LUCIO MONACO

PROLEGOMENA ALLA RIFORMA DEL DIRITTO PENALE DELL'INFORMATICA NELL'ORDINAMENTO GIURIDICO DELLA REPUBBLICA DI SAN MARINO

1. Premessa. La criminalità informatica: un fenomeno in espansione

Le economie mondiali e la società globalmente intesa hanno subìto radicali trasformazioni per effetto dell'espansione della rete, soprattutto a partire dalla c.d. bolla di internet esplosa nel 2000. La rete riveste ormai importanza strategica in ogni settore: l'*e-commerce* è in costante crescita e sottrae fette sempre più importanti al mercato reale; il massiccio utilizzo da parte di imprese e pubbliche amministrazioni delle comunicazioni elettroniche è favorita dall'abbattimento dei costi relativi alle barriere spazio-temporali di trasmissione dei dati.

Da Internet dipende la funzionalità delle infrastrutture critiche degli Stati, come la rete idrica, elettrica, le telecomunicazioni e i mezzi di *intelligence* a difesa della sovranità nazionale. La tecnologia informatica è divenuta essenziale anche sotto il profilo sociologico, per quanto attiene alle interazioni tra persone, attraverso i *social network*, forum, *blog*. Ciò ha comportato la moltiplicazione delle identità digitali, quali proiezioni delle molteplici sfaccettature della personalità degli utenti in carne ed ossa.

Il web è stato concepito come strumento tecnologico per la circolazione di dati e informazioni. Ha altresì assunto il ruolo di volano della conoscenza e catalizzatore dei principi di democraticità e uguaglianza nella misura in cui concede l'accesso indiscriminato al sapere. La sua vitalità è destinata ad accrescersi in forza del c.d. **effetto di rete**: quanto più una rete è estesa

ed altamente utilizzata, tanto più acquista valore, perché cresce l'utilità che ciascuno può ricavarne e incentiva al suo utilizzo coloro che ancora non lo fanno. Altro fattore di crescita di internet è la sua configurazione come bene non rivale: l'utilizzo contestuale da parte di più utenti non diminuisce l'utilità che gli uni e gli altri possono trarne.

Alla luce di queste considerazioni, è evidente come la sicurezza delle reti e delle informazioni si elevi a interesse giuridico di primaria importanza per la stessa preservazione e il progresso dell'umanità. La sicurezza informatica può addirittura declinarsi come un "bene comune", ossia come un bene indispensabile per la collettività, al pari delle risorse naturali (fonti idriche, riserve naturali, etc.)[1].

Qualsiasi strategia di contrasto al *cybercrime* è destinata a fallire se non tiene conto della dimensione ultrastatuale del fenomeno. L'armonizzazione più estesa possibile delle discipline penalistiche sostanziali e processuali tra le nazioni costituisce un imprescindibile punto di partenza. Consapevole di ciò, per esempio, l'Unione europea ha incluso la criminalità informatica tra le nove materie tassative che consentono l'adozione di direttive in materia penale (art. 83 TFUE[2]). È in discussione, inoltre, una proposta di direttiva (2013/48/UE) che ha a oggetto la sicurezza delle reti e delle informazioni, in quanto ritenuta «*precondizione per la creazione di un ambiente virtuale affidabile per lo scambio di servizi su scala mondiale*»[3].

---

[1] La categoria giuridica dei beni comuni nasce come alternativa a quelle di beni privati e pubblici, per affermare l'idea di appartenenza collettiva di quelle risorse, naturali o artificiali, materiali o immateriali, necessarie per la comunità.

[2] « ***Articolo 83.*** *- 1. Il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni.*

Dette sfere di criminalità sono le seguenti: terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata.

In funzione dell'evoluzione della criminalità, il Consiglio può adottare una decisione che individua altre sfere di criminalità che rispondono ai criteri di cui al presente paragrafo. Esso delibera all'unanimità previa approvazione del Parlamento europeo.

2. (omissis)

3. (omissis)».

[3] Relazione alla proposta di direttiva 2013/48/UE. Tale proposta prevede l'adozione di un modello di gestione condivisa, secondo un apparato di regole cautelari e precauzionali, nel quale la sanzione penale funge da incentivo alla loro osservanza.

Secondo le statistiche italiane riportate nel rapporto CLUSIT 2013, la frequenza degli incidenti è aumentata nel complesso del 250% in un solo anno; il *cybercrime* è diventato la causa di oltre il 50% degli attacchi nel 2012, con una crescita anno su anno del numero di attacchi di oltre il 270%[4]. Da questi dati si evince come la traslazione della vita reale su quella virtuale per effetto dell'utilizzo massivo di Internet abbia inevitabilmente comportato l'incremento del suo impiego anche per fini illeciti (c.d. *dual use*).

L'espressione "reati informatici" può essere intesa in due accezioni:

1. reati informatici in senso ampio, comprensivi di tutti gli illeciti comuni commessi mediante lo strumento informatico (per esempio, la diffamazione *online*);
2. reati informatici in senso stretto, in riferimento a quelle figure di reato nelle quali l'elemento informatico – la connessione, l'elaboratore, i sistemi informatici e telematici, il software - si presenta come elemento imprescindibile e caratterizzante della fattispecie, sicché non è possibile estendere alcuna fattispecie 'comune' per la profonda diversità strutturale (ad esempio, l'accesso abusivo a sistema informatico o telematico, art. 615-*ter*, c.p., la frode informatica art. 640-*ter* c.p.).

Le statistiche dimostrano il fallimento delle politiche di autogoverno della rete, pur vivacemente caldeggiate dai sostenitori della *net neutrality*[5].

---

[4] Si tratta del rapporto annuale sulla sicurezza informatica in Italia dell'associazione italiana per la sicurezza informatica (CLUSIT) che prende in considerazione gli anni 2011, 2012 e i primi sei mesi del 2013. È possibile consultare il rapporto CLUSIT al seguente link: http://www.assintel.it/wp-content/uploads/2012/11/Rapporto_Clusit-2013_Settembre.pdf

[5] I sostenitori della *net neutrality* (neutralità della rete) basano il loro pensiero su considerazioni legate all'architettura di Internet. Dal punto di vista tecnico, infatti, la si basa su determinati strumenti tecnici (i protocolli) che esprimono una specifica filosofia tecnologica: la riduzione al minimo delle operazioni che la rete deve compiere, attribuendo tutte le attività più importanti ai punti terminali della rete stessa, vale a dire al computer del mittente e a quello del destinatario del messaggio. Al contrario, le apparecchiature che si trovano ad operare tra i due punti terminali e che governano il traffico della rete (*router* e *gateway*) si limitano a trasmettere i pacchetti. Proprio l'indifferenza verso i contenuti veicolati rappresenta il nocciolo duro del principio di neutralità della rete. Questo principio costituisce, in primo luogo, una garanzia di "*innovazione decentrata*", perché in questo modo la rete può essere utilizzata per qualsiasi nuova soluzione tecnologica o nuovo modello economico. In secondo luogo, declinata come assenza di discriminazioni rispetto al contenuto del messaggio veicolato e alla natura del mittente, la neutralità determina importanti risvolti sul piano sociale e politico, favorendo la libera circolazione delle idee, dei principi e delle opinioni. In sostanza, i sostenitori della *net neutrality* non escludono che la trasmissione di certi contenuti sia vietata dal diritto, né che certi messaggi siano eliminati al punto di arrivo (come

Al contrario, di fronte alla tutela dei beni primari per la pacifica convivenza e sicurezza, è difficile sostenere le tesi a favore l'estromissione dello Stato o di Convenzioni internazionali che regolamentino talune attività o l'utilizzo di determinate tecnologie. L'intervento del legislatore penale a tutela dei beni giuridici che rischiano di essere lesi attraverso i crimini informatici appare necessario in considerazione della maggior carica lesiva delle violazioni commesse *online*. Si pensi al caso della pedopornografia, il cui livello di pericolosità prima dell'avvento di internet era pressoché minimo, mentre ora ha assunto dimensioni elefantiache, tanto da creare un vero e proprio mercato occulto di scambi.

2. La Convenzione di Budapest e la legislazione penale sammarinese

La Convenzione di Budapest del 23 novembre 2001 costituisce ancor oggi il principale strumento giuridico di contrasto della criminalità informatica. Molteplici sono le motivazioni che hanno indotto il Consiglio d'Europa alla sua adozione: dai profondi cambiamenti provocati dalla digitalizzazione, convergenza e globalizzazione delle reti informatiche, alla preoccupazione per l'utilizzo per fini illeciti della rete, a fronte delle lacune normative riscontrate dalla prassi. La Convenzione mira a istituire, tra gli stati aderenti, una normativa penale e processuale omogenea, in grado di eliminare le zone franche per il crimine *online* e risolvere i delicati problemi di giurisdizione e perseguibilità da esso posti. Le caratteristiche del *web*, infatti, costituiscono un terreno fertile per la proliferazione dei reati: deterritorializzazione e ubiquità hanno comportato l'annientamento delle limitazioni temporali e dei confini spaziali sui quali si reggeva il principio di sovranità territoriale; la neutralità si atteggia a peculiarità strutturale di Internet e, declinata come libertà di circolazione dei dati e indifferenza verso i contenuti veicolati in rete, si è tradotta in un ricettacolo per i malintenzionati, a causa dell'assenza di controlli.

---

accade per i filtri anti-spamming). Negano piuttosto che l'attuazione dei divieti giuridici o di preferenza di determinati utenti sia affidata agli *internet service providers*, in quanto soggetti che filtrano e veicolano i pacchetti di dati.

D'altra parte, avverso questa corrente di pensiero si impongono considerazioni di ordine economico: garantire l'assoluta neutralità della rete può trasformarsi in un fattore di incertezza per gli operatori economici con conseguente riduzione degli investimenti in quel servizio, tecnologia o infrastruttura.

Come è noto, la Convenzione è articolata in quattro capitoli ("*Definizioni*", "*Misure da adottare a livello nazionale in tema di diritto sostanziale e processuale*", "*Cooperazione internazionale*", "*Clausole finali*"), a loro volta suddivisi in sezioni. Il secondo capitolo concernente le "*Misure da adottare a livello nazionale*", è strutturato in due sezioni: l'una dedicata al diritto penale sostanziale e l'altra al diritto processuale. La lettura della sezione relativa al diritto penale sostanziale consente di affermare che le condotte tipiche descritte dalla Convenzione sono, nel loro complesso, conformi ai criteri di imputazione cui si ispira il codice penale del 1974, suggerendo una riforma coerente rispetto ai principi generali della responsabilità penale della Repubblica di San Marino e con l'impianto liberale del codice stesso.

La Convenzione si limita a descrivere gli elementi essenziali comuni alle singole fattispecie, rimandando al legislatore nazionale l'adozione di misure legislative e di altra natura essenziali per introdurre norme penali.

La sezione di diritto penale sostanziale raggruppa le singole fattispecie in relazione al bene giuridico minacciato o leso. Il titolo primo si occupa dei "*Reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici*".

L'art. 2 descrive le condotte intenzionali di *accesso illecito a tutto o a parte di un sistema informatico senza diritto*, rimettendo alla discrezionalità di ciascun ordinamento la possibilità di prevedere: 1) la condizione obiettiva di punibilità relativa alla protezione del sistema oggetto di accesso abusivo mediante misure di sicurezza; 2) il dolo specifico ("*con l'intento di ottenere dati informatici, o altri intenti disonesti*").

Viene, altresì, richiesta la criminalizzazione dell'*intercettazione illegale* operata con mezzi tecnici, di trasmissioni pubbliche di dati informatici che partono da, o giungono, o si trovano all'interno di un sistema informatico, comprese le emissioni elettromagnetiche (art. 3). Il singolo stato può prevedere che il fatto sia punito solo in presenza di dolo specifico (con intenti disonesti) o soltanto in relazione ad un sistema di computer che è connesso ad un altro computer. Un'altra ipotesi di reato è quella relativa all'*interferenza dei dati*, che consiste nell'intenzionale danneggiamento, cancellazione, deterioramento, alterazione o soppressione di dati informatici senza diritto, con la possibilità, per ciascuno stato, di circoscrivere l'area penalmente rilevante al caso che dal comportamento derivino ingenti danni (art. 4).

È imposta l'incriminazione *dell'interferenza del sistema*, che consiste nel fatto di ostacolare gravemente senza diritto il funzionamento di un sistema informatico mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici (art. 5). Il titolo I si conclude con il reato di *uso improprio di*

dispositivi che si sostanzia nella produzione, vendita, approvvigionamento per l'uso, l'importazione, la distribuzione o altra forma di messa a disposizione di: 1) un dispositivo come un programma per computer, destinato o utilizzato principalmente al fine di commettere uno dei reati descritti negli articoli da 2 a 5; 2) una password del computer, un codice di accesso o informazioni simili, con il fine di utilizzo per la commissione di uno dei reati di cui agli articoli da 2 a 5. È incriminato anche il mero possesso di uno dei due oggetti descritti, purché risulti finalizzato a commettere i reati sopra indicati (art. 6). Si specifica che tale condotta costituisce reato solo nel caso in cui si persegua lo scopo di commettere uno dei reati di cui agli articoli da 2 a 5 della Convenzione.

Il titolo II è intitolato "*Reati informatici connessi*" e prevede due ipotesi di reato. La prima concerne la *falsificazione di computer connessi*, consistente nella condotta dolosa di ingresso, alterazione, cancellazione o soppressione, senza diritto, di dati informatici, con possibilità di circoscrivere la responsabilità penale alle ipotesi di dolo specifico ("*intento di frode o simile intento disonesto*"; art. 7). La seconda fattispecie, formulata come reato di evento, attiene alla *frode informatica*, che si sostanzia nell'arrecare a terzi una perdita di proprietà e nel procurarsi, senza diritto, un beneficio economico per sé o un terzo, attraverso l'ingresso, alterazione, cancellazione o soppressione di dati informatici, oppure mediante qualsiasi interferenza con il funzionamento di un sistema informatico caratterizzata dal fine fraudolento o disonesto (art. 8).

Il titolo III, rubricato "*Reati relativi ai contenuti*", consta di una sola norma, l'art. 9, dedicato alla criminalizzazione della pornografia infantile. Tale fattispecie è strutturata come reato a base dolosa consistente nel: a) produrre materiale pedopornografico ai fini della distribuzione attraverso un sistema informatico; b) offrire o mettere a disposizione materiale pedopornografico attraverso un sistema informatico; c) distribuire o trasmettere materiale pedopornografico attraverso un sistema informatico per sé o per un'altra persona; e) possedere materiale pedopornografico in un sistema informatico o su supporto di memorizzazione di dati informatici. La norma precisa che per "*pornografia infantile*" deve intendersi il materiale pornografico che rappresenta visivamente: a) un minore coinvolto in condotte sessualmente esplicite; b) una persona che sembra un minore in atteggiamenti sessuali espliciti; c) immagini realistiche che rappresentano un minore in atteggiamenti sessuali espliciti. Per "*minore*" si intendono tutte le persone di età inferiore ai diciotto anni, con possibilità di abbassare il limite di età ai sedici anni. Tuttavia, lo stato può decidere di limitare l'incriminazione alle sole condotte descritte nei punti a) e b) e circoscrivere il termine

'pornografia infantile' al solo materiale che ritrae un minore coinvolto in condotte sessualmente esplicite.

Il titolo IV è dedicato ai "*Reati in materia di violazione del diritto d'autore e dei diritti connessi*": l'unico articolo di cui consta prevede la piena discrezionalità di ciascuno Stato in ordine all'introduzione di sanzioni penali, a condizione che siano disponibili altri efficaci rimedi e che tale riserva non sia in contrasto con gli obblighi assunti a livello internazionale (art. 10).

Il titolo V conclude la parte relativa al diritto penale sostanziale, con riferimenti alla responsabilità concorsuale, al tentativo di reato, nonché alla responsabilità da reato delle persone giuridiche (artt. 11, 12). L'art. 13 attiene alle sanzioni e misure: la norma si limita a prescrivere l'adozione di sanzioni efficaci, proporzionate e dissuasive, comprensive delle misure privative della libertà personale. Le singole ipotesi sopra considerate non indicano alcuna cornice edittale, ma demandano la scelta relativa al *quantum* di pena esigibile alla discrezionalità dei legislatori nazionali.

La Repubblica di San Marino non ha ancora ratificato la Convenzione di Budapest. Il codice penale sammarinese non contiene un catalogo di crimini informatici in senso stretto (accesso abusivo, interferenze illecite, interferenza di dati e danneggiamento informatico).

Recentemente è stata varata una dettagliata normativa in materia di frodi e falsificazioni (l. 29 luglio 2013, n. 102) che ha modificato talune fattispecie incriminatrici, come l'art. 204-*bis* (uso indebito di strumenti di pagamento), art. 401-*bis* (frodi e falsificazioni di strumenti di pagamento diversi dai contanti), art. 403 (fabbricazione, detenzione, acquisto, alienazione di strumenti o materiali di contraffazione) ed ha introdotto la frode informatica (art. 204-*ter*) [6].

Rispetto ai quattro gruppi descritti nella Convenzione di Budapest, allo stato si presenta la seguente situazione normativa: in ordine al titolo I ("*Reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici*") si registra un vuoto di tutela per quanto riguarda l'accesso abusivo, le intercettazioni e le interferenze illecite di dati e del sistema e uso improprio di dispositivi. Sarà pertanto necessario introdurre fattispecie di reato corrispondenti.

Per quanto attiene al titolo II, non si rinviene nel codice penale alcuna disposizione concernente il c.d. falso informatico. Si dovrà quindi proce-

[6] Sul fronte civilistico, con L. 23 maggio 2013, n. 58 è stata adottata un'apposita normativa sull'uso delle comunicazioni elettroniche e dell'*e-commerce*.

dere ad aggiornare il catalogo delle fattispecie poste a presidio della fede pubblica (artt. 295 – 302 c.p.s.m.). In merito alla frode informatica, la fattispecie enunciata dall'art. 204-*ter* c.p.s.m. risulta conforme alla descrizione operata dal Consiglio d'Europa.

In relazione al titolo III, ossia alla pedopornografia, tale fattispecie è stata inserita in un'apposita disposizione, all'art. 177-*ter* c.p.s.m., ad opera della legge 30 aprile 2002, n. 61. La tipizzazione operata dal legislatore sammarinese ricomprende gli elementi essenziali del reato formulati dall'art. 9 della Convenzione.

Le esigenze di armonizzazione per la tutela del diritto d'autore (art. 10 Conv.) possono, altresì, ritenersi soddisfatte dalla disciplina sammarinese in materia. Quest'ultima si articola in un doppio livello sanzionatorio: penale, per le condotte di cui all'art. 202 c.p.s.m. e amministrativo, ai sensi della legge 29 gennaio 1996, n. 5, art. 118.

Nell'ordinamento sammarinese è stata recentemente emanata la legge 29 luglio 2013, n. 99, istitutiva della responsabilità da reato delle persone giuridiche. La normativa, molto simile alla disciplina italiana che regola la materia, soddisfa le istanze di criminalizzazione poste dall'art. 12 della Convenzione[7].

[7] L. 29/07/2013, n. 99: « ***Art. 2 (casi di responsabilità)***

Le persone giuridiche sono responsabili:

a) per i reati dolosi commessi per loro conto o comunque nel loro interesse da persona che aveva il potere di agire per la persona giuridica stessa;

b) per i reati commessi nello svolgimento dell'attività della persona giuridica se il reato è stato reso possibile da una lacuna organizzativa ascrivibile alla persona giuridica, alla carenza di sorveglianza o controllo ovvero quando sia stato commesso su indicazione dei vertici organizzativi o gestionali dello stesso.

(*omissis*)».

Schema riepilogativo

CONVENZIONE DI BUDAPEST	DISCIPLINA PENALE DI SAN MARINO
TITOLO I REATI CONTRO LA RISERVATEZZA, L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI E DEI SISTEMI INFORMATICI	**TUTELA CARENTE**
TITOLO II REATI INFORMATICI CONNESSI **Art. 7 (falsificazioni computer connessi)**	**TUTELA PARZIALE: CARENTE artt. 295 - 302** L. 20 luglio 2005, n. 115 (legge sul documento informatico e la firma elettronica)
Art. 8 (frode informatica)	Art. 204-*ter* c.p. **frodi informatiche** (inserito nel c.p.s.m. dalla L 29 luglio 2013, n. 102) **L. 20 luglio 2005, n. 115, art. 6 (responsabilità) prevede a carico del prestatore di servizi di certificazione la sola responsabilità civile nella forma del risarcimento del danno**
TITOLO III REATI RELATIVI AI CONTENUTI	Art. 177-*ter* c.p. **pornografia minorile**
TITOLO IV REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE E DEI DIRITTI CONNESSI	Art. 202 c.p. **Usurpazione di beni immateriali** L. 29/01/1996, n. 5 **depenalizzazione diritto d'autore**, Art.118
TITOLO V ART. 12 RESPONSABILITÀ AZIENDALE	L. 29/07/2013, n. 99, **Responsabilità della persona giuridica**

3. La necessità del raffronto con la legislazione italiana: elementi di comparazione ed armonizzazione tra paesi confinanti.

3. 1 La risposta italiana alla criminalità informatica e la ratifica della Convenzione di Budapest.

Il legislatore italiano, su impulso della prassi e delle fonti sovranazionali, ha provveduto progressivamente ad aggiornare il codice penale Rocco. Il primo intervento in materia di criminalità informatica risale al 1993 ed ha introdotto le fattispecie a tutela del domicilio informatico (artt. 615-*ter*, 615-*quater* e 615-*quinquies*), quelle a protezione dell'inviolabilità dei segreti (artt. 617-*quater*, 617-*quinquies* e 617-*sexies*), il danneggiamento di sistemi informatici e telematici (art. 635-*bis*) e la frode informatica (art. 640-*ter*). Sicché è possibile affermare che già prima della Convenzione di Budapest e della sua ratifica ad opera della legge 18 marzo 2008 n. 48, l'ordinamento italiano aveva esteso la tutela penale alle ipotesi contemplate nel titolo I della Convenzione ("*Reati contro la riservatezza, l'integrità e la disponibilità dei dati dei sistemi informatici*").

L'esperienza italiana costituisce un termine di paragone utile nella prospettiva di costruzione di fattispecie penali, perché l'Italia è stato il secondo paese europeo, dopo la Francia, ad adottare una legge organica per reprimere i crimini informatici (L. 547/1993). Sicché essa può contare sui risultati applicativi evidenziati nel corso degli anni, quale banco di prova per vagliare le criticità delle singole fattispecie: si pensi, alle sezioni unite della Corte di Cassazione del 2012 in merito all'interpretazione della fattispecie di accesso abusivo a sistema informatico, nel caso di soggetto formalmente legittimato all'accesso, ma che si introduca o trattenga nel sistema per fini che esulano le condizioni d'uso stabilite dal titolare[8].

Le ipotesi relative al domicilio informatico sono descritte negli artt. 615-*ter*, 615-*quater* e 615-*quinquies*. L'*accesso abusivo a sistema informatico* (art. 615-*ter*) incrimina la condotta di colui che si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il

[8] Cass., Sez. un., 27.10.2011 (dep. 7.2.2012), n. 4694, Pres. Lupo, Rel. Fiale, ric. C.; massima: è penalmente illecita la condotta di un soggetto che, pur legittimato all'accesso a un sistema informatico o telematico, violi condizioni e limiti imposti dal titolare per disciplinarlo, a nulla rilevando scopi e finalità dell'accesso stesso.

diritto di escluderlo. Il bene giuridico tutelato appare, secondo una prima lettura che guarda al bene giuridico di categoria, il c.d. domicilio informatico, declinato come estensione virtuale del soggetto, uno spazio "ideale" oltre che fisico, nel quale sono contenuti i dati informatici di pertinenza dell'utente[9]. Una differente interpretazione assume la riservatezza informatica come bene giuridico protetto: tale qualificazione consente di configurare la fattispecie come reato di danno, indipendentemente dal fine perseguito dal soggetto attivo con l'intrusione[10]. Ad un'attenta disamina della norma, accanto alla riservatezza dei dati e dei programmi contenuti in un sistema informatico, è compresente la tutela dell'integrità del sistema (art. 615-*ter*, co. 2, n. 3 in relazione ad interessi militari, di ordine pubblico, sicurezza pubblica, sanità o, più in generale, di qualsiasi interesse pubblico). In tale accezione, la fattispecie sarebbe inquadrabile tra i reato di pericolo astratto e costituirebbe la tutela anticipata di un interesse patrimoniale: la condotta di accesso abusivo sarebbe causalmente orientata al danneggiamento del sistema. Il legislatore italiano ha inoltre deciso di limitare l'incriminazione alla condizione obiettiva di punibilità che si tratti di sistema protetto da misure di sicurezza (secondo un'opzione di politica criminale che la Convenzione del 2002 rimette alla discrezionalità del legislatore nazionale).

L'art. 615-*quater*, attiene alla *detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici* e punisce la condotta di chi al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo. Si tratta di una norma che incrimina una condotta prodromica alla commissione di un accesso abusivo e di conseguenza la fattispecie si declina come reato di pericolo astratto: è incriminata una condotta nella quale è insita la probabilità di commissione di ulteriori azioni illecite contro i sistemi informatici o telematici.

La fattispecie di *diffusione di programmi diretti a danneggiare o interrompere un sistema informatico* (art. 615-*quinquies*) è stata modificata

---

[9] Cassazione penale, sezione IV, 4 ottobre 1999, in *Foro it*., 2000, II 133; Cassazione penale, sezione V, 30 settembre 2008, Romano, in *Mass. Ufficiale*, 242938.

[10] G. Pica, *Diritto penale delle tecnologie informatiche,* Utet, Torino 1997; G. Pica, *Internet*, in *Dig. disc. pen., I Agg*., Utet, Torino 2004.

dalla legge di ratifica della Convenzione di Budapest, che ha provveduto: a) ad estendere la protezione alle "apparecchiature" e ai "dispositivi", rispetto ai soli programmi informatici; b) ad ampliare il ventaglio delle condotte sanzionabili: mentre con la precedente formulazione la mera detenzione non era punibile, ora invece incorre in sanzione penale non solo chi diffonda, comunichi, consegni o, comunque, metta a disposizione programmi, apparecchiature o dispositivi, ma anche chi produca, importi, si procuri ovvero riproduca tali software o hardware; c) a restringere l'area penalmente rilevante mediante la previsione del dolo specifico ("*allo scopo di danneggiare illecitamente un sistema informatico o telematico*"). La norma mira a tutelare il corretto funzionamento delle tecnologie informatiche ed è strutturata come reato di ostacolo, attenendo a condotte prodromiche al danneggiamento. Per questa ragione si è dubitato della corretta collocazione nell'ambito dei reati a tutela del domicilio informatico.

Il limite principale delle fattispecie a tutela del domicilio informatico si riscontra nel modo in cui sono state formulate, ossia mediante la riproposizione della medesima struttura delle fattispecie esistenti misurate sul dato esperienziale del mondo fisico. Questo difetto strutturale è indice di scarsa conoscenza da parte del legislatore della realtà virtuale e dei meccanismi tecnici di funzionamento. D'altra parte, negli anni '90, al legislatore mancava la consapevolezza delle potenzialità lesive di internet, soprattutto per il fatto che la sua utilizzazione di massa e diversificata si colloca agli inizi del nuovo secolo.

I delitti descritti nella sezione del codice penale dedicata alla tutela della inviolabilità dei segreti (artt. 617 ss., c.p.) sono ascrivibili al novero dei reati a tutela della riservatezza delle comunicazioni informatiche (titolo I della Convenzione, artt. 3 e 7). L'articolo 617-*quater* punisce *chiunque fraudolentemente, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe*. Inoltre, il comma secondo incrimina, salvo che il fatto costituisca più grave reato, chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni. Il bene giuridico tutelato è la riservatezza delle comunicazioni informatiche rispetto all'indebita captazione o rivelazione. La scelta del verbo "*intercettare*" al posto della mera "*presa di cognizione*" di cui all'art. 617 c.p., induce a pensare che la fattispecie sia finalizzata a tutelare soltanto la presa di cognizione derivante dall'intromissione nel corso di una comunicazione, commessa mediante il ricorso a mezzi idonei ad ingannare ("*fraudolentemente*").

L'articolo 617-*quinquies* sanziona *l'installazione, fuori dai casi consentiti*

dalla legge, di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. Il riferimento alla capacità delle apparecchiature di intercettare, impedire o interrompere le comunicazioni, assieme alla sussistenza del dolo specifico, serve a restringere l'area dell'illecito penale. La norma è finalizzata a realizzare una tutela anticipata della riservatezza dei dati o delle informazioni.

La condotta incriminata dall'art. 617-*sexies* consiste nella *falsa formazione o alterazione o soppressione, in tutto o in parte, del contenuto anche occasionalmente intercettato di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, al fine di procurare a sé o altri un vantaggio o arrecare un danno ad altri*. Si ritiene che la norma sia finalizzata a proteggere l'esistenza e l'autenticità – intesa come formazione veritiera dell'informazione e come conformità della stessa al testo originario – del contenuto delle comunicazioni [11]. Le condotte alternative devono essere connotate da dolo specifico.

La legge di ratifica della Convenzione di Budapest interviene ad ampliare il novero delle fattispecie relative al danneggiamento informatico. Il legislatore del 2008 ha adattato la normativa interna secondo l'impianto degli artt. 4 e 5 della Convenzione di Budapest, distinguendo, da un lato, il danneggiamento dei dati, programmi e informazioni e, dall'altro, il danneggiamento dei sistemi informatici. L'art. 635-*bis* (*danneggiamento di informazioni, dati e programmi informatici*) viene modificato: la condotta attiva attualmente consiste nella modalità alternative di distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui. La vecchia formulazione si limitava a prevedere la distruzione, il deterioramento o l'inservibilità, in tutto o in parte, di sistemi informatici o telematici altrui, o programmi, o dati o informazioni altrui. È mutato il regime di procedibilità: non più d'ufficio, ma a querela di parte.

Sono state aggiunte tre fattispecie ulteriori: l'art. 635-*ter* (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*) consistente nel commettere un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Sta-

[11] *Sub* Art. 617-*quater*, in *Commentario breve al Codice penale*, Crespi, Forti, Zuccalà, CEDAM, 2008, 1738.

to o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Il reato è aggravato qualora dal fatto derivi la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici. Tali condotte erano sanzionate dall'art. 420, comma III c.p., ove il delitto era strutturato come reato a consumazione anticipata, in termini di attentato a impianti di pubblica utilità (ed alle informazioni ivi contenute) [12]. Tale comma è stato abrogato, assieme al II comma, dalla legge 48/2008. Anche in questo caso, si anticipa la soglia di punibilità al compimento di atti diretti, ossia caratterizzati dal fine di distruzione o altra modalità vietata. Le condotte devono riguardare: 1) dati, informazioni e programmi utilizzati dagli enti pubblici; 2) dati, informazioni e programmi di pubblica utilità (e dunque sia pubblici che privati, purché siano destinati a soddisfare un interesse di natura pubblica). Si è in presenza di un reato aggravato dall'evento, sicché il fatto sussiste anche in assenza di qualunque effettivo deterioramento o soppressione dei dati, pur dovendosi necessariamente richiedere l'idoneità dell'azione a produrre tale effetto.

L'art. 635-*quater* (*Danneggiamento di sistemi informatici e telematici*) punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. La fattispecie è strutturata come reato di evento, il cui oggetto materiale del reato consiste non più nei dati o nelle informazioni, ma nei sistemi informatici o telematici.

L'art. 635-*quinquies* (*danneggiamento di sistemi informatici o telematici di pubblica utilità*) corrisponde al "vecchio" reato di attentato a sistema informatico o telematico di pubblica utilità (art. 420, comma II) e si configura quando il fatto descritto nell'art. 635-*quater* è diretto a distruggere, danneg-

[12] « ***Art. 420. – Attentato ad impianti di pubblica utilità***

1. Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.

[2. La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in esso contenuti.]

[3. Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è della reclusione da tre a otto anni.]».

giare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Si tratta di un reato a consumazione anticipata, nel quale è previsto un ampliamento delle condotte punibili, come quelle consistenti nel rendere inservibile, ovvero a ostacolarne gravemente il funzionamento.

Nel complesso, il rafforzamento della tutela contro le forme di danneggiamento informatico sembra consolidare quella tesi dottrinaria a sostegno della nascita di una nuova categoria di bene giuridico: il bene informatico.

La legge di ratifica della Convenzione di Budapest ha integrato e modificato incisivamente i reati in tema di falso informatico, inseriti, nel codice penale, dalla l. 23 dicembre 1993, n. 547. Il legislatore italiano ha provveduto a modificare il disposto dell'art. 491-*bis*, ossia quella norma che estende ai documenti informatici pubblici e privati, mediante la tecnica del rinvio *per relationem*, le fattispecie di falso in atti pubblici e scritture private. Il bene giuridico tutelato attiene all'affidamento sulla genuinità di determinati documenti e sui fatti in essi rappresentati. Nella formulazione originaria la disposizione al secondo comma, esplicitava la nozione di "*documento informatico*", soppressa nel 2008, a causa dei problemi interpretativi che recava e per il fatto che non si sarebbe creata alcuna lacuna, poiché, nel 2005, era stato approvato il codice dell'amministrazione pubblica digitale contenente un'esplicita definizione[13]. Inoltre, al primo comma la responsabilità penale è stata circoscritta al caso in cui si tratti di documento informatico pubblico o privato avente efficacia probatoria. È stata infine introdotta la nuova fattispecie di "*false dichiarazione o attestazioni al certificatore di firma elettronica sulla identità o qualità personali proprie o di altri*" (art. 495-*bis* c.p.). Per il corretto funzionamento della fattispecie occorre fare riferimento al codice

[13] « ***Art. 491-bis. Documenti informatici***

1. (*omissis*)

2- *A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli* ».

Tale nozione contenente il riferimento al "supporto" sembrava attribuire più rilevanza all'elemento materiale sul quale era contenuto, piuttosto che al contenuto; inoltre non precisava cosa dovesse intendersi per "efficacia probatoria" dei dati e delle informazioni la cui falsificazione assumeva rilievo penale.

Ad ogni modo, la definizione di documento informatico si trova nel codice dell'amministrazione digitale, d. lgs. 7 marzo 2005, n. 82, art. 1, lett. p): «*ogni rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*».

dell'amministrazione pubblica digitale, il d. lgs. 82/2005, che attribuisce al CNIPA (centro nazionale per l'informatica nella pubblica amministrazione) la competenza alla tenuta dell'elenco pubblico dei certificatori accreditati per la firma digitale. Esso identifica, inoltre, quali dichiarazioni o attestazioni devono essere rilasciate al certificatore elettronico per l'ottenimento della firma elettronica qualificata o digitale. In sostanza, la responsabilità del falso informatico va interpretata e coordinata con la legge sulla digitalizzazione della pubblica amministrazione.

Il legislatore del 1993 ha introdotto nel codice penale la fattispecie di frode informatica (art. 640-*ter*). Tale *novum* si è reso necessario a causa della profonda diversità strutturale tra truffa comune e frode informatica. Infatti, gli "*artifizi e raggiri*", mediante i quali l'agente induce in errore il soggetto passivo e si procura un ingiusto profitto con altrui danno (art. 640, truffa comune), risultano di difficile estensione quando il soggetto passivo è un elaboratore elettronico. Nella frode informatica, questi elementi sono sostituiti dall'alterazione in qualsiasi modo del funzionamento di un sistema informatico e telematico o dall'intervento senza diritto e con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti. In tal modo, la norma si presta a sanzionare anche fattispecie più simili al reato di furto (art. 624 c.p.), come nel caso di furto di informazioni, ossia nel caso di sottrazione di dati e di informazioni telematiche dalle quali è possibile conseguire un profitto. Il fatto tipizzato nell'art. 640-*ter* risulta pienamente sovrapponibile all'ipotesi convenzionale. La legge di ratifica della Convenzione sul *cybercrime* ha previsto una nuova ipotesi di reato (art. 640-*quinquies*): la frode informatica del soggetto che presta servizi di certificazione di firma digitale. Si tratta di un reato proprio, perché soggetto attivo può essere soltanto il prestatore del servizio di certificazione di firma digitale. La condotta tipica si sostanzia nella violazione degli obblighi di legge (art. 32, d. lgs. 82/2005) per il rilascio di un certificato qualificato, purchè sia connotata dal fine di procurare a sé o ad altri un ingiusto profitto o arrecare ad altri un danno.

Risultano altresì soddisfatte le esigenze di armonizzazione in materia di pedopornografia (art. 9 Conv.). Tale disciplina è stata oggetto di più interventi legislativi, da ultimo mediante la l. 38/2006, che ha modificato le fattispecie di cui agli artt. 600-*ter*, (*pornografia minorile*), 600-*quater* (*detenzione di materiale pornografico*) ed inserito l'art. 600- *quater.I* (*pornografia virtuale*). Questa riforma merita di essere segnalata non soltanto per l'aggiornamento degli strumenti di investigazione, ma anche perché tenta di superare la prospettiva analogica nell'elaborazione delle norme

penali che si può evincere, ad esempio, dall'analisi delle fattispecie di danneggiamento.

Per quanto attiene ai reati commessi in materia di violazione del diritto d'autore (art. 10 Conv.), l'Italia ha aggiornato la normativa del 1941, n. 633 con il d. lgs. 6 maggio 1999, n. 1691 e la legge 18 agosto 2000, n. 248, estendendo la tutela penale e amministrativa anche al software e alle banche dati quali opere dell'ingegno.

Infine, in merito alla responsabilità degli enti di cui all'art. 12 della Convenzione, la legge 48 del 2008 ha previsto l'introduzione, tra i reati presupposto della responsabilità delle persone giuridiche di cui al d. lgs. 231/2001 (responsabilità amministrativa degli enti), dei delitti informatici e di trattamento illecito dei dati (art. 24-*bis*).

Schema riepilogativo

CONVENZIONE DI BUDAPEST	DISCIPLINA PENALE ITALIANA
TITOLO I **REATI CONTRO LA RISERVATEZZA, L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI E DEI SISTEMI INFORMATICI**	Art. 615-*ter* **accesso abusivo ad un sistema informatico o telematico (**intr. L. 547/1993) Art. 615-*quater* **detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici** (intr. L. 547/1993) Art. 615-*quinquies* **diffusione di programmi diretti a danneggiare o interrompere un sistema informatico** (intr. L. 547/1993, mod. L. 48/2008) Art. 617-*quater* **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche** (intr. L. 547/1993) Art. 617-*quinquies* **installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche** (intr. L. 547/1993) Art. 617-*sexies* **falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche** (intr. L. 547/1993) Art. 635-*bis* **danneggiamento di sistemi informatici o telematici** (intr. L. 547/1993, mod. L. 48/2008) Art. 635-*ter* **danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o di pubblica utilità** (intr. L. 48/2008) Art. 635-*quater* **danneggiamento di sistemi informatici o telematici (**intr. L. 48/2008) Art. 635-*quinquies* **danneggiamento di sistemi informatici o telematici di pubblica utilità** (intr. L. 48/2008)

TITOLO II REATI INFORMATICI CONNESSI	Art. 491- *bis* **documenti informatici** Art. 495-*bis* **false dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri** Art. 640-*ter*, **frode informatica** (intr. L. 547/1993) Art. 640-*quinquies*, **frode informatica del soggetto che presta servizi di certificazione di firma elettronica** (intr. L. 48/2008)
TITOLO III REATI RELATIVI AI CONTENUTI	Art. 600-*ter* **pornografia minorile** (int. d. lgs. n. 269/1998, mod. L. 38/2006) Art. 600-*quater* **detenzione di materiale pornografico** (int. d. lgs. n. 269/1998, mod. L. 38/2006) Art. 600-*quater*.1. **pornografia virtuale** (intr. L. 38/2006)
TITOLO IV REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE E DEI DIRITTI CONNESSI	L. 22 aprile 1941, n. 633 (mod. d. lgs. 6 maggio 1999, n. 1691 e l. 18 agosto 2000, n. 248)
TITOLO V ART. 12 RESPONSABILITÀ AZIENDALE	L. 48 del 2008 ha previsto l'introduzione, all'art. 24-*bis*, tra i reati presupposto della responsabilità delle persone giuridiche di cui al d. lgs. 231/2001, dei delitti informatici e di trattamento illecito di dati divengono reati.

4. Discipline penalistiche a confronto: individuazione delle possibili modalità d'intervento nell'ordinamento sammarinese.

È opportuno, a questo punto, dar corso alla comparazione tra la disciplina penale italiana e , ove possibile, l'omologa sammarinese. Il passaggio risulta indispensabile al fine di individuare le possibili scelte d'intervento ed evitare così che molteplici beni informatici risultino sforniti della necessaria tutela penale.

La prima fattispecie oggetto d'esame è quella di cui all'art. 615-*ter*, c.p.

italiano "*Accesso abusivo ad un sistema informatico o telematico*". In considerazione della caratterizzazione plurioffensiva che annovera, tra i beni giuridici tutelati dalla norma, il domicilio informatico e l'integrità del sistema informatico, nonché della condotta richiesta ai fini della realizzazione del reato, si rileva la mancanza, nell'ordinamento sammarinese, di un'omologa fattispecie. Potrebbe ravvisarsi una correlazione con la fattispecie ex art. 204-*ter* (*frode informatica*), laddove essa punisce chi, tra le altre cose, interferisce con il funzionamento di un programma o di un sistema informatico; l'interferenza implica, quale condotta prodromica, l'accesso. È tuttavia richiesto il dolo specifico per l'integrazione del reato: il soggetto deve agire al fine di procurare, a sé o ad altri, un ingiusto profitto. Sicché il mero accesso abusivo ad un sistema informatico o telematico non costituisce di per sé condotta penalmente perseguibile.

La successiva fattispecie italiana di "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*" (art. 615-*quater*) non trova alcun corrispettivo nella disciplina sammarinese. Tale previsione potrebbe essere accorpata a quella di cui all'art. 615-*ter*, in quanto condotta ad essa prodromica. La norma si preoccupa di tutelare il corretto funzionamento delle tecnologie informatiche, al pari del successivo art. 615-*quinquies* che attiene alla diffusione di programmi diretti a danneggiare o interrompere un sistema informatico. Quest'ultimo delitto presenta una qualche assonanza con l'art. 403 del codice penale sammarinese, nella misura in cui punisce chiunque «*produce, riceve, detiene o in altra maniera ottiene, acquista, vende o cede fraudolentemente ad altri: – strumenti, articoli, programmi informatici o altri mezzi appositamente allestiti per commettere i misfatti di cui agli articoli 204 bis, 204 ter o comunque atti, per la loro natura, alla contraffazione o all'alterazione*».

La riservatezza delle comunicazioni informatiche rispetto all'indebita captazione o rivelazione è tutelata mediante la fattispecie di cui all'art. 617-*quater*, *"Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche"*. Il codice penale di San Marino non conosce attualmente alcuna fattispecie similare. Considerato il bene giuridico che la norma si preoccupa di salvaguardare e la sovrapponibilità delle condotte tipiche, in un'ottica di redazione della fattispecie, si potrebbe pensare all'assorbimento della presente figura di reato nella già affrontata ipotesi di "*Accesso abusivo ad un sistema informatico o telematico"*. Si tratterebbe di una scelta coerente la relazione di stretta interdipendenza cronologica e fattuale dei due reati: l'art. 617-*quater* può essere configurato come una mera progressione della condotta criminosa, aggravata del precedente accesso abusivo.

Mancano completamente sanzioni per chi installa apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies*) o per chi falsifica, altera o sopprime il contenuto di comunicazioni informatiche o telematiche (art. 617-*sexies*).

Il *"Danneggiamento di informazioni, dati e programmi informatici"* di cui all'art. 635-*bis* non sembra potersi ascrivere entro l'area della vigente disciplina sammarinese di danneggiamento (art. 203 primo periodo), che punisce chiunque distrugga, disperda o danneggi in qualsiasi modo la cosa altrui. Quest'ultima può, infatti, essere rappresentata sia da un bene mobile, sia da un immobile legittimamente posseduto o detenuto. L'estensione allo strumento informatico rappresenta un'operazione ermeneutica sostanzialmente analogica *in malam partem* e pertanto da evitare.

Il successivo articolo 635-*ter* punisce chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici utilizzati dallo Stato, da altro ente pubblico, ad essi pertinenti o comunque di pubblica utilità. Appare chiaro che si è in presenza di un reato aggravato dall'evento che mira a tutelare il corretto funzionamento dei sistemi informatici dell'amministrazione statale. Anche per questa seconda tipologia di reato l'attuale codice penale sammarinese risulta deficitario, nell'impossibilità di forzare il dato letterale fino a ricomprendere i sistemi informatici o telematici, entro l'area semantica "beni pubblici o destinati all'uso pubblico" di cui all'art. 203, comma II, se non con esiti sostanzialmente creativi preclusi all'interprete.

Ulteriore fattispecie di danneggiamento è quella prevista dall'art. 635-*quater* il cui oggetto materiale non consiste più nei dati o nelle informazioni (come avviene per il 635-*bis*), bensì nei sistemi informatici o telematici. Si è in questo modo notevolmente ampliato il ventaglio delle condotte astrattamente perseguibili, essendo sufficiente la prova della mera alterazione, seppur grave, del sistema. Anche in questo caso sarà necessaria l'introduzione di una fattispecie *ad hoc* per l'ordinamento sammarinese, che non prevede alcuna forma di protezione nei confronti di aggressioni di tal genere.

Il rafforzamento delle tutele avverso le forme di danneggiamento informatico si completa con la previsione di cui all'art. 635-*quinquies*, *danneggiamento di sistemi informatici o telematici di pubblica utilità*, introdotto con la legge del 2008. La fattispecie si concretizza qualora si renda inservibile o si ostacoli il funzionamento dei suddetti sistemi: anche in questo caso il codice penale sammarinese dovrà essere aggiornato con un'apposita norma che la contempli.

Schema riepilogativo

CONVENZIONE DI BUDAPEST	DISCIPLINA PENALE ITALIANA	DISCIPLINA PENALE SAMMARINESE
TITOLO I REATI CONTRO LA RISERVATEZZA, L'INTEGRITA' E LA DISPONIBILITÀ DEI DATI E DEI SISTEMI INFORMATICI	Art. 615-*ter* **Accesso abusivo ad un sistema informatico o telematico**	Art. 204-*ter* **Frodi informatiche** Nella misura in cui si punisce chi, tra le altre cose, "*interferisce con il funzionamento di un programma o di un sistema informatico*" poiché l'interferenza implica quale condotta prodromica l'accesso, la quale, tuttavia non rientra nell'area della fattispecie, dato che essa richiede la sussistenza del fine di procurare a se o ad altri un ingiusto profitto. **TUTELA INSODDISFACENTE**
	Art. 615-*quater* **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici** (fattispecie che, nell'ottica di introduzione nel codice penale sammarinese potrebbe essere accorpata a quella di cui all'Art. 615-*ter*, in quanto condotta ad essa prodromica)	**NORMATIVA CARENTE**
	Art. 615-*quinquies* **Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico**	Art. 403 **Fabbricazione, detenzione, acquisto, alienazione di strumenti o materiali di contraffazione** [introdotto con legge n.102 del 23 luglio 2013 "Disposizioni penali contro le frodi e le falsificazioni"], nella misura in cui punisce chiunque «*produce, riceve, detiene o in altra maniera ottiene, acquista,* ***vende*** *o* ***cede*** *fraudolentemente ad altri: - strumenti, articoli,* ***programmi informatici*** *o altri mezzi* ***appositamente allestiti per commettere i misfatti di cui agli articoli*** *204 bis,* ***204 ter (****..) o comunque atti, per la loro natura, alla contraffazione o all'alterazione*».

	Art. 617-*quater* **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche** (Fattispecie che nell'ottica di riformulazione potrà essere riassorbita nell'art. 615-*ter*)	**NORMATIVA CARENTE**
	Art. 617-*quinquies* **Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche**	**NORMATIVA CARENTE**
	Art. 617-*sexies* **Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche**	**NORMATIVA CARENTE**
	Art. 635-*bis* **Danneggiamento di informazioni, dati e programmi informatici**	Art. 203 **Danneggiamento** "*Chiunque distrugge, disperde o danneggia in qualsiasi modo la cosa altrui..*" La **cosa** (oggetto del reato) può essere rappresentata sia da un bene mobile che immobile legittimamente posseduto o detenuto. Tuttavia, l'estensione allo strumento informatico rappresenta un'operazione ermeneutica sostanzialmente analogica *in malam partem* e pertanto da evitare. **NORMATIVA CARENTE**
	Art. 635-*ter* **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità**	**NORMATIVA CARENTE**
	Art. 635-*quater* **Danneggiamento di sistemi informatici e telematici**	**NORMATIVA CARENTE**
	Art. 635-*quinquies* **Danneggiamento di sistemi informatici o telematici di pubblica utilità**	**NORMATIVA CARENTE**

TITOLO II REATI INFORMATICI CONNESSI	Art. 491-*bis* **Documenti informatici**	**NORMATIVA CARENTE (artt. 295 – 302)**
	Art. 495-*bis* **Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri** [D. lgs. 7 marzo 2005, n. 82 (codice dell'amministrazione pubblica digitale)]	L. 20 luglio 2005, n. 115 (legge sul documento informatico e la firma elettronica)
	Art. 640-*bis* **Frode informatica** "*Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a se o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 516 a euro 1032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1549 se ricorre una delle circostanze previste dal n.1 del secondo comma dell'Art. 640 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. […]*"	Art. 204-*ter* cp **Frodi informatiche** "*1. È punito con la prigionia di secondo grado chiunque, senza autorizzazione, al fine di procurare a sé o ad altri un ingiusto profitto, introduce, altera, sopprime dati elettronici, o comunque interferisce con il funzionamento di un programma o di un sistema informatico.* *2. Si applica la prigionia di terzo grado qualora la frode informatica abbia cagionato un danno di rilevante gravità.* *3. Si applica la prigionia di quarto grado qualora la condotta fraudolenta abbia prodotto un trasferimento non autorizzato di denaro o valori in danno al titolare..*".
	Art. 640-*quinquies* **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica**	**L. 20 luglio 2005, n. 115, art. 6 (responsabilità) prevede a carico del prestatore di servizi di certificazione la sola responsabilità civile nella forma del risarcimento del danno**

TITOLO III REATI RELATIVI AI CONTENUTI	Art. 600-*ter* **Pornografia minorile** Art. 600-*quater* **Detenzione di materiale pornografico** Art. 600 *quater*.1 **Pornografia virtuale**	Art. 177-*ter* **Pornografia minorile** Art. 177-*ter* **Pornografia minorile** Art. 177-*ter* co. IV, **Pornografia minorile** (nella misura in cui prevede l'utilizzo di sistemi telematici per la diffusione di materiale pornografico minorile)
TITOLO IV REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE E DEI DIRITTI CONNESSI	Art. 171, L. 22 aprile 1941, n. 633 Art. 171-*bis,* L. 22 aprile 1941, n. 633 Art. 171- *ter,* L. 22 aprile 1941, n. 633	Art. 202 **Usurpazione di beni immateriali** Sanzione amministrativa di cui all'art.118 della legge n.5 del 29 gennaio 1996 (depenalizzazione diritto d'autore)
TITOLO V ART. 12 RESPONSABILITÀ AZIENDALE	Art. 24-*bis*, d.lgs. 231 del 2001 **Delitti informatici e trattamento illecito di dati**	Art. 2, L. 29 luglio 2013, n. 99 Responsabilità della persona giuridica

5. Riflessioni conclusive sulla necessità di riforma del codice penale sammarinese in relazione ai beni informatici.

A conclusione di questa breve disamina, occorre considerare l'opportunità politico-criminale in ordine ad una riforma del codice penale sammarinese che aggiorni il catalogo dei beni giuridici penalmente tutelati in relazione ai reati informatici.

Si è soliti distinguere all'interno di questa categoria quattro macroaree di tutela:

1. i reati che tutelano la riservatezza dei dati informatici e delle comunicazioni elettroniche;
2. i reati che tutelano l'integrità dei dati e dei sistemi informatici;
3. i reati che proteggono la veridicità dei dati informatici;

4. i reati ad alta tecnologia, ossia quei reati che vengono commessi mediante l'utilizzo dello strumento informatico o telematico: si pensi alla frode informatica, al riciclaggio di capitali, al terrorismo via internet.

La ratifica della Convenzione di Budapest focalizza l'attenzione su ciascuno di questi beni giuridici; essa rappresenta un passaggio irrinunciabile nella prospettiva di contrasto del *cybercrime*, quale fenomeno che supera la dimensione statuale e richiede, di conseguenza, il coordinamento dell'azione a livello internazionale. Tale obiettivo può essere conseguito soltanto attraverso l'armonizzazione delle legislazioni statali preesistenti.

L'importanza del *domicilio informatico* quale bene giuridico oggetto di tutela penale emerge dalla lettura dei precedenti paragrafi, in particolare in relazione alle fattispecie di accesso abusivo italiane. Allo stesso modo, il paragrafo introduttivo segnala l'opportunità di sanzionare penalmente i reati ad alta tecnologia.

Qualche parola in più occorre spendere in relazione alla *riservatezza* e *all'integrità dei dati*, quali interessi tra loro connessi, come si evince sia dalla normativa europea e italiana di recepimento, sia a livello della giurisprudenza delle Corti sovranazionali. La Repubblica di San Marino ha aderito alla Convenzione europea dei diritti dell'uomo ed è quindi tenuta ad attuare i diritti fondamentali, che la Corte europea dei diritto dell'uomo provvede progressivamente ad attualizzare. D'altro canto, sebbene l'Unione europea non annoveri San Marino tra i suoi Stati membri, la sua politica di contrasto della criminalità informatica può essere richiamata per due ordini di ragioni: in primo luogo, per la dimensione transazionale dei reati informatici di cui sopra si è detto. In secondo luogo, dal punto di vista applicativo, gli stessi diritti fondamentali di cui è paladina la Corte europea dei diritti dell'uomo costituiscono gli interessi e le finalità sottese ad una determinata disciplina comunitaria: si pensi alla nozione di riservatezza. Sicché, nelle sue pronunce, la Corte del Lussemburgo è solita mutuare le accezioni di questi diritti-principi, secondo le coordinate individuate dalla Corte di Strasburgo.

La nozione di *sicurezza informatica* contenuta nella proposta di direttiva n. 48/2013 tenta di fare chiarezza in merito alle implicazioni penalistiche e di politica criminale che si celano dietro questa etichetta scarsamente rappresentativa di contenuto. Nell'ottica del legislatore sovraordinato, la sicurezza assurge ormai a bene giuridico meritevole di tutela, in quanto interesse strategico per gli stati. Essa è intesa come «*la* ***capacità*** *di una rete o di un sistema informativo* ***di resistere****, a un determinato livello di riservatezza, a eventi imprevisti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei relativi servizi*

offerti o accessibili tramite tale rete o sistema informativo» (art. 3, n. 2, prop. Dir. 48/2013). In sostanza, il grado di sicurezza si valuta in base alla capacità di resistenza agli attacchi esterni (c.d. resilienza), con il limite del rispetto della riservatezza. La rete non è sicura, quando eventi dolosi o imprevisti compromettono la *disponibilità*, *l'autenticità*, *l'integrità* e la *riservatezza* dei dati (art. 3, n. 2). Ciò vuol dire che la sicurezza informatica comprende in sé: 1) sia la potenziale compromissione della riservatezza, come esposizione dei dati a rischi di una loro apprensione ad opera di terzi; 2) sia la semplice perdita di disponibilità dei dati da parte del suo titolare, fino alla compromissione della loro autenticità e integrità.

Questo passaggio è particolarmente delicato e l'elaborazione della prassi aiuta a comprendere i rapporti tra riservatezza e integrità dei dati. La giurisprudenza sovranazionale ha infatti ampliato le latitudini applicative di questo diritto fondamentale riconducibile agli artt. 7 (vita personale e familiare) e 8 (protezione dei dati personali) della Carta di Nizza e all'art. 8 (diritto al rispetto della vita privata e familiare) della CEDU. Il diritto fondamentale alla riservatezza traslato sulla dimensione digitale è stato declinato, in un primo momento, come 'diritto di essere lasciati soli', ossia nella preservazione di una sfera 'intima' del soggetto, inaccessibile alle intrusioni esterne. Con lo sviluppo delle tecnologie informatiche, in particolare con la diffusione degli strumenti di monitoraggio dei dati di navigazione che consentono di creare profili piuttosto definiti per ciascun utente, alla riservatezza della vita privata si sovrappone il profilo relativo alla protezione dell'integrità, autenticità e soprattutto disponibilità dei dati personali. Questi ultimi divengono proiezione, nella realtà virtuale, di porzioni della personalità reale. Basti pensare alla frequenza con la quale sul *web* vengono richiesti, per l'accesso alla rete, per compiere determinate attività o operazioni, informazioni e dati personali dei quali l'utente è destinato a perdere il controllo non appena li trasmette: egli, pur avvertito dall'informativa sulla privacy, non è in grado di controllare il posizionamento in rete e la sorte effettiva di tali dati presso i terzi. Fin dalla pronuncia della Corte costituzionale tedesca del 2008, sul monitoraggio indiscriminato, sono stati evidenziati i legami tra garanzia di integrità della rete e la c.d. autodeterminazione informativa[14]. Essa consiste nel diritto ad essere informati e decidere consapevolmente in merito alla raccolta, gestione ed utilizzo, da parte di terzi, dei propri dati personali: rientra perciò nell'ambito della riservatezza. La Corte, ancorando

[14] Corte costituzionale tedesca, 27 febbraio 2008, BvR 370/07.

la propria valutazione al principio di proporzionalità, ha ritenuto che il monitoraggio indiscriminato dell'attività degli utenti sulla rete costituisca una misura eccessiva e troppo invasiva della sfera personale perfino rispetto ai fini di contrasto e prevenzione del crimine e del terrorismo internazionale.

Ancor più drastica è la situazione nel caso in cui le informazioni vengano pubblicate sul *web*: l'utente perde la disponibilità del dato, che, a quel punto, è potenzialmente suscettibile di apprensione da parte di qualsiasi utente abbia accesso alla fonte in cui è pubblicato. A questo proposito, la Corte di Giustizia ha di recente incluso nella tutela della riservatezza informatica, il c.d. diritto all'oblio, ossia la pretesa del cittadino di rimozione dalla rete delle informazioni ritenute dannose per la sua reputazione o comunque pregiudizievoli, in mancanza di un interesse di natura pubblica all'accesso generalizzato [15]. In sostanza, la deindicizzazione dei *link* di ricerca sarebbe necessaria quando i dati relativi alla persona non si presentano più adeguati all'identità virtuale nella propria attualità.

Di queste evoluzioni della prassi occorre ormai tenere conto, da quando la giurisprudenza delle Corti sovranazionali è divenuta, nei fatti, vera e propria fonte di diritto penale: in particolare, le interpretazioni adeguatrici della Corte EDU con la forza propulsiva dei diritti fondamentali sono capaci di penetrare nel tessuto normativo ed innovare il dettato legislativo per via esegetica.

La particolare attenzione alla riservatezza dei dati ed alla loro integrità emersa a livello giurisprudenziale costituisce un indizio ulteriore in ordine all'opzione politico-criminale a favore dell'introduzione nel codice penale sammarinese di un catalogo di reati informatici a tutela di questi diritti fondamentali di nuova generazione.

****

Poste tali premesse metodologiche e sistematiche, è ora disponibile il contesto politico-criminale e comparatistico in cui l'aggiornamento del diritto penale dell'informatica nel codice penale sammarinese può utilmente svolgersi.

[15] CoGUE, sentenza 13 maggio 2014, Google Spain SL, Google Inc. contro Agencia Espanola de Proteccion de Datos (AEPD), Marco Costeja Gonzále.