIPENSARE ALLA COOPERAZIONE INTERNAZIONALE IN MATERIA DI CRIMINALITÀ E GIUSTIZIA

Lèspansione transnazionale della criminalità organizzata richiede una corrispondente espansione internazionale delle leggi, delle autorità investigative e della giustizia penale. Negli ultimi decenni la cooperazione internazionale nel campo della criminalità e della giustizia è stata in qualche modo accelerata dall'allarme suscitato dai fenomeni del terrorismo e del traffico di stupefacenti, mentre oggigiorno è stata promossa dalla

crescente sofisticazione delle organizzazioni criminali e dall'influenza esercitata dal processo di globalizzazione sulle imprese sia legittime che criminali.

Da tempo si parla di spazio giuridico europeo, si discute anche di un codice penale europeo. Il problema è semplice: i criminali si muovono a livello transnazionale, hanno già creato uno spazio internazionale, mentre investigatori e procuratori sono limitati dalla giurisdizione. I primi attraversano le frontiere senza documenti, mentre i secondi hanno bisogno dei lenti trattati di estradizione e delle rogatorie internazionali. Nonostante la semplicità di questa osservazione, devono essere sottolineate alcune gravi difficoltà che si incontrano nel momento in cui si cerca di mettere in pratica una politica di prevenzione e di contrasto al crimine transnazionale. In assenza di una discussione approfondita, la cooperazione internazionale rischia di diventare un "rito" e l'assistenza tecnica una forma di solidarietà che i paesi ricchi pagano ai paesi poveri, indipendentemente dalla soluzione dei loro problemi. Se così fosse, c'è il rischio che dopo l'"entusiasmo" creativo di questi anni seguano le "delusioni". Affrontare oggi questi problemi significa credere fermamente che una seria cooperazione internazionale costituisce l'unico modo serio di realizzare una lotta efficace alla criminalità organizzata transnazionale.

Le differenze esistenti all'interno dei singoli sistemi giuridici rendono assai difficile una cooperazione piena e stabile nel campo della criminalità e della giustizia penale, ed in particolare modo un processo che porti all'armonizzazione delle leggi e dei regolamenti. Non è un problema di strumenti. Quelli ci sono e si possono creare. Manca la chiarezza su che cosa deve intendersi per cooperazione internazionale, sui suoi limiti ma anche sulle sue grandi capacità.

Le differenze culturali sono profonde, specialmente quando si riferiscono al *trade-off* esistente tra il rispetto dei diritti umani e l'effettività delle sanzioni criminali. A queste devono aggiungersi altre differenze, di tipo organizzativo, esistenti all'interno delle strutture di investigazione e di giustizia, che contribuiscono a render più comlicata la cooperazione internazionale poiché le interazioni tra i differenti attori del sistema penale variano da sistema a sistema. Il Ministro di Giustizia, il Ministro degli Interni ed il pubblico ministero rivestono ruoli diversi ed hanno a che fare con diverse autorità in ciascuna giurisdizione. diversi paesi.

Nonostante queste difficoltà, nel corso degli anni si è costruita una sorta di storia della cooperazione internazionale, che si può suddividere il tre fasi. Il primo stadio è stato quello della consapevolezza del problema e della nascita di alcuni strumenti multilaterali e bilaterali come i trattati di estradizione. Il secondo stadio è stato quello caratterizzato dall'impulso alla creazione di meccanismi internazionali e di apparati normativ. A partire dalla Convenzione di Vienna contro il Traffico Illecito di Stupefacenti e di Sostanze Psicotrope del 1988, dal Gruppo di Azione Finanziaria Internazionale dei sette paesi più industrializzati del mondo, dal Gruppo sulla Criminalità Organizzata dei P8, dalla Convenzione del Consiglio dEuropa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato del 1990, dalla Direttiva Europea Anti-Riciclaggio 91/308, dalle raccomandazioni emanate dall'Organizzazione degli Stati Americani in poi, un crescente numero di paesi ha cominciato a modificare o adattare la propria legislazione nazionale alle norme ed ai regolamenti contenuti in questi accordi. Il risultato di questa trasformazione da "*soft laws*" delle convenzioni internazionali in "*hard laws*" degli stati è stato

quello di creare una base per combattere la criminalità organizzata, il traffico di stupefacenti ed il riciclaggio di proventi illeciti.

Il terzo stadio dovrà essere quello della cooperazione orientata verso obiettivi precisi. Questi tre momenti (consapevolezza, impulso, obiettivi) hanno una loro logica conseguente e fanno parte integrante della storia passata e presente di questi processi. Sono i processi che trasformano la criminalità in un problema internazionale e sono questi processi che richiedono un governo globale del problema "criminalità". La cooperazione internazionale è il requisito necessario per questo governo globale. Più saremo capaci di farla funzionare, più riusciremo a governare i processi in atto che pongono oggi la questione criminale al centro di fenomeni internazionali e locali complessi come la miseria, le migrazioni, la violenza. Guardare al problema della criminalità organizzata transnazionale per come oggi si presenta può essere fuorviante. Occorre capirne le tendenze per cogliere i livelli della sua azione. Non c'è una strategia unica delle varie criminalità organizzate, né potrebbe esserci se non nella mente di qualche scrittore. Ci sono invece tante strategie che alzano il livello dello scontro tra chi ha a cuore il problema mondiale della coesistenza pacifica e dello sviluppo ordinato e chi invece approfitta dei nodi deboli del mondo contemporaneo per realizzare profitti economici e politici. Il traffico internazionale di armi e quello in grande scala degli emigranti sono soltanto alcuni degli indicatori importanti del livello globale al quale questo scontro si pone.

La giustizia penale rappresenta una sfera delicata dei governi nazionali poiché è direttamente coinvolta con la libertà degli individui e con il mantenimento dell'ordine sociale, e i singoli stati sono restii a cedere parte della loro sovranità in questo campo alla comunità internazionale. Riproporsi alcune domande può servire ad orientare la discussione. Quali sono le ragioni di fondo della cooperazione internazionale e dell'assistenza tecnica in materia di criminalità e giustizia penale? Perché alcuni paesi sottraggono risorse al proprio sviluppo interno per investirle in strutture, personale e assistenza tecnica ad altri paesi? E ancora, se il problema è quello degli interessi in gioco, si può parlare di un interesse astratto della comunità internazionale oppure si deve parlare di aggregazioni di interessi nazionali?

Il diritto internazionale ci ha abituato a queste oscillazioni tra la forma del bene comune e la sua applicazione in aggregazioni di interessi. In tutta una serie di fattori, il diritto internazionale ha scritto le regole dello scambio tra interessi nazionali e quelli sovranazionali, ma nel settore del diritto e della procedura penali queste regole sono difficili da scrivere perché sono ancora poco chiari e spesso sono confusi gli interessi in gioco. Se questi fossero chiari, come erroneamente si crede, già da tempo si sarebbero superati gli ostacoli formali e si sarebbero scritte queste regole. Se non si sono scritte è perché l'ambito della giustizia penale rappresenta il settore più delicato del governo della società e nessun paese è disponibile, oggi, a cedere parte di questo governo e quindi parte di questa sovranità alla comunità internazionale.

La filosofia della cooperazione internazionale in materia di criminalità e giustizia penale va quindi letta usando la chiave degli interessi in gioco e delle loro possibili aggregazioni. I paesi sono gelosi della loro sovranità in materia penale perché riguarda il bene prezioso delle libertà individuali (da limitare o da espandere a seconda dei casi) ma cooperano tra

di loro perché pensano che attraverso questa cooperazione si possano ottenere maggiori vantaggi a minori costi di quelli che otterrebbero con l'azione individuale.

La nuova filosofia della cooperazione internazionale basata sugli interessi può essere rappresentata come una spirale tra efficacia e sua legittimazione. La cooperazione internazionale può diventare efficace e per questo legittimata soltanto se le attività alle quali dà luogo producono benefici a tutti i paesi - e quindi alla comunità internazionale maggiori di quelli che un singolo paese potrebbe ottenere attraverso la sua azione individuale. Più i paesi diventeranno consapevoli delle difficoltà e dei costi di trattare individualmente problemi di giustizia penale, più guarderanno agli strumenti ed ai meccanismi della cooperazione internazionale come le soluzioni per i loro problemi e conseguentemente essi legittimeranno la cooperazione internazionale, che, a sua volta, più sarà legittimata dalla vasta partecipazione dei paesi, maggiormente sarà diventata efficace.

Nonostante si possa essere soddisfatti con i traguardi raggiunti sorpassando gli ostacoli rappresentati dalle differenze esistenti nelle diverse giurisdizioni dei singoli stati, è importante non perdere di vista l'obbiettivo principale, che rimane quello di sviluppare ulteriormente ed in modo più ampio la cooperazione internazionale in materia di criminalità organizzata transnazionale e di giustizia penale. Se c'è qualcosa che si può imparare dall'esperienza maturata in questi ultimi trent'anni di cooperazione internazionale, è forse che la criminalità transnazionale può essere combattuta efficacemente solo mediante un'azione concertata di tutti gli stati.

Il progetto che deve essere discusso riguarda il come affrontare prima della fine di questo secolo il terzo stadio della cooperazione internazionale. Devono essere chiariti, specificati ed elaborati i principi nonché gli obiettivi da raggiungere nella maniera più efficiente ed efficace possibile. Identificando chiaramente gli obiettivi ed i metodi di una cooperazione internazionale effettiva si rende più remoto il pericolo che l'attività di cooperazione possa decadere a mero rituale o sia preda di interessi politici di singole nazioni.

Se saranno chiare le finalità della cooperazione internazionale e si saranno creati degli efficaci strumenti di cooperazione multilaterale, la cooperazione bilaterale ne verrà arricchita perchè liberata dagli adempimenti dirottati sul piano multilaterale. Un errore di fondo è infatti quello di mettere in contrapposizione le due forme di cooperazione quando ambedue hanno le loro specificità e diverse ragioni di essere. Ritornare proprio a queste specificità è d'obbligo per poter governare meglio tutti i processi. Cooperazione multilaterale e bilaterale devono essere necessariamente integrate sia per sinergie politiche che economiche. E occorre che i vari organismi che decidono in materia inizino a rendere operativa questa integrazione attraverso tre livelli: (a) quello dell'informazione sugli interventi in corso da parte dei vari paesi ed agenzie internazionali (b) quello dell'analisi del bisogno di interventi e della loro programmazione, (c) quello della decisione sulle priorità e di controllo dei risultati. Solo così, attraverso una razionalizzzazione dei processi decisionali ed una loro spoliticizzazione, si potranno avere risultati seri in termini di lotta alla criminalità.

L'obbiettivo è quello di arrestare, per quanto possibile, l'espansione internazionale delle organizzazioni criminali, avviando processi di armonizzazione delle politiche sia

preventive che repressive tra tutti i paesi. La logica di questo intervento è che occorre arrivare ad una equalizzazione del rischio per i criminali nei vari paesi per rendere loro meno convenienti i processi di globalizzazione. La consapevolezza che ovunque andranno troveranno lo stesso rischio nell'essere individuati, arrestati, condannati ed i proventi delle loro attività confiscati, li porterà a ridurre le dimensioni dei loro traffici. L'equalizzazione del rischio per i criminali deve corrispondere ad una scelta strategica della comunità internazionale, quella cioè di stabilire una serie di misure minime che tutti i paesi devono predisporre. E quando alcuni paesi non sono in grado di fare fronte, la comunità internazionale deve adoperarsi per raggiungere, attraverso forme di assistenza tecnica mirate, questo obiettivo.

La cooperazione che intercorre tra le forze di polizia ed i magistrati di diversi paesi di solito avviene ad un livello informale, lasciando tutto alle capacità ed alla buona volontà degli ufficiali piuttosto che ai meccanismi previsti dagli accordi internazionali. Se fosse possibile tracciare una comparazione circa l'effettività delle investigazioni intraprese dalle autorità investigative sulla base di cooperazione formale e collaborazione informale, il risultato sarebbe di certo a favore delle collaborazioni informali, misurate sia in termini di riduzione della criminalità sia in termini di costi. Nonostante ciò, non si vuole qui consigliare di abbandonare i meccanismi formali di cooperazione a favore di quelli informali. Piuttosto, il punto è che è necessario focalizzare gli obiettivi che si propongono gli accordi internazionali ed analizzare periodicamente i risultati ottenuti per determinare quali obiettivi si siano raggiunti e sia in caso di orientare diversamente le strategie elaborate.

Identificare un obiettivo chiaro per una cooperazione transnazionale non è sufficiente ad assicurare un controllo ed un contrasto effettivi della criminalità. Devono essere fatti degli investimenti strategici in due aree: risorse umane e tecnologia. La criminalità transnazionale, in particolare modo i gruppi criminali coinvolti in attività illecite che presentano un alto grado di sofisticazione, per essere contrastati necessitano di una controparte in grado di utilizzare tutti gli strumenti e le nuove tecnologie a disposizione sul mercato. Le autorità investigative devono infatti essere in grado di ricostruire le transazioni finanziarie più complesse utilizzando le tecnologie informatiche più sofisticate. Il solo modo di attuare una campagna contro la criminalità transnazionale è quello di introdurre nei paesi all'interno delle forze investigative lo stesso tipo di professionalizzazione e di flessibilità organizzativa che caratterizza le organizzazioni criminali transnazionali.

Da alcuni anni si parla di riformare le Nazioni Unite in modo tale da farle diventare una organizzazione più efficiente ed in grado di prendere le decisioni necessarie per assicurare la pace e la sicurezza nel mondo. A seguito della nomina di Kofi Annan al ruolo di Segretario Generale, nel luglio del 1997 è stato proposto un piano di riforma per raggiungere questo traguardo. L'obiettivo principale è quello di razionalizzare la struttura unendo gli uffici e le agenzie che all'interno dell'ONU si occupano degli stessi problemi o di problemi simili. In base al piano di riforma proposto, le unità che si occupano dei problemi legati alla criminalità e alla giustizia penale verrebbero sotto un unico ufficio a cui sarebbe affidato il compito di coordinare nel migliore dei modi le attività, riducendo la verticalizzazione della struttura ed evitando sprechi di risorse. L'obiettivo è quello di arrestare, per quanto possibile, l'espansione internazionale delle organizzazioni criminali,

avviando processi di armonizzazione delle politiche sia preventive che repressive tra tutti i paesi.

I problemi di sicurezza e ordine pubblico causati dalla criminalità organizzata transnazionale possono essere affrontati solo mediante l'azione dell'ONU e questo periodo di trasformazioni all'interno dell'organizzazione dovrebbe essere sfruttato al meglio al fine di formulare delle risposte adeguate che consentano d iaffrontare il problema criminalità organizzata transnazionale in maniera effettiva e sistematica. Gli stati che guardano con sfiducia a questa opportunità che si presenta loro oggi, si guarderanno con vergogna negli anni a venire se non intraprenderanno le azioni necessarie, poiché l'unica alternativa *status quo* che può solamente portare ad un aumento della criminalità, della povertà e ad uno spreco indicibile di risorse.

BIBLIOGRAFIA

Adams J.A.M. (1996), “Controlling cyberspace: Applying the Computer Fraud and Abuse Act to The Internet”, Santa Clara Computer and High Technology Law Journal, 2 agosto

Adler F., Mueller G.O.W. e Laufer W.S. (1995). *Criminology* (seconda edizione) New York: McGraw-Hill.

Alexander, Kern Jr e Munro Robert (1996), “Cyberpayments: Internet and Electronic Money Laundering: Countdown to the Year 2000”, Journal of Financial Crime, 4 (2), Novembre

Annan Kofi, “Renewing the United Nations: A Programme for Reform” (Documento #A/51/950), Nazioni Unite, New York 1997

Backhouse James (1995) “Getting the Adjustment Right: Controls and Computer Security”, Journal of Financial Crime, 3 (1), luglio

Belgium, Austria e ICMPD, “Harmonisation of the Legislation to Combat Trafficking in Aliens”, paper presented at the Third Meeting of the Expert Group of the Budapest Group, Budapest, 15-16 giugno 1995

Charney S., Alexander K. (1996), “Computer Crime”, Emory Law Journal, Emory University School of Law, estate

Commission des Communautes Europeennes, (1997), Protection des Interets Financiers des Communautes - Lutte contre la fraude Rapport Annuel 1996, Bruxelles, mimeo

Drinkhall Jim (1997), “Internet Fraud”, Journal of Financial Crime, 4 (3), gennaio

FATF (1990), “Financial Action Task Force on Money Laundering Report”, Parigi, mimeo

Giacomelli Giorgio (1996) the Profit Out of Crime by Policing the Money Laundries”, International Herald Tribune, 4 marzo

IOM - Migration Information Programme (1995), Trafficking and Prostitution: the Growing Exploitation of Migrant Women from Central and Eastern Europe, Budapest

IOM - Migration Information programme (1997), The Baltic Route: The Trafficking of Migrants Through Lithuania, Budapest

IOM, “Multilateral Effort to Combat Trafficking in Migrants: an International Agency Perspective”, paper presented at the International Conference on Migration and Crime: Global and Regional Problems and Responses, Courmayeur, 5-8 ottobre 1996

Mitchell John (1996) Computer Related Crime: The Role of Control in its Prevention, Detection and Correction - Part II”, Journal of Financial Crime, 3 (3), gennaio

Organizational Intelligence Unit (1995), Overview of International Organized Crime, mimeo

Rosenoer J. (1997), CyberLaw, The Law of the Internet, New York: Springer-Verlag Inc.

Savona E.U., Adamoli S., Zoffi P. (1995) con la collaborazione di DeFeo M., Organised Crime across the Borders, HEUNI Papers No. 6, Helsinki

Savona Ernesto Ugo (1996), “European Money Trials”, Transnational Organised Crime, 2 (4), Inverno

Savona E.U., Da Col G., Di Nicola A. (1997), “Migrazioni e criminalità in Europa”, in L. Tomasi (a cura di), Razzismo e Società Plurietnica. Conflitti etnici e razzismi giovanili in Europa, Milano, F. Angeli

Savona E.U., Di Nicola A. (1998) “Migrazioni e criminalità. Trent’anni dopo”, Rassegna Italiana di Criminologia, IX (1)

Secretariat of the Inter-Governmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia (1995a), Summary Description of the Legislation on Alien Trafficking in States in Europe, North America and Australia, Ginevra, dicembre

Shelley Louise I. (1995), “Transnational Organized Crime”, Journal of International Affairs, 48 (2), inverno

Siemens M., “European Responses to the Phenomenon of Illegal Migration: National and International Initiatives”, paper presented at the International Conference on Migration and Crime: Global and Regional Problems and Responses, Courmayeur, 5-8 ottobre 1996

SIPRI, (1992) Annual Yearbook

Smith P.J. (1994), “Illegal Chinese Immigrants Everywhere, and No Let up in Sight”, International Herald Tribune, 26 maggio

Transcrime (1996), Migrazione e criminalità - la dimensione internazionale del problema, Milano, CNPDS

Ulrich C.J. (1995), “Alien Smuggling and Uncontrolled Migrations in Northern Europe and the Baltic Region”, HEUNI Papers No. 7, Helsinki

Ulrich C.J. (1996), “Crime and Security in Post-Soviet Era”, CJ Europe, 6 (1), gennaio - febbraio

UNDCP (1994) “Drugs and development”, Discussion Paper prepared for the World Summit on Social Development, giugno

UNDP (1997) Human development report 1997, New York-Oxford: Oxford University Press

Wharton Econometrics Forecasting Ass. Inc., “The Income of Organized Crime”, President’s Commission on Organized Crime, The Impact: Organized Crime Today, aprile 1986

Widgren J., “Multilateral Co-operation to Combat Trafficking in Migrants and the Role of International Organizations”, paper presented at the Eleventh IOM Seminar on International Response to Trafficking in migrants and the Safeguarding of Migrant Rights, Geneva, 26-28 ottobre 1994

Williams P. (1994), “Threat Assessment”, in Five Papers Prepared for the Crime Prevention and Criminal Justice Branch, Nazioni Unite, Vienna

Winer J.M. (1996), “Alien Smuggling: Transnational Crime Against National Borders”, presentation to the Working Group on Organized Crime, National Strategy Information Centre, Washington, DC, October 8, Trends in Organized Crime, 2 (2), Inverno

WTO, International Trade, Focus Newsletter, (18), aprile 1997