I VINCOLI DERIVANTI DAL TRATTATO DI BUDAPEST E DALLE RISOLUZIONI COMUNITARIE: I RISULTATI RAGGIUNTI DALLA COMMISSIONE "NORDIO".

"Governi del Mondo, stanchi giganti di carne e di acciaio, io vengo dal Cyberspazio, la nuova dimora della Mente. A nome del futuro, chiedo a voi, esseri del passato, di lasciarci soli. Non siete graditi fra di noi. Non avete alcuna sovranità sui luoghi dove ci incontriamo."

Universalmente noto, questo è l'incipit della "*Dichiarazione di indipendenza del Cyberspazio*" diffusa dall'autore John Perry Barlow quasi 10 anni fa.

Uno dei fulcri di tale dichiarazione è costituito dall'affermazione secondo cui "*Voi non conoscete la nostra cultura, la nostra etica, e nemmeno i codici non scritti che danno alla nostra società più ordine di quello che potrebbe essere ottenuto dalle vostre imposizioni.*".

Se tanta spocchia induce al sorriso chi tratta, quotidianamente, con criminali efferati, nondimeno la questione è terribilmente seria.

Non ci si può nascondere l'esistenza di una nuova frontiera globalizzante rappresentata dall'informatica e dalla sua pervasiva diffusione in tutti gli ambiti sociali ed economici. E, com'è noto, le "nuove frontiere" sono tipici luoghi di anomia e, pertanto, quanto mai adatti per l'insorgere di "nuovi crimini".

Né possono ancora sussistere dubbi in ordine alla necessità di normare tale magmatica novità, a costo di indisporre i cybernauti.

A tal fine, e per evitare che la "novità" –in quanto tale- spaventi, appare opportuno comprenderne profondamente significati e portata.

Innanzitutto si pone la questione del significato dei neologismi ormai entrati nel linguaggio comune.

Ad esempio: cosa vuol dire "*INFORMATICA*"?

Il termine non è altro che la sintesi delle parole *INFORMAZIONE* e *AUTOMATICA*.

E "*TELEMATICA*"? La sintesi delle parole *TELETRASMISSIONE* e *INFORMATICA*, quindi "trasmissione di informazioni automatiche".

Si tornerà sull'importanza dei significati terminologici (anche alla luce del costituzionale principio di tassatività delle norme

penali); per ora il breve vocabolario serve per sgrezzare la materia.
Altro termine famigerato è "*HACKER*". Esso deriva da *HACK* che potrebbe liberamente tradursi in "AZIONE GOLIARDICA".
In realtà il termine può datarsi all'anno 1958, allorché gli studenti del Massachussets Institute of Technology, di Boston, iniziarono a prodigarsi nel migliorare, giorno per giorno, la tecnologia di un plastico di ferrovia con il metodo del "*metterci continuamente le mani sopra*".
Per sviluppare il detto plastico quei goliardi iniziarono a sottrarre congegni dagli impianti dell'ateneo ed ogni azione "truffaldina" ma finalizzata al "gioco" veniva denominata "*HACK*". Quando, l'anno successivo, fu istituito il primo corso di informatica basato sullo studio dei primi mainframe consegnati all'istituto dalla DIGITAL, quei geniali e tecnologici goliardi trovarono il loro nuovo "parco giochi" e si buttarono a capofitto in quella nuova tecnologia per smontarla e rimontarla testandone ogni possibile potenzialità, mantenendo fede al vecchio sperimentato metodo dell' "*hands-on*".
L'*HACKER* non era altro che lo studente coinvolto in quel giocoso studio.
Oggi, quasi dimenticata la romantica e goliardica origine, il termine *HACKER* è diventato sinonimo di "trasgressore digitale" e *HACKING* è solo l'ingresso in un sistema informatico effettuato illegalmente e con fini "malvagi".
Tra le azioni di *HACKING* ormai universalmente conosciute e patite vanno annoverate il c.d. "*Network sniffing*": una particolare modalità di intercettazione di dati informatici destinati a terzi; il "*Denial of Service*" : un mezzo per influire negativamente sul funzionamento di un sistema informatico; l' "*IP spoofing*": la sostituzione dell'identità di un computer falsificandone i codici di riconoscimento in rete; la creazione e la diffusione di "*virus*": programmi autoreplicanti, spesso "maligni", capaci di alterare il funzionamento del sistema operativo o di singole applicazioni, trasportati in rete da "*Trojan Horse*".
E' evidente che ciascuna delle condotte di tal specie non può non rilevare in ambito giuridico-penale poiché appare chiara la loro potenzialità di offesa a beni giuridicamente tutelati.
Altrettanto evidente che una norma strutturata con approcci antiquati e non condivisa a livello internazionale non può

trattare con adeguatezza una materia così sfuggente, ontologicamente transnazionale ed in continua evoluzione (il metodo dell' "*hands-on*" è stato mantenuto inalterato), né può arginare stabilmente il fenomeno.
Ma la risposta dell'Ordinamento deve esserci e deve essere conforme ai principi del diritto penale costituzionalmente orientato, senza inaccettabili violazioni del principio di tassatività.
Tale risposta, oltre che adeguata ai principi costituzionali, non potrà, poi, divergere dai contenuti dei trattati internazionali e delle risoluzioni comunitarie.
Orbene, a questo punto appaiono sufficientemente indicati i confini ed i motivi dell'intervento normativo penale.
Proprio entro tali confini si è mossa la Commissione di Studio per la riforma del Codice Penale, presieduta dal dott. Carlo Nordio, dopo aver lungamente esaminato le attuali fattispecie, introdotte –negli ultimi anni- nel sistema penale italiano.
Con la maggiore possibile osservanza dei dettati costituzionali ed in applicazione dei principi contenuti, in particolare, dal Trattato di Budapest[1] e dalle risoluzioni C.E. in materia[2], si è proceduto, inizialmente, a fissare le definizioni indispensabili.

---

[1] **CONVENTION SUR LA CYBERCRIMINALITÉ Budapest, 23.XI.2001.**
Chapitre I – Terminologie
Article 1 –Définitions
Aux fins de la présente Convention,
A) l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;
B) l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;
C) l'expression «fournisseur de services» désigne:
I- toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et
II- toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
D) «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

[2] **Proposta di DECISIONE-QUADRO DEL CONSIGLIO relativa agli attacchi contro i sistemi di informazione 19.04.2002.**
Articolo 2 - Definizioni
La proposta decisione quadro del Consiglio contiene la seguenti definizioni:
a)"reti di comunicazione elettronica". Questa definizione è la stessa di quella adottata dal Consiglio e dal Parlamento europeo il 14 febbraio 2002 nella direttiva che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica .
b)"computer". Questa definizione si basa sull'articolo 1 della convenzione internazionale sulla criminalità telematica ("cibercriminalità"). Nella definizione rientrano anche ad esempio,

Il primo punto dell'elaborato le contiene tutte:
"Ai fini del presente codice per "reti di comunicazione elettronica" s'intendono i sistemi di trasmissione e le

---

personal computer "stand-alone", personal organiser digitali, set-top-box digitali, videoregistratori personali e telefoni cellulari (purché abbiano qualche funzione di trattamento di dati, ad esempio i telefoni WAP e di terza generazione), che non rientrerebbero nella sola definizione di reti di comunicazione elettronica.

c)"dati informatici". Questa definizione è costruita a partire dalla definizione di dati dell'ISO . Non è volta a designare anche oggetti fisici come i libri. Tuttavia, comprende i libri immagazzinati sotto forma di dati informatici (ad esempio, salvati in forma elettronica come un documento di trattamento di testi) oppure trasformati in dati informatici mediante uno scanner. Per questa ragione, la definizione chiarisce che i dati informatici devono essere stati "creati o tradotti in una forma" adatta al trattamento in un sistema di informazione o adatti a creare una funzione in un sistema di informazione.

d)"sistema di informazione". La definizione di sistema di informazione è tratta, originariamente, da quella adottata dall'OCSE nel 1992 nelle sue linee guida per la sicurezza dei sistemi di informazione e poggia sulle definizioni che precedono relative alle reti di comunicazione elettronica, computer e dati informatici. Il termine è anche stato usato in strumenti normativi comunitari precedenti, quali la decisione del Consiglio del 31 marzo 1992 nel settore della sicurezza dei sistemi di informazione e nella raccomandazione del Consiglio del 7 aprile 1995 su criteri comuni per la valutazione della sicurezza delle tecnologie d'informazione. La definizione si vuole neutra per quanto riguarda la tecnologia, e intesa a riflettere accuratamente il concetto di reti interconnesse e sistemi contenenti dati. Vi rientrano sia l'hardware che il software del sistema, ma non il contenuto dell'informazione stessa. Vi rientrano anche i sistemi "stand alone". Secondo la Commissione, è auspicabile estendere la tutela del diritto penale anche ai computer stand-alone e non limitarla ai soli sistemi interconnessi.

e)"persona giuridica". Si tratta di una definizione standard presente in precedenti decisioni quadro del Consiglio.

f) "persona autorizzata" . Significa ogni persona che ha il diritto, per contratto o per legge, o il permesso legittimo di usare, gestire, controllare, collaudare, condurre ricerche scientifiche o comunque far funzionare un sistema di informazione e che agisce in conformità con tale diritto o permesso. Rientrano in questa nozione coloro che agiscono con il consenso legittimo di chi possiede tale esplicita autorizzazione. È particolarmente importante che le seguenti categorie di persone e di attività legittime non siano (nei limiti dei diritti, dei permessi e delle responsabilità della persona e nel rispetto della legislazione comunitaria in materia di protezione dei dati e segretezza delle comunicazioni) penalizzate al momento dell'attuazione della presente decisione quadro nelle legislazioni nazionali:

– azioni degli utenti abituali, sia per uso privato che professionale, compreso l'uso da parte di tali utenti di una cifratura per proteggere le proprie comunicazioni e i propri dati;

– decompilazione, entro i limiti di cui alla direttiva 91/250/CEE del 14 maggio 1991 relativa alla tutela giuridica dei programmi per elaboratore

– azioni dei gestori, dei soggetti addetti al controllo e degli operatori delle reti e dei sistemi;

– azioni delle persone autorizzate a collaudare un sistema, sia che si tratti di personale interno alla società sia che si tratti di persone designate dall'esterno ed autorizzate a collaudare la sicurezza del sistema;

– ricerca scientifica legittima.

g)"senza diritto". Si tratta di una definizione ampia, che lascia una certa flessibilità agli Stati membri nel decidere l'esatto ambito del reato. Ciononostante, per assistere gli Stati nell'attuazione della decisione quadro del Consiglio nel diritto nazionale, la Commissione ritiene necessario indicare che alcune attività non devono ricadere nell'ambito del reato. Non è possibile, e probabilmente neanche auspicabile, stilare un elenco esaustivo di esenzioni a livello di Unione europea. Ma l'espressione "senza diritto" prende come punto di partenza le definizioni precedenti in modo da escludere la condotta delle persone autorizzate. Inoltre, essa esclude qualsiasi altra condotta riconosciuta come lecita dal diritto nazionale, compresi i mezzi di difesa generici e altri tipi di precedenti riconosciuti nel diritto nazionale.

apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasportare segnali con mezzi a filo, radio, ottici o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri fisse (a commutazione di circuito o di pacchetto, compreso Internet) e mobili, i sistemi elettrici a cavo, nella misura in cui siano usati per trasmettere segnali, le reti usate per l'emissione radiofonica e televisiva, e le reti di teledistribuzione via cavo, indipendentemente dal tipo di informazione trasportato.
Per "computer" s'intende qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma.
Per "dati informatici" s'intende qualsiasi rappresentazione di fatti, informazioni o concetti creata o trasformata in modo tale da poter essere trattata da un sistema di informazione, compreso un programma atto far svolgere una funzione ad un sistema di informazione.
Per "sistema di informazione" s'intendono computer e reti elettroniche di comunicazione, nonché dati informatici immagazzinati, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione.
Per "persona autorizzata" s'intende qualsiasi persona fisica o giuridica che abbia il diritto, per contratto o per legge, oppure il permesso legittimo di usare, gestire, sorvegliare, collaudare, condurre ricerche scientifiche legittime o in altro modo operare un sistema di informazione e che agisce in conformità con tale diritto o permesso.
Per "fornitore di servizi informatici" si intende:
1. qualunque persona, fisica o giuridica, che consente agli utenti dei propri servizi di comunicare attraverso un sistema di informazione;
2. qualunque persona, fisica o giuridica, che elabora o archivia dati informatici per conto di terzi;
Per "trasmissione di dati" si intende qualsiasi comunicazione di dati informatici attraverso un sistema di informazione.".
Dopo aver concordato l'ambito definitorio –che appare adeguatamente comprensibile e dettagliato- si è passati alla compilazione delle singole fattispecie incriminatrici[3] [4] tutte

[3] **CONVENTION SUR LA CYBERCRIMINALITÉ Budapest, 23.XI.2001.**
Article 2 – Accès illégal
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout

ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.
Article 4 – Atteinte à l'intégrité des données
1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.
2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.
Article 5 – Atteinte à l'intégrité du système
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.
Article 6 – Abus de dispositifs
1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:
a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:
i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;
ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,
dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et
b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.
2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.
3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

[4] **Proposta di DECISIONE-QUADRO DEL CONSIGLIO relativa agli attacchi contro i sistemi di informazione 19.04.2002.**
Articolo 3 - Accesso illecito a sistemi di informazione
Gli Stati membri provvedono a che l'accesso intenzionale, senza diritto, ad un sistema di informazione o ad una parte dello stesso sia punito come reato qualora sia commesso:

connotate dall'elemento soggettivo del dolo (talvolta anche specifico):

" ***(Intrusione abusiva)*** *Chiunque, senza autorizzazione, con qualunque mezzo, si introduce ovvero si mantiene in un sistema di informazione."*

In questa prima fattispecie si è ritenuto di dover tutelare primariamente il bene giuridico del "*domicilio informatico*" (così come elaborato dalla giurisprudenza di legittimità), dalle condotte (libere) lesive sia attive (l'introdursi) che passive (il mantenersi).

*"**(Intercettazione abusiva)** Chiunque, senza autorizzazione, intercetta, con qualunque mezzo, trasmissioni non pubbliche di dati informatici, incluse le emissioni elettromagnetiche provenienti da un sistema di informazione, idonee ad individuare i dati informatici in esso contenuti.".*

Anche in quest'ipotesi il bene giuridico tutelato è costituito dal "*domicilio informatico*" (e, ancor prima, dalla "riservatezza") ma la condotta ha ad oggetto i dati (che nella precedente potrebbero non ancora esistere) a prescindere dall'intrusione: i dati, infatti, potrebbe essere captati anche dall'esterno del sistema.

*"**(Uso abusivo dei dati acquisiti)** Chiunque, senza autorizzazione, fa uso di dati informatici comunque acquisiti.".*

Qui i "dati" si distaccano dal "sistema" ed è il loro uso illegale ad essere sanzionato. Il modello "storico" utilizzato è quello ricavabile dagli attuali artt.489 e 648 c.p., trattandosi, in vero, di un reato di "ulteriore offesa".

---

i) nei confronti di una qualsiasi parte di un sistema di informazione sottoposto a misure di protezione specifiche; o

ii) con l'intento di cagionare danni ad una persona fisica o giuridica; o

iii) con l'intento di procurare un vantaggio economico.

Articolo 4 - Interferenza illecita con sistemi di informazione

Gli Stati membri provvedono a che le seguenti condotte intenzionali, senza diritto, siano punite come reato:

a)il fatto di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili;

b)il fatto di cancellare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici in un sistema di informazione qualora ciò venga commesso nell'intento di cagionare un danno a persone fisiche o giuridiche.

Articolo 5 - Istigazione, favoreggiamento, complicità e tentativo

1.Gli Stati membri provvedono a che l'istigazione, il favoreggiamento, la complicità e il tentativo nella commissione dei reati di cui agli articoli 3 e 4 siano puniti come reato.

2.Gli Stati membri provvedono a che il tentativo di commettere i reati di cui agli articoli 3 e 4 sia punito come reato.

*"**(Rivelazione del contenuto di dati informatici)** Chiunque, essendo venuto a cognizione del contenuto di altrui dati informatici, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto.".*

Ancora una volta si è ritenuto di perseguire le lesioni alla "riservatezza" prescindendo dalla legittimità dell'originaria cognizione ma vincolando la sussistenza del reato alla mancanza di una "giusta causa" ovvero alla finalizzazione del conseguimento di un profitto.

*"**(Danneggiamento e distruzione di dati informatici)** Chiunque, senza autorizzazione, con qualsiasi mezzo, danneggia, cancella, deteriora, modifica, altera, rende in tutto o in parte inutilizzabili o inaccessibili ovvero sopprime altrui dati informatici.".*

In tale ipotesi criminosa (strutturata in più fattispecie alternative) la condotta è plurioffensiva poiché ai beni giuridici della riservatezza e della sfera "domiciliare" si aggiunge quello della proprietà/possesso inteso anche in senso "intellettuale".

*"**(Alterazione di sistemi informatici)** Chiunque, senza autorizzazione, con qualsiasi mezzo, impedisce, ostacola ovvero interrompe il funzionamento di un sistema di informazione mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili.".*

A differenza dell'ipotesi precedente, in questa fattispecie (anch'essa strutturata in più fattispecie alternative) oggetto della tutela è la "libertà di comunicazione".

*"**(Detenzione abusiva di strumenti informatici)** Chiunque produce, importa, vende, cede, detiene strumenti o programmi informatici ovvero codici d'accesso a sistemi di informazione destinati alla commissione dei reati del presente capo.".*

Trattasi di norma, di pericolo concreto, che anticipa la tutela ma –è evidente- potrebbe porre problemi interpretativi in ordine alla "tipicità" della destinazione illecita. In realtà, però, tale potenziale problema è solo apparente se si considera che la norma in parola è stata ideata in riferimento a "*strumenti o programmi*" connotati dalla univocità della loro funzione. Ad esempio il programma "*Brute Force*" non ha altre applicazioni se non quella di "*bucare*" (*rectius* : individuare) le password di siti o caselle di posta elettronica.

*"**(Falsificazione informatica)** Chiunque falsifica dati informatici utilizzati o utilizzabili quali documenti pubblici o privati.".*

In quest'ipotesi (che afferma la tutela, già operante nelle attuali norme relative ai "falsi", anche dei beni giuridici della buona fede e dell'affidamento) la novità è rappresentata dalla parificazione dei documenti, sia pubblici che privati, e dalla tutela anticipata alla fase di creazione ed anche al potenziale utilizzo del documento (si pensi, ad esempio, ai dati anagrafici contenuti nelle banche dati comunali).[5]

*"**(Frode informatica)** Chiunque, al fine di trarne un ingiusto profitto, per sé o per altri, introduce, altera, cancella o sopprime dati informatici contenuti in un sistema di informazione ovvero interferisce nel funzionamento di un sistema di informazione anche mediante uso di dati informatici illegittimamente detenuti.".*

Qui si ritenuto di delimitare l'alvo del penalmente rilevante introducendo la "specificità" del dolo. [6]

*"**(Uso illegale di dati criptati o steganografati)** Chiunque, al fine di organizzare o commettere ovvero di consentire che altri organizzino o commettano reati per i quali è previsto l'arresto obbligatorio in flagranza, trasmette, mediante un sistema di informazione, dati informatici criptati o steganografati.".*

Una delle più rilevanti novità, nel lavoro della "Commissione Nordio", è costituita dalla criminalizzazione di questa forma, particolarmente subdola, di contributo materiale (agevolatore

---

[5] **CONVENTION SUR LA CYBERCRIMINALITÉ Budapest, 23.XI.2001**
Article 7 – Falsification informatique
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

[6] **CONVENTION SUR LA CYBERCRIMINALITÉ Budapest, 23.XI.2001**
Article 8 – Fraude informatique
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:
a par toute introduction, altération, effacement ou suppression de données informatiques;
b par toute forme d'atteinte au fonctionnement d'un système informatique,
dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

o necessario) nei delitti realizzati da persone in concorso fra loro. La specificità della fattispecie in parola (tipizzata appunto da dolo specifico) sta nella considerazione "pratica" della frequenza con cui la criminalità (anche non organizzata) si sia tecnologicamente attrezzata. E' ormai fatto notorio che le comunicazioni organizzatorie avvengono per via telematica occultando i messaggi "segreti" all'interno di *files* apparentemente "irrilevanti" mediante programmi informatici di criptazione o di steganografia. E' ovvio che il vaglio politico di tale nuova incriminazione sarà demandato (come del resto tutto il "progetto" di riforma") agli organi legislativi.

*"**(Intrusione abusiva qualificata dall'agente)***

Il pubblico agente che, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, senza autorizzazione, si introduce, con qualunque mezzo, in un sistema di informazione

L'investigatore privato, anche se esercente in maniera abusiva tale professione, che, senza autorizzazione, si introduce, con qualunque mezzo, in un sistema di informazione.

Il fornitore di servizi informatici che, abusando di tale sua qualità, senza autorizzazione, si introduce, con qualunque mezzo, in un sistema di informazione".

In virtù della scelta -operata dalla Commissione- di limitare al massimo la proliferazione di "circostanze" privilegiando la compilazione di fattispecie autonome, si è ritenuto di rendere autonome le soprascritte ipotesi di *"Intrusione abusiva"* qualificate dall'agente.

*"**(Intrusione abusiva violenta)** Chiunque, senza autorizzazione, con minaccia o violenza alle persone ovvero con violenza sulle cose, si introduce, con qualunque mezzo, in un sistema di informazione.".*

Lo stesso criterio è stato utilizzato per questa fattispecie a base violenta.

*"**(Intrusione abusiva in sistemi di informazione di interesse pubblico)** Chiunque, senza autorizzazione, si introduce, con qualunque mezzo, in un sistema di informazione di interesse militare o relativo all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.*

***(Intercettazione abusiva di trasmissioni di dati informatici di interesse pubblico)** Chiunque, senza*

autorizzazione, intercetta, con qualunque mezzo, trasmissioni non pubbliche di dati informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, incluse le emissioni elettromagnetiche, provenienti da un sistema di informazione di interesse pubblico, idonee ad individuare i dati informatici in esso contenuti.

(Intercettazione abusiva di trasmissioni di dati informatici di interesse pubblico commessa dal fornitore di servizi informatici).

Il fornitore di servizi informatici che, abusando di tale sua qualità, senza autorizzazione, intercetta, con qualunque mezzo, trasmissioni non pubbliche di dati informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, incluse le emissioni elettromagnetiche, provenienti da un sistema di informazione di interesse pubblico, idonee ad individuare i dati informatici in esso contenuti.

(Rivelazione del contenuto di dati informatici di interesse pubblico).

Chiunque, essendo venuto a cognizione del contenuto di dati informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, incluse le emissioni elettromagnetiche, provenienti da un sistema di informazione di interesse pubblico, idonee ad individuare i dati informatici in esso contenuti, lo rivela ovvero lo impiega a proprio o altrui profitto.

(Danneggiamento e distruzione di dati informatici di interesse pubblico)

Chiunque, senza autorizzazione, con qualsiasi mezzo, danneggia, cancella, deteriora, modifica, altera, rende in tutto o in parte inutilizzabili o inaccessibili ovvero sopprime dati informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

(Alterazione di sistemi di informazione di interesse pubblico)

Chiunque, senza autorizzazione, con qualsiasi mezzo, impedisce, ostacola ovvero interrompe il funzionamento di un sistema di informazione di interesse militare o relativo

all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili.

(Detenzione abusiva di strumenti informatici commessa dal fornitore di servizi informatici)

Il fornitore di servizi informatici che produce, importa, vende, cede, detiene strumenti o programmi informatici ovvero codici d'accesso a sistemi di informazione destinati alla commissione dei reati del presente capo.

(Uso illegale di dati criptati o steganografati commesso dal fornitore di servizi informatici)

Il fornitore di servizi informatici che, al fine di organizzare o commettere ovvero di consentire che altri organizzino o commettano reati per i quali è previsto l'arresto obbligatorio in flagranza, trasmette, mediante un sistema di informazione, dati informatici criptati o steganografati.

(Uso illegale di dati criptati o steganografati per finalità di terrorismo)

Chiunque, al fine di organizzare o commettere ovvero di consentire che altri organizzino o commettano reati con finalità di terrorismo o di eversione dell'ordine democratico, comunica, mediante un sistema di informazione, dati informatici criptati o steganografati.".

In tutte le sopra riportate ipotesi si è mantenuta la direttiva di "autonomizzare" le fattispecie le quali, di volta in volta, si caratterizzano per le qualità dei sistemi o dei dati tutelati (l'interesse pubblico) ovvero per le qualifiche degli agenti (il fornitore dei servizi) ovvero per le finalità della condotta (di terrorismo o eversione).

Sempre in relazione ai trattati internazionali si è ritenuto, allo stato, di mantenere tra i "delitti dell'informatica" anche la norma relativa alla pornopedofilia informatica.[7]

---

[7] **CONVENTION SUR LA CYBERCRIMINALITÉ Budapest, 23.XI.2001**

Article 9 – Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;

b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

*"**(Pornografia infantile)***
Chiunque:
A) produce rappresentazioni di pornografia infantile al fine di cederle ovvero diffonderle attraverso un sistema di informazione;
B) offre o mette a disposizione rappresentazioni di pornografia infantile attraverso un sistema di informazione;
C) trasmette rappresentazioni di pornografia infantile attraverso un sistema di informazione;
D) procura, per sé o per altri, rappresentazioni di pornografia infantile attraverso un sistema di informazione;
Per rappresentazione di pornografia infantile si intende qualunque materiale pornografico che ritrae, rappresenta visivamente ovvero raffigura:
1) un minore degli anni 14 implicato o coinvolto in una condotta sessualmente esplicita, fra cui l'esibizione lasciva dei genitali o dell'area pubica;
2) una persona reale avente le caratteristiche morfologiche di un minore degli anni 14, implicata o coinvolta nella condotta di cui al punto che precede.
3) immagini informatiche realistiche di un minore degli anni 14 implicato o coinvolto nella suddetta condotta.
(Detenzione di materiale di pornopedofilia informatica)
Chiunque detiene rappresentazioni di pornografia infantile attraverso un sistema di informazione o uno strumento di archiviazione di dati informatici.".
Data l'esclusione del verbo "sfruttare" attualmente contenuto dall'art.600-ter c.p. (e per cui si è ritenuto –da parte della Suprema Corte- di individuare i beni giuridici tutelati nella

---

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:

a un mineur se livrant à un comportement sexuellement explicite;

b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

"libertà sessuale" e nel "libero sviluppo della personalità" del minore), e considerata la necessitata (per trattato internazionale)[8] criminalizzazione del c.d. *Morphing* (e cioè il ritrarre, rappresentare visivamente ovvero raffigurare sia una persona reale avente le caratteristiche morfologiche un minore degli anni 14 implicata o coinvolta in condotte sessualmente esplicite e sia immagini informatiche virtuali ma realistiche di un minore degli anni 14, implicato o coinvolto nelle suddette condotte) la tutela si è riversata sul bene giuridico del "buon costume" (esplicitamente costituzionale poiché previsto dall'art.21, comma VI, Cost. secondo cui "*Sono vietate tutte le manifestazioni contrarie al buon costume*", che rappresenta, contemporaneamente, la delimitazione all'altrettanto costituzionale "diritto di manifestare liberamente il proprio pensiero").
Malgrado gli obblighi internazionali suddetti, però, è stato, (per ora e salvo diverse scelte della Commissione e, ovviamente, del Legislatore) proposto di considerare "bambino" non il soggetto di età inferiore agli anni 18 bensì quello di età inferiore agli anni 14.
E ciò non per mera "insubordinazione" ma per considerazioni sistematico-normative.
Invero, è indispensabile ricavare dal sistema attuale la definizione dell'età prevista per prestare validamente il consenso sessuale.
A ciò provvede il disposto di cui all'art. 609-quater c.p. secondo cui, in assenza di violenza o minaccia o abuso di autorità, il soggetto quattordicenne è libero di compiere atti sessuali, salvo che tali atti siano compiuti con l'ascendente, il genitore anche adottivo, il tutore, ovvero altra persona cui, per ragioni di cura, di educazione, di istruzione, di vigilanza o di custodia, il minore è affidato o che abbia, con quest'ultimo, una relazione di convivenza. In questi casi l'età del "consenso sessuale" è elevata a 16 anni. Ma scende addirittura a 13 se gli atti sessuali vengono compiuti con soggetto infrasedicenne (o comunque di età che non superi di 3 anni quella dell'infraquattordicenne).
Se così è appare quantomeno asistemico fissare a 18 anni il limite massimo dell'infanzia.

---

[8] "Convention sur la cybercriminalité - Budapest, 23.XI.2001" e "Decisione Quadro 2004/68/GAI del Consiglio dell'Unione Europea del 22 dicembre 2003, relativa alla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile".

Diversamente opinando si rischierebbe di introdurre nell'Ordinamento un nuovo reato "senza vittima" a sfondo esclusivamente etico, con tutti i problemi filosofico-giuridici che tale categoria di reati comporta, posto che la condotta richiesta non sarebbe quella di "sfruttamento" di un bambino ("sfruttamento" inteso come il perseguimento di un qualunque profitto, anche non lucrativo) bensì quella dell'utilizzo di immagini di persone che lecitamente si esibiscono, con proprio valido consenso, in condotte sessualmente esplicite.

Chiude l'elaborato proposto una norma che, verosimilmente, più di altre susciterà discussioni:

"(Inosservanza dei provvedimenti dell'Autorità commessa dal fornitore di servizi informatici)

Il fornitore di servizi informatici che non provvede a rimuovere o cancellare dati informatici ovvero impedire la trasmissione dei medesimi dati, a seguito di provvedimento legalmente dato dall'Autorità o di ordine impartito dal Giudice.".

Con tale norma (modellata sull'attuale art.650 c.p.) si è voluto vincolare il fornitore di servizi informatici alle disposizioni legittimamente impartite dall'Autorità Amministrativa e dal Giudice (si badi, non dal Pubblico Ministero), senza obbligare il medesimo fornitore ad esercitare preventivamente un controllo (in realtà pressoché impossibile) ma imponendogli di "oscurare" trasmissioni di dati illegali o illegittime.

Antonio Leonardo Tanga