Rapporto e avamprogetti relativi alla modifica del Codice penale svizzero e del Codice penale militare

concernente

la responsabilità penale dei provider e le competenze della Confederazione per il perseguimento di reati commessi mediante reti di comunicazione elettronica (criminalità in rete)

Berna, ottobre 2004

Compendio **3**

1. Situazione attuale **4**
1.1 Commissione peritale "Criminalità in rete" **4**
1.2 Gruppo di lavoro "Genesis" **5**

2. Responsabilità penale dei provider (avamprogetto A) **7**
2.1 Commissione peritale "Criminalità in rete" **7**
2.11 Responsabilità penale dei provider 8
2.12 Competenza federale per il perseguimento penale 8
2.13 Proposte per altri ambiti giuridici 9
2.2 Parere e proposta del Consiglio federale **9**
2.21 Responsabilità penale dei provider 9
2.22 Misure fiancheggiatrici 11
2.221 Diritto civile 11
2.222 Diritto amministrativo 12
2.223 Altre misure legislative 12
2.3 Commento delle singole disposizioni **13**
2.31 Codice penale 13
2.311 Completamento del titolo marginale nella 6ª sezione del Titolo secondo del Codice penale 14
2.312 Responsabilità penale dei provider 14
2.32 Codice penale militare 19
2.4 Avamprogetto A **20**
2.41 Codice penale svizzero 20
2.42 Codice penale militare 22

3. Competenze della Confederazione in caso di reati commessi mediante reti di comunicazione elettronica (avamprogetto B) **24**
3.1 Proposte del gruppo di lavoro "Genesis" **24**
3.11 Perseguimento penale in caso di reati commessi mediante reti di comunicazione elettronica 24
3.12 Analisi dell'operazione "Genesis" 24
3.13 Non spetta alla Confederazione perseguire la criminalità in rete 25
3.14 Modello proposto 25
3.15 Variante 1 (competenza d'indagine dell'MPC ai sensi dell'articolo 259 della legge federale del 15 giugno 1934 sulla procedura penale [PP], basata su un'alta vigilanza della Confederazione) 26
3.16 Variante 2 (competenza d'indagine dell'autorità federale competente) 26
3.17 Misure fiancheggiatrici 27
3.2 Parere e proposta del Consiglio federale **27**
3.21 Non spetta alla Confederazione perseguire la criminalità in rete 27
3.22 Competenze d'indagine delle autorità federali 28
3.23 Misure fiancheggiatrici 29
3.3 Commento dell'articolo 344 AP-CP (Competenze della Confederazione in caso di reati commessi mediante reti di comunicazione elettronica) **30**
3.31 Collocazione sistematica e titolo marginale del nuovo articolo 344 AP-CP 30
3.32 Capoverso 1 30
3.33 Capoverso 2 31
3.4 Codice penale militare **31**
3.5 Avamprogetto B Codice penale svizzero **32**

Compendio

Il rapido sviluppo delle tecnologie dell'informazione e delle reti informatiche quali Internet o la telefonia mobile ha condizionato più di ogni altra cosa la vita e il modo di comunicare delle persone negli ultimi anni. Oggi un utente può richiamare informazioni provenienti da ogni parte del mondo operando da qualsiasi postazione in rete. Il rovescio della medaglia è costituito dal fatto che le reti di comunicazione elettronica permettono di commettere reati restando appostati in qualsiasi luogo del pianeta. La cosiddetta criminalità in rete è in costante aumento e il Codice penale e il Codice penale militare in vigore (CP/CPM) non offrono sempre risposte chiare in merito alla responsabilità penale dei provider, vale a dire dei vari fornitori di servizi coinvolti nella commissione di tali reati a motivo dell'infrastruttura tecnica che mettono a disposizione. Esistono tre tipi di provider: il fornitore di contenuti o content provider carica su Internet i contenuti propri o ricevuti da terzi; l'hosting provider mette a disposizione dei propri clienti, i fornitori di contenuti, uno spazio di memoria sul quale questi possono proporre i loro contenuti; il fornitore di accesso o access provider offre agli utenti o user lo strumentario tecnico per accedere a Internet.

La criminalità in rete, forte del suo impatto globale, pone il perseguimento penale di fronte a nuove sfide. La competenza delle autorità inquirenti dei Cantoni è fortemente limitata nel caso di inchieste complesse, specie di quelle relative a reati informatici transfrontalieri. Non di rado mancano infatti criminalisti specializzati e l'attrezzatura del caso. Inoltre, all'inizio delle indagini, spesso non è ancora nota l'autorità inquirente cantonale competente. È indispensabile migliorare le condizioni quadro della collaborazione tra Confederazione e Cantoni per tenere il passo nella lotta a questa moderna forma di criminalità.

Il Consiglio federale appoggia la presente revisione del Codice penale e del Codice penale militare, volta a disciplinare la responsabilità penale dei provider e a rendere più efficace il perseguimento penale dei reati commessi in rete migliorando le condizioni quadro della cooperazione tra la Confederazione e i Cantoni. Il progetto è annunciato nelle linee direttive del programma di legislatura 2003-2007 (FF 2004 1006).

Il Consiglio federale ha steso un rapporto con due avamprogetti per permettere una formazione differenziata della volontà politica. L'avamprogetto A verte sulla responsabilità penale dei provider, l'avamprogetto B sulle competenze della Confederazione per il perseguimento di reati commessi mediante reti di comunicazione elettronica.

1. Situazione attuale

1.1 Commissione peritale "Criminalità in rete"

Nell'estate del 1998, l'allora Polizia federale appurò che in Internet continuavano a circolare liberamente contenuti a sfondo razzista, sebbene in Svizzera fossero stati oggetto di condanne per violazione dell'articolo 261bis CP. La Polizia federale indirizzò quindi una circolare agli offerenti svizzeri di prestazioni Internet (*Internet Service Provider*, ISP), invitandoli a vagliare la possibilità di bloccare l'accesso alle pagine incriminate. Tale intervento suscitò una certa agitazione tra i provider e sfociò nella creazione di un gruppo di contatto composto da rappresentanti degli organi federali interessati e dei provider.

Poiché in seno al gruppo di contatto non fu possibile chiarire la questione della responsabilità penale dei provider per contenuti illeciti, l'Ufficio federale di giustizia (UFG) fu incaricato di elaborare una perizia in materia. Nella sua perizia del 24 dicembre 1999[1], l'UFG confermò il principio della responsabilità sussidiaria ai sensi del diritto penale dei media anche per un semplice fornitore di accesso, a condizione che un'autorità inquirente lo avesse chiaramente reso attento dei contenuti illeciti. In caso di inapplicabilità del diritto penale dei media, i provider potevano comunque essere puniti in quanto complici del reato principale.

Non condividendo quanto emerso dalla perizia dell'UFG, i provider incaricarono i professori di diritto penale Niggli, Riklin e Stratenwerth di esaminare a loro volta la questione della responsabilità. L'esito della loro perizia dell'ottobre 2000[2] smentì le conclusioni a cui era giunta la perizia dell'UFG. I tre professori giudicarono tuttavia poco chiara la situazione giuridica e sottolinearono la necessità di legiferare.

Il 14 dicembre 2000, il consigliere agli Stati Thomas Pfisterer presentò una mozione mirante a impedire gli abusi di Internet e a prevedere una sanzione penale per la criminalità in Internet (Mozione 00.3714)[3]. A tale scopo il Consiglio federale veniva invitato a creare, nell'ambito del diritto penale o di eventuali altre singole disposizioni, una regolamentazione che favorisse la certezza del diritto. Nella motivazione l'autore della mozione raccomandò di ispirarsi alla direttiva dell'Unione europea (UE) sul commercio elettronico[4], formulando inoltre una proposta legislativa. Nel 2001 la mozione Pfisterer fu accolta dai due rami del Parlamento.

Il 22 novembre 2001, sulla base di tali sviluppi, l'allora capo del Dipartimento federale di giustizia e polizia (DFGP) istituì una commissione peritale presieduta dall'allora vicedirettore dell'UFG, dott. Peter Müller, e composta da rappresentanti del mondo giuridico, dei provider e dell'Amministrazione federale. Il suo incarico consisteva nello studiare i mezzi per impedire o punire i reati commessi mediante Internet e, in particolare, per disciplinare la responsabilità penale in Internet. La commissione peritale "Criminalità in rete" ha presentato il suo rapporto nell'estate del 2003[5].

---

1 Perizia pubblicata in GAAC 64 75.
2 Perizia riprodotta in medialex, numero speciale 1/2000.
3 Boll. Uff. **2001** S 27.
4 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico" – "Direttiva sull'*e-commerce*").
5 Rapporto della commissione peritale "Criminalità in rete", DFGP, giugno 2003.

1.2 Gruppo di lavoro "Genesis"

Nell'estate del 2002 i corpi di polizia della maggior parte dei Cantoni, in collaborazione con l'Ufficio federale di polizia (fedpol), condussero un'operazione col nome in codice "Genesis", contro la pedopornografia in Internet. Fu un'operazione organizzata su scala nazionale e di proporzioni mai viste prima in Svizzera. Il gran numero di procedimenti da avviare in parallelo e la loro distribuzione su vari Cantoni costituirono una novità per le autorità inquirenti svizzere. Per venirne a capo, la Polizia giudiziaria federale (PGF) ne assicurò il coordinamento a livello nazionale, senza però disporre né di reali possibilità d'indagine nella prima fase procedurale precedente la designazione delle autorità inquirenti competenti, né della facoltà di impartire istruzioni. Compete infatti ai Cantoni perseguire i reati di pornografia (art. 197 CP) commessi attraverso Internet o in altro modo. L'operazione "Genesis" ha evidenziato con chiarezza la necessità di legiferare in materia di cooperazione tra la Confederazione e i Cantoni nei casi sottoposti alla giurisdizione cantonale e caratterizzati da un gran numero di persone implicate in vari Cantoni.

L'operazione "Genesis" ha suscitato vivo interesse nell'opinione pubblica e nel mondo politico, ambienti già particolarmente sensibili alle questioni legate alla pedopornografia in Internet e alla criminalità in Internet in generale[6]. Il 26 settembre 2002 l'allora consigliera nazionale Regine Aeppli Wartmann presentò un'iniziativa parlamentare (02.452) chiedendo di creare una competenza della Confederazione sul modello del "Progetto efficienza" (art. 340bis CP) per perseguire la criminalità in rete[7]. L'11 dicembre 2003 il Consiglio nazionale ha dato seguito all'iniziativa.

Alla luce di tali fatti, nell'autunno 2002 il capo del DFGP incaricò fedpol di analizzare le condizioni quadro giuridiche e organizzative dell'operazione "Genesis" in vista di futuri casi simili e di elaborare proposte per migliorare la collaborazione tra la Confederazione e i Cantoni. A tale scopo fu creato il gruppo di lavoro "Genesis", composto da rappresentanti della polizia e delle autorità giudiziarie, della Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS), della Conferenza delle autorità inquirenti svizzere (CAIS) nonché di organi federali (fedpol, Ministero pubblico della Confederazione e UFG). Il gruppo di lavoro "Genesis" ha presentato il suo rapporto nel novembre del 2003[8].

Agli inizi del 2003, ossia pressappoco sei mesi dopo il via all'operazione "Genesis", è diventato operativo il Servizio di coordinamento nazionale per la lotta contro la criminalità su Internet (SCOCI). Tale servizio cofinanziato dalla Confederazione e da 25 Cantoni (tutti tranne Zurigo) è annesso a fedpol e affianca le autorità inquirenti dei

---

[6] Si vedano in materia i seguenti interventi parlamentari: Mozione Aeppli Wartmann Regine (01.3196), Miglioramento della procedura nella lotta alla criminalità su Internet; Mozione Commissione degli affari giuridici CN (01.3012), Lotta contro la pedofilia; Interpellanza Tillmanns Pierre (00.3235), Lotta contro la pedofilia; Mozione Commissione speciale 00.16-CN (00.3206), Criminalità di ampie proporzioni. Criminalità elettronica; Interpellanza Freund Jakob (00.3059), Attività illegali su Internet. Ruolo di sorveglianza della Confederazione; In. cant. Ginevra (00.314), Lotta alla pedofilia; Mozione von Felten Margrith (98.3467), Criminalità su Internet. Responsabilità dei provider; Mozione Jeanprêtre Francine (97.3487), Lotta contro la pornografia infantile su reti di dati; Postulato Commissione affari giuridici CN (96.3005), Pedopornografia su Internet.

[7] Boll. Uff. **2003** N 1967.

[8] Rapporto "Modello per un perseguimento penale efficiente in casi di criminalità in rete su scala intercantonale o internazionale", del gruppo di lavoro "Genesis", Berna, 12 novembre 2003.

Cantoni e della Confederazione nell'individuare gli abusi punibili di Internet (*monitoring*), nell'esaminare e attribuire le comunicazioni di sospetto pervenute (*clearing*) e nell'analizzare la criminalità su Internet. A prescindere dall'attività di SCOCI, restano tuttavia invariate le competenze e gli obblighi in materia d'indagine attribuiti alle autorità inquirenti, vale a dire che tali competenze spettano nella maggior parte dei casi ai Cantoni. Inoltre, SCOCI non ha alcuna facoltà di impartire istruzioni alle autorità inquirenti competenti.

2. Responsabilità penale dei provider (avamprogetto A)

2.1 Commissione peritale "Criminalità in rete"

Nel suo rapporto la commissione peritale "Criminalità in rete" illustra come il diritto penale dei media in vigore dal 1° aprile 1998 non si addica a Internet [9]. Secondo le disposizioni del diritto penale dei media (art. 27, 27bis e 322bis CP), l'atto punibile è commesso mediante pubblicazione in un mezzo di comunicazione e consumato per effetto di tale pubblicazione. In linea di principio è punibile soltanto l'autore (art. 27 cpv. 1 CP). Qualora questi non possa essere individuato o tradotto davanti a un tribunale svizzero (art. 27 cpv. 2 CP), l'articolo 322bis prevede una punibilità sussidiaria ed esclusiva del redattore responsabile o, in sua assenza, della persona responsabile della pubblicazione (cosiddetta responsabilità a cascata). L'attuale diritto penale dei media si basa su una cooperazione tra autori, redattori e altre persone responsabili della pubblicazione.

La normativa non si addice all'*hosting provider*, che di norma si limita a gestire l'infrastruttura tecnica necessaria a rendere disponibili le informazioni e non può quindi essere considerato responsabile della pubblicazione. Lo stesso vale anche per il fornitore di accesso nella misura in cui si limita a offrire un accesso a Internet.

La commissione peritale riconosce che le regole generali del Codice penale sulla reità e sulla partecipazione lasciano irrisolte numerose questioni inerenti all'*hosting provider* e al fornitore di accesso. La descrizione dell'atto materiale nella relativa disposizione penale determina se l'*hosting provider* è autore o soltanto complice del reato in questione. Nelle fattispecie riguardanti Internet, la linea che separa il ruolo di autore da quello di complice non è molto nitida. Secondo l'articolo 197 numero 1 CP, l'*hosting provider* potrebbe ad esempio rendersi autore di un reato per il solo fatto di rendere accessibili scritti pornografici a persone minori di sedici anni. Tuttavia, l'*hosting provider* si limita generalmente a mettere a disposizione dei suoi clienti uno spazio di memoria sul suo elaboratore, per cui molto spesso è all'oscuro del tipo di informazioni memorizzate sul suo computer. Può venirlo a sapere soltanto se gli perviene una segnalazione specifica o se effettua egli stesso controlli preventivi.

Infine, stando a una decisione del Tribunale federale del 1999[10], non tutti gli atti che possono essere pubblicati nei media e si consumano attraverso tale pubblicazione costituiscono un reato mediatico. Il Tribunale federale rileva esplicitamente che la rappresentazione di atti di cruda violenza (art. 135 CP), la pornografia dura (art. 197 n. 3 CP) e la negazione di genocidio (in particolare per quel che concerne il caso di Auschwitz, art. 261bis cpv. 4 CP) non costituiscono reati mediatici. Il Tribunale federale ha motivato la sua decisione specificando in sostanza come il legislatore mirasse a impedire la pubblicazione dei contenuti illegali e non intendesse certo accordare una posizione privilegiata a un determinato gruppo di soggetti coinvolti nella commissione del reato ai sensi del diritto penale dei media (art. 27 CP). Inoltre la ratifica della Convenzione internazionale contro la discriminazione razziale[11] impone alla Svizzera l'obbligo di diritto internazionale di perseguire, senza eccezione, ogni diffusione di affermazioni a sfondo razzista. La dottrina ha comunque riservato molte critiche a

[9] Rapporto della commissione peritale "Criminalità in rete", op. cit., pag. 59 segg.; 65 seg.
[10] DTF **125** IV 206 segg.
[11] FF **1992** III 217.

tale decisione[12], ma la commissione peritale è del parere che la situazione poco chiara sul piano della dottrina e della giurisprudenza dimostra la necessità di disciplinare la responsabilità penale dei provider coinvolti nella criminalità in rete.

Il rapporto peritale verte su due tematiche (cfr. *infra* n. 2.11 e 2.12) trasposte in proposte; la commissione ha inoltre fornito spunti per altri ambiti giuridici (cfr. n. 2.13).

2.11 Responsabilità penale dei provider

La commissione peritale propone di completare il Codice penale inserendo una nuova normativa speciale relativa alla responsabilità penale dei provider (nuovi art. 27 e 322bis AP-CP), in sintonia con certe disposizioni estere tese ad attuare la direttiva dell'Unione europea sul commercio elettronico. La nuova normativa sancisce in sostanza il principio secondo cui le disposizioni generali del Codice penale in materia di reità e di complicità si applicano ai provider che partecipano attivamente alla commissione di reati. Il provider è però esente da pena se si limita a offrire accesso automatico a Internet, mentre è punibile se non interviene per impedire l'accesso a un contenuto illecito di cui viene a sapere o si accorge soltanto in un secondo tempo[13].

2.12 Competenza federale per il perseguimento penale

Oltre a SCOCI (cfr. *supra* n. 1.2), gestito dall'inizio del 2003 dalla Confederazione in collaborazione con i Cantoni, la commissione peritale propone la competenza della Confederazione per determinati casi, sul modello del Progetto efficienza[14] (art. 340bis CP). Tale competenza federale entrerebbe in gioco segnatamente qualora il reato commesso mediante reti di comunicazione elettronica sia stato perpetrato in più Cantoni e non abbia un riferimento prevalente in uno di essi, o qualora si riveli necessario un coordinamento delle indagini in più Cantoni. Il Ministero pubblico della Confederazione (MPC) deve inoltre avere la facoltà di aprire un'indagine e in tal modo fondare la giurisdizione federale qualora un'autorità cantonale competente solleciti la ripresa della procedura.

Questa proposta della commissione peritale prende spunto dall'iniziativa parlamentare Aeppli Wartmann (cfr. *supra* n. 1.2).

---

[12] Franz Riklin, *Kaskadenhaftung – quo vadis*? Medialex 2000, 208; Franz Riklin/Günter Stratenwerth, *diritto penale dei media/Kaskadenhaftung*, in: Niggli/Riklin/Stratenwerth (ed.), *Die strafrechtliche Verantwortlichkeit von Internet-Providern*, medialex edizione speciale 2000, pag. 13 segg.; Dorrit Schleiminger/Christoph Mettler, *Strafbarkeit der Medienverantwortlichen im Falle der Rassendiskriminierung*, art. 27, art. 261bis cpv. 4 CP, osservazioni alla DTF **125** IV 206 segg., AJP 2000, pag. 1039 segg.; Jörg Rehberg/ Andreas Donatsch, *Strafrecht, Verbrechenslehre*, 7^{a} edizione, Zurigo 2001, pag. 166; Christian Schwarzenegger, E-*Commerce – Die strafrechtliche Dimension*, in: Arter/Jörg (ed.), *Internet-Recht und Electronic Commerce Law*, Lachen e S. Gallo 2001, pag. 349 segg.; Franz Riklin, *Strafrecht, Allgemeiner Teil*, 2^{a} edizione, Zurigo 2002, pag. 245; Franz Zeller, in: Niggli/Wiprächtiger, *Basler Kommentar*, CP I, Basilea 2003, ad art. 27, n. 32.

[13] Rapporto della commissione peritale "Criminalità in rete", op. cit., pag. 90 segg.

[14] Lo scopo del Progetto efficienza è di migliorare l'efficienza e la legalità costituzionale nel perseguire tutti i reati commessi prevalentemente all'estero o in più Cantoni (FF **1998** 1529); in vigore dal 1° gennaio 2002; (RU **2001** 3071 3076).

2.13 Proposte per altri ambiti giuridici

Per la commissione peritale è anche concepibile adottare, tra l'altro, nuove misure di diritto amministrativo in aggiunta al diritto penale, al fine di prevenire la commissione di reati in reti di comunicazione elettronica. Ricorda però che simili misure collidono sovente con vincoli di ordine costituzionale, in particolare con il diritto fondamentale alla libera comunicazione e il principio della proporzionalità degli interventi delle autorità.

La commissione peritale ritiene inoltre auspicabile chiarire sul piano legislativo determinate questioni legate alla responsabilità civile nell'ambito della criminalità in rete.

La commissione peritale commenta inoltre altre procedure legislative in corso all'epoca in materia di criminalità in rete, fornendo raccomandazioni in merito[15].

2.2 Parere e proposta del Consiglio federale

È indubbio che il rapido sviluppo delle tecnologie dell'informazione e delle reti informatiche si ripercuota pure sull'attività criminale. Da un lato i nuovi mezzi tecnici agevolano la commissione di reati "classici", quali diffamazione, rappresentazione di atti di cruda violenza, pornografia o discriminazione razziale. Dall'altro la tecnologia e le reti informatiche danno adito a nuove forme di criminalità quali l'acquisizione illecita di dati o il danneggiamento di dati per mezzo di virus informatici.

Combattere e perseguire con efficacia la criminalità in rete, come chiesto dagli interventi parlamentari citati in precedenza (in particolare la mozione Pfisterer e l'iniziativa parlamentare Aeppli Wartmann; cfr. *supra* n. 1.1 e 1.2), è altresì una linea direttiva del programma di legislatura 2003-2007. Il Consiglio federale intende infatti esaminare le norme legali allo scopo di introdurre competenze d'indagine a livello federale e di determinare la responsabilità penale dei provider.

La revisione del Codice penale ordinario comporta tradizionalmente la modifica del Codice penale militare qualora la medesima disposizione figuri in entrambe le leggi.

2.21 Responsabilità penale dei provider

Il diritto penale vigente non disciplina esplicitamente la responsabilità dei provider per contenuti illegali in Internet. In ragione del parallelismo[16] con il diritto penale dei media, occorreva innanzitutto chiarire se anche le fattispecie relative alla criminalità in rete fossero rette dagli articoli 27 e 322bis CP e dall'articolo 26*a* CPM o se andassero giudicate secondo le regole generali del Codice penale o del Codice penale militare, in particolare quelle in materia di complicità (art. 25 CP e art. 23 CPM).

[15] Rapporto della commissione peritale "Criminalità in rete", op. cit., pag. 136 segg.

[16] Anche i reati informatici vertono sulla pubblicazione (preparazione), la diffusione e il consumo (utilizzo) di informazioni. Inoltre numerose persone sono coinvolte nella pubblicazione e nella diffusione.

Analizzate le possibilità offerte dal diritto penale in vigore e considerate la dottrina esistente nonché la giurisprudenza del Tribunale federale, la commissione peritale giunge alla conclusione che, nei casi di criminalità in rete, l'applicabilità del diritto penale dei media e delle disposizioni generali in materia di complicità è controversa. Alla luce dell'auspicata certezza del diritto, la commissione peritale ritiene pertanto necessario legiferare anche in questo ambito.

Il Consiglio federale condivide il giudizio della commissione peritale e propone di disciplinare in termini espliciti la responsabilità penale dei provider nel Codice penale e nel Codice penale militare.

La normativa ripresa dalla commissione peritale prevede che i provider siano per principio punibili, ai sensi delle disposizioni generali del Codice penale e del Codice penale militare in materia di reità e di complicità, per i contenuti illegali circolanti nella rete di comunicazione elettronica. Il fornitore di contenuti, che carica su Internet i contenuti propri o ricevuti da terzi, è punibile come autore dei contenuti illegali a lui riconducibili. Il fornitore di accesso è punibile come correo, istigatore o complice nella misura in cui partecipa attivamente ai reati commessi dal fornitore di contenuti e non si limita a offrire accesso automatico a Internet. L'*hosting provider* è punibile qualora, sin dall'inizio, sia a conoscenza del fatto che il fornitore di contenuti intende sfruttare lo spazio di memoria concessogli per caricare informazioni illegali.

Tuttavia, la nuova normativa prevede le seguenti riserve a tale punibilità di principio dei provider:

- si applicano l'articolo 27 CP o 26*a* CPM (nuovi art. 27bis AP-CP e 26*b* AP-CPM) se il fornitore di contenuti è un autore o un redattore ai sensi del vigente diritto penale dei media, ossia se commette un reato in una pubblicazione *on line*, ad esempio in un quotidiano pubblicato su Internet;

- l'*hosting provider* è esente da pena se, nel momento in cui mette lo spazio di memoria a disposizione del fornitore di contenuti, non è a conoscenza del tipo di informazioni che questo intende inserire e inserirà in rete. L'*hosting provider* è tuttavia punibile se, una volta venuto a sapere o preso atto del carattere illegale dei dati memorizzati sul suo server, non interviene per impedirne l'utilizzo, sebbene ne abbia i mezzi tecnici e lo si possa ragionevolmente pretendere. L'*hosting provider* è pure punibile se omette di informare le autorità inquirenti dei contenuti illegali portati a sua conoscenza o ricevuti da terzi. Sono equiparati all'*hosting provider* i fornitori di motori di ricerca automatica quali google.com, altavista.com, ecc.;

- non è punibile il fornitore di accesso che si limita a offrire accesso automatico a Internet. Tale impunità è riconducibile alla natura prettamente tecnica della fornitura di accesso. Non è punita nemmeno la memorizzazione temporanea generata automaticamente in seguito all'interrogazione da parte di un utente.

L'aspetto fondamentale di tale disposizione consiste nel fatto che la punibilità o l'impunità non è determinata soltanto dalla natura del provider, ma anche dalla funzione svolta nello specifico atto di comunicazione. Il mero fatto di essere ad esempio un fornitore di accesso non costituisce necessariamente un motivo di esenzione dalla pena.

La nuova normativa si basa sulle disposizioni vigenti del Codice penale e del Codice penale militare. L'entrata in vigore della modifica del 13 dicembre 2002 del Codice penale svizzero (FF *2002* 7352; Disposizioni generali, Dell'attuazione e dell'applicazione del Codice penale) e della modifica del 21 marzo 2003 del Codice penale militare (FF *2003* 2438) comporta naturalmente la rinumerazione degli articoli. I nuovi articoli 27, 27bis e 27ter AP-CP diventeranno gli articoli 28, 28*a* e 28*b* nCP, mentre i nuovi articoli 26*a*, 26*b* e 26*c* AP-CPM diventeranno gli articoli 27, 27*a* e 27*b* nCPM.

Alla luce dei risultati della consultazione concernente la revisione, nel frattempo sospesa, della legge federale sulle lotterie e le scommesse, il Consiglio federale è altresì convinto che la responsabilità penale dei provider vada disciplinata nel Codice penale e nel Codice penale militare, e non in una legge federale distinta. I partecipanti alla consultazione hanno respinto in modo inequivocabile la disposizione penale inserita nell'avamprogetto della nuova legge sulle lotterie, finalizzata a punire i provider fornitori di giochi vietati con la detenzione fino a un anno o con una multa fino a un milione di franchi, in casi gravi addirittura con la reclusione fino a cinque anni o la detenzione non inferiore a un anno. Gli interpellati si sono piuttosto detti favorevoli all'idea di definire la questione della responsabilità penale dei provider nel Codice penale, come proposto dalla commissione peritale "Criminalità in rete".

Con la presente revisione del Codice penale e del Codice penale militare, il Consiglio federale propone una soluzione legale differenziata, che tiene conto delle peculiarità tecniche di Internet e si ispira alle disposizioni in materia adottate da altri Paesi, in particolare da quelli limitrofi. Una di queste è la direttiva UE sul commercio elettronico, che si prefigge di creare un quadro giuridico teso ad assicurare la libera circolazione dei servizi della società dell'informazione. La revisione del Codice penale e del Codice penale militare concretizza quanto chiesto dalla mozione Pfisterer, introducendo una regolamentazione praticabile, improntata alla certezza del diritto e in sintonia con il diritto degli Stati limitrofi. Il metodo proposto per determinare la responsabilità penale rispecchia le variegate funzioni svolte dai *provider* in Internet.

2.22 Misure fiancheggiatrici

Oltre a tale normativa penale, il Consiglio federale ha esaminato pure le seguenti misure fiancheggiatrici di natura amministrativa o civile.

2.221 Diritto civile

La commissione peritale "Criminalità in rete" giudica lacunosa e poco chiara la situazione normativa svizzera in materia di responsabilità civile degli *hosting provider* e dei fornitori di accesso[17]. La commissione ne deduce la necessità di legiferare per realizzare in tempi brevi la certezza del diritto. La commissione peritale propone di disciplinare la materia, ispirandosi alla direttiva UE sul commercio elettronico, nella legge federale sul commercio elettronico o nell'ambito della revisione e dell'unificazione del diritto in materia di responsabilità civile (legge sulla responsabilità civile).

Il Consiglio federale non condivide tale parere della commissione peritale. La situazione normativa in materia di responsabilità civile dei provider non è né lacunosa né

[17] Rapporto della commissione peritale "Criminalità in rete", op. cit., pag. 83.

poco chiara. La disposizione pertinente è infatti l'articolo 50 CO, secondo cui istigatori, autori e complici sono tenuti in solido per il danno cagionato. Alla stregua degli altri casi di eventuale responsabilità, spetta alla prassi stabilire le condizioni che devono essere adempiute nel caso specifico perché un provider sia considerato correo ai sensi di tale disposizione. Lo stesso vale per la valutazione di pretese indipendenti dalla colpa e finalizzate a proibire o a far cessare una lesione, ad esempio le valutazioni atte a stabilire se un testo caricato o destinato a essere caricato in Internet è lesivo della personalità (art. 28 CC).

A differenza di quanto deciso per il diritto penale, il legislatore si è detto contrario a uno speciale diritto civile dei media. L'attuale regime ha dato buoni frutti e non ha prodotto risultati inaccettabili – come ha dovuto ammettere la commissione peritale stessa. Il Consiglio federale è del parere che il legislatore non sia tenuto a fornire un ulteriore contributo alla certezza del diritto; difatti la commissione peritale non ha formulato proposte in merito. La decisione si prospetterebbe diversa tutt'al più se l'istanza politica consistesse nello scusare la condotta dei provider in proporzioni finora sconosciute. Tuttavia, tale non può e non deve essere l'obiettivo di un progetto teso in primo luogo a combattere la criminalità in rete.

Il Consiglio federale ricorda inoltre che è stata sospesa la revisione del diritto sulla responsabilità civile e che la futura legge federale sul commercio elettronico si orienta in primo luogo a istanze di protezione dei consumatori. Ecco perché la legge federale sul commercio elettronico non potrebbe accogliere disposizioni in materia di responsabilità dei provider nemmeno se fosse necessario legiferare sul piano del diritto privato.

2.222 Diritto amministrativo

Il Consiglio federale condivide quanto esposto dalla commissione peritale[18] in merito a eventuali misure preventive di diritto amministrativo, che in effetti collliderebbero con il divieto di censura. La libertà di espressione non permetterebbe nemmeno di imporre ai provider più obblighi di diritto amministrativo di quanti non siano implicitamente previsti agli articoli 27 e 322bis AP-CP e all'articolo 26*a* AP-CPM. La normativa proposta prevede di punire l'*hosting provider* che sappia "con certezza" che un terzo commette un reato servendosi delle sue infrastrutture. L'*hosting provider* non è insomma tenuto a verificare di continuo che un terzo non commetta reati.

2.223 Altre misure legislative

Il Consiglio federale condivide il parere della commissione peritale anche per quanto riguarda eventuali altre misure legislative nell'ambito della criminalità in rete. Ritiene quindi che la Convenzione del Consiglio d'Europa sulla cibercriminalità possa divenire uno strumento importante per combattere questo tipo di reati. È fondamentalmente nell'interesse della Svizzera e dell'assistenza giudiziaria internazionale che un numero quanto più consistente di Paesi raggiunga uno standard uniforme nella lotta a questo tipo di criminalità. Tale uniformazione presuppone però che la Convenzione sia attuata su larga scala sul piano internazionale, condizione finora non adempiuta a causa della materia assai complessa, che lascia molto spazio all'interpretazione, e del campo di applicazione particolarmente ampio delle disposizioni procedurali. A

[18] Rapporto della commissione peritale "Criminalità in rete", op. cit., pag. 76 segg.

media scadenza, la necessità di adeguare il diritto svizzero dipenderà in larga misura dall'uso fatto della possibilità di formulare dichiarazioni e riserve al testo della Convenzione. In ogni caso è necessario coordinare i lavori con quelli relativi al Codice di procedura penale svizzero.

Non è tuttavia necessario accogliere le richieste della commissione peritale[19] integrando la legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)[20]. Nella sua decisione pubblicata il 27 aprile 2004[21], la Commissione di ricorso del Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni afferma infatti che il legislatore, con l'articolo 14 capoverso 4 LSCPT, ha voluto creare una disposizione speciale volta a istituire una procedura semplificata per informare le autorità di ogni reato commesso mediante Internet al fine di identificarne l'autore. Tale obbligo d'informazione delle autorità si applica indipendentemente dal fatto che i dati soggiacciano al segreto delle telecomunicazioni. Ecco perché le richieste di informazioni ai sensi dell'articolo 14 capoverso 4 LSCPT non sono considerate provvedimenti di sorveglianza nemmeno se si riferiscono a un indirizzo IP assegnato in chiave dinamica e hanno per oggetto dati contestuali o dati atti a identificare l'utente. Il tenore dell'articolo 14 capoverso 4 LSCPT ne rispecchia quindi lo scopo. In sostanza il provider è tenuto a informare le autorità di ogni reato commesso mediante Internet, indipendentemente dal catalogo di reati inserito all'articolo 3 LSCPT, e inoltre tale obbligo d'informazione non si limita a un determinato tipo di dati.

2.3 Commento delle singole disposizioni[22]

2.31 Codice penale

Come accennato in precedenza, esiste un certo parallelismo tra il disciplinamento proposto e l'attuale diritto penale dei media. Tuttavia le norme proposte non possono, per molti versi, essere considerate una copia speculare degli articoli 27 e 322bis CP e dell'articolo 26*a* CPM. La nuova normativa contempla infatti qualsiasi reato informatico, per cui a differenza del diritto penale dei media non si limita ai reati mediatici. Il diritto penale dei media prevede la responsabilità penale del redattore responsabile o della persona responsabile della pubblicazione soltanto a condizione che l'autore non possa essere individuato o tradotto davanti a un tribunale svizzero (responsabilità a cascata). Tale esclusione della responsabilità penale non è prevista per i reati commessi mediante reti di comunicazione elettronica. L'*hosting provider* resta punibile ai sensi dell'articolo 322bis AP-CP, anche se l'autore o il fornitore di contenuti può essere individuato o tradotto davanti a un tribunale svizzero. Inoltre, al contrario dei reati mediatici, i reati informatici commessi per negligenza non sono puniti (art. 322bis per. 2 CP).

---

[19] Rapporto della commissione peritale "Criminalità in rete", op. cit., pag. 142 seg.
[20] RS **780.1**
[21] La decisione del 27.4.2004 della Commissione di ricorso DATEC può essere consultata all'indirizzo http://www.reko-inum.admin.ch/it/display_file.php?fname=114010669724120&query= .
[22] Per ulteriori informazioni cfr. il rapporto della commissione peritale "Criminalità in rete", in particolare pag. 93 segg.

2.311 Completamento del titolo marginale nella 6ª sezione del Titolo secondo del Codice penale

La nozione di "reti di comunicazione elettronica", inserita nel titolo marginale nella 6ª sezione del Titolo secondo del Codice penale, ha un carattere tecnologicamente neutrale e, di proposito, non fa riferimento esclusivo a Internet. La nozione di reti di comunicazione non comprende unicamente l'interconnessione di computer, ma anche altri mezzi di telecomunicazione. È possibile trasmettere ad esempio una dichiarazione lesiva dell'onore o un'immagine di carattere pornografico avvalendosi sia di Internet (e-mail, WWW) sia della rete di telefonia mobile (SMS, MMS) o di una rete locale (LAN). Il ricorso alla tecnologia di Internet non è quindi indispensabile. Non ha alcuna importanza il fatto che le informazioni in questione siano trasmesse via cavo o via etere, o quale infrastruttura venga impiegata per la trasmissione (linee telefoniche, linee elettriche, ecc.). È irrilevante che si tratti di informazioni a senso unico (come ad es. nelle tradizionali trasmissioni radiotelevisive) o interattive, ossia basate su uno scambio di dati (come ad es. nelle conversazioni telefoniche o nella posta elettronica).

La nozione di "reti di comunicazione elettronica" è finalizzata a contemplare tutti i reati commessi trasmettendo, preparando o mettendo a disposizione informazioni in reti di telecomunicazione. Ai reati mediatici "classici" continua ad applicarsi il diritto penale dei media, che viene integrato nella nuova normativa (come art. 27bis e art. 322bis n. 2 AP-CP).

2.312 Responsabilità penale dei provider

Articolo 27 AP-CP: punibilità nelle reti di comunicazione elettronica

Come esposto in precedenza, la nozione di "reti di comunicazione elettronica" ha un'accezione più ampia rispetto al concetto di "media". Ecco perché la nuova disposizione sulla punibilità nelle reti di comunicazione elettronica viene inserita all'inizio dell'intera normativa, mentre l'attuale disposizione penale sui media segue all'articolo 27bis AP-CP. Per la medesima ragione, la trasposizione avviene nel nuovo articolo 322bis AP-CP. L'attuale articolo 322bis CP viene ripreso come numero 2 della nuova disposizione. L'attuale articolo 27bis (tutela delle fonti) CP diventa il nuovo articolo 27ter AP-CP.

Capoverso 1: fornitore di contenuti

Il capoverso 1 del nuovo articolo 27 AP-CP prevede che ai provider si applichino in primo luogo le regole generali del Codice penale, ossia quelle relative all'autore, alla correità, alla complicità e all'istigazione. Tale principio si applica al fornitore di contenuti in qualità di autore dell'informazione illegale, ma anche al fornitore di accesso o all'*hosting provider* che partecipi attivamente alla preparazione o alla messa a disposizione di informazioni illegali. La punibilità o l'impunità del provider non è dunque determinata dalla sua natura, ma dalla funzione che assolve nell'atto di comunicazione specifico. Tale principio si applica con riserva delle disposizioni ai capoversi 2 - 4.

I concetti di "trasmissione, preparazione e messa a disposizione" indicano tre operazioni fondamentali per comunicare in rete. Trasmettere significa inviare e ricevere informazioni elettroniche via cavo o via radio, preparare equivale a caricare le infor-

mazioni su un supporto di memoria comune e accessibile al pubblico mediante reti di comunicazione elettronica, mentre mettere a disposizione vuol dire gestire un supporto di memoria sul quale sono caricate le informazioni. L'ultimo anello di tale catena di comunicazione è l'utente che richiama l'informazione e in tale qualità non è punibile. Dal 1° aprile 2002 è tuttavia punito chi memorizza o scarica (*download*) file a contenuto pornografico (art. 197 n. 3bis CP).

La nozione di "informazioni" è ampia e include in particolare anche i programmi informatici. Il termine è usato sia nella legge sulle telecomunicazioni[23] sia nella direttiva sul commercio elettronico. Pertanto la normativa proposta non si limita ai "reati di espressione" commessi in Internet, quali ad esempio la rappresentazione di atti di cruda violenza (art. 135 CP), la pornografia (art. 197 CP) o la discriminazione razziale (art. 261bis CP), ma risulta più circostanziata. Contempla infatti anche gli altri reati informatici, quali ad esempio le istruzioni per creare virus informatici (art. 144bis CP) o le offerte fraudolente sul web (art. 146 CP), nonché i reati in materia di diritti d'autore, quali ad esempio la pirateria musicale (art. 67 e 69 legge sul diritto d'autore; LDA[24]).

Capoverso 2: delimitazione rispetto al diritto penale dei media

Si applica quanto previsto all'articolo 27bis AP-CP se il fornitore di contenuti è autore o redattore ai sensi del diritto penale dei media (art. 27 CP e 27bis AP-CP), vale a dire che il reato è commesso mediante pubblicazione in un mezzo di comunicazione *on line* quale ad esempio un quotidiano pubblicato in Internet. Tuttavia la riserva contempla soltanto gli autori e i redattori, e non le persone responsabili della pubblicazione secondo l'attuale articolo 27 capoverso 2 CP. Per i reati commessi attraverso procedure automatizzate in reti di comunicazione elettronica, si prevede infatti di sottoporre alla nuova normativa gli *hosting provider* e i fornitori d'accesso responsabili della pubblicazione, fatta eccezione per gli autori e i redattori. A tale scopo la riserva in favore del diritto penale dei media si limita agli autori e ai redattori.

Capoverso 3: hosting provider

Il capoverso 3 distingue il caso ordinario del trasferimento automatico di dati il cui contenuto è sconosciuto all'*hosting provider* dai casi in cui egli viene *a posteriori* a conoscenza della rilevanza penale delle informazioni. Nel primo caso egli è esente da pena, mentre nel secondo è punibile giusta l'articolo 322bis numero 1 AP-CP.

Molti utenti del web iniziano a navigare avviando un cosiddetto motore di ricerca (come ad es. google.ch o altavista.com). La novità consiste nel fatto che, dal profilo del diritto penale, i gestori di tali motori di ricerca vengono equiparati agli *hosting provider*. Tale integrazione dell'articolo 3 secondo periodo è necessaria giacché le informazioni contenute nell'indice del motore di ricerca non appartengono più a "terzi" ai sensi del primo periodo. Infatti le informazioni caricate sul server del gestore del motore di ricerca non sono messe a disposizione da un qualsiasi fornitore di contenuti, ma alimentano la banca dati allestita automaticamente dal gestore stesso. Le informazioni figuranti nell'indice appartengono al gestore, ragion per cui si applica l'articolo 27 capoverso 1 AP-CP.

---

[23] Cfr. in merito la definizione legale all'art. 3 lett. a della legge sulle telecomunicazioni del 30 aprile 1997 (LTC; RS **784.10**): "informazioni: segni, segnali, caratteri, immagini, suoni e rappresentazioni di qualunque altro genere destinati all'uomo, ad altri esseri viventi o a macchine".

[24] RS **231.1**.

Capoverso 4: fornitore di accesso

Come menzionato e illustrato in precedenza, in caso di applicazione delle disposizioni generali del Codice penale, non è da escludere che il fornitore di accesso sia punito ad esempio come complice del fornitore di contenuti nella commissione del reato principale. Di norma comunque l'*access provider* si limita a fornire accesso a Internet. Secondo il capoverso 4 la sua partecipazione non è punibile se si limita alla mera fornitura di accesso. L'utente si avvale dei vari servizi Internet per comunicare o per raccogliere informazioni, e a tale scopo deve poter accedere alla rete.

La disposizione considera fornitura di accesso anche la memorizzazione automatica, intermedia e temporanea di informazioni di terzi. A differenza di quanto stabilito dalla direttiva UE sul commercio elettronico[25], il Consiglio federale propone di non fare distinzioni tra la memorizzazione intermedia per motivi tecnici e il cosiddetto *proxy-caching*, vale a dire la memorizzazione intermedia e temporanea da parte del fornitore di accesso allo scopo di permettere a tutti suoi i clienti di richiamare con maggiore facilità i dati relativi ai contenuti visitati più frequentemente. Tale soluzione flessibile è da preferire a una normativa più specifica. In un ambito in costante evoluzione tecnica, infatti, una delimitazione generale e astratta risulta alquanto inattuabile. L'impunità non si estende al cosiddetto *mirroring*, ossia alla replica attiva di una determinata offerta Internet su un altro server, ad esempio per ridurre i tempi di accesso a un server particolarmente sovraccarico. Sono contemplati soltanto i casi di memorizzazione generata automaticamente in seguito alla richiesta di un utente.

Articolo 27bis AP-CP: punibilità dei media

L'articolo 27bis AP-CP riprende quanto previsto all'attuale articolo 27 CP con l'aggiunta che il capoverso 2 rinvia all'articolo 322bis numero 2 AP-CP.

Articolo 322bis AP-CP: mancata opposizione a reati commessi in reti di comunicazione elettronica e nei media

Numero 1 comma 1

Il comma 1 disciplina la punibilità dell'*hosting provider*, sancita dall'articolo 27 numero 3 AP-CP. Si tratta di un vero reato speciale che presuppone la messa a disposizione automatica di informazioni di terzi in una rete di comunicazione. Rientrano chiaramente in tale definizione gli *hosting provider*, sui cui server i clienti (fornitori di contenuti) caricano informazioni che sfuggono al controllo degli *hosting provider*.

Il comma 1 del numero 1 sancisce un vero e proprio reato di omissione. All'*hosting provider* viene in pratica rimproverato di non essere intervenuto, pur avendone la possibilità tecnica e sebbene fosse ragionevolmente esigibile, per impedire l'utilizzo di un file di cui sapeva con certezza che presentava ad esempio contenuti a sfondo razzista, pornografici o istiganti all'uso della violenza. Il nucleo essenziale dell'illiceità non risiede pertanto nella partecipazione al reato principale, ma bensì nell'inattività dimostrata di fronte all'ulteriore diffusione dell'informazione illegale.

[25] Cfr. art. 12 par. 2 e art. 13 della direttiva sul commercio elettronico.

È necessario che, per mezzo delle informazioni di terzi, venga commesso un reato. Da un lato entrano in considerazione i reati considerati "classici" della criminalità in rete, quali la rappresentazione di atti di cruda violenza (art. 135 CP), la pornografia (art. 197 CP) o la discriminazione razziale (art. 261bis CP). Dall'altro fanno parte del gruppo di atti punibili anche tutti i reati per la cui commissione è ipotizzabile l'impiego di mezzi di comunicazione elettronica, quali i cosiddetti reati informatici, ma pure i reati patrimoniali classici (ad es. la truffa, art. 146 CP) o le infrazioni ai sensi del diritto penale accessorio, in particolare quelle in materia di concorrenza sleale o di protezione dei marchi.

Numero 1 comma 2

Per fondare la punibilità dell'atto di omissione, il numero 1 comma 1 esige la consapevolezza dell'*hosting provider*. Ci si chiede pertanto come vada valutata la posizione dell'*hosting provider* che non acquisisce tale certezza per il fatto che, ad esempio, ha ricevuto segnalazioni incomplete. Rinunciando a intervenire in un simile caso, l'*hosting provider* non potrà mai acquisire la certezza richiesta dal comma 1 e resterà quindi impunito. È quanto intende impedire il nuovo comma 2 secondo cui l'*hosting provider* è pure punibile se omette di portare alla conoscenza delle autorità inquirenti le informazioni, segnalate da terzi, per mezzo delle quali è commesso un reato. È importante che tale obbligo di trasmissione scaturisca soltanto da segnalazioni indirizzate all'*hosting provider* a titolo individuale, e non sulla base di informazioni generalmente accessibili attraverso la stampa, la radio o la televisione.

L'*hosting provider* è inoltre tenuto a trasmettere unicamente le segnalazioni riguardanti i file che ospita sul suo server. È pertanto soggetto a tale obbligo di trasmissione soltanto l'*hosting provider* che non sia in grado di acquisire la certezza e resti inattivo sebbene abbia ricevuto segnalazioni incomplete o lacunose. In tal senso non si tratta di un obbligo generale di denuncia sebbene un *hosting provider* circospetto trasmetterà alle autorità inquirenti tutte le segnalazioni ricevute.

I commi 1 e 2 realizzano l'obiettivo politico-giuridico volto a coinvolgere gli *hosting provider* nella lotta contro i contenuti illegali su Internet. Non si può esigere che gli *hosting provider* impediscano ai loro clienti di commettere reati pubblicando informazioni sul server Internet: gli *hosting provider* non hanno infatti alcun influsso sul processo di caricamento dei contenuti. È per contro possibile esortare gli *hosting provider* – e in questo consiste appunto il vero obiettivo legislativo – a limitare gli effetti di tali reati e a impedire la presa di conoscenza dei relativi contenuti, rendendone impossibile l'uso sul piano tecnico o trasmettendo le segnalazioni ricevute alle autorità inquirenti in conformità con il comma 2.

Sia il comma 1 sia il comma 2 comminano la detenzione (da tre giorni a tre anni; art. 36 CP) o la multa (fino a 40 000 franchi; art. 48 CP)[26]. Si tratta di una comminatoria adeguata ai reati principali; infatti gli articoli 135, 197 e 261bis CP prevedono anch'essi la detenzione o la multa. La comminatoria proposta risulta giustificata anche dall'obiettivo politico-giuridico perseguito; dal momento che i contenuti illeciti vengono resi

[26] Con l'entrata in vigore la modifica del 13 dicembre 2002 del Codice penale (FF **2002** 7352; Disposizioni generali, Dell'attuazione e dell'applicazione del Codice penale), i termini "detenzione" e "multa" saranno sostituiti con "pena detentiva fino a tre anni" e "pena pecuniaria". Dal momento che la pena pecuniaria sarà commisurata in base al nuovo sistema delle aliquote giornaliere, l'importo massimo salirà a 1 080 000 franchi (360 aliquote giornaliere di 3000 franchi ciascuna; cfr. art. 34 nCP).

inaccessibili, il coinvolgimento dell'*hosting provider* permette infatti di contenere gli effetti del reato commesso dal suo cliente.

Numero 1 comma 3

Nel caso in cui il reato commesso in Internet sia perseguibile unicamente a querela di parte, il comma 3 prevede di renderlo punibile soltanto se la querela è stata sporta. In caso contrario non viene promossa azione nemmeno nei confronti dell'*hosting provider*. Il Codice penale conosce una normativa analoga per la ricettazione (art. 160 CP). Quando l'*hosting provider* riceve una segnalazione riguardante un reato perseguibile solo a querela di parte, in genere non sa se è stata sporta una querela. Nel dubbio trasmetterà la segnalazione indipendentemente dall'esigenza di una querela. Il comma 3 intende impedire che l'*hosting provider* venga ingiustamente punito per non aver trasmesso una segnalazione secondo il comma 2, benché la persona lesa dal presunto reato abbia rinunciato al perseguimento e quindi anche a una sanzione.

Numero 1 comma 4

Qual è il diritto determinante per valutare se si è in presenza di un reato? La risposta a questa domanda è inserita al comma 4: "Il diritto svizzero è determinante per valutare se per mezzo di un'informazione viene commesso un reato". L'*hosting provider* deve essere perseguibile anche nei casi in cui l'atto contestato non è punibile secondo il diritto del luogo in cui è stato commesso.

In questo contesto potrebbero assumere rilevanza pratica ad esempio talune idee esternate in Paesi della sfera giuridica americana o australiana e considerate discriminatorie dal diritto svizzero, ma esenti da pena in tali Paesi perché rientranti nella libertà di espressione. La punibilità dell'*hosting provider* prevista ai commi 1 e 2 è finalizzata a impedire che l'informazione punibile possa continuare a essere richiamata da un server svizzero. Questo chiaramente soltanto nella misura in cui i relativi file contengano informazioni illegali ai sensi del diritto svizzero.

Numero 1 comma 5

Il comma 5 prevede che vengano cancellate le informazioni di cui ai commi 1 e 2, ossia quelle per mezzo delle quali viene commesso un reato. In quanto *pendant* della confisca (art. 58 CP), la cancellazione delle informazioni ha carattere materiale ed è ordinata dal giudice nella sentenza. Il comma 5 non costituisce una disposizione processuale analoga al sequestro che permetterebbe già alle autorità inquirenti di bloccare provvisoriamente l'accesso alle informazioni. Una disposizione del genere è riservata alla legislazione procedurale penale. Nella fattispecie, l'accento è posto sull'ordine di blocco impartito dalle autorità inquirenti; tale blocco, essendo una misura coercitiva processuale, deve essere retto da disposizioni pertinenti.

Una volta cancellati i contenuti illegali, non deve essere possibile ripristinarli. Come accennato in precedenza, il giudice ordina la cancellazione delle informazioni in caso di condanna dell'*hosting provider*. Per determinare la misura in cui una cancellazione entra in linea di conto anche qualora l'imputato venga assolto o la causa archiviata, la commissione peritale propone quanto segue. Se un *hosting provider* non viene condannato, ad esempio perché non è possibile provare la sua consapevolezza riguardo alla punibilità dell'informazione, ma gli è imputabile unicamente il dolo even-

tuale, il giudice può comunque ordinare la cancellazione, anche "a prescindere dalla sovranità penale svizzera". Si creerebbe infatti una situazione insoddisfacente dal profilo politico-giuridico se la sentenza di assoluzione dell'*hosting provider* stabilisse che un fornitore di contenuti ha caricato sul server dell'*hosting provider* informazioni di carattere penalmente rilevante, ma che non è possibile cancellare tali dati poiché il reato commesso dal fornitore di contenuti non sottostà alla sovranità penale svizzera. Per la cancellazione non occorre pertanto che il reato del fornitore di contenuti sottostia alla sovranità penale svizzera. Le informazioni sul server Internet dell'*hosting provider* vengono cancellate in ogni caso.

Numero 2

Il numero 2 riprende la normativa dell'attuale articolo 322bis CP, prevedendo però un rinvio all'articolo 27bis AP-CP.

2.32 Codice penale militare

La revisione del Codice penale ordinario comporta tradizionalmente la modifica del Codice penale militare qualora la medesima disposizione figuri in entrambe le leggi (cfr. *infra* n. 2.42).

2.4 Avamprogetto A

2.41 Codice penale svizzero

(nuovo titolo) 6. Punibilità nelle reti di comunicazione elettronica e nei media[27]

Articolo 27 AP-CP ***Punibilità nelle reti di comunicazione elettronica[28]***

[1] Se un reato è commesso mediante trasmissione, preparazione o messa a disposizione di informazioni in una rete di comunicazione elettronica, si applicano le disposizioni generali sulla reità e la partecipazione contenute nella presente legge. È fatto salvo quanto segue.

[2] Se l'autore del reato è l'autore dell'opera o il redattore ai sensi dell'articolo 27bis, la punibilità è retta da questa disposizione.

[3] Chiunque mette automaticamente a disposizione informazioni di terzi per un loro impiego in una rete di comunicazione elettronica, è punibile alle condizioni dell'articolo 322bis numero 1. La messa a disposizione di un elenco nel quale vengono registrate automaticamente informazioni di terzi è considerata messa a disposizione di informazioni di terzi.

[4] Non è punibile chi fornisce unicamente accesso a una rete di comunicazione elettronica. Una memorizzazione temporanea di informazioni di terzi, generata automaticamente in seguito all'interrogazione di un utente, è considerata fornitura di accesso.

Articolo 27 CP diventa articolo 27bis AP-CP ***Punibilità dei media[29]***

[1] ...

[2] Qualora l'autore dell'opera non possa essere individuato o non possa essere tradotto davanti a un tribunale svizzero, è punito il redattore responsabile giusta l'articolo 322bis numero 2. In sua mancanza, è punita giusta il numero 2 del medesimo articolo la persona responsabile della pubblicazione.

[3] ...

[4] ...

---

[27] Con l'entrata in vigore la modifica del 13 dicembre 2002 del Codice penale (FF **2002** 7352; Disposizioni generali, Dell'attuazione e dell'applicazione del Codice penale), il titolo *6. Punibilità dei media* è sostituito con il titolo *6. Punibilità nelle reti di comunicazione elettronica e nei media*.

[28] Con l'entrata in vigore la modifica del 13 dicembre 2002 del Codice penale (FF **2002** 7352; Disposizioni generali, Dell'attuazione e dell'applicazione del Codice penale), l'art. 27 diventa art. 28.

[29] Con l'entrata in vigore la revisione del 13 dicembre 2002 della Parte generale del Codice penale (FF **2002** 7352), art. 27bis diventa art. 28*a*.

Articolo 27bis CP diventa articolo 27ter AP-CP ***Tutela delle fonti***[30]**, e il suo testo resta identico**

Articolo 322bis AP-CP ***Mancata opposizione a reati commessi in reti di comunicazione elettronica e nei media***

1. Chiunque mette automaticamente a disposizione informazioni di terzi in una rete di comunicazione elettronica, sapendo con certezza che per mezzo di tali informazioni è commesso un reato, e non impedisce l'impiego di tali informazioni, anche se ciò sarebbe tecnicamente possibile e lo si possa ragionevolmente pretendere, è punito con la detenzione o con la multa[31].

Chiunque mette automaticamente a disposizione informazioni di terzi in una rete di comunicazione elettronica, per mezzo delle quali è commesso un reato, e omette di trasmettere alle autorità di perseguimento penale segnalazioni di terzi a lui indirizzate e pervenute, riguardanti tali informazioni, è punito con la detenzione o con la multa.

Se il reato è perseguibile solo a querela di parte, esso è punibile unicamente se la querela è stata sporta.

Il diritto svizzero è determinante per valutare se per mezzo di un'informazione viene commesso un reato.

Le informazioni di cui ai commi 1 e 2 vengono cancellate a prescindere dalla sovranità penale svizzera.

2. Chiunque, in quanto responsabile giusta l'articolo 27bis capoversi 2 e 3, intenzionalmente non impedisce una pubblicazione con la quale è commesso un reato, è punito con la detenzione o con la multa. Se ha agito per negligenza, la pena è dell'arresto o della multa.

---

30 Con l'entrata in vigore la modifica del 13 dicembre 2002 del Codice penale (FF **2002** 7352; Disposizioni generali, Dell'attuazione e dell'applicazione del Codice penale), l'art. 27ter diventa art. 28*b*.

31 Con l'entrata in vigore la modifica del 13 dicembre 2002 del Codice penale (FF **2002** 7352; Disposizioni generali, Dell'attuazione e dell'applicazione del Codice penale), i termini "detenzione" e "multa" saranno sostituiti con le espressioni "pena detentiva fino a tre anni" e "pena pecuniaria". Dal momento che la pena pecuniaria è commisurata in base al nuovo sistema delle aliquote giornaliere, l'importo massimo salirà a 1 080 000 franchi (360 aliquote giornaliere di 3000 franchi ciascuna; cfr. art. 34 nCP).

2.42 Codice penale militare

(nuovo titolo) 8. Punibilità nelle reti di comunicazione elettronica e nei media[32]

Articolo 26*a* AP-CPM *Punibilità nelle reti di comunicazione elettronica*[33]

[1] Se un reato è commesso mediante trasmissione, preparazione o messa a disposizione di informazioni in una rete di comunicazione elettronica, si applicano le disposizioni generali sulla reità e la partecipazione contenute nella presente legge. È fatto salvo quanto segue.

[2] Se l'autore del reato è l'autore dell'opera o il redattore ai sensi dell'articolo 26*b*, la punibilità è retta da questa disposizione.

[3] Chiunque mette automaticamente a disposizione informazioni di terzi per un loro impiego in una rete di comunicazione elettronica, è punibile alle condizioni dell'articolo 322bis numero 1. La messa a disposizione di un elenco nel quale vengono registrate automaticamente informazioni di terzi è considerata messa a disposizione di informazioni di terzi.

[4] Non è punibile chi fornisce unicamente accesso a una rete di comunicazione elettronica. Una memorizzazione temporanea di informazioni di terzi, generata automaticamente in seguito all'interrogazione di un utente, è considerata fornitura di accesso.

Articolo 26*a* CP diventa articolo 26*b* AP-CPM *Punibilità dei media*[34]

[1] ...

[2] Qualora l'autore dell'opera non possa essere individuato o non possa essere tradotto davanti a un tribunale svizzero, è punito il redattore responsabile giusta l'articolo 322bis numero 2 del Codice penale. In sua mancanza, è punita giusta l'articolo 322bis numero 2 del Codice penale la persona responsabile della pubblicazione.

[3] ...

[4] ...

---

[32] Con l'entrata in vigore la modifica del 21 marzo 2003 del Codice penale militare (FF **2003** 2438; Disposizioni generali, Entrata in vigore ed applicazione del Codice), il titolo *8. Punibilità nelle reti di comunicazione elettronica e nei media* è sostituito con il titolo *6. Punibilità nelle reti di comunicazione elettronica e nei media*.

[33] Con l'entrata in vigore la modifica del 21 marzo 2003 del Codice penale militare (FF **2003** 2438; Disposizioni generali, Entrata in vigore ed applicazione del Codice), l'art. 26*a* diventa art. 27.

[34] Con l'entrata in vigore la modifica del 21 marzo 2003 del Codice penale militare (FF **2003** 2438; Disposizioni generali, Entrata in vigore ed applicazione del Codice), l'art. 26*b* diventa art. 27*a*.

Articolo 26*b* CPM diventa articolo 26*c* AP-CPM	***Tutela delle fonti*[35], e il suo testo resta identico**

[35] Con l'entrata in vigore la modifica del 21 marzo 2003 del Codice penale militare (FF **2003** 2438; Disposizioni generali, Entrata in vigore ed applicazione del Codice), art. 26*c* diventa art. 27*b.*

3. Competenze della Confederazione in caso di reati commessi mediante reti di comunicazione elettronica (avamprogetto B)

3.1 Proposte del gruppo di lavoro "Genesis"

Il gruppo di lavoro "Genesis" ha sostanzialmente esaminato proposte di miglioramento sul piano giuridico, apparse necessarie dopo un'analisi approfondita dell'operazione "Genesis" e volte a rendere più efficiente il perseguimento penale della criminalità in rete.

3.11 Perseguimento penale in caso di reati commessi mediante reti di comunicazione elettronica

Nel suo rapporto[36] il gruppo di lavoro "Genesis" illustra perché le indagini nell'ambito della criminalità in rete costituiscono una grande sfida sia in termini di risorse umane sia dal profilo tecnico. Le difficoltà sono molteplici. Ricordiamo ad esempio l'assicurazione delle prove, che richiede un grande spiegamento di forze e mezzi tecnici visto che il mondo virtuale delle reti di comunicazione elettronica permette facilmente di mantenere l'anonimato o di far perdere le proprie tracce una volta commesso il reato. Non di rado poi i casi sono complessi e ricchi di risvolti internazionali e, alla stregua di "Genesis", rilevano della competenza di vari Cantoni. Infine vi è il costo non irrilevante per l'attrezzatura tecnica come pure per la formazione e il perfezionamento degli inquirenti.

3.12 Analisi dell'operazione "Genesis"

L'operazione "Genesis" ha evidenziato la particolare problematica legata alla lotta contro la criminalità in Internet. La grande quantità di materiale probatorio sequestrato e la competenza congiunta di 25 Cantoni per il perseguimento penale (ad eccezione di Appenzello Interno) hanno posto le autorità inquirenti svizzere di fronte a una situazione senza precedenti.

L'analisi del gruppo di lavoro "Genesis" giunge alla conclusione che occorre intervenire sul piano della cooperazione tra la Confederazione e i Cantoni, in particolare per quanto riguarda la preparazione di operazioni quali "Genesis", l'analisi tecnica del materiale probatorio, la formazione degli inquirenti e i contatti mediatici. A ciò si aggiunge un altro handicap decisivo: la Confederazione non è per legge autorizzata a effettuare verifiche centralizzate ad esempio sui dati dei clienti presso le società emittenti di carte di credito. Tale competenza avrebbe permesso alle autorità federali di accertare con maggiore rapidità la competenza cantonale nel corso dell'operazione "Genesis" e di assegnare quindi senza indugio i casi ai Cantoni. La mancanza di una base legale ha altresì impedito alla Confederazione di incidere sulla durata dei procedimenti nei 25 Cantoni coinvolti, rendendo particolarmente difficile il coordinamento da parte di fedpol.

[36] Rapporto del gruppo di lavoro "Genesis", op. cit., pag. 32 seg.

Gli ultimi due problemi citati, cui è riconducibile un'importante perdita di efficienza, vanno localizzati nella prima fase procedurale. Il perseguimento penale della maggior parte dei reati commessi mediante Internet compete ai Cantoni[37], mentre la Confederazione in tali casi ha unicamente la facoltà di coordinare le indagini intercantonali e internazionali[38]. Il quadro legale non permette comunque alle autorità federali né di condurre indagini autonome né di invitare i Cantoni a farlo.

Tuttavia gli strumenti a disposizione non bastano per una lotta efficace alla criminalità in rete. Infatti il potenziale criminoso dei mezzi di comunicazione elettronica aumenta in proporzione al numero di persone in possesso di tali mezzi e in grado di sfruttarne appieno le potenzialità tecniche. Esperienze precedenti hanno inoltre dimostrato che anche il futuro riserverà un aumento dei casi analoghi distribuiti su diversi Cantoni. Il gruppo di lavoro "Genesis" ribadisce[39] pertanto l'utilità di conferire alla Confederazione la facoltà di condurre indagini centralizzate nella prima fase del procedimento penale.

3.13 Non spetta alla Confederazione perseguire la criminalità in rete

Il gruppo di lavoro respinge tuttavia la proposta di conferire alla Confederazione una competenza centralizzata per perseguire i reati commessi in reti di comunicazione, come auspicato dall'iniziativa parlamentare Aeppli Wartmann (cfr. *supra* n. 1.2) e dalla commissione peritale "Criminalità in rete" (cfr. *supra* n. 2.12).

Tale richiesta si spinge troppo lontano e non sarebbe giustificata nemmeno dal profilo materiale[40]. Verrebbe ad esempio messa in discussione la suddivisione dei compiti nell'ambito del perseguimento penale, sancita dalla Costituzione (competenza cantonale quale regola, competenza federale quale eccezione), poiché i Cantoni si vedrebbero costretti a cedere alla Confederazione una parte non indifferente delle loro competenze. L'analisi dell'operazione "Genesis" ha inoltre permesso di constatare che i problemi principali si concentrano nella prima fase procedurale, per cui non è necessario affidare alla Confederazione l'intero procedimento[41].

3.14 Modello proposto

Il gruppo di lavoro "Genesis", ispirandosi alla legislazione in materia di stupefacenti[42], ha elaborato un modello che permette di centralizzare il perseguimento penale presso la Confederazione nella prima fase procedurale, senza tuttavia intaccare la competenza dei Cantoni in materia. Il gruppo di lavoro ha quindi concretizzato tale idea formulando due varianti (cfr. *infra* n. 3.15 e 3.16)[43] e proponendo di integrare il Codi-

---

[37] Cfr. art. 343 CP.

[38] Cfr. art. 2 lett. b della legge federale sugli Uffici centrali di polizia giudiziaria della Confederazione (LUC; RS **360**) e art. 3 dell'ordinanza del 30 novembre 2001 sull'adempimento di compiti di polizia giudiziaria in seno all'Ufficio federale di polizia (RS **360.1**).

[39] Rapporto del gruppo di lavoro "Genesis", op. cit., pag. 5 segg.

[40] Rapporto del gruppo di lavoro "Genesis", op. cit., pag. 7 segg.

[41] Rapporto del gruppo di lavoro "Genesis", op. cit., pag. 24 seg.

[42] Legge federale del 3 ottobre 1951 sugli stupefacenti e sulle sostanze psicotrope (Legge sugli stupefacenti, LStup); RS **812.121.**

[43] Rapporto del gruppo di lavoro "Genesis", op. cit., pag. 9 segg. e 20 segg.

ce penale per dotare le autorità inquirenti di uno strumento d'indagine attuabile senza oneri eccessivi e in tempi relativamente brevi.

3.15 Variante 1 (competenza d'indagine dell'MPC ai sensi dell'articolo 259 della legge federale del 15 giugno 1934 sulla procedura penale [PP][44], basata su un'alta vigilanza della Confederazione)

La struttura del modello proposto si ispira, come illustrato in precedenza, a quanto disposto dalla legge federale sugli stupefacenti (cfr. art. 29 cpv. 4 LStup, in combinato disposto con l'articolo 259 PP).

Tale modello presenta le seguenti caratteristiche: in virtù dell'articolo 259 PP, l'MPC può ordinare indagini se i reati sono stati totalmente o parzialmente commessi all'estero o in più Cantoni, come nel caso dell'operazione "Genesis", a condizione tuttavia che la Confederazione disponga di un diritto di alta vigilanza per il perseguimento dei reati in questione. Tale diritto di alta vigilanza non è previsto né nell'ambito speciale della pornografia (art. 197 CP) né in quello generale della criminalità in rete; andrebbe pertanto introdotto.

Il gruppo di lavoro propone quindi di creare un articolo 343bis AP-CP, che preveda l'alta vigilanza della Confederazione per il perseguimento di reati commessi mediante reti di comunicazione elettronica.

L'introduzione di tale alta vigilanza permetterebbe inoltre di applicare, oltre all'articolo 259 PP, anche l'articolo 258 PP che conferirebbe alla Confederazione la competenza di impartire istruzioni alle autorità inquirenti dei Cantoni per chiedere loro di aprire un procedimento e di provvedere all'istruzione.

3.16 Variante 2 (competenza d'indagine dell'autorità federale competente)

La variante 2 proposta dal gruppo di lavoro "Genesis" rinuncia a introdurre una speciale e generale alta vigilanza della Confederazione, pur perseguendo il medesimo obiettivo della variante 1.

Nei casi di criminalità in rete, in cui i reati sono parzialmente o integralmente commessi all'estero o in più Cantoni, l'autorità federale competente deve poter ordinare singole indagini pressanti senza per questo fondare una giurisdizione federale. Anche in tal caso la Confederazione potrebbe impartire istruzioni ai Cantoni al fine di coordinare le indagini sul piano intercantonale e internazionale.

A tale scopo si propone di creare un articolo 343bis AP-CP, che conferisca alle autorità federali competenti tale facoltà di svolgere indagini e di impartire istruzioni.

[44] RS **312.0.**

3.17 Misure fiancheggiatrici

A guisa di misura fiancheggiatrice, il gruppo di lavoro "Genesis" propone inoltre di completare la legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)[45]. In tal modo si intende imporre ai *provider* l'obbligo di informare le autorità federali competenti in merito a determinati dati contestuali anche al di fuori di un procedimento penale formale. Ne risulterebbe una maggiore celerità nell'assegnare i casi alle autorità inquirenti competenti dei Cantoni[46].

3.2 Parere e proposta del Consiglio federale

L'operazione "Genesis" ha evidenziato la necessità di legiferare in materia di cooperazione tra la Confederazione e i Cantoni allorché sono coinvolti un gran numero di persone e vari Cantoni. Nel caso specifico di "Genesis", la Confederazione ha dovuto affrontare il problema della propria "non competenza" nella prima fase delle indagini, finalizzata in particolare a identificare le singole persone in vista dell'assegnazione alle autorità inquirenti competenti dei Cantoni, a rilevare e a mettere al sicuro il materiale probatorio e a trattare i casi. L'assenza di una competenza di impartire istruzioni ha inoltre impedito di sincronizzare l'avvio delle indagini; ne è conseguita un'informazione differita dell'opinione pubblica, che ha permesso a certune persone implicate di venire a conoscenza delle indagini anzitempo e indi di eliminare le prove. L'analisi presentata dal gruppo di lavoro "Genesis" ha convinto il Consiglio federale della necessità di intervenire sul piano legislativo.

Come menzionato in precedenza (cfr. *supra* n. 2.2), combattere e perseguire in modo efficace la criminalità in rete è altresì un obiettivo dichiarato del programma di legislatura 2003-2007 del Consiglio federale.

3.21 Non spetta alla Confederazione perseguire la criminalità in rete

Il Consiglio federale ha soppesato vantaggi e svantaggi dei due modelli proposti, ossia la *competenza della Confederazione*, suggerita dalla commissione peritale "Criminalità in rete" (cfr. *supra* n. 2.12), e la *possibilità per la Confederazione di condurre indagini nella prima fase procedurale,* raccomandata dal gruppo di lavoro "Genesis" (cfr. *supra* n. 3.14 - 3.16). Il Consiglio federale è contrario a una competenza della Confederazione nel senso di una giurisdizione federale; a sostegno del suo parere adduce i motivi esposti qui di seguito.

La competenza della Confederazione metterebbe in discussione la suddivisione dei compiti nell'ambito del perseguimento penale, sancita dalla Costituzione (competenza cantonale quale regola, giurisdizione federale quale eccezione), poiché costringerebbe i Cantoni a rinunciare a una parte non indifferente delle loro competenze. Attribuendo le competenze in funzione dello strumento del reato, si rischierebbe inoltre di indagare in parallelo sulla medesima fattispecie. La pornografia diffusa al cinema o nella stampa rientrerebbe ad esempio nella competenza esclusiva dei Cantoni, men-

[45] RS **780.1**.
[46] Rapporto del gruppo di lavoro "Genesis", op. cit., pag. 27 seg.

tre quella diffusa mediante strumenti di comunicazione elettronica competerebbe alla Confederazione. Tale inefficacia nel perseguimento penale va evitata. Inoltre tali indagini altro non sono che le classiche attività di polizia svolte nel caso di reati individuali (interrogatori, sequestri, ecc.). Trattandosi di attività in cui i Cantoni hanno maturato più esperienza, le autorità inquirenti della Confederazione dipenderebbero dai Cantoni per il sostegno personale e logistico, soprattutto nelle grosse operazioni. Ne conseguirebbe un onere troppo elevato per i Cantoni, e questo per un settore che non sarebbe più di loro competenza. L'analisi dell'operazione "Genesis" ha infine permesso di constatare che i problemi principali si concentravano nella prima fase procedurale: non è quindi necessario che la Confederazione conduca l'intero procedimento. Inoltre, l'attuazione della competenza federale richiederebbe parecchio tempo a causa della profonda trasformazione necessaria nel sistema di perseguimento penale e renderebbe necessaria una riorganizzazione dei relativi settori della Confederazione. Occorrerebbe pure aumentare in maniera consistente le risorse finanziarie e il personale della Confederazione, analogamente a quanto chiesto nell'ambito del progetto efficienza, richiesta insostenibile vista l'attuale situazione delle finanze federali.

3.22 Competenze d'indagine delle autorità federali

Il Consiglio federale condivide il giudizio del gruppo di lavoro "Genesis", che evidenzia una lacuna nell'attuale sistema di perseguimento penale nell'ambito dalla criminalità in rete. Tale lacuna può essere colmata conferendo alle autorità federali la possibilità di indagare nella prima fase procedurale.

Il Consiglio federale ha esaminato con cura le due varianti proposte dal gruppo di lavoro "Genesis" (cfr. *supra* n. 3.15 e 3.16).

Entrambe le varianti si prefiggono il medesimo obiettivo, ossia di attribuire alla Confederazione la competenza di indagare e di impartire istruzioni nei casi che coinvolgono un gran numero di persone e, presumibilmente, vari Cantoni. Tuttavia, le soluzioni adottate a tal scopo divergono alquanto.

La *variante 1* punta su un *diritto di alta vigilanza* della Confederazione, alla stregua di quanto accade nel diritto in materia di stupefacenti (LStup). Tuttavia, nella LStup, l'alta vigilanza della Confederazione porta sull'intero atto normativo e non soltanto sulle disposizioni penali. Un'alta vigilanza limitata esclusivamente al perseguimento di determinati reati secondo il Codice penale, così come proposta dal gruppo di lavoro "Genesis", costituirebbe una novità assoluta e risulterebbe poco definita. Il Consiglio federale si rende conto di come questa variante permetta alle autorità inquirenti di adottare procedure comprovate e familiari perché riprese dalla LStup. Tuttavia sussiste qualche differenza rispetto all'ambito della criminalità in rete, dove verrebbe infatti fondata un'alta vigilanza in merito a un numero imprecisato di disposizioni del Codice penale e del diritto penale accessorio. Ecco perché il Consiglio federale esclude tale variante.

La *variante 2* del gruppo di lavoro "Genesis" permette di raggiungere lo stesso obiettivo in direttissima. Le nuove competenze della Confederazione sono oggetto di una definizione diretta ed esaustiva nel Codice penale. Tuttavia, il tenore della variante

2[47] non soddisfa del tutto i criteri di chiarezza e di precisione in termini di lingua e di contenuto, richiesti nel Codice penale, fatto suscettibile di infondere insicurezza nelle autorità chiamate ad applicare il diritto. Inoltre il passo "…o in più Cantoni…" esclude tutti i casi in cui le persone sospette sono sì più di una, ma è coinvolto soltanto un Cantone. Allo stesso modo il testo proposto non si applicherebbe nemmeno nel caso di una sola persona sospetta e più Cantoni coinvolti. Ecco perché tale normativa appare poco adeguata

Partendo da tale variante 2, il Consiglio federale propone un nuovo articolo 344 AP-CP (cfr. *infra* n. 3.3). Il nuovo articolo permette all'MPC e alla PGF di svolgere le prime indagini pressanti nei casi in cui un reato sottoposto alla giurisdizione cantonale è stato commesso mediante reti di comunicazione elettronica e il Cantone competente non è ancora stato determinato. Tali competenze d'indagine dell'MPC e della PGF nella prima fase procedurale non fondano alcuna giurisdizione federale (cfr. *infra* n. 3.4). La PGF può inoltre coordinare le indagini impartendo istruzioni.

Sebbene tale proposta estenda di poco le competenze d'indagine della Confederazione, la sua attuazione richiede risorse in termini di persone e di mezzi finanziari. Una prima stima ritiene necessario creare circa 13 posti federali supplementari. Va considerato che tale stima poggia su valori empirici relativi al coordinamento di procedure nell'ambito della pedopornografia. Tuttavia le risorse da attribuire alle autorità inquirenti dovranno orientarsi in una certa misura anche al crescente potenziale criminoso di questo fenomeno sociale.

Il Consiglio federale si rende conto che le competenze proposte per la Confederazione rientrano nell'ambito della giurisdizione cantonale, ragion per cui andrebbero disciplinate nel Codice di procedura penale svizzero. Tuttavia occorre legiferare subito in materia di criminalità in rete, mentre passeranno ancora vari anni prima che tale Codice entri in vigore. Ecco perché si è optato per la via più rapida, consistente nel completare il Codice penale.

Il Consiglio federale ritiene che il nuovo articolo 344 AP-CP sia una normativa necessaria e opportuna, atta a migliorare la cooperazione tra la Confederazione e i Cantoni e a rendere quindi più efficace il perseguimento della criminalità in rete.

3.23 Misure fiancheggiatrici

Per i motivi esposti in precedenza (cfr. *supra* n. 2.223) e contrariamente a quanto proposto dal gruppo di lavoro "Genesis" (cfr. *supra* n. 3.17), il Consiglio federale non ritiene necessario completare la LCPT[48].

[47] Rapporto del gruppo di lavoro "Genesis", op. cit., pag. 21
[48] RS **780.1**.

3.3 Commento dell’articolo 344 AP-CP (competenze della Confederazione in caso di reati commessi mediante reti di comunicazione elettronica)

Il nuovo articolo 344 AP-CP tiene conto delle peculiarità del perseguimento penale nei casi di criminalità in rete sottoposti alla giurisdizione cantonale e per i quali le autorità federali (MPC e/o PGF), sulla base delle informazioni disponibili, non conoscono ancora né le autorità inquirenti né i Cantoni cui spetta la competenza. Rientrano tra l’altro in tale fattispecie anche i casi in cui le autorità federali ricevono informazioni dall’estero, in base a cui un gran numero di persone in vari Cantoni è sospettato di aver commesso un reato. È comunque pure ipotizzabile che l’informazione provenga dalla Svizzera e che gli indiziati siano assoggettati alle autorità inquirenti di un unico Cantone, non ancora noto in questa fase procedurale. In questi casi non ha senso – e l’analisi dell’operazione "Genesi" lo ha mostrato in modo inequivocabile – trasmettere tali informazioni, così come sono state ricevute, a tutti i Cantoni affinché ciascuno svolga per sé le stesse indagini, tra l’altro per accertare la propria competenza. È proprio questa fase di inchiesta preliminare a costituire il vero problema.

3.31 Collocazione sistematica e titolo marginale del nuovo articolo 344 AP-CP

La collocazione sistematica come nuovo articolo 344 AP-CP con il numero marginale 3, inserito dopo l’attuale articolo 343 CP dal titolo marginale "2. Giurisdizione cantonale", intende puntualizzare che la disposizione non crea una nuova giurisdizione federale. Onde escludere qualsiasi incertezza in merito, il capoverso 1 esplicita il concetto recitando "... un reato sottoposto alla giurisdizione cantonale …". Il titolo marginale parla di "competenze" per specificare che non sono intese soltanto le competenze d’indagine, ma anche le competenze di impartire istruzioni e di coordinare le indagini, come esplicitato al capoverso 2 dell’articolo 344 AP-CP.

3.32 Capoverso 1

Il nuovo articolo 344 AP-CP è inteso in particolare per i casi la cui complessità è determinata da due circostanze: i reati segnalati in Svizzera o all'estero sono stati commessi da un gran numero di persone in vari Cantoni e il mondo virtuale delle reti di comunicazione elettronica richiede metodi investigativi che si differenzino da quelle del mondo reale e si sviluppino a pari passo con il progresso tecnico. Il testo proposto è formulato in modo generico affinché le autorità inquirenti della Confederazione possano avviare le indagini in ogni caso sottoposto alla giurisdizione cantonale e comprendente un reato commesso medianti reti di comunicazione elettronica, a condizione che non sia ancora stato determinato il Cantone cui compete il perseguimento penale. Per poter svolgere le prime indagini necessarie, l'MPC e la PGF necessitano di una competenza legale di cui non dispongono in virtù del diritto in vigore. L'MPC e la PGF indagano a norma degli articoli 100 segg. PP. All'MPC compete la direzione della polizia giudiziaria (art. 15 e 17 PP). La PGF svolge il lavoro principale di cui alla nuova disposizione, vale a dire che si occupa di curare i contatti con i Cantoni e di analizzare e preparare le informazioni ricevute. In questa prima fase procedurale in cui la competenza spetta alla Confederazione, anche la polizia cantonale fa parte della polizia giudiziaria della Confederazione nella misura in cui contribuisce

alle prime indagini (art. 17 PP). L'MPC le trasmette il caso in conformità con l'articolo 107 PP dopo aver svolto le prime indagini pressanti.

L'espressione "le prime indagini pressanti" comprende sia le indagini svolte per determinare le autorità inquirenti competenti dei Cantoni sia tutti i provvedimenti immediati volti ad assicurare le prove. Alla luce delle esperienze maturate finora, si tratta in particolare di indagini di carattere tecnico, finalizzate a identificare i detentori delle carte di credito presso le banche e le società emittenti come pure i titolari sospetti di indirizzi e-mail presso i provider svizzeri. Il contesto tecnico in rapida evoluzione non permette tuttavia di considerare esaustive le misure elencate.

3.33 Capoverso 2

Il capoverso 2 conferisce alla PGF il diritto di impartire istruzioni alle autorità inquirenti cantonali nei procedimenti di cui al capoverso 1. La disposizione si prefigge di garantire, tra l'altro, che le indagini vengano avviate in parallelo e che il pubblico venga informato in concomitanza. Lo scopo è di evitare che persone implicate vengano a conoscenza delle indagini e possano eliminare prove preziose – come avvenuto nel corso dell'operazione "Genesis".

Il capoverso 2 contempla le istruzioni nel caso specifico e non le istruzioni generali altrimenti usate quale strumento di vigilanza. I destinatari infatti non sono i governi cantonali, ma le autorità inquirenti dei Cantoni. Al contrario delle istruzioni generali volte ad attuare il diritto federale, ad esempio sotto forma di circolare, tali istruzioni delle autorità federali all'indirizzo di determinate autorità cantonali sono inconsuete poiché costituiscono un'interferenza nell'ordinamento intercantonale delle competenze. Tuttavia la competenza di impartire istruzioni va per quanto possibile disciplinata in una legge, nella misura in cui risulti giustificata dal profilo materiale. Ecco perché il capoverso 2 sancisce tale competenza.

Il concetto stesso di istruzione e l'assenza di mezzi per procedere rendono superfluo l'aggettivo "vincolante" previsto nella variante 2 del gruppo di lavoro "Genesis"[49]. Infatti un'istruzione è sempre vincolante, altrimenti diventa una raccomandazione.

3.4 Codice penale militare

Per il Codice penale militare non è necessario un disciplinamento analogo a quello proposto dall'avamprogetto B, dal momento che sono difficilmente concepibili casi pertinenti inerenti alla sfera militare. Inoltre il Codice penale militare prevede di deferire tali casi alle autorità civili competenti (cfr. art. 221 CPM).

[49] Rapporto del gruppo di lavoro "Genesis", op. cit., pag. 21.

3.5 Avamprogetto B Codice penale svizzero

Articolo 344 AP-CP

3. Competenze della Confederazione in caso di reati commessi mediante reti di comunicazione elettronica

[1] Se sorge il sospetto che un reato sottoposto alla giurisdizione cantonale sia stato commesso mediante reti di comunicazione elettronica e se non è ancora stato determinato il Cantone cui compete il perseguimento penale, il Ministero pubblico della Confederazione e la Polizia giudiziaria federale possono svolgere le prime indagini pressanti. Nel farlo applicano la legge federale del 15 giugno 1934 sulla procedura penale.

[2] La Polizia giudiziaria federale può coordinare le indagini impartendo istruzioni alle autorità cantonali di perseguimento penale.