CONVEGNI

ADELMO MANNA

Bozza di Risoluzioni per la I Sezione (*)

I partecipanti al Seminario Preparatorio per la Sezione I che si è tenuto a Verona dal 28 al 30 novembre 2012, propongono le seguenti risoluzioni al XIX Congresso Internazionale di Diritto Penale, che si terrà a Rio de Janeiro dal 31 agosto al 6 settembre 2014;

Considerando che la vita delle persone nel 21° secolo è fortemente influenzata e modellata dalle tecnologie dell'informazione e della comunicazione (TIC), nonché dalle opportunità e dai rischi offerti dalla società dell'informazione e *cyber*spazio, e che quindi i crimini in questi settori riguardano importanti interessi personali e collettivi;

Riconoscendo che gli Stati hanno compiuto sforzi notevoli nel definire e perseguire i reati che possono influenzare l'integrità dei sistemi TIC e *cyber*spazio, così come gli interessi delle persone in questi settori;

Tenendo presente i rischi associati ad un sovra estensione di repressione criminale in questi settori soprattutto per la libertà di espressione e di raccolta delle informazioni;

Definendo le reti TIC come sistemi che rendono possibile l'acquisizione, la lavorazione, la conservazione e la diffusione di informazioni audio, video, testuali e numeriche attraverso le reti informatiche e/o di telecomunicazione, e ciberspazio come ogni spazio di comunicazione condotta con l'ausilio di tali reti TIC;

Con riferimento agli strumenti internazionali importanti che cercano di guidare e coordinare gli sforzi e di armonizzare la legislazione, per esempio, la Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001, la direttiva CE sul commercio elettronico 2000/31/CE, la decisione quadro 2005/222/JHA UE relativa agli attacchi contro i sistemi di informazione e la direttiva sulla conservazione dei dati CE 2006/24/CE;

Ricordando l'importanza dei principi fondamentali della legislazione e della giurisprudenza penale, come il principio di legalità, il principio del danno che limita la criminalizzazione di comportamenti che sono nocivi o concretamente pericolosi per interessi personali o collettivi, il principio di colpevolezza , e

(*) Trad. a cura del Prof. A. Manna.

il principio di proporzionalità tra la gravità del reato e la gravità della reazione dello Stato;
Basandosi sui dibattiti e sulle risoluzioni dei passati Congressi Internazionali di Diritto Penale, in particolare le risoluzioni del XV Congresso Internazionale del 1994 a Rio de Janeiro, sezione II, sui crimini informatici e altri crimini contro la tecnologia dell'informazione;
Raccomandano quanto segue:

A. Considerazioni generali per la legislazione penale

1. TIC e *cyber*spazio hanno creato interessi specifici che devono essere rispettati e protetti, per esempio, l'integrità e la *privacy* dei sistemi TIC e delle identità personali in ciberspazio. Autori di alcuni reati tradizionali, come per esempio di frode, di falsificazione e violazione dei diritti d'autore, fanno uso di reti TIC e di ciberspazio, aumentando così la pericolosità del loro comportamento o aggiungendo una nuova qualità. Legislazioni, tribunali e sistemi giudiziari penali devono accettare la sfida di adattarsi a questa situazione.

2. Perché l'integrità delle reti TIC e del *cyber*spazio è di vitale importanza per le società moderne, tra cui i *media*, e i comportamenti dannosi o pericolosi in questi settori possono influenzare importanti interessi, gli Stati dovrebbero elaborare politiche efficaci rispetto alla protezione delle reti TIC ed ai relativi interessi. Tali politiche dovrebbero essere proporzionate e coerenti con la politica criminale generale. Esse dovrebbero essere continuamente aggiornate al fine di evitare nuove forme di comportamenti dannosi o pericolosi.

3. D'altra parte, un eccesso di regolamentazione e la criminalizzazione del *cyber*spazio dovrebbero essere evitati perché mettono in pericolo la stessa libertà di comunicazione che è il segno caratteristico del *cyber*spazio. I legislatori dovrebbero essere consapevoli che la disciplina delle condotte, l'adozione di leggi penali e l'imposizione di misure restrittive di controllo sproporzionate nel ciberspazio possono interferire con i diritti fondamentali, in particolare la libertà di espressione e la libertà di raccolta delle informazioni.

4. La politica criminale deve essere coerente con il principio del danno. Le legislazioni non devono, infatti, criminalizzare comportamenti che violino solo le norme morali, ma che non danneggiano o non creano un pericolo concreto per gli interessi di una persona o per un interesse collettivo bisognoso di

protezione.

B. Le alternative alle sanzioni penali

5. Gli utenti della rete TIC ed i fornitori di sistemi dovrebbero essere incoraggiati a proteggere la sicurezza delle reti , anche attraverso l'autoregolamentazione dei fornitori stessi. Il trascurare delle misure di sicurezza non dovrebbe portare a responsabilità penale da parte degli utenti, salvo che nel caso in cui le persone responsabili per i dati altrui violino gli obblighi specifici per il mantenimento in sicurezza dei dati. Il mancato rispetto delle misure di sicurezza da parte degli utenti non dovrebbe quindi diminuire la responsabilità penale degli autori dei reati.

6. Poiché i divieti penali comportano forte riprovazione morale e possono stigmatizzare i trasgressori, gli Stati dovrebbero esaminare attentamente se le misure non penali possano essere altrettanto efficaci nel prevenire attacchi sulle reti TIC e gli abusi della libertà del *cyber*spazio.
a) Provvedimenti giudiziari di risarcimento dei danni alle vittime conformemente al diritto civile, così come strumenti di giustizia riparativi possono integrare valide alternative.
b) Misure amministrative, ad esempio impedire o rimuovere l'accesso a siti *web* offensivi, possono anche svolgere un effetto preventivo sufficiente e possono così rendere l'uso del diritto penale inutile. Tuttavia, le misure amministrative non dovrebbero essere sproporzionate o trasformarsi in "pratiche di censura" applicate dalle stesse autorità esecutive.
c) Se necessario ai fini della deterrenza, i legislatori potrebbero anche considerare di permettere la memorizzazione di dati che rendono possibile, sotto controllo giurisdizionale effettivo, la successiva identificazione degli utenti sospettati di gravi reati.

C. Principio di legalità

7. Il principio di legalità impone che i reati in materia di TIC e *cyber*spazio siano definiti dalla legge. Questo vale anche per la definizione dei doveri e degli obblighi delle persone fisiche e giuridiche nella misura in cui la loro violazione può portare alla responsabilità penale. I legislatori dovrebbero utilizzare termini che definiscano il comportamento vietato nel modo più preciso possibile e quando la tecnologia cambia, la legge dovrebbe essere modificata.
La giurisprudenza, infine, non dovrebbe estendere la formulazione dei divieti

penali di là del loro significato letterale.

D. Estensione delle leggi penali

8. Molti legislatori hanno incriminato semplici atti preparatori per vere e proprie violazioni ai sistemi TIC ed al *cyber*spazio, come la produzione, la distribuzione e il possesso di *virus* informatici. Tali "estensioni" del diritto penale sono legittime solo nella misura in cui gli atti preparatori, in quanto tali, creino un elevato rischio di causare un danno od un pericolo concreto per gli interessi tutelati altrui. Qualora gli atti preparatori siano resi punibili, la sanzione deve risultare comunque meno grave, rispetto al reato in senso proprio cioè legato alla commissione di c.d. atti esecutivi (si vedano a questo proposito le Risoluzioni del XVIII Congresso Internazionale di Diritto Penale di Istanbul 2009, sezione I (A)).

9. La criminalizzazione del possesso di *software* non dovrebbe portare a limitazioni indebite sul legittimo uso del *software*.

10. Il semplice possesso e la visualizzazione dei dati possono essere resi punibili solo quando il possesso e la visualizzazione sono intenzionali e quando è altamente probabile che possano causare direttamente o indirettamente danni a persone.

11. I fornitori di servizi di rete TIC non dovrebbero essere obbligati a censurare i contenuti che essi elaborano. La loro responsabilità penale a tale riguardo dovrebbe essere limitata ai casi in cui siano stati avvertiti, in modo affidabile e specifico, dell'esistenza di contenuti proibiti nel loro dominio, e non abbiano tempestivamente adottato le misure ragionevolmente necessarie per il ripristino di uno *status* conforme alla legge.

E. Cooperazione internazionale

12. Le politiche di giustizia penale per la protezione delle reti TIC e ciberspazio e gli interessi degli utenti dovrebbero essere armonizzate a livello mondiale al fine di garantire una protezione efficace, per evitare gravi discrepanze tra disposizioni della stessa materia, per migliorare la cooperazione internazionale e, infine, per evitare conflitti di giurisdizione.