Conferenza internazionale

Cybercrime: Global Phenomenon and Its Challenges
Cybercrime: un fenomeno globale e le sue sfide

Courmayeur, Mont Blanc, 2-4 dicembre 2011

Report di:

Roberto Flor*

Introduzione.
La "rivoluzione informatica", l'esponenziale sviluppo delle nuove tecnologie e l'attuale assetto della società di Internet hanno comportato dei cambiamenti epocali determinando una serie di trasformazioni in ogni settore della vita umana.
Il "paradigma digitale-tecnologico" non poteva non influenzare le scelte politiche ed economiche di tutti gli ordinamenti giuridici, chiamati a rispondere a diversificate esigenze di tutela ed a situazioni spesso emergenziali, dovute alla comparsa non solo di nuovi strumenti e metodologie utilizzabili per commettere reati "tradizionali" o "comuni", ma altresì di nuovi fenomeni criminali che non sempre hanno trovato una risposta sul piano legislativo. La loro continua e progressiva mutazione rendono evidente il passaggio dalla fase c.d. dei *computer crimes* a quella dell'"epoca di Internet", in cui proprio il *cyberspace* diviene l´ ambiente ideale e privilegiato per la realizzazione di molteplici, diverse e nuove forme di *cybercrime.*
Da questa premessa nasce l'idea della conferenza: *Cybercrime: un fenomeno globale e le sue sfide*, promossa dall'International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme-ISPAC, dal Centro Nazionale di Prevenzione e Difesa Sociale-CNPDS, dalla Courmayeur Foundation in cooperazoine con l'United Nations Office on Drugs and Crime-UNODC ed il Korean Institute of Criminology-KIC di Seoul.

Sessione I.
La prima sessione - dopo i saluti di benvenuto e la breve esposizione dei motivi che hanno portato all'organizzazione di questo importante incontro e dei suoi obiettivi - è stata aperta da **Ulrich Sieber** (direttore del Max Planck Institut für ausländisches und internationales Strafrecht di Freiburg i. Br.) con una ricca introduzione sul fenomeno "*cybercrime*" e sulle prospettive di contrasto, sia sul piano repressivo che su quello preventivo, prendendo in considerazione gli strumenti penali sostanziali e processuali.
Sieber non ha solamente richiamato l'attualità e l'importanza di analizzare il fenomeno, nelle sue molteplici forme di manifestazione, ma ha anche evidenziato il suo carattere congenitamente transnazionale che necessita di una risposta sovranazionale comune.
I riferimenti all'esigenza di ammodernamento dei sistemi penali sono stati arricchiti, da un lato, dai rilievi ottimistici legati alla ratifica della convenzione del Consiglio d'Europa sulla criminalità informatica del 2001 e, dall'altro lato, dalla prospettiva di intervento europeo considerando l'attuale assetto delle competenze penali dell'Unione dopo l'entrata in vigore del Trattato di Lisbona. L'art. 83 TFUE, infatti, include fra i settori di criminalità grave e

* *Roberto Flor* è ricercatore in diritto penale e professore aggregato in diritto penale dell'informatica presso la Facoltà di Giurisprudenza dell'Università di Verona.

transnazionale, rispetto ai quali l'Unione può prevedere elementi minimi delle fattispecie penali, la "criminalità informatica". E' già stata presentata, in questo contesto, la proposta di direttiva contro gli attacchi ai sistemi informatici, che fa proprie le disposizioni già adottate dalla decisione quadro 2005/222/GAI.
Sul piano della procedura penale Sieber non ha mancato di rilevare i rischi dovuti all'inefficacia di alcuni attuali strumenti "tradizionali" di contrasto, invitando alla riflessione sull'opportunità di adottare nuovi mezzi investigativi e di ricerca della prova governati, a livello almeno europeo, da regole comuni, rafforzando, al contempo, la cooperazione fra organismi investigativi, nonché fra settore pubblico e settore privato (in particolare con gli Internet Service Providers).
Il contrasto a gravi forme di criminalità, compresa quella informatica, potrebbe passare anche attraverso la disciplina di strumenti preventivi. Il sottile riferimento è stato non tanto, o non solo, alla normativa sul c.d. *data retention*, ma soprattutto al monitoraggio della rete o alla c.d. *online search*, purchè siano disciplinati nel rispetto di alcuni elevati standard di garanzia per la tutela dei diritti fondamentali dell'individuo.
La disposizione normativa deve esprimere, in altri termini, il corretto bilanciamento fra gli interessi contrapposti (repressione e prevenzione di gravi forme di criminalità informatica e la protezione dei diritti fondamentali).
Queste considerazioni si legano a due importanti sentenze della Corte Costituzionale tedesca rispettivamente sulla c.d. Online Durchsuchung (2008) e sul c.d. data retention (2010).
Con la prima decisione, in particolare, il Bundesverfassungsgericht, ha dichiarato incostituzionali il § 5 co. 2, n. 11 della Legge sulla protezione della Costituzione del North Rhein Westfalia che aveva autorizzato un organismo di *intelligence* a "protezione della Costituzione" ad effettuare due tipi di misure d'indagine: il monitoraggio e la ricognizione segreti di Internet e l' accesso segreto a sistemi informatici. Sono venuti in rilievo, in particolare, due diritti fondamentali, espressione del diritto generale alla personalità. Il primo è il "diritto di autodeterminazione informativa" (Recht auf informationelle Selbstbestimmung), che va oltre la tutela della *privacy* e non si limita ad informazioni sensibili per loro natura, ma conferisce alla persona, in linea di principio, il potere di determinare, in sè, la divulgazione e l'utilizzo dei suoi dati personali, anche se connotati da un contenuto informativo minimo, che amplia la tutela della libertà della vita privata in termini di diritti fondamentali. Il secondo è il diritto fondamentale alla garanzia della riservatezza e dell'integrità dei sistemi informatici, in quanto i sistemi informatici oggetto di indagine possono contenere dati personali della persona in misura e diversità tali da facilitare la conoscenza di parti significative della sua vita o della sua personalità in ambiti sia privati che economico-professionali.
Il necessario bilanciamento fra contrapposte esigenze, che considerino la tutela della libertà delle persone e la sicurezza, anche dei rapporti giuridici che si svolgono nel cyberspace, è stato ripreso puntualmente da **Emilio Viano** (Professore, Department of Justice, Law and Society, American University e Washington College of Law, Washington DC), che ha evidenziato le criticità rispetto al diritto alla riservatezza degli individui ed alla sicurezza. La definizione di quest'ultima è stata ampia. Essa è stata intesa come sicurezza dello Stato, sicurezza dei cittadini e sicurezza dei sistemi informatici, dei dati e delle informazioni.
L'intervento di **Giovanni Buttarelli** (dell'ufficio del Garante europeo per la protezione dei dati) si è coerentemente inserito in questa sessione. Il relatore ha evidenziato il mutato contesto sociale, in cui le tecnologie sono ormai indispensabili in ogni settore della vita umana, affermando che il cyberspace non è più un "far away concept". Oggi vi è la consapevolezza degli obiettivi e degli effetti dei cyberattacks, che ormai costituiscono una parte integrante della società dell'informazione. Il contrasto alla criminalità informatica comporta, da un lato, il necessario trattamento di dati personali e, dall'altro lato, elevati rischi di violazione del diritto alla privacy dei cittadini, soprattutto nell'attuale contesto globale e alla luce di nuovi e mutevoli

fenomeni che sfruttano i nuovi prodotti dell'evoluzione tecnologica come, ad esempio, il cloud computing, in cui gli stessi dati possono trovarsi, nello stesso momento, in molteplici luoghi diversi.
Dopo aver brevemente illustrato l'importanza della Convenzione Cybercrime e della sua attuazione nella lotta alla criminalità informatica, Buttarelli ha richiamato l'opinione 4/2001 dell'art. 29WP in merito al necessario bilanciamento fra esigenze repressive e di contrasto al cybercrime e la tutela della sicurezza e della riservatezza dei cittadini, in particolare con riferimento agli strumenti di ricerca della prova previsti dalla stessa Convenzione applicabili non solo ai reati informatici in senso stretto ("related to computer systems and data"), ma anche a tutti gli altri illeciti per i quali la raccolta della prova avviene in forma elettronica.
L'art. 15 della Convenzione Cybercrime esprime la preoccupazione connessa alle potenzialità "invasive" di mezzi investigativi a "carattere tecnologico" o, in ogni modo, nell'ambito della lotta alla criminalità informatica, i quali devono rispettare, in particolare, i limiti imposti dalla Convenzione dei diritti dell'uomo e delle libertà fondamentali, il cui art. 8 tutela il rispetto della vita privata e familiare.
La compressione del diritto fondamentale risulta però essere ammissibile se proporzionata. Il principio di propozionalità, dunque, diviene il criterio guida essenziale, anche per trasporre le disposizioni processuali della Convenzione Cybercrime.
Buttarelli ha portato, quale esempio concreto di applicazione del principio di proporzionalità, il c.d. freezing traffic data, richiamando altresì le disposizioni di fonte europea (in particolare la direttiva 24/2006/CE) in materia di data retention. In particolare, le disposizioni sul c.d. freezing traffic data dovrebbero essere considerate appropriate e utili in ordinamenti che non prevedono una conservazione dei dati di traffico su larga scala e per lunghi periodi di tempo.
In questo campo l'applicazione del principio di proporzionalità dovrebbe guidare il legislatore a valutare cautamente l'uso di tali strumenti, da contenere i limiti delle safeguards rinvenibili non solo dalla Convenzione dei diritti dell'uomo e delle libertà fondamentali, ma anche dall'art. 15 della Convenzione Cybercrime e dalle stesse disposizioni europee in materia di data retention.
Buttarelli ha sollevato, inoltre, una ulteriore questione, squisitamente legata ai problemi di competenza e giurisdizione, ritenendo insufficiente la disposizione di cui all'art. 22 della Convenzione Cybercrime.
Egli ha portato l'esempio dell'ordinamento giuridico italiano, in cui trova applicazione il principio di ubiquità.
Gli Stati dovrebbero attuare sforzi superiori per garantire una agevole risoluzione dei conflitti di competenza e giurisdizione, funzionali alla maggiore tutela delle vittime dei reati informatici.
La relazione si è chiusa, in primo luogo, con la breve illustrazione delle prospettive del diritto europeo dopo l'entrata in vigore del Trattato di Lisbona e in subiecta materia, con il richiamo alla proposta di direttiva contro gli attacchi ai sistemi di informazione (che, abrogando la decisione quadro 2005/222/GAI, ne riprende le disposizioni).
In secondo luogo, Buttarelli ha affermato che non è necessaria una sistematica sorveglianza degli utenti in Internet e che dovrebbe essere definitivamente disattesa la "credenza popolare" che meno privacy equivale a maggiore sicurezza.
Il raccordo fra le sessioni I e II di **Ben Hayes** (Statewatch) ha avuto ad oggetto il tema del monitoraggio relativo al rispetto delle libertà civili in Europa, in particolare le riflessioni sul bilanciamento fra le esigenze di contrasto di gravi forme di criminalità, compresi i cybercrimes, l'accesso alle informazioni in rete e la tutela dei diritti fondamentali.

Sessione II.
La capacità degli Stati di rispondere alle minacce della criminalità informatica dipende altresì dalla comprensione dei fenomeni, indispensabile per una politica preventiva.

La sessione II, presieduta da **Joon Oh Jang** (Senior Research Fellow, Director of International Center for Criminal Justice, Korean Institute of Criminolgy – KIC) si è aperta con gli interventi di **Gillian Murray** (Chief, Focal Point for Cybercrime, Conference Support Section, Division for Treaty Affairs UNODC) e di **Carla Licciardello** (Project Officer on Cybersecurity, International Telecommunication Union – ITU), che hanno contribuito a far comprendere, da un lato, l'utilità di un approccio sovranazionale diretto alla collaborazione fra Stati e fra i diversi organisimi investigativi e, dall'altro lato, l'importanza delle strategie e delle policy di sicurezza informatica. UNODC e ITU hanno già sottoscritto, nel maggio 2011, un Memorandum of Understanding (MoU) per assistere gli Stati membri ad attuare politiche di diminuzione dei rischi posti da fenomeni criminosi riconducibili al settore "cybercrime", con lo scopo di garantire l'utilizzo sicuro delle tecnologie della comunicazione e dell'informazione. Il MoU contiene linee guida che consentono ai due organismi di collaborare congiuntamente per assistere concretamente gli Stati nella predisposizione ed attuazione di politiche di cybersecurity, mettendo a disposizione risorse ed expertise per proporre misure legali sul piano nazionale, ma nell'ambito di una prospettiva di cooperazione internazionale.
Licciardello ha illustrato, in primo luogo, i contenuti della Global Cybersecurity Agenda (GCA) ed i suoi cinque pilastri: misure legali, misure tecniche e procedurali, strutture organizzative, capacity building, cooperazione internazionale.
In secondo luogo, ha portato l'esempio delle iniziative nella lotta alla pedopornografia online (child online protection initiative).
Anche le aggressioni alla sicurezza ed alla riservatezza dei sistemi informatici, dei dati e delle informazioni costituiscono uno dei fenomeni più allarmanti.
Thomas Holt (Associate Professor, School of Criminal Justice Michigan State University, USA) ha dimostrato non solo l'esistenza di un vero e proprio "mercato nero" e illegale della compravendita dei dati e delle informazioni personali (dai riferimenti di carte di credito e di pagamento, ai dati relativi a conti correnti, passaporti e codici fiscali), ma anche la sua vitalità e la sua espansione.
Holt ha illustrato le modalità concrete con cui venditori e compratori si mettono in contatto, nonché le metodologie più frequenti per ottenere illecitamente informazioni riservate, evidenziando come la creazione di network personali, talvolta "accreditati" da veri e propri gruppi o organizzazioni criminali, e la reputazione dei venditori siano fra gli elementi più importanti dell'illegal market e della sua affidabilità.
La vittimizzazione di massa è un tratto caratteristico di fenomeni crimosi.
Ma molti altri sono i fatti illeciti che trovano in Internet il luogo ideale di manifestazione, o che vengono posti in essere attraverso le nuove tecnologie.
Il mutamento del contesto sociale dovuto alla dipendenza dalle tecnologie dell'informazione e della comunicazione ha contribuito alla vittimizzazione di massa o, utilizzando le parole di **Jaishankar** (Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Executive Director, Centre for Cyber Victim Counselling, India), alla c.d. cyber victimization. Secondo i dati riportati dal relatore, che prende spunto dal Norton Cybercrime Report 2011, più di un milione di persone al giorno sono vittime di cybercrimes (50000 ogni ora, 820 al minuto e 14 ogni secondo). Il 70% degli adulti hanno avuto almeno un'esperienza, quali vittime del reato, nel settore della criminalità informatica. Gli attacchi più frequenti riguardano la diffusione di virus e malware, nonché i phishing attacks, la cui diffusione è facilitata anche dai nuovi devices. Molto spesso questi attacchi trovano ambiente fertile nell'ambito della pornografia online (molte vittime di virus o malware stavano visualizzando o scaricando materiale pornografico). Le perdite stimate, considerando il target studiato (in 24 paesi del mondo), ammontano a quasi 400 miliardi di dollari.
Malgrado queste cifre il rapporto ha evidenziato una scarsa sensibilità nell'approccio alla cyber security da parte delle vittime.

Sul piano psicologico, le vittime hanno dimostrato rabbia e frustrazione.
I nuovi trends della cyber victimization portano a ritenere altamente sensibili e vulnerabili i minori.
La seconda parte di questa sessione, presieduta da **Duncan Chappell** (Professor of Criminal Law, Faculty of Law, University of Sydney), è stata aperta da **Rob McCusker** (Director of Centre for Fraud and Financial Crime, University of Teesside Middlesbrough, UK), che ha delineato i tratti essenziali della criminalità informatica organizzata (Organised Cyber Crime). Secondo il relatore non si tratta di un mito, ma di un fenomeno transnazionale, guidato da obiettivi di consistenti profitti ed in contatto simbiotico con la corruzione. I fattori contingenti (globalizzazione dei sistemi informativi, misure di contrasto locali e non coordinate fra loro, non solo fra diversi Stati ma anche all'interno degli stessi ordinamenti) alimentano l'evoluzione e la diffusione di attività illecite organizzate che sfruttano le potenzialità offerte dalle nuove tecnologie e dalla rete.
D'altronde queste ultime sono sempre state utilizzate dalla criminalità organizzata "tradizionale", anche per commettere crimini comuni (ad esempio, le attività preparatorie, quali la pianificazione e l'organizzazione di una attività illecita sfruttando mezzi comunicativi quali l'email e skype).
Egli, partendo dalle lacune nelle definizioni di cybercrime, hight tech crime, computer crime, digital crime e technology crime, ha distinto fra il crimine organizzato tradizionale nel cyberspace e la criminalità nel cyberspace che è organizzata.
I fattori emblematici della connettività 24/7 (24 ore su 24 per 7 giorni su 7) e la possibilità di creare, da parte del consumatore digitale, ma anche dell'autore dei reati, di molteplici identità virtuali distribuite per innumerevoli networks, costituiscono l'ambiente ideale anche per il trasferimento e l'occultamento di fondi illeciti (provenienti da altri reati, non necessariamente informatici in senso stretto). McCusker non ha esitato ad affermare che nell'odierna società dell'informazione i dati hanno maggior valore del denaro. "Una volta speso, il denaro sparisce", ma i dati "possono essere sempre riutilizzati per creare ulteriori e maggiori ricchezze". Per questi motivi sarebbe necessaria la distinzione fra le due forme di criminalità (organizzata nel cyberspace e nel cyberspace organizzata), che potrebbe comportare la predisposizione di diverse misure preventive e di contrasto, maggiormente compatibili e adattabili alle peculiarità di due fenomeni, che hanno in comune l'ambiente ideale di manifestazione: il cyberspace.
L'importanza di strumenti investigativi adeguati, che considerino la natura transnazionale della criminalità informatica, è stata sottolineata anche da **Roberto Fernandez Alonso** (Europol Cybercrime Center, The Netherlands), che ha illustrato il sistema ICROS (Internet Crime Reporting Online System), le funzioni e le competenze di Europol e le strategie di contrasto al cybercrime. In particolare ha chiarito il ruolo di supporto di Europol, anche nei campi della formazione e della computer forensics.

Sessione III.
La terza sessione si è aperta con l'efficace introduzione di **Luis Arroyo Zapatero** (Director, Instituto de de Derecho Penal Europeo e Internacional, Ciudad Real, España), che ha ribadito, richiamando la pregnante premessa di Ulrich Sieber, l'importanza di un approccio sovranazionale con riferimento sia allo studio del fenomeno, che sui piani di politica criminale, per la previsione di fattispecie penali e di disposizioni processuali comuni o ampiamente armonizzate, e di cooperazione internazionale.
Un ruolo decisivo è assunto dall'analisi comparata con altri sistemi extra-europei, che hanno introdotto specifiche disposizioni in subiecta materia.
Pi Yong (Professor School of Law, Wuhan University, China) ha illustrato la recente legislazione cinese, dividendo il suo intervento in 3 parti: diritto penale sostanziale, procedura penale, disposizioni in materia di giurisdizione e competenza.

Dopo una breve introduzione storica sull'evoluzione del cybercrime in Cina (dagli anni '80 al 1994, anno in cui Internet ha iniziato ad essere largamente utilizzato dai cinesi), egli ha posto l'attenzione sullo stretto legame della criminalità informatica principalmente con la criminalità economica.
Sul piano normativo, nel 1994 è stata introdotta la prima legge sui computer crimes. Con la diffusione del fenomeno, dopo l'avvento di Internet, ed il passaggio dal computer crime al cybercrime, questo apparato normativo è stato modificato nel 1997, 2000 e 2009.
Secondo Pi Yong la risposta normativa cinese è stata lenta e, ancora oggi, si assiste alla presenza di gravi lacune come, in primo luogo, nel settore della raccolta, della ricerca e dell'ammissibilità della prova elettronica, in cui mancano specifiche disposizioni. In secondo luogo, la Cina non ha ancora sottoscritto alcun accordo di cooperazione e non ha aderito alla Convenzione del Consiglio d'Europa sulla criminalità informatica.
In particolare, per quanto riguarda il diritto penale sostanziale, l'ordinamento cinese prevede i reati di accesso abusivo a sistemi informatici o telematici ("in the fields of State affairs, national defense construction or sophisticated science and technology"), il procurarsi illegalmente dati e informazioni ("illegal invading the computer system that is not belong to the computer system described above or using other technical method to obtain computer data in the computer system"), il controllo illegale di un sistema informatico, fornire programmi per l'accesso illegale o per il controllo illegale dei sistemi informatici, il danneggiamento informatico (distruzione di un sistema informatico o di dati).
Inoltre, nel caso in cui i dati e le informazioni vengano illegalmente trasferite o vendute è applicabile l'art. 312 c.p.
Nel caso in cui, invece, il Service Provider fornisca un ausilio nella commissione degli illeciti penali, può rispondere a titolo di concorso nel reato.
Sul piano sostanziale, dunque, secondo Pi Yong l'ordinamento cinese recepisce, di fatto, le indicazioni contenute nella Convenzione Cybercrime e della decisione quadro dell'Unione europea sugli attacchi contro i sistemi informatici.
Sul piano della procedura penale, il relatore ha subito criticato l'attuale sistema normativo, che solo attraverso alcune interpretazioni da parte della giurisprudenza prevede norme per la ricerca e la raccolta della prova elettronica e le modalità della sua acquisizione, compresa la sua analisi.
In particolare si assiste, in Cina, al ricorso a strumenti normativi extrapenali, estesi tramite l'intepretazione giudiziale alle attività investigative della polizia dirette a raccogliere gli elementi probatori.
Più dettagliatamente, il data retention trova una sua specifica disciplina, ma non costituisce una misura investigativa di natura penale. Esso viene però utilizzato nelle indagini in materia di cybercrime.
Inoltre, solo dopo il 2010, a seguito dell'interpretazione da parte dei giudici, le disposizioni sulla detenzione e sulla copia dei dati in formato video e audio sono state estese ai dati in formato elettronico.
Per quanto riguarda, invece, la c.d. real time collection of electronic data, la proposta di modifica del codice di procedura penale, avanzata nel 2012, prevede integrazioni al codice di rito in materia di prova elettronica e misure investigative a carattere tecnologico, che includono altresì la sorveglianza elettronica (elctronic surveillance).
Pi Yong ha affermato che i dati raccolti attraverso questa ultima misura non possono, de jure condito, essere utilizzati dal giudice, ma potrebbero essere di ausilio per la ricerca di ulteriori prove. In sostanza, egli ha ammesso che, malgrado una lacuna legislativa, questo strumento investigativo viene utilizzato, tanto che il problema posto riguarda l'utilizzabilità o meno dei dati e delle informazioni reperiti.

Con riferimento alla prova elettronica, invece, non sono presenti, ad oggi, specifiche disposizioni. Si assiste all'espansione delle norme sulla raccolta della prova non elettronica, attraverso una interpretazione forzata, con l'obiettivo di poter ammettere l'electronic evidence.
Una ulteriore fattore critico nell'attuale società dell'informazione, a parere del relatore, è l'assenza, in Cina, di disposizioni speciali in materia di giurisdizione.
Trovano applicazione gli art. 6 e 12 c.p. Alla luce di queste norme il diritto cinese esercita una rilevante forza di attrazione in quanto si applica se il fatto o l'effetto del cybercrime si realizzano in Cina, ovvero se il luogo in cui viene commesso il reato si trova in territorio cinese.
Questa valenza attrattiva perde forza, e tali disposizioni non si applicano, se un cinese commette un reato informatico al di fuori del territorio cinese punito, nel massimo, a meno di 3 anni.
In definitiva la disciplina appena descritta è conforme all'art. 22 della Convenzione Cybercrime.
Vi è da ribadire, però, che la Cina non ha sottofirmato alcun accordo internazionale in subiecta materia e non si rinvengono specifici meccanismi di cooperazione giudiziaria.
Sul lato pratico, però, il relatore ha riportato che la Cina ha fornito il suo aiuto in molteplici casi di cybercrimes aventi carattere transnazionale (dal 2004 al 2010 la Cina ha aiutato più di 40 Stati in più di 700 casi).
Pi Yong ha concluso con una nota critica sulla Convenzione Cybercrime, affermando che si tratta del prodotto di un organismo internazionale "regionale" che ha limitati effetti nei paesi extra- europei.
La Cina, ma anche la Russia, ad esempio, non sono parti della Convenzione. In altri termini, il Consiglio d'Europa non può considerarsi l'unico promotore dell'armonizzazione delle legislazioni, ma necessita di un approccio globale e della cooperazione con altri organismi (ad esempio le Nazioni Unite).
Ad ogni modo, l'ordinamento giuridico cinese, anche a seguito della più recenti modifiche, è conforme al dettato della Convenzione Cybercrime e a quello della decisione quadro europea sugli attacchi contro i sistemi di informazione.
La strada da percorrere è ancora impervia, sia sul piano della procedura penale, sia su quello della cooperazione internazionale e della giurisidizione.
I delicati problemi di giurisdizione e le lacune sul piano del diritto processuale penale caratterizzano anche l'ordinamento giuridico iraniano.
Batoul Pakzad e **Ghassem Ghassemi** hanno efficacemente e molto chiaramente illustrato le tappe fondamentali nella lotta al cybercrime in Iran. Dopo aver brevemente percorso il background storico della diffusione di questo fenomeno criminoso ed aver riportato alcuni dati statistici sulla sua dimensione (citando i casi di pornografia, frode, violazione del copyright, accesso abusivo a conti correnti bancari), considerando la crescita progressiva dell'uso di Internet in Iran (passato da 250.000 utenti nel 2000, il 4% della popolazione, a 33.200.000 utenti nel 2010, ossia il 43% della popolazione), i relatori hanno delineato i tratti essenziali del sistema iraniano ed esposto il quarto ed il quinto programma di sviluppo, nonché le linee guida per la cyber space security.
Gli obiettivi principali sono: proteggere l'identità nazionale e religiosa ed il valore umano della società; rispettare le libertà civili e la privacy; assicurare l'integrità e la sicurezza nazionale, nonché la sicurezza delle infrastrutture; tutelare i diritti di proprietà intellettuale.
Sul piano legislativo, dal 2000 sono stati adottati almeno 5 importanti provvedimenti: protection of sofware copyright act (2000); e-commerce act (2003); military criminal act (2003); cybercrime act (2009); free access to information act (2007).
Per quanto riguarda il diritto penale sostanziale, Pakzad e Ghassemi hanno suddiviso sistematicamente i reati informatici in sette categorie:

1. Offese alla confidenzialità-riservatezza di dati e sistemi (accesso abusivo a sistemi informatici violando le misure di sicurezza, intercettazione illegale, spionaggio; questo ultimo si realizza violando le misure di sicurezza di sistemi informatici contenenti dati

segreti, ottenendo l'accesso a tali dati, fornendo l'accesso a terzi non autorizzati, rivelando dati segreti o fornendo l'accesso a Stati stranieri, organizzazioni o società; lo spionaggio può essere anche di natura colposa)

2. Offese alla autenticità dei dati e dei sistemi (falsità informatiche, quali l'alterazione di dati o la fraudolenta creazioni di dati; uso di dati falsi)
3. Offese all'integrità di dati e sistemi (danneggiamento di dati e di sistemi e cyberterrorism; questo ultimo è previsto dalla sec. 11 del cybercrime act: ogni interferenza realizzata su dati o sistemi, o il denial of access a sistemi informatici necessari per servizi essenziali, quali i servizi medici o per la somministrazione di acqua, energia, telecomunicazioni, trasporti, servizi bancari al pubblico, con l'intenzione di disturbare la sicurezza pubblica e la pace).
4. Offese alla disponibilità di dati e sistemi (denial of access a dati o sistemi; uso illegale della larghezza di banda; mancata prevenzione rispetto all'accesso a contenuti penalmente rilevanti; questo ultimo è applicabile agli ISPs, che hanno l'obbligo di filtrare i contenuti dichiarati di rilevanza penale da un comitato statale indipendente ad hoc; se il provider intenzionalmente non applica filtri per tali scopi, può essere soggetto alla sanzione del divieto di proseguire la sua attività professionale; se il fatto è colposo è invece applicabile una sanzione pecuniaria)
5. Computer related crimes (frode informatica, furto di dati, offese alla decenza ed alla morale pubblica e offese alla dignità; in queste ultime due vengono ricondotti i fatti di pedopornografia minorile, nonché i fenomeni di incoraggiamento, provocazione, facilitazione di un crimine contro la dignità, o di abuso di droghe, o di commissione di un suicidio o di una devianza sessuale o altri crimini violenti; sono ricondotti ai crimini contro la dignità i fatti di diffamazione o ogni altro fatto che possa offendere la dignità del soggetto, di danneggiarlo o di disturbare la pace pubblica).
6. Accessory crimes (la distribuzione o la produzione di malware o di altri tools per la commissione di reati informatici; distribuzione di materiale informativo su come commettere un reato informatico; procurare a favore di altri l'accesso abusivo a sistemi informatici o a dati e informazioni)
7. E-commerce crimes (violazioni del copyright, violazione di segreti commerciali o marchi, violazioni di diritti individuali, falsa pubblicità commerciale)

Infine, in Iran è prevista anche la responsabilità penale degli enti, se il reato è commesso a beneficio dell'ente e da parte di chi ha il potere di direzione, anche se solo una parte delle attività della persona giuridica è penalmente rilevante.
Sul piano del diritto processuale, si rinvengono disposizioni in materia di data retention (con una durata simile a quella prevista, in media, dalla maggior parte degli Stati europei, ossia 6 mesi) per l'accertamento di tutti i reati. E' però necessario un ordine/provvedimento del giudice per la preservazione e la produzione delle informazioni.
Vi sono, inoltre, disposizioni in materia di perquisizione e sequestro di dati e sistemi informatici, nonché in materia di raccolta della prova elettronica. Il valore di questa ultima è soggetto a tre requisiti essenziali: integrità, affidabilità e "non ripudio".

Sessione IV.
L'ultima sessione, presieduta da **Gillian Murray** (Chief, Focal Point for Cybercrime, Conference Support Section, Division for Treaty Affairs UNODC), si è aperta con la relazione di **Alexander Seger** (Secretary Cybercrime Convention Committee and Head of Data Protection and Cybercrime Division, Council of Europe, Strasburg), che ha ripreso il tema dell'Octopus Conference, Cooperation against Cybercrime 2011, a 10 anni dalla firma della Convenzione sulla criminalità informatica.

Il relatore ha illustrato il percorso storico della convenzione, sino alle più recenti ratifiche da parte di molteplici Stati (32 sono i Paesi che hanno ratificato il trattato, che però ha costituito anche una importante linea guida per altri Stati, che hanno introdotto nei loro ordinamenti specifici reati informatici o adottato strumenti processuali conformandoli a quelli previsti dalla convenzione).
Seger ha fornito alcuni importanti *key messages*, che costituiscono il risultato dell'analisi dei risultati raggiunti a 10 anni dalla firma della Convenzione Cybercrime:

1. il fenomeno cybercrime è in continuo movimento e sia gli Stati che gli organisimi internazionali non possono permettersi di abbassare la guardia;
2. l'assistenza tecnica ha contribuito ad incrementare la capacità degli Stati ad implementare misure e best practices nella lotta al fenomeno;
3. è necessario migliorare i meccanismi di cooperazione internazionale. In questo senso la Convenzione può costituire una linea guida importante;
4. rispetto alla commissione di gravi reati (come quelli di pedopornografia minorile) sono stati fatti enormi passi avanti. Sarebbero auspicabili però misure di take down in Internet (ossia il coinvolgimento degli ISPs in una fase anche preventiva e inibitoria, nonché per l'adozione di filtri o di controlli mirati)
5. sussistono ancora molte differenze, sia sul piano del diritto penale sostanziale che su quello della procedura penale. Questa ultima, in particolare, dovrebbe essere oggetto di uno sforzo ulteriore per creare le condizioni per l'adozione di regole comuni in materia di ricerca e raccolta della prova elettronica;
6. una completa legislazione, armonizzata con gli standard internazionali costituisce un fattore chiave nella lotta al cybercrime. A questa devono però aggiungersi una serie di attività volte ad incentivare la cooperazione internazionale, la cooperazione fra i settori pubblico e privato, nonché la formazione degli appartenenti agli organi investigativi.

Secondo Seger il futuro della cooperazione internazionale nella lotta al cybercrime dipende dall'attuazione degli standard già esistenti e dalla rimozione degli ostacoli che impediscono la piena efficacia dei mezzi investigativi come, ad esempio, quelli legati al libero scambio di informazioni.
L'intervento di **Stein Schjolberg** (Judge, Co-chair of the EastWest Institute (EWI) Cybercrime Legal Working Group, Oslo) è stato incentrato sulla opportunità di Tribunale penale internazionale per giudicare i cybercrimes, considerato il loro carattere globale.
La stessa Corte penale internazionale potrebbe giocare un ruolo fondamentale nella lotta alla criminalità informatica, in particolare contro gravi e coordinati attacchi a infrastrutture critiche.
Se questi "gravi crimini" sono inclusi nella giurisdizione della Corte, lo Statuto di Roma disporrebbe di un articolato adeguato in materia di investigazioni.
E' auspicabile, ad ogni modo, la creazione di un Tribunale penale internazionale per il cyberspace, ossia una corte delle Nazioni Unite istituita tramite una risoluzione del Consiglio di sicurezza (ex capitolo VII della Carta delle Nazioni Unite), che dovrebbe avere competenza in materia di gravi reati informatici e cyberattacks globali, con giurisdizione per le violazioni dei trattati in materia di cybercrime e gli attacchi informatici globali e coordinati a danno di infrastrutture informative critiche.
Per quanto riguarda la disciplina sulla ricerca e l'acquisizione della prova, il Tribunale dovrebbe seguire le disposizioni procedurali previste per gli altri tribunali penali internazionali (ad esempio quelli per la Yugoslavia ed il Ruanda).
Il sistema di lotta al cybercrime non sarebbe completo, secondo il relatore, senza la creazione di una Taskforce globale, attraverso il prezioso lavoro dell'Interpol. Egli ha proposto come modelli la PceU (U.K.), la ICSPA e la NCIJTF (FBI, U.S.A.).
L'intervento di **Marco Gercke** (Director, Cybercrime Research Institute, Köln University, Germany) ha fornito un quadro ricco e sistematico delle nuove tendenze di armonizzazione

nella lotta al cybercrime, partendo dalle "fonti" (in primis Convenzione Cybercrime e nuove competenze penali dell'Unione Europea), passando per le tecniche di tutela di importanti interessi e giungendo alle prospettive di armonizzazione dei mezzi processuali.
Gercke ha ripreso le linee del suo lavoro "Understanding cybercrime" e ha premesso i maggiori cambiamenti sociali apportati dalle nuove tecnologie e da Internet (la crescita degli utenti di Internet, la disponibilità di accesso alle risorse, la disponibilità delle informazioni, la carenza di meccanismi di controllo e la dimensione internazionale della rete, a cui si aggiungono l'automazione, la rapidità della trasmissione dei dati e le misure di sicurezza disponibili).
Egli ha evidenziato l'importanza delle esigenze locali nell'armonizzazione del diritto penale, considerando non solo i paesi industrializzati, ma anche quelli in via di sviluppo.
Ma l'armonizzazione delle discipline giuridiche costituisce solo, secondo il relatore, uno degli obiettivi da raggiungere nella lotta al cybercrime, assieme all'adozione di adeguate misure tecniche e procedurali, alla predisposizioni di strutture organizzative idonee ed alla cooperazione internazionale (cfr. Global Cybersecurity Agenda).
L'intervento di Gercke ha seguito la linea argomentativa impostata da Sieber, sia in introduzione della sessione I, che negli interventi successivi in occasione dello spazio di discussione: i caratteri congeniti del cybercrime (transnazionalità), la sua "potenzialità lesiva" di importanti beni giuridici, dovuta alla dipendenza dalle tecnologie e da Internet dell'attuale società, nonchè il "ritardo" nella risposta normativa, che risulta essere maggiore sul piano dei mezzi processuali o pre-processuali di contrasto e prevenzione. Si tratta di connotazioni su cui riflettere e che rafforzano la necessità di un "approccio globale" che possa tradursi anche nella predisposizione di regole comuni ed efficaci, sul piano non solo del diritto penale sostanziale, ma anche processuale.
Miguel Ontiversos Alonso (Director of the National Institute for Criminal Science of Mexico, Mexico - OAS) ha chiuso la sessione con una relazione avente ad oggetto la c.d. "auto-difesa tecnologica" (cyber-self-defense), valorizzando l'importanza della disciplina e dell'uso di strumenti tecnologici per la protezione dei sistemi informatici e dei dati che dovrebbero considerare una metodologia almeno trifasica (rilevamento/tracciamento degli attacchi o dei rischi, valutazione e analisi, predisposizione delle contromisure).
Le osservazioni del relatore si inseriscono nella discussione relativa alla stessa funzione preventiva delle misure legali di contrasto alla criminalità informatica.

Conclusioni

La conferneza internazionale "**Cybercrime Global Phenomenon and Its Challenges**" ha costituito una importante occasione di confronto fra i maggiori esperti del settore (accademici, operatori, tecnici, membri di organismi investigativi e rappresentanti di organismi internazionali), dando vita, in ogni sessione, ad un vivace dibattito con il pubblico.
Essa ha, da un lato, evidenziato, nel suo complesso, i rischi dovuti all'esponenziale diffusione del fenomeno "cybercrime" rispetto alla tutela di importanti beni giuridici.
Dall'altro lato, è emersa la delicata questione del bilanciamento fra esigenze di contrasto del fenomeno e quelle connesse alla tutela dei diritti fondamentali della persona, in primis la riservatezza e la sicurezza ed integrità dei sistemi informatici, dei dati e delle informazioni.
Inoltre, ad oggi, i maggiori ostacoli alla cooperazione internazionale rimangono le difficoltà di adozione di una politica comune e lo scambio di informazioni, a livello regionale e sovranazionale.
Anche se è stata percorsa molta strada nella lotta al cybercrime (si pensi, oltre alla Convenzione Cybercrime ed alle iniziative ed alle prospettive europee, anche alla Dichiarazione di Bangkok sulle Sinergie e sulle Risposte: Alleanze Strategiche nella Prevenzione del Crimine e nella Giustizia Penale, approvata dalla risoluzione 60/177 dell'Assemblea Generale del dicembre 2005, alla Dichiarazione di Salvador de Bahia, a seguito del 12° Congresso delle Nazioni Unite

su Prevenzione del Crimine e Giustizia Penale, al lavoro svolto da UNODC) è emersa la necessità di migliorare l'attività di *capacity-building*, l'assistenza tecnica, la reciproca assistenza legale e la cooperazione internazionale, nonché l'armonizzazione della disciplina penale sostanziale e processuale.
Sotto questo ultimo aspetto, lo sguardo ora volge all'Europa ed alle nuove competenze penali in materia di Cybercrime. Le linee di politica criminale europea, infatti, dovrebbero considerare non solo gli strumenti internazionali esistenti, ma anche l'approccio di importanti Stati extra-europei, nonché quello dei Paesi in via di sviluppo.
Questo approccio costituirebbe già un passo fondamentale nella lotta ad un "fenomeno globale" che necessita di "risposte globali".