10.058

Messaggio concernente l'approvazione e l'attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità

del 18 giugno 2010

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il messaggio concernente l'approvazione e l'attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità.

Nel contempo, vi proponiamo di togliere di ruolo il seguente intervento parlamentare:

2001 M 07.3629 Convenzione sulla criminalità informatica
(N Glanzmann-Hunkeler, 3.10.2007)

Gradite, onorevoli presidenti e consiglieri, l'espressione della nostra alta considerazione.

18 giugno 2010

In nome del Consiglio federale svizzero:

La presidente della Confederazione, Doris Leuthard
La cancelliera della Confederazione, Corina Casanova

Compendio

La Convenzione del Consiglio d'Europa del 23 novembre 2001 sulla cibercriminalità (o criminalità informatica), entrata in vigore il 1° luglio 2004, è il primo, e finora unico, trattato internazionale sulla criminalità informatica e in rete. Gli Stati aderenti sono tenuti ad adeguare la propria legislazione alle sfide delle nuove tecnologie informatiche. La Svizzera soddisfa già molti dei requisiti per l'attuazione, tuttavia è necessario apportare ancora alcune modifiche puntuali al Codice penale e alla legge sull'assistenza in materia penale, nonché presentare alcune riserve e dichiarazioni all'atto della ratifica.

Nella prima parte la Convenzione contiene disposizioni penali sostanziali, che mirano ad armonizzare il diritto penale degli Stati aderenti. Nella seconda parte vengono fissate le regole da seguire nella procedura penale, prevalentemente per l'acquisizione e la conservazione di prove costituite da dati elettronici nelle inchieste penali. Infine, vengono stabiliti i criteri della cooperazione internazionale in materia penale, che deve essere caratterizzata da rapidità ed efficienza.

La Svizzera ha sottoscritto la Convenzione il 23 novembre 2001. Il Codice di diritto processuale penale svizzero approvato dal Parlamento il 5 ottobre 2007, che entrerà in vigore il 1° gennaio 2011, soddisfa i requisiti della Convenzione. Inoltre il Parlamento ha accolto la mozione Glanzmann-Hunkeler (07.3629) riguardante la ratifica della Convenzione del Consiglio d'Europa.

Grazie alle disposizioni in materia di «diritto penale informatico», entrate in vigore il 1° gennaio 1995, il diritto penale sostanziale rispetta per ampi tratti i requisiti della Convenzione. Occorre però adeguare la fattispecie penale dell'accesso illegale a un sistema per l'elaborazione di dati, il cosiddetto hacking (art. 143bis CP). A tal fine si prevede di ampliare la gamma di atti passibili di pena, in modo da rendere perseguibili anche coloro che mettono a disposizione programmi, password o altri dati nella consapevolezza che saranno usati per accedere illegalmente a un sistema informatico. Inoltre, sebbene non richiesto dalla Convenzione, si propone di eliminare dall'articolo 143bis CP la caratteristica, criticata a varie riprese, dell'assenza di fini di lucro.

Nell'ambito della cooperazione internazionale, per l'attuazione degli articoli 30 e 33 della Convenzione, è indispensabile introdurre una nuova disposizione (nuovo art. 18b AIMP), che attribuisca all'autorità d'esecuzione svizzera la facoltà di ordinare la trasmissione dei dati elettronici relativi al traffico informatico prima della conclusione della procedura di assistenza giudiziaria. Questa misura è giustificata dalla labilità dei dati elettronici. Tuttavia, la sua applicazione è prevista soltanto in due casi ben determinati ed è soggetta a restrizioni tali da garantire un'adeguata protezione dei diritti degli interessati. La revisione proposta non riguarda i dati relativi al contenuto di comunicazioni elettroniche.

Indice

Messaggio

1 Punti essenziali della Convenzione

1.1 Situazione iniziale e genesi della Convenzione

Lo sviluppo sempre più rapido e avanzato delle tecnologie informatiche sottopone tutta la nostra società a una continua trasformazione e permette, tra l'altro, di semplificare operazioni e compiti quotidiani nell'ambito della comunicazione: nel giro di pochi secondi i dati desiderati possono essere inviati a destinatari in tutto il mondo oppure comunicati a numerose persone e istituzioni, indipendentemente dal luogo in cui hanno origine o sono conservati. Le informazioni salvate nei sistemi informatici possono essere consultate, richiamate e scaricate da una cerchia definita o indefinita di persone.

Ai vantaggi economici, politici e sociali di questo sviluppo globale si contrappongono, però, anche conseguenze negative. Lo sviluppo tecnologico, da cui ampie fasce della popolazione traggono beneficio, permette al contempo di compiere nuovi reati oppure reati «tradizionali» con nuovi mezzi «digitali». La frode perpetrata utilizzando reti informatiche, la diffusione di contenuti illeciti tramite Internet e l'istigazione all'odio, alla violenza e al terrorismo sono solo alcuni degli aspetti che la collettività e le organizzazioni nazionali e internazionali si trovano a dover affrontare da qualche tempo.

Nell'aprile 1997 un gruppo di esperti incaricato dal Comitato dei ministri del Consiglio d'Europa iniziò a elaborare una bozza di convenzione sulla cibercriminalità. Oltre agli Stati membri, parteciparono ai negoziati gli Stati Uniti d'America, il Canada, il Sud Africa e il Giappone. I lavori proseguirono fino alla primavera del 2001. Dopo l'approvazione del testo da parte delle competenti commissioni, la Convenzione fu sottoscritta a Budapest il 23 novembre 2001; tra i firmatari figurava anche la Svizzera. La Convenzione è entrata in vigore il 1° luglio 2004 e finora è stata ratificata da 26 Stati[1].

1.2 Contenuto della Convenzione

La Convenzione del Consiglio d'Europa sulla cibercriminalità è il primo, e finora l'unico, trattato internazionale sulla criminalità informatica e in rete. Gli Stati aderenti si impegnano ad adeguare il proprio diritto penale sostanziale, il proprio diritto processuale penale e le proprie norme in materia di assistenza giudiziaria alle sfide poste dalle nuove tecnologie informatiche.

La prima parte della Convenzione contiene disposizioni penali sostanziali, che mirano ad armonizzare il diritto penale delle Parti, le quali sono tra l'altro obbligate a punire la frode informatica, il furto di dati, la falsificazione di documenti mediante computer e l'accesso a sistemi informatici protetti (art. 2–8), nonché ogni forma di pedopornografia in Internet e la sua diffusione (art. 9). Vanno inoltre rese punibili le

[1] Stato: maggio 2010. Il testo della Convenzione e del rapporto esplicativo del Consiglio d'Europa (a cui si farà riferimento anche in seguito) è consultabile alla pagina internet: http://conventions.coe.int (STE n. 185).

violazioni del diritto dei beni immateriali commesse per via elettronica (art. 10), e le imprese devono essere obbligate a rispondere dei reati definiti dalla Convenzione (art. 12).

Nella seconda parte vengono fissate le norme per la procedura penale. Sono prevalentemente contemplate le questioni legate all'acquisizione e alla conservazione di prove costituite da dati elettronici nelle inchieste penali (art. 16–21). I dati elettronici possono essere modificati nel giro di pochi secondi, accedendovi anche a grande distanza. È quindi necessario garantire che, nel caso di un'inchiesta penale, tali dati possano essere prodotti nella loro forma autentica, senza il rischio che vengano falsificati o eliminati nel corso della procedura. Ciò presuppone che alle autorità inquirenti sia attribuita la facoltà di accedere rapidamente ai dati in questione per poterli conservare inalterati.

Infine, la terza parte della Convenzione stabilisce i criteri della cooperazione internazionale in materia penale (assistenza giudiziaria, estradizione, misure provvisorie ecc.; art. 23–35), che deve essere impostata sulla rapidità e l'efficienza.

1.3 Valutazione della Convenzione

La Convenzione del Consiglio d'Europa sulla cibercriminalità risponde alle nuove sfide poste dalle tecnologie informatiche[2] che la comunità internazionale si trova a dover affrontare e riconosce la necessità di combattere e prevenire in modo efficace la criminalità in rete non solo all'interno del Paese, ma anche al di fuori dei confini nazionali. L'invito della Convenzione ad armonizzare le legislazioni nazionali su scala europea e globale e a rafforzare la collaborazione internazionale va accolto favorevolmente. Negli Stati che hanno già attuato la Convenzione si stanno registrando i primi effetti positivi. In vari Paesi la legislazione in materia di criminalità informatica è stata adeguata sulla base dei parametri di riferimento stabiliti dalla Convenzione e delle conoscenze messe a disposizione dal Consiglio d'Europa e dai suoi membri.

Tuttavia, il peso attuale della Convenzione sulla cibercriminalità non va sopravvalutato. In molti Paesi l'infrastruttura per la lotta alla cibercriminalità (attrezzatura tecnica e risorse delle autorità, possibilità di sorveglianza) resta da migliorare. Gli Stati aderenti che dispongono di strumenti efficienti e differenziati per la lotta ai crimini informatici e di un corrispondente meccanismo di assistenza giudiziaria reputano limitati gli effetti pratici della Convenzione finora riscontrati, non da ultimo perché manca un sistema di monitoraggio e tali Stati continuano a scambiarsi poche informazioni[3]. Il Consiglio d'Europa e la comunità di Stati si stanno impegnando affinché la Convenzione possa trasformarsi sempre più in uno strumento efficace ed essenziale della lotta alla criminalità in rete. La Svizzera ha contribuito ai lavori e in quanto Stato membro potrà svolgere il proprio ruolo con maggiore vigore.

2 Cfr. n. 1.1.

3 A questa conclusione è giunto anche il Comitato contro la cibercriminalità del Consiglio d'Europa (T-CY) in occasione della sua assemblea annuale.

1.4 Rapporto con l'Unione europea

L'attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità non pone problemi per quanto riguarda la compatibilità del diritto svizzero con il diritto dell'Unione europea (UE). Alla Convenzione ha già aderito un ristretto numero di Stati membri dell'UE, mentre in diversi altri Stati membri si sta procedendo all'attuazione.

1.5 La procedura di consultazione

Con decisione del 13 marzo 2009 il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia (DFGP) di avviare la consultazione in merito all'avamprogetto di modifica del Codice penale svizzero e della legge del 20 marzo 1981 sull'assistenza internazionale in materia penale (AIMP), nonché al relativo rapporto esplicativo. Il DFGP ha quindi invitato i Cantoni, i partiti rappresentati nell'Assemblea federale e le istituzioni e le organizzazioni interessate a esprimere la propria posizione entro il 30 giugno 2009. Sono pervenute 74 risposte.

L'attuazione e la ratifica della Convenzione del Consiglio d'Europa hanno riscosso ampio consenso. 21 Cantoni e la maggioranza dei partiti politici e delle organizzazioni appoggiano espressamente l'adesione della Svizzera alla Convenzione e le modifiche legislative proposte[4]. Alcuni partecipanti chiedono addirittura modifiche più incisive, altri invece reputano troppo ampie le disposizioni proposte. Tre partecipanti chiedono di rinunciare all'attuazione della Convenzione.

I commenti e le critiche relativi alle modifiche di legge proposte sono affrontati nella discussione delle singole disposizioni, nonché nel numero 2.5.

2 Le disposizioni della Convenzione e il loro rapporto con il diritto svizzero

2.1 Capitolo I: Terminologia

Articolo 1 Definizioni

L'articolo 1 definisce i concetti di «sistema informatico», «dati informatici», «fornitore di servizi» (*service provider*) e «dati relativi al traffico informatico» ai fini dell'applicazione della Convenzione. Dai dati relativi al traffico informatico si evincono in particolare informazioni sul mittente, il destinatario, l'orario, la durata, la dimensione e il percorso di un messaggio. In questo la terminologia della Convenzione si discosta dall'articolo 2 lettera g dell'ordinanza del 31 ottobre 2001[5] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT), in cui si fa riferimento ai dati che i fornitori di servizi registrano per certificare gli invii. Inoltre il termine usato nella Convenzione si riferisce al traffico di dati elettronici, mentre l'articolo 2 lettera g OSCPT è applicabile anche alla corrispondenza postale e al traffico delle telecomunicazioni. Il concetto viene analizzato più in dettaglio nel quadro della seconda e della terza parte della Convenzio-

4 Quattro Cantoni hanno rinunciato a esprimersi in merito al contenuto.
5 RS **780.11**

ne[6]. Tuttavia, all'atto pratico, le definizioni dei termini della Convenzione non si discostano in modo sostanziale dai concetti utilizzati in Svizzera.

2.2 Capitolo II: Provvedimenti da adottare a livello nazionale

Articolo 2 Accesso illecito

L'articolo 2 della Convenzione intende uniformare la punibilità dell'attività di hacking su scala internazionale. Devono essere puniti tutti coloro che accedono intenzionalmente e illecitamente a un sistema informatico o a parte di esso. Le Parti possono presentare una dichiarazione[7], in base alla quale, per considerare sanzionabile l'accesso a un sistema informatico, devono sussistere ulteriori condizioni quali la violazione di misure di sicurezza, l'intenzione di procurarsi dati, un altro intento illegale oppure il collegamento a un altro sistema informatico.

L'articolo 143bis del Codice penale svizzero (CP)[8] sanziona l'accesso illecito a dati da parte dei cosiddetti hacker. In base a tale articolo è punibile chiunque, senza fine di lucro, si introduca indebitamente, per mezzo di un dispositivo di trasmissione dei dati, in un sistema altrui per l'elaborazione di dati specialmente protetto contro ogni suo accesso.

I requisiti dell'articolo 2 della Convenzione vengono essenzialmente soddisfatti dall'articolo 143bis CP. L'unica differenza consiste nel presupposto della protezione del sistema previsto da quest'ultimo. Non è tuttavia necessario modificare l'articolo, ma basta dichiarare che, affinché sussista il reato, è necessario che vengano violate le misure di sicurezza del sistema[9]. Altre dichiarazioni in merito all'articolo 2 della Convenzione appaiono invece superflue. La legislazione non deve essere ulteriormente adeguata in relazione a questo punto.

Il tenore dell'articolo 143bis CP, secondo cui è punibile l'azione commessa senza fine di lucro, è stata più volte criticata dalla dottrina[10], la quale contesta il fatto che ai sensi di tale articolo chi agisce per curiosità è passibile di sanzione, mentre, in determinate circostanze, chi agisce a fine di lucro rimane impunito. Questa critica non tiene conto del fatto che l'accesso a un sistema di elaborazione di dati con intento di lucro è spesso finalizzato a reperire dati elettronici per l'utilizzo in proprio o da parte di terzi. In questo caso, la punibilità è garantita dall'articolo 143 CP[11], che

6 Art. 14 segg.
7 Cfr. art. 40 della Convenzione.
8 RS **311**
9 Una dichiarazione di uguale o simile tenore in merito all'art. 2 è già stata rilasciata da numerosi Stati aderenti; cfr. il corrispondente elenco delle dichiarazioni degli Stati all'indirizzo http://conventions.coe.int/. La possibilità di esprimere dichiarazioni e riserve è stata esplicitamente prevista al momento della stesura della Convenzione come parte integrante del testo tenuto volutamente semplice (cfr. n. 49 e 50 del rapporto esplicativo della Convenzione, nota 1).
10 Ph. Weissenberger, in: *Basler Kommentar, Strafrecht II,* Basilea 2007, n. 25 ad art. 143bis; S. Trechsel et al., *Schweizerisches Strafgesetzbuch, Praxiskommentar*, San Gallo 2008, n. 10 ad art. 143bis.
11 Acquisizione illecita di dati.

prevede una pena addirittura superiore rispetto all'articolo 143bis[12]. Se il soggetto agisce non per procurarsi dei dati, ma per ricavare un profitto dalla propria condotta (per esempio costringendo un terzo a compiere una determinata azione sulla base del semplice accesso a un sistema oppure della minaccia di danneggiamento dei dati), vanno applicate le pertinenti disposizioni penali a tutela del patrimonio o della libertà[13].

Il criterio dell'assenza dell'intento di lucro dell'articolo 143bis CP appare tuttavia controverso e chiaramente il legislatore non intendeva stabilirne l'applicazione unicamente in senso restrittivo. Gli addetti ai lavori si trovano di fronte al non facile quesito sul motivo della restrizione espressa dalla formulazione «senza fine di lucro» e sul fondamento della punibilità dell'azione, ben più riprovevole, commessa *con intento di lucro*[14]. Inoltre, la caratteristica dell'assenza dell'intento di lucro entra inevitabilmente in conflitto con la proposta di ampliare la gamma di atti passibili di pena[15], avanzata in relazione all'articolo 6 della Convenzione al fine di sanzionare anche la diffusione di una password *con* intento di lucro e di evitare possibili lacune in termini di punibilità.

Per tale motivo si propone di cassare la caratteristica dell'assenza dell'intento di lucro nell'articolo 143bis CP (per la dicitura cfr. quanto esposto in merito all'articolo 6 della Convenzione). La fattispecie dell'hacking (attualmente ancora associata all'assenza dell'intento di lucro) viene estesa anche ad azioni commesse a fine di lucro. In tal modo si esplicita la volontà del legislatore di rendere punibile in ogni caso l'accesso a un sistema a fine di lucro e si tengono in considerazione le critiche espresse. Il rischio di una lacuna dell'articolo 143bis CP in termini di punibilità viene così arginato: se, con intento di lucro, un soggetto penetra per via elettronica in un sistema protetto e si appropria dei dati ivi contenuti, è punibile come in passato per acquisizione illecita di dati (art. 143 CP), in quanto compie un reato ai sensi dell'articolo 143bis CP.

Articolo 3 Intercettazione illecita

Ai sensi dell'articolo 3 della Convenzione, commette un reato chi con strumenti tecnici intercetta intenzionalmente e illecitamente dati informatici non pubblici, incluse le emissioni elettromagnetiche. Per *intercettazione* si intende l'ascolto, la sorveglianza, il reperimento oppure la registrazione di dati[16]. Come per l'articolo 2 della Convenzione, le Parti hanno la possibilità di stabilire ulteriori condizioni per la configurazione di questo reato, quali il collegamento del sistema intercettato a un altro sistema informatico oppure l'esistenza di un ulteriore intento illegale. Nel diritto penale svizzero non esiste alcuna disposizione equivalente all'articolo 3 della Convenzione, i cui requisiti sono solo parzialmente soddisfatti da varie norme. L'articolo 321ter CP tutela il segreto postale e delle telecomunicazioni, la cui violazione è punita con una pena detentiva sino a tre anni o con una pena pecuniaria. A

12 Questa concezione è stata difesa anche nell'ambito dei dibattiti parlamentari, cfr. boll. sten. del Consiglio Nazionale, 1993, pag. 935 segg.
13 Cfr. p. es. l'art. 156 (estorsione) oppure l'art. 181 CP (coazione).
14 Nel disegno di legge originario del Consiglio federale le due norme contenute negli art. 143 e 143bis CP erano unificate (cfr. FF **1991** II 829). In questa versione iniziale, l'atto compiuto senza fine di lucro era considerato una variante della fattispecie principale.
15 Cfr. ibid.
16 N. 53 del rapporto esplicativo della Convenzione (cfr. nota 1).

differenza di quanto richiesto dalla Convenzione, però, questo articolo si applica essenzialmente ai funzionari e ad altri soggetti che occupano posizioni di particolare rilevanza. La fattispecie di reato stabilita nell'articolo 143bis CP (hacking) si limita all'accesso a un sistema informatico; la norma non tutela i dispositivi di trasmissione come tali, se non quando costituiscono impianti informatici ai sensi dell'articolo stesso[17].

In base all'articolo 143 CP[18], è punibile colui che con intento di lucro si procura dati a lui non destinati e specialmente protetti contro il suo accesso non autorizzato, registrati o trasmessi elettronicamente o in modo simile. Con il termine *procurarsi* ai sensi del Codice penale si intende l'acquisizione della facoltà di disporre dei dati. Non è necessario che il soggetto salvi le informazioni su un supporto informatico di sua proprietà. È sufficiente che possa impiegare le conoscenze acquisite per i suoi fini[19]. L'atto di procurarsi dati ai sensi del Codice penale comprende in particolare l'intercettazione e l'ascolto di emissioni elettromagnetiche provenienti da un sistema informatico o un impianto di trasmissione di dati[20].

Il requisito della protezione limita il campo di applicazione dell'articolo 143 CP ai casi in cui il soggetto autorizzato al trattamento dei dati esprime la volontà che i dati non siano accessibili oppure lo siano solo limitatamente. Oltre che chiudendo a chiave stanze e contenitori, questo scopo può essere dichiarato e raggiunto utilizzando sistemi di cifratura, codici di accesso, chiavi biometriche oppure password. La protezione deve essere *sufficiente, in condizioni normali,* a impedire l'accesso non autorizzato[21]. Non è per esempio necessario che vengano adottate altre specifiche misure di sicurezza[22] in aggiunta a una comune protezione contro gli accessi indesiderati e i virus. L'accesso illecito a dati non protetti o il loro utilizzo non autorizzato[23] non rientrano per contro nella fattispecie di reato in questione.

L'articolo 3 della Convenzione si riferisce, tuttavia, solo all'intercettazione illecita di *trasmissioni* di dati informatici, alle quali di norma sono imposti solo limitati requisiti di sicurezza[24]. In questi casi, la punibilità ai sensi dell'articolo 143 CP non va di regola vincolata alla presenza di protezioni supplementari, come l'utilizzo di tecniche di cifratura, nella misura in cui le circostanze rendono palese che i dati non devono essere accessibili[25]. L'articolo 143 CP rispetta quindi le disposizioni dell'articolo 3 della Convenzione. Il traffico non pubblico di dati non deve essere assoggettato a condizioni di protezione particolari. Le disposizioni del Codice penale prevedono, tuttavia, che l'azione persegua fini di lucro. È quindi necessario presentare una corrispondente dichiarazione.

17 N. Schmid, *Computerkriminalität*, Zurigo 1994, § 5 n. 16.
18 Acquisizione illecita di dati.
19 Eventualmente, senza però effettivamente farne uso (N. Schmid, op. cit., § 4 n. 40 seg.).
20 N. Schmid, loc. cit., § 4 n. 30 e n. 51.
21 Cfr. Weissenberger, op. cit., n. 18 ad art. 143.
22 P. es. in caso di attacco con i cosiddetti «virus troiani»; cfr. sentenza della 2ª Corte penale del Tribunale superiore del Cantone di Berna del 13.09.2007, n. SK 2007/187.
23 P. es. in caso di computer utilizzato da più utenti oppure di uso illecito di dati ricevuti in custodia.
24 Cfr. Chr. Schwarzenegger, «*Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime*», in: *Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel*, Zurigo 2002, pag. 305 segg.
25 P. es., a seconda dell'accessibilità dei dati, il server attraverso cui vengono scambiati deve disporre di misure di sicurezza simili a quelle di una postazione di lavoro collegata in rete, mentre le linee attraverso cui passano i dati in sé non devono essere di norma protette contro possibili accessi in modo speciale (sistemi di allarme, canali protetti per cavi).

In base al rapporto esplicativo della Convenzione[26], anche il flusso di informazioni all'interno di un computer costituisce una trasmissione di dati ai sensi dell'articolo 3. Tale flusso comprende, tra l'altro, le trasmissioni *wireless*, rese sempre più frequenti dal crescente sviluppo tecnologico, tra computer e dispositivi periferici (p. es. stampanti, tastiere, schermi). I dati così trasmessi possono essere intercettati se si dispone di attrezzature tecniche e conoscenze adeguate e se il livello di sicurezza è basso; ciononostante sono considerati sicuri contro accessi indebiti grazie al loro carattere non pubblico, al loro percorso generalmente limitato, nonché al fatto che chi desidera appropriarsene illecitamente deve prendere specifici provvedimenti per accedervi. L'articolo 143 CP può essere applicato anche in questo caso[27]. Non è necessario ricorrere a una modifica della legislazione in aggiunta alla dichiarazione menzionata in precedenza.

Articolo 4 Attacco all'integrità dei dati

L'articolo 4 della Convenzione punisce il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici, commessi intenzionalmente e illecitamente. Una Parte può riservarsi il diritto di esigere il verificarsi di un danno considerevole come presupposto per la punibilità[28].

Ai sensi dell'articolo 144bis CP (Danneggiamento di dati), è punito, a querela di parte, chiunque illecitamente cancelli, modifichi o renda inservibili dati registrati o trasmessi elettronicamente o in modo simile. Rende inservibili i dati chiunque ne impedisca l'uso – anche solo temporaneamente – alla persona che ha diritto di utilizzarli[29]. La fattispecie risulta adempiuta già con l'esecuzione di un cosiddetto «attacco *denial of service*», che consiste nell'invio incessante di pacchetti di dati a un computer, il cui funzionamento viene così (temporaneamente) bloccato[30]. La soppressione di dati ai sensi della Convenzione è quindi coperta dal diritto vigente. Lo stesso vale per il danneggiamento e il deterioramento, che rientrano nelle varianti dell'alterazione/inservibilità. Il requisito della punibilità è garantito dall'articolo 144bis CP.

Articolo 5 Attacco all'integrità di un sistema

In base all'articolo 5 della Convenzione, è punibile chiunque ostacoli, intenzionalmente, illecitamente e in modo serio il funzionamento di un sistema informatico inserendo, trasmettendo, danneggiando, cancellando, deteriorando, alterando o sopprimendo dati informatici. Con l'espressione *in modo serio* si intende in particolare l'invio di dati in forma, quantità o frequenza tali da ostacolare notevolmente il funzionamento di un computer[31]. L'invio di e-mail di massa[32] non richiesto non è coperto dalla disposizione[33].

26 N. 55; cfr. nota 1.
27 Se una persona viene a conoscenza di «emissioni» di terzi senza un'azione mirata o senza la sua volontà, p. es. attraverso un router, manca il corrispondente intento doloso.
28 Art. 42 della Convenzione. Alcuni Stati hanno già sfruttato la possibilità di avanzare tale riserva, cfr. http://conventions.coe.int/.
29 N. Schmid, op. cit., n. 29 ad art. 144bis; Stratenwerth, loc. cit., n. 49 in relazione al § 14; cfr. anche n. 61 del rapporto esplicativo (nota 1).
30 Cfr. Weissenberger, op. cit., n. 23 ad art. 144bis.
31 Cfr. sopra: blocco doloso di un computer, n. 67 del rapporto esplicativo (nota 1).

La fattispecie rientra nel reato di danneggiamento dei dati di cui all'articolo 144bis CP, che punisce chiunque renda i dati (anche temporaneamente) inservibili e impedisca di accedervi per un periodo di tempo considerevole[34].

Articolo 6 Uso abusivo di dispositivi

Disposizioni della Convenzione

L'articolo 6 della Convenzione punisce chiunque illecitamente e intenzionalmente produca, venda, procuri per l'uso, importi, distribuisca o metta a disposizione in altro modo dispositivi, programmi[35], codici di accesso e password utilizzati per commettere un reato ai sensi dei precedenti articoli[36]. Oltre che l'atto in sé, dev'essere intenzionale anche il compimento dei reati di cui agli articoli 2–5[37]. In altre parole: chiunque venda o ceda un programma deve farlo deliberatamente e nella consapevolezza che esso verrà utilizzato nell'ambito di uno dei reati descritti. Altrettanto punibile è il possesso di tali elementi con l'intento di utilizzarli per compiere uno dei reati citati[38].

Anche in questo caso la Convenzione offre agli Stati membri la possibilità di esprimere riserve e introdurre deroghe vincolando, ad esempio, la punibilità al possesso di un numero minimo di dispositivi. Secondo il paragrafo 3 dell'articolo 6, le Parti possono avvalersi di una riserva generale[39], che però non può pregiudicare la punibilità di chiunque venda, distribuisca o metta a disposizione password, codici o altri dati simili che permettono di accedere a un sistema informatico.

Integrazione dell'articolo 143bis CP

Ai sensi dell'articolo 144bis numero 2 CP deve essere punito chiunque allestisca, introduca, metta in circolazione, propagandi, offra o renda comunque accessibili programmi che sa o deve presumere destinati al danneggiamento o alla modifica di dati, o dia indicazioni per allestirli. Si tratta di una disposizione penale contro i cosiddetti virus informatici, che sanziona gli atti preliminari risultanti in un danneggiamento dei dati. Per il danneggiamento di dati commesso da un terzo è sufficiente il dolo eventuale[40].

L'articolo 6 della Convenzione è coperto, nella sua essenza, dal menzionato articolo del Codice penale. Inoltre, ai casi particolari in cui lo scopo non consiste nel modificare o cancellare i dati oppure in cui non si mettono in circolazione programmi, possono essere applicate le disposizioni sul tentativo e la complicità[41] in combinato disposto con gli articoli 143 e 143bis CP.

32 «*Spamming*». Il 1° aprile 2007 è entrata in vigore una disposizione corrispondente (art. 3 lett. o della legge federale del 19 dicembre 1986 contro la concorrenza sleale; RS **241**, FF **2003** 6883).
33 N. 69 del rapporto esplicativo (cfr. nota 1).
34 Cfr. commento all'art. 4 della Convenzione.
35 P. es. programmi virus, cfr. n. 72 del rapporto esplicativo (nota 1).
36 Art. 6 par. 1 lett. a.
37 Art. 6 par. 1 lett. a *in fine*.
38 Art. 6 par. 1 lett. b.
39 Art. 42 della Convenzione.
40 Cfr. DTF **129** IV 230.
41 Art. 22 e art. 25 CP.

Sulla base di quanto affermato dalla dottrina e dalla giurisprudenza in merito al tentativo (incompiuto) ai sensi dell'articolo 22 capoverso 1 CP[42], in determinate circostanze la produzione o il possesso di dispositivi o programmi con l'intenzione di utilizzarli illegalmente possono essere considerati un tentativo di questo tipo, soggetto a sanzione. Se esistono prove legalmente sufficienti a dimostrazione che il produttore o detentore perseguiva uno scopo illegale – presupposto da cui parte la Convenzione – significa che la persona in questione ha verosimilmente manifestato il suo intento concretizzando il tentativo (pur non avendo fatto il necessario per portare a termine l'atto).

Viene punito come complice chiunque aiuti intenzionalmente altri a commettere un crimine o un delitto e dunque favorisca in via subordinata l'atto intenzionale di un terzo[43]. Non è necessario che il complice conosca né la vittima né l'autore né le specifiche modalità del reato[44]. Chi introduce, procura e distribuisce intenzionalmente dispositivi, password e programmi nella consapevolezza che saranno utilizzati per commettere reati può rendersi complice delle fattispecie penali previste dal diritto informatico. Va tuttavia ricordato che, oltre alla tentata complicità, non è punito nemmeno il favoreggiamento di un atto principale (ancora) intentato. Come spiegato in precedenza, sono indispensabili un collegamento e un nesso in termini di contenuto e di tempo con un reato concretamente pianificato.

In base al principio dell'accessorietà effettiva[45], di norma non è punibile chi possiede o fabbrica un dispositivo con l'intenzione che, in un futuro indeterminato, venga impiegato per scopi illeciti da un terzo indefinito. Manca, infatti, il nesso indispensabile con un atto principale, perlomeno tentato. In base al diritto vigente, se una persona cede, per esempio, un codice di accesso[46] con l'intenzione di renderlo utilizzabile per un reato indefinito, senza che venga però compiuto un reato specifico, tale condotta non è sanzionabile. La Convenzione stabilisce invece il contrario[47]. Occorre quindi integrare l'articolo 143bis con una disposizione che contempli la diffusione illegale di codici d'accesso o dati simili e, analogamente all'articolo 144bis numero 2 CP (danneggiamento di dati), punisca le azioni preliminari al reato di hacking[48].

La diffusione di codici di accesso e altri dati, resa soggetta a sanzione, deve essere configurata come un reato perseguibile d'ufficio. A differenza della variante dell'accesso effettivo, nel caso della semplice diffusione di programmi, non si può di norma identificare alcun oggetto concreto preso di mira né un soggetto avente diritto alla querela. Questo vale, ad esempio, per la diffusione in Internet di dati che fondamentalmente permetterebbero di accedere a una molteplicità di sistemi dotati della stessa protezione.

La formula «sa o deve presumere», utilizzata anche per altre fattispecie, ha principalmente lo scopo di rendere più facile provare l'intenzione dolosa quando l'autore era a conoscenza di circostanze che gli dovevano far supporre un probabile utilizzo

42 Cfr. DTF **114** IV 114, **119** IV 227; S. Trechsel / P. Noll, *Schweizerisches Strafrecht, AT I*, Zurigo 1998, pag. 174 segg.
43 Cfr. S. Trechsel, op. cit., n. 1 ad art. 25.
44 Forster, in: *Basler Kommentar, StGB I*, 2003, n. 19 ad art. 25.
45 Cfr. S. Trechsel, op. cit., n. 24 segg. avanti l'art. 24.
46 E non un programma ai sensi della legge.
47 Cfr. art. 6 par. 3.
48 Cfr. Schmid, op. cit., n. 31 ad art. 143bis.

illecito dei dati[49]. La commissione per negligenza non è punibile. La vendita di dispositivi o dati «*dual use*»[50] continua a essere ammessa a determinate condizioni (cfr. di seguito) e a fronte di determinati provvedimenti. Non sono punibili le misure adottate per garantire la qualità dei sistemi propri e su incarico di terzi. I dubbi espressi a tale proposito dall'industria della tecnologia dell'informazione nell'ambito della procedura di consultazione[51] sono infondati. Altrettanto legale rimane la formazione di specialisti del settore della tecnologia dell'informazione, in cui viene discusso e concretizzato l'impiego di «strumenti di hacking»[52].

Al contrario è punibile (per l'atto in sé e per l'ulteriore utilizzo dei dati) la diffusione intenzionale o irresponsabile di programmi e altri dati, quando il loro contenuto sensibile, la cerchia dei destinatari o altre circostanze fanno apparire evidente l'impiego illecito di tali strumenti. La diffusione irresponsabile di strumenti di hacking tra persone inclini al crimine non deve rimanere impunita.

I test di sicurezza sui sistemi informatici, i cosiddetti «*vulnerability assessment*», eseguiti dal gestore o da un terzo da questi incaricato, così come lo sviluppo di nuovi software a tale scopo sono considerati atti effettuati o predisposti dagli aventi diritto e rimangono impuniti[53].

Inoltre, si prevede di eliminare il requisito giuridico della mancanza dell'intento di lucro (cfr. quanto esposto in relazione all'art. 3 della Convenzione), per rendere plausibile la punibilità degli «atti preliminari» anche dal punto di vista sistematico, indipendentemente dallo scopo di lucro.

La modifica proposta della fattispecie risponde ai requisiti della Convenzione e prevede di limitare, lievemente e in maniera commisurata, i possibili atti sanzionabili rispetto alla fattispecie penale di danneggiamento di dati attualmente in vigore[54]. Saranno pertanto punibili il fatto di *rendere accessibili* e la *messa in circolazione* di dati (due atti interpretabili in senso lato e in parte sovrapposti in termini di contenuto).

Per quanto riguarda il possesso, l'introduzione e la produzione di dati, appare opportuno che la Svizzera avanzi una riserva restrittiva, ammesso che tali atti non puntino a danneggiare o a modificare dati o che non siano da qualificare come forme di complicità o come tentativo punibile di commettere un altro reato[55].

Articolo 7 Falsificazione informatica

Si dichiara punibile l'inserimento, l'alterazione, la cancellazione e la soppressione intenzionali e illeciti di dati, da cui risultano dati non autentici, con l'intento di farli

49 Cfr. Weissenberger, op. cit., n. 67 segg. ad art. 160 con ulteriori rimandi.
50 Dati o dispositivi con possibilità di doppio impiego, ossia legale e illegale.
51 Cfr. n. 1.4.
52 In questo caso vi è una differenza sostanziale rispetto al tenore dell'art. 202*c* del Codice penale tedesco (predisposizione dello spionaggio e dell'intercettazione di dati), che punisce la cessione di tali programmi indipendentemente dall'intenzione di chi agisce e che è stato più volte criticato nella pratica. Il contenuto di questa disposizione è stato però notevolmente relativizzato da una decisione del 18 maggio 2009 della Corte costituzionale federale tedesca.
53 Anche a tale proposito sono stati espressi dubbi durante la procedura di consultazione (cfr. sopra).
54 In particolare per quanto riguarda la produzione e l'introduzione di dati.
55 In particolare art. 143 e 143bis CP.

apparire autentici a fini legali. Le Parti possono rilasciare una dichiarazione[56] per stabilire il presupposto di un'intenzione fraudolenta o altrettanto illegale.

Se l'autore non è autorizzato ad accedere ai dati, si applica la disposizione penale del danneggiamento dei dati[57]. Se invece l'autore interviene su un processo di elaborazione di dati con conseguente danno o trasferimento patrimoniale, si applica l'articolo 147 CP (Abuso di un impianto per l'elaborazione di dati). Del resto, la fattispecie della falsificazione di documenti o del relativo tentativo si applica anche nel caso di documenti e dati elettronici[58]. Pertanto il diritto vigente equivale alla corrispondente disposizione della Convenzione. È tuttavia necessario rilasciare una dichiarazione per specificare che, come elemento aggiuntivo, deve sussistere l'intento di arrecare un danno o di procurare un vantaggio.

Articolo 8 Frode informatica

L'articolo 8 della Convenzione considera punibile chiunque cagioni intenzionalmente e illecitamente un danno patrimoniale a terzi con l'intento fraudolento o illegale di procurare a sé o a un altro un beneficio patrimoniale. Il danno patrimoniale deve essere provocato inserendo, alterando, sopprimendo o cancellando dati informatici (lett. a) oppure danneggiando altrimenti il funzionamento di un sistema informatico (lett. b).

L'articolo 147 CP punisce l'abuso di un impianto per l'elaborazione di dati. La norma penale contempla il caso in cui, a differenza della frode «classica»[59], il trasferimento patrimoniale non è dovuto a un errore umano provocato dall'autore del reato, ma è ottenuto manipolando semplicemente i dati[60]. Si ha utilizzo di dati falsi ai sensi dell'articolo penale ad esempio quando l'autore del reato modifica, cancella, sposta o cambia in altro modo i dati, rendendoli diversi da quelli originari. I dati possono essere considerati non autentici anche quando non vengono inseriti nel momento «giusto». Altrettanto punibile è colui che, «servendosi di un analogo procedimento», interviene su un processo di trattamento o di trasmissione di dati, provocando o dissimulando un trasferimento patrimoniale.

L'articolo 8 della Convenzione è coperto dall'articolo 147 CP. L'avvenuto trasferimento patrimoniale è un fatto oggettivo e deve sussistere perché il reato sia considerato compiuto. Non è invece necessario che l'autore tragga un beneficio effettivo dall'operazione. Anche nel caso di processi di elaborazione di dati, se il trasferimento patrimoniale è dovuto a un errore umano provocato dall'autore del reato, si configura la «normale» fattispecie della frode, che in tal caso ha la precedenza sulla disposizione penale in discussione[61].

Articolo 9 Reati di pedopornografia

Ai sensi dell'articolo 9 della Convenzione è passibile di pena chi, servendosi di un sistema informatico, intenzionalmente offre, rende accessibile, diffonde, trasmette,

56 Art. 40 della Convenzione.
57 Art. 144bis n. 1 CP.
58 Art. 251 in combinato disposto con l'art. 110 cpv. 4 CP.
59 Ai sensi dell'art. 146 CP.
60 Cfr. a questo proposito anche N. Schmid, op. cit., n. 1 in relazione al § 7.
61 Cfr. N. Schmid, loc. cit., n. 161 in relazione al § 7.

reperisce o possiede pedopornografia oppure la produce per la diffusione tramite computer.

L'articolo 197 numeri 3 e 3bis CP punisce le corrispondenti condotte, in particolare il possesso o l'acquisizione di materiale pedopornografico su supporti informatici. Il diritto penale svizzero include anche le «immagini realistiche» («*realistic images*») ai sensi dell'articolo 9 paragrafo 2 lettera c della Convenzione[62]. Non occorre avvalersi di riserve.

L'articolo 9 paragrafo 2 lettera b della Convenzione si riferisce alla raffigurazione di un soggetto che sembra essere un minore («*a person appearing to be a minor*»). Il contenuto della disposizione non è del tutto univoco; nemmeno il rapporto esplicativo fornisce chiarimenti esaustivi a tale proposito. Se si intendono persone la cui minore età non può essere stabilita con certezza, il giudice svizzero può decidere, nell'ambito della apprezzamento delle prove, se effettivamente nella rappresentazione si tratti di un atto con un minore e infliggere all'autore la corrispondente pena. I requisiti della Convenzione sarebbero quindi adempiuti. Se, invece, come diverse versioni linguistiche sembrano indicare, la Convenzione intende la raffigurazione di una persona adulta[63] che ha le sembianze di un minore, la raffigurazione è difficilmente punibile secondo il diritto svizzero in vigore. È vero che tali rappresentazioni possono avere un effetto altrettanto degenerante su chi le guarda, ma il loro potenziale pericoloso e il loro significato reale sono ridotti rispetto agli effetti fatali e degeneranti della rappresentazione pedopornografica «effettiva», sia per i minori vittime di abusi che per gli spettatori. Estendere la punibilità non appare quindi opportuno, poiché si acuirebbero ulteriormente i problemi di delimitazione già esistenti. Si prevede di presentare una riserva in merito all'applicazione in Svizzera della lettera b del paragrafo 2.

Per «minori» ai sensi dell'articolo 197 CP si intendono, stando alla dottrina prevalente e agli addetti del settore, tutti i soggetti di età inferiore ai 16 anni[64], ossia all'età protetta ai sensi dell'articolo 187 CP (Atti sessuali con fanciulli). Secondo una concezione più volte espressa, questa soglia d'età non dovrebbe però essere l'unico criterio per stabilire il divieto assoluto di tali raffigurazioni. Un'analisi approfondita potrebbe rivelare la necessità di sanzionare anche la raffigurazione di giovani al di sopra dei 16 anni, ma fisicamente poco sviluppati; inoltre bisognerebbe considerare come elemento decisivo anche l'impressione convogliata e l'evidente orientamento allo spettatore pedofilo[65]. Nell'ambito dell'implementazione e della ratifica della Convenzione vi è la possibilità di dichiarare[66] l'intenzione di applicare il limite di età di 16 anni anche in riferimento all'articolo 9 paragrafo 3. La Svizzera ricorrerà a tale dichiarazione, dato che il diritto interno prevede normalmente un limite d'età di 16 anni (fatte salve alcune eccezioni).

A livello internazionale aumentano le richieste di introdurre un limite d'età perentorio di 18 anni. La Svizzera non vuole precludersi la possibilità di partecipare a queste riflessioni e discussioni, poiché sono rilevanti anche per il nostro Paese. La necessità e l'opportunità di modificare il limite d'età per la punibilità degli atti

62 Cfr. messaggio del 10 maggio 2000 concernente la modifica del CP e del CPM, FF **2000** 2609.
63 P. es. l'età della persona raffigurata può essere provata.
64 Cfr. Schwaibold/Meng, *Basler Kommentar*, loc. cit., n. 21 segg. ad art. 197.
65 Cfr. sopra.
66 Art. 40 della Convenzione.

sessuali con minori e delle corrispondenti raffigurazioni dovranno essere verificate più in dettaglio nel contesto della programmata firma e successiva attuazione della Convenzione del Consiglio d'Europa per la protezione dei bambini contro lo sfruttamento e gli abusi sessuali del 15 ottobre 2007[67].

Articolo 10 Reati contro la proprietà intellettuale e diritti affini

La Svizzera ha ratificato tutte le convenzioni indicate nell'articolo 10 della Convenzione del Consiglio d'Europa sulla cibercriminalità elencate qui di seguito:

- Convenzione di Berna sulla protezione delle opere letterarie e artistiche, riveduta a Parigi il 24 luglio 1971[68];
- Convenzione internazionale per la protezione degli artisti, interpreti ed esecutori, produttori di fonogrammi e organismi di radiodiffusione del 26 ottobre 1961[69];
- Accordo sugli aspetti commerciali dei diritti sulla proprietà intellettuale[70];
- Trattato OMPI sulla proprietà intellettuale del 20 dicembre 1996[71];
- Trattato OMPI sull'interpretazione e l'esecuzione e i fonogrammi del 20 dicembre 1996[72].

Con la revisione parziale del 5 ottobre 2007[73] della legge sul diritto d'autore (LDA)[74], entrata in vigore il 1° luglio 2008, la legislazione svizzera è stata adeguata ai due trattati OMPI (WCT e WPPT), ratificati ed entrati in vigore in Svizzera contemporaneamente a tale revisione.

Nell'articolo 10 la versione francese, a differenza di quella tedesca, si discosta dalla terminologia comunemente utilizzata in Svizzera[75]. Come precisato nel rapporto esplicativo del Consiglio d'Europa, con l'aggiunta dell'espressione «tenendo fede agli obblighi assunti» in tutti e due i paragrafi dell'articolo 10, si chiarisce che le Parti della presente Convenzione non sono obbligate ad applicare gli accordi elencati a cui non aderiscono[76]. Il testo della Convenzione è quindi formulato in modo che le Parti non siano soggette a obblighi derivanti da trattati internazionali che non hanno ratificato. La Svizzera ha aderito alla Convenzione di Berna, alla Convenzione di Roma, all'Accordo TRIPS e ai Trattati WCT e WPPT. È dunque necessario appurare gli obblighi derivanti da queste convenzioni che è tenuta ad adempiere in seguito all'adesione alla Convenzione del Consiglio d'Europa sulla cibercriminalità.

67 Cfr. http://conventions.coe.int (STE 201).
68 RS **0.231.15**
69 Convenzione di Roma; RS **0.231.171**.
70 Accordo TRIPS, Allegato 1C all'accordo del 15 aprile 1994 che istituisce l'Organizzazione mondiale del commercio; RS **0.632.20**.
71 WCT; RS **0.231.151**
72 WPPT; RS **0.231.171.1**
73 RU **2008** 2497 2502; FF **2006** 3135
74 RS **231.1**
75 Nella versione francese dell'art. 10 viene utilizzata una terminologia leggermente diversa. Il termine «copyright» è tradotto con «propriété intellectuelle» (ted. *geistiges Eigentum*), anziché con «droit d'auteur» (ted. *Urheberrecht*). Inoltre, non sempre sono stati ripresi i titoli ufficiali francesi delle convenzioni internazionali citate (cfr. Accordo TRIPS e Trattato WCT). A livello internazionale, in francese viene utilizzato il termine «droits connexes», mentre in Svizzera questi diritti sono definiti come «droits voisins» (ted. *verwandte Schutzrechte*).
76 N. 110 *in fine* del rapporto esplicativo (nota 1).

Nella LDA la Svizzera ha riconosciuto i diritti sanciti dalle convenzioni ratificate. Gli articoli 67–69*a* definiscono come fattispecie penali la violazione del diritto d'autore e la lesione dei diritti di protezione affini. Queste disposizioni permettono anche di perseguire reati commessi «utilizzando un sistema informatico», come richiesto dall'articolo 10 della Convenzione.

La LDA soddisfa anche il requisito dell'intenzionalità, punendo atti commessi «deliberatamente», e il presupposto che la violazione avvenga «su scala commerciale», stabilendo il perseguimento d'ufficio dei reati commessi «per mestiere». Addirittura si spinge oltre, prevedendo il perseguimento a querela della parte lesa in tutti gli altri casi.

Inoltre, la revisione e l'adeguamento della LDA ai Trattati WCT e WPPT permette alla Svizzera di rispettare tutti gli obblighi imposti dall'articolo 10 della Convenzione.

Articolo 11 Tentativo, complicità e istigazione

L'articolo 11 della Convenzione è coperto dal diritto penale svizzero in vigore e in particolare dagli articoli 22, 24 e 25 CP.

Articolo 12 Responsabilità delle persone giuridiche

Ai sensi dell'articolo 12, una persona giuridica deve poter essere ritenuta responsabile dei reati stabiliti dalla Convenzione commessi a suo vantaggio da una persona fisica con mansioni direttive all'interno dell'impresa (par. 1). Un'impresa deve inoltre poter essere tenuta a rispondere di un reato ai sensi della Convenzione commesso a suo vantaggio da una persona fisica che agisce sotto la sua direzione, se viene dimostrata una mancanza di controllo da parte di una persona con mansioni direttive (par. 2).

La responsabilità può essere di natura civile, amministrativa o penale (par. 3) e non deve pregiudicare l'eventuale responsabilità della persona fisica che ha commesso il reato (par. 4).

Molte convenzioni internazionali in materia di diritto penale degli ultimi anni contengono disposizioni simili, se non addirittura identiche, sulla responsabilità delle persone giuridiche. La Convenzione penale del Consiglio d'Europa sulla corruzione del 27 gennaio 1999[77], per esempio, prevede la responsabilità delle imprese, senza tuttavia affrontare espressamente l'aspetto civile, amministrativo o penale[78]. Le Parti devono assicurarsi che anche le persone giuridiche siano assoggettate ad adeguate sanzioni o misure, incluse sanzioni pecuniarie[79]. La Convenzione salvaguarda il principio ancora ampiamente diffuso, nonostante una tendenza internazionale contraria, secondo cui una persona giuridica non può essere punita.

La responsabilità penale delle persone giuridiche è stata introdotta nel diritto svizzero il 1° ottobre 2003[80]. Una responsabilità primaria dell'impresa sussiste per un numero ridotto di categorie di reato, quando l'impresa può essere accusata di non

77 STE 173, art. 18; RS **0.311.55**.
78 Nel rapporto esplicativo (n. 86) viene tuttavia sottolineato che gli Stati non sono obbligati a introdurre la responsabilità delle persone giuridiche.
79 Cfr. art. 13 della Convenzione.
80 Oggi art. 102 e 102*a* CP.

aver preso tutte le misure ragionevoli e indispensabili per impedire il reato[81]. I reati previsti dalla Convenzione[82] non rientrano nelle categorie di reato menzionate[83].

Nell'ordinamento giuridico svizzero è stata contemporaneamente introdotta anche una responsabilità penale sussidiaria di carattere generale delle persone giuridiche, nel caso in cui il reato sia stato commesso a fini aziendali e non possa essere ascritto a una persona fisica precisa a causa di una carente organizzazione interna[84]. La pena consiste in una multa fino a cinque milioni di franchi. Questa responsabilità penale comprende tutti i crimini e i delitti riconosciuti dall'ordinamento giuridico svizzero[85] e quindi tutti i reati previsti dalla Convenzione. Rispetto a quest'ultima, la responsabilità sancita dal Codice penale svizzero ha una portata più ampia: nel primo caso è limitata ai reati commessi a vantaggio della persona giuridica da parte di un membro della direzione, mentre nel secondo caso insorge come conseguenza di ogni crimine o delitto commesso a fini aziendali da una persona fisica nell'esercizio di un dovere societario. Ai sensi dell'articolo 102 capoverso 1 CP è tuttavia possibile sanzionare una persona giuridica solo quando la condotta non può essere ascritta ad alcuna persona fisica.

L'articolo 12 paragrafo 4 della Convenzione stabilisce che la responsabilità della persona giuridica non deve pregiudicare la responsabilità dell'autore del reato. Tuttavia questa disposizione non impone espressamente agli Stati aderenti alla Convenzione l'obbligo di istituire una responsabilità penale parallela. Il rapporto esplicativo alla Convenzione non fornisce ulteriori chiarimenti a tale proposito.

La responsabilità sussidiaria della persona giuridica prevista dal diritto svizzero non si contrappone alla punibilità della persona fisica e quindi non ne pregiudica la responsabilità. Si applica quando, per carente organizzazione interna dell'impresa, non è possibile comminare una pena all'autore del reato. L'articolo 102 capoverso 1 CP non contraddice quindi l'articolo 12 paragrafo 4 della Convenzione, perché la responsabilità penale della persona fisica che ha commesso il reato non viene esclusa dalla responsabilità sussidiaria dell'impresa. Questa duplice responsabilità è esemplificata dalla seguente situazione: se, condannata l'impresa, viene individuata la persona fisica colpevole della condotta illecita e se l'iniziale impossibilità di imputare il reato a una persona precisa era dovuta alla carente organizzazione dell'impresa, nulla vieta di punire entrambe le parti, la persona fisica e quella giuridica[86].

Oltre alla responsabilità penale, sono a disposizione lo strumento della responsabilità amministrativa e le corrispondenti sanzioni per la prevenzione diretta di danni futuri, quali la revoca di un'autorizzazione o il rifiuto di ammettere un'impresa in un segmento del mercato o in un settore di attività. L'ordinamento giuridico svizzero conosce diversi meccanismi del genere, che però non possono essere applicati in modo capillare a tutte le imprese e sono rilevanti solo in determinati settori del mercato e dell'economia. Sanzioni amministrative possono essere comminate alle imprese soggette a sorveglianza statale: l'Autorità federale di vigilanza sui mercati finanziari può, per esempio, revocare l'autorizzazione d'esercizio a un istituto ban-

81 Art. 102 cpv. 2 CP.
82 Art. 2–9 della Convenzione.
83 Nell'elenco sono riportate soprattutto fattispecie di corruzione e il reato di riciclaggio di denaro.
84 Art. 102 cpv. 1 CP.
85 Reati puniti con una pena detentiva o con una pena pecuniaria; cfr. art. 10 CP.
86 Cfr. Niggli/Gfeller, *Basler Kommentar*, Basilea 2007, n. 113 ad art. 102.

cario che non soddisfa più i presupposti per l'autorizzazione o che viola in modo grave i propri obblighi legali[87].

Inoltre, le unioni di persone e gli istituti con uno scopo illecito o immorale non possono ottenere la personalità giuridica e devono di conseguenza essere sciolti con attribuzione del patrimonio agli enti pubblici[88]. Se vi sono carenze nell'organizzazione di una società e non vi si pone rimedio entro il termine indicato, il giudice può procedere allo scioglimento della società[89]. Infine, sono a disposizione misure e strumenti di diritto civile per chiamare a rispondere dei danni cagionati le imprese a vantaggio delle quali un dipendente con funzioni dirigenziali ha commesso un reato o è venuto meno ai suoi obblighi di sorveglianza permettendo a un altro dipendente di compiere il reato in questione.

Riassumendo si può quindi affermare che il diritto svizzero soddisfa ampiamente i requisiti dell'articolo 12 della Convenzione. La normativa vigente in materia di responsabilità penale sussidiaria supera in parte quanto richiesto dalla Convenzione e garantisce che crimini e delitti compiuti nel quadro dello scopo di un'impresa siano puniti anche quando l'atto non può essere ascritto ad alcuna persona fisica a causa di carenze organizzative. Tuttavia, una responsabilità penale ad ampio raggio dell'impresa, che superi i requisiti minimi stabiliti dalla Convenzione, potrebbe essere istituita solo attraverso l'assunzione dei reati previsti dalla Convenzione nell'elenco svizzero dei reati che danno luogo a responsabilità primaria[90], un ampliamento generale del relativo ambito di applicazione[91] oppure una modifica concettuale della legislazione svizzera nel settore della responsabilità delle persone giuridiche. In questo contesto si rinuncia a una modifica tanto radicale, poiché il diritto svizzero già soddisfa ampiamente i requisiti della Convenzione.

Articolo 13 Sanzioni e misure

Il paragrafo 1 dell'articolo 13 obbliga le Parti ad assicurarsi che i reati fissati nella Convenzione siano puniti con sanzioni adeguate, tra cui anche la pena detentiva. Il diritto svizzero in vigore soddisfa tale requisito, dal momento che per tutti questi reati è prevista la pena privativa della libertà.

In base al paragrafo 2, anche le persone giuridiche di cui all'articolo 12 devono essere soggette a sanzioni o misure proporzionate, di natura penale o non penale, che comprendano in ogni caso sanzioni pecuniarie. Il diritto svizzero adempie anche questa condizione, prevedendo, oltre alla responsabilità penale sussidiaria delle imprese[92], punita con multe fino a cinque milioni di franchi, anche sanzioni efficaci, proporzionate e dissuasive, inflitte alle imprese colpevoli con sentenze o decisioni civili o amministrative.

87 Art. 23quinquies della legge sulle banche dell'8 novembre 1934; RS **952.0**.
88 Art. 52 e art. 57 CC; RS **210**.
89 Art. 731*b* del Codice delle obbligazioni, RS **220**. Questa disposizione è entrata in vigore il 1° gennaio 2008 e, secondo le statistiche disponibili, ha portato a un notevole aumento del numero di procedimenti fallimentari.
90 È quanto è stato fatto per l'applicazione della menzionata Convenzione penale del Consiglio d'Europa sulla corruzione, dove il collegamento tra i reati della Convenzione e l'attività economica delle imprese è tuttavia di gran lunga maggiore.
91 P. es. l'applicazione della responsabilità primaria dell'impresa per tutti i crimini e i delitti.
92 Cfr. sopra, art. 12.

Articolo 14 Campo di applicazione delle disposizioni procedurali

Il paragrafo 2 lettera b di questo articolo enuncia il principio secondo cui le successive disposizioni procedurali vanno applicate non solo al perseguimento dei reati previsti dalla Convenzione, ma in generale a tutti i reati commessi attraverso un sistema informatico. Inoltre, il paragrafo 2 lettera c stabilisce che le disposizioni si applicano anche all'insieme delle prove elettroniche di un reato[93]. In tal modo la Convenzione vuole garantire che i dati salvati elettronicamente nel contesto di un procedimento penale possano essere utilizzati come mezzi di prova nell'ambito dello stesso, esattamente come gli «analoghi» mezzi di prova tradizionali[94].

Partendo da questo campo di applicazione ampliato, occorre verificare se sia necessario apportare delle modifiche dal punto di vista procedurale e in che misura per esempio le norme processuali in materia di sorveglianza, di sequestro, di confisca e di assunzione delle prove in generale siano applicabili anche ai mezzi elettronici.

Il diritto processuale nazionale in senso lato è disciplinato, da un lato, dai diversi codici di procedura penale della Confederazione e dei Cantoni e, dall'altro, dalla legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni in vigore dal 1° gennaio 2002[95] e dalla sua ordinanza[96]. La LSCPT rimarrà valida anche dopo l'entrata in vigore del Codice di procedura penale del 5 ottobre 2007[97] (esecuzione della sorveglianza). Le norme di procedura penale[98] saranno invece inserite nel CPP. Nel caso di specie si fa riferimento al diritto in vigore, mentre, laddove le norme del CPP prevedono novità essenziali, si fa riferimento a queste ultime.

L'articolo 14 paragrafo 3 lettera b è dedicato ai cosiddetti «gruppi definiti di utenti», come ad esempio quelli delle reti elettroniche aziendali. Ai sensi dell'articolo 1 capoverso 4 e dell'articolo 15 capoverso 8 LSCPT, i gestori di reti di telecomunicazione interne e di centralini privati debbono tollerare la sorveglianza, nonché fornire le informazioni necessarie; queste misure permettono essenzialmente di ottenere e mettere al sicuro i dati anche in questo ambito non pubblico[99].

Articolo 15 Condizioni e salvaguardie

L'articolo 15 obbliga le Parti a rispettare i diritti umani e le libertà fondamentali, garantendone la tutela nell'ambito dell'attuazione della Convenzione. In particolare va rispettato il principio della proporzionalità delle procedure. Pertanto, la misura coercitiva deve essere commisurata alla gravità e al tipo di reato e non comportare effetti e costi sproporzionati.

Articolo 16 Conservazione rapida di dati informatici memorizzati

L'articolo 16 della Convenzione obbliga le Parti ad assicurarsi che le competenti autorità inquirenti possano ordinare od ottenere che i dati informatici memorizzati

93 «*De toute infraction pénale*».
94 Cfr. n. 141 del rapporto esplicativo.
95 LSCPT; RS **780.1**
96 OSCPT; RS **780.11**
97 CPP; FF **2007** 6327, entrata in vigore programmata per l'1.1.2011.
98 Art. 3–10 LSCPT.
99 A condizione che i dati siano disponibili. I gestori di reti interne non sono obbligati a conservare dati.

vengano messi al sicuro velocemente[100]. Se l'ordine di conservazione è indirizzato a un'altra persona, per esempio a un fornitore di prestazioni, questi può essere obbligato a conservare i dati inalterati per un determinato periodo di tempo.

I vari codici di procedura penale svizzeri rispettano la condizione della conservazione rapida, in quanto consentono di mettere velocemente al sicuro i dati elettronici nell'ambito dell'assunzione e della conservazione di mezzi di prova da parte delle autorità inquirenti, purché sia rispettato il principio della proporzionalità. In base al Codice di procedura penale del 5 ottobre 2007[101], i supporti e i documenti elettronici rientrano nel concetto di mezzi di prova materiali e di conseguenza possono essere messi agli atti[102] o sequestrati in seguito a perquisizione[103].

La Convenzione suggerisce inoltre la possibilità di ottenere una prima conservazione emanando una decisione che obblighi un terzo (affidabile) a mettere al sicuro i dati. Le Parti non sono però obbligate a introdurre tali «*preservation orders*»[104]. È sufficiente che i dati possano essere messi al sicuro dalle autorità stesse.

Il diritto svizzero in vigore risponde almeno in parte all'invito della Convenzione per quanto riguarda specifici dati in possesso dei fornitori di servizi Internet. Ai sensi della LSCPT i provider sono obbligati a conservare per sei mesi i dati relativi al traffico e alla fatturazione[105]. Nel singolo caso, una decisione dell'autorità competente può però imporre loro di mettere i dati temporaneamente al sicuro. La possibilità di obbligare chiunque a conservare dati in ottemperanza a una decisione sarebbe però eccessiva in questo contesto e risulterebbe inoltre difficilmente conciliabile con l'articolo 15 della Convenzione (principio della proporzionalità). Il diritto in vigore soddisfa i requisiti della Convenzione.

Articolo 17 Rapida conservazione e trasmissione di dati relativi al traffico informatico

L'articolo 17 impone che la conservazione dei dati relativi al traffico informatico[106] prevista dall'articolo 16 venga garantita anche nel caso in cui in una comunicazione siano coinvolti più fornitori di servizi (par. 1 lett. a).

100 Inclusi i dati relativi al collegamento, indicanti i partecipanti, l'orario, la durata e il percorso della comunicazione; cfr. anche art. 2 lett. g OSCPT.
101 Cfr. quanto esposto in merito all'art. 14 della Convenzione.
102 Art. 192 segg. CCP.
103 Art. 246 segg. CCP.
104 Cfr. n. 160 del rapporto esplicativo (nota 1).
105 Art. 15 cpv. 3 LSCPT: conservazione di dati necessari all'identificazione degli utenti, nonché di dati relativi al traffico e alla fatturazione. Nel quadro della revisione della LSCPT è prevista l'estensione del termine a un anno (anche se non è richiesta dalla Convenzione: n. 161 *in fine* del rapporto esplicativo). Cfr. anche la decisione del 2 marzo 2010 della Corte costituzionale federale tedesca di Karlsruhe, secondo cui la conservazione dei cosiddetti dati di scorta (*Vorratsdatenspeicherung*) può essere effettuata solo nel rispetto di rigide condizioni costituzionali e in relazione a reati gravi, ma non in modo generalizzato (www.bundesverfassungsgericht.de).
106 I cosiddetti «*traffic data*» riguardano l'origine, il destinatario, l'orario e la durata o il percorso della comunicazione, ma non consentono necessariamente di risalire direttamente all'identità e all'indirizzo del mittente (art. 1 lett. d della Convenzione, cfr. n. 30 del rapporto esplicativo, nota 1). Si può trattare anche dell'indirizzo IP. Le Parti sono libere di proteggere diversi tipi di dati relativi al traffico informatico (n. 31 del rapporto esplicativo).

L'ordinamento giuridico svizzero rispetta quanto stabilito dal paragrafo 1 lettera a. In base all'articolo 15 capoverso 3 LSCPT i fornitori di un servizio sono tenuti a conservare per sei mesi i dati necessari per l'identificazione dei partecipanti, nonché i dati relativi al traffico e alla fatturazione. Se sono coinvolti più fornitori, l'autorità attribuisce a uno di loro l'incarico di sorveglianza, obbligando gli altri fornitori a comunicare a quest'ultimo i loro dati (art. 15 par. 2). Il fatto che diversi fornitori di servizi siano coinvolti in una comunicazione non pregiudica quindi la conservazione rapida dei dati relativi al traffico informatico.

Il paragrafo 1 lettera b prevede che il fornitore di servizi destinatario dell'ordine di conservare i dati relativi al traffico informatico fornisca alle autorità competenti i dati necessari per risalire a ulteriori provider e al percorso della comunicazione. Le autorità inquirenti devono specificare in modo sufficientemente dettagliato i dati che desiderano ottenere. L'obiettivo di questa procedura non consiste nell'individuare per nome l'autore o il destinatario dei messaggi[107].

Con l'entrata in vigore del Codice di procedura penale del 5 ottobre 2007, il ministero pubblico potrà richiedere informazioni sui collegamenti (mittente e destinatario, orario) e altri dati relativi al traffico e alla fatturazione per tutti i crimini e delitti (art. 273 CPP). L'ordine deve essere approvato dal giudice dei provvedimenti coercitivi, ma non presuppone un reato specifico fissato in un elenco e può essere richiesto con effetto retroattivo. Tenuto conto del principio della proporzionalità[108], l'esclusione di semplici contravvenzioni non inficia l'adempimento dei requisiti della Convenzione, che sono quindi soddisfatti dal diritto vigente.

Inoltre, l'articolo 14 capoverso 4 LSCPT rimane applicabile per tutti i reati commessi in Internet[109], incluse le contravvenzioni. In base a questa disposizione, il provider è tenuto a fornire all'autorità competente tutte le informazioni che consentono di identificare l'autore del reato, tra cui anche informazioni e dati che permettono di stabilire il percorso della comunicazione. L'articolo 14 capoverso 4 va applicato in modo capillare a tutto il settore «Internet»[110] e si riferisce a indirizzi IP sia statici che dinamici[111]. In entrambi i casi non si può partire dal presupposto di una misura di sorveglianza in senso tradizionale ai sensi della LSCPT; l'autorità inquirente può avanzare una domanda direttamente al servizio competente, indipendentemente dal reato contestato[112].

107 N. 169 del rapporto esplicativo (cfr. nota 1).
108 Art. 15 della Convenzione.
109 Questo termine può rappresentare una restrizione rispetto ai reati «commessi tramite l'utilizzo di un sistema informatico».
110 Cfr. decisione della Commissione di ricorso DATEC del 27.04.2007, J-2003-162, consultabile all'indirizzo www.reko-inum.admin.ch.
111 Un indirizzo IP (*Internet protocol*) *statico* è costituito da un numero univoco composto da quattro serie di cifre assegnato ad ogni computer connesso ad Internet.
Un indirizzo IP *dinamico*, invece, viene assegnato in modo non permanente e temporaneo a una connessione fissa. Oggi come in passato rappresenta il caso più frequente e viene attribuito all'utente dal service provider selezionato per la durata della sessione Internet. Ne risulta che lo stesso indirizzo dinamico viene utilizzato ogni giorno da numerose persone. Dal punto di vista tecnico, è necessario consultare retroattivamente i cosiddetti *log file* per identificare l'utente che stava usando l'indirizzo in un determinato momento.
112 L'elenco dell'art. 3 LSCPT non è applicabile.

Articolo 18 Ingiunzione di produrre dati

Ai sensi dell'articolo 18 paragrafo 1 lettera a, l'autorità inquirente competente può obbligare chiunque a fornire dati informatici memorizzati che si trovano in suo possesso. Questa disposizione è coperta dal diritto svizzero (obbligo di edizione della persona non indiziata) ed è ripresa nella sua essenza anche nel Codice di procedura penale[113]. In caso di rifiuto vi è la possibilità di applicare misure coercitive.

Inoltre, i fornitori di servizi (par. 1 lett. b) sono obbligati a fornire, su ordine dell'autorità competente, i dati dei clienti[114], ma non quelli riguardanti il collegamento o il contenuto. L'articolo 18 paragrafo 1 lettera b della Convenzione non disciplina quindi l'identificazione di coloro che partecipano a trasferimenti diretti e specifici di dati, ma l'identificazione dei partecipanti in rete, indipendentemente dal traffico di dati avvenuto o imminente. In questa fase non si pone il problema della loro sorveglianza[115]. Come già esposto in merito all'articolo 17 della Convenzione, l'autorità inquirente può richiedere informazioni concernenti collegamenti e dati relativi al traffico e alla fatturazione per tutti i crimini e i delitti[116]. L'ordine deve essere approvato dal giudice dei provvedimenti coercitivi, ma non presuppone un reato specifico riportato in un elenco e può essere richiesto con effetto retroattivo.

L'articolo 14 capoverso 4 LSCPT si applica anche in questo caso[117]. Vanno forniti in particolare il nome e l'indirizzo dell'utente, nonché altri elementi dell'indirizzo ai sensi della legge del 30 aprile 1997 sulle telecomunicazioni[118].

L'articolo 18 paragrafo 1 lettera b della Convenzione si limita ai dati conservati dal provider e non specifica in che misura e per quanto tempo le informazioni debbano essere memorizzate e rese disponibili. Se nel singolo caso, a causa della normativa nazionale, tali dati non sono (più) reperibili, ciò non costituisce una violazione dei requisiti della Convenzione.

Il diritto svizzero rispetta quanto stabilito dall'articolo 18 della Convenzione, soprattutto tenendo conto delle disposizioni del Codice di procedura penale.

Articolo 19 Perquisizione e sequestro di dati informatici memorizzati

L'articolo 19 paragrafi 1 e 3 obbliga le Parti ad adottare normative che consentano alle autorità competenti di perquisire e mettere al sicuro nel proprio territorio dati informatici e supporti per la loro conservazione. Come i beni mobili, anche i dati informatici devono poter essere sequestrati e resi accessibili. Deve inoltre essere possibile sequestrare anche i computer[119]. I presupposti per tali perquisizioni devono essere essenzialmente gli stessi di quelli per il reperimento di mezzi di prova «tradizionali».

Nel presente caso non si tratta essenzialmente di questioni inerenti al diritto delle telecomunicazioni o della sorveglianza del relativo traffico. Trovano quindi applicazione le normative nazionali sull'acquisizione e la conservazione delle prove. Nume-

113 Cfr. art. 263 segg. CPP, soprattutto art. 265: obbligo di consegna.
114 «*Subscriber information*», p. es. identità del cliente, informazioni sui pagamenti.
115 L'elenco di reati dell'art. 3 LSCPT non può essere applicato nemmeno in questo caso.
116 Art. 273 CPP.
117 Cfr. sopra.
118 LTC; RS **784.10**
119 N. 187 del rapporto esplicativo (cfr. nota 1).

rosi esempi pratici degli ultimi anni[120] hanno dimostrato che i codici cantonali di procedura penale sono sufficienti a soddisfare i requisiti in materia e permettono di effettuare la perquisizione e il sequestro di dati e computer. Anche il Codice di procedura penale del 5 ottobre 2007 prevede, a tratti esplicitamente, la perquisizione e il sequestro di dati elettronici e supporti informatici[121].

L'articolo 19 si riferisce ai dati informatici memorizzati e, in linea di massima, può essere applicato nei confronti di chiunque. Ci si può chiedere in che misura questa facoltà di accesso dell'autorità di perseguimento penale valga anche per i dati salvati dai provider (per es. dati dei clienti relativi al contenuto) e se ne derivi una limitazione della protezione offerta dal segreto delle telecomunicazioni. Il testo della Convenzione non fornisce alcuna spiegazione. Tuttavia il rapporto esplicativo stabilisce che gli Stati sono liberi di proteggere la comunicazione come tale anche in questo ambito. In tal modo, per esempio, un messaggio temporaneamente salvato da un provider e non ancora visualizzato dal mittente può essere considerato parte della comunicazione[122], godendo così della relativa protezione. Di conseguenza, può essere comunicato dal fornitore del servizio solo sulla base di una decisione giudiziaria e a determinate condizioni. Ad ogni modo, i dati non sono più protetti dal segreto delle telecomunicazioni nel momento in cui vengono memorizzati nel supporto di salvataggio del destinatario, dove possono essere messi sotto sequestro[123]. Pertanto, l'articolo 19 della Convenzione non scalza i principi nazionali esistenti in materia di segreto delle telecomunicazioni.

Il paragrafo 2 prevede che le autorità, una volta penetrate in un primo sistema informatico, possano accedere, laddove legalmente consentito, anche a un eventuale ulteriore sistema collegato per perquisirlo. Tale facoltà ampliata può essere concretata nel diritto nazionale. La disposizione è esplicita nel non autorizzare la perquisizione di supporti informatici in territorio straniero, a meno che non siano rispettate alcune condizioni aggiuntive (cfr. art. 32 della Convenzione) o non venga richiesta l'assistenza giudiziaria. Il diritto svizzero offre la possibilità di accedere, nell'ambito di una perquisizione, a un altro sistema di dati collegato[124]. Ciò presuppone tuttavia che la facoltà dell'autorità si estenda anche al contesto allargato, circostanza riconosciuta dal tenore della disposizione della Convenzione[125].

Il paragrafo 4 stabilisce, su richiesta delle autorità, l'obbligo di informazione a carico di terzi, per esempio un amministratore di sistema, in modo che si possa accedere ai dati. La LSCPT prevede tali obblighi per determinati settori[126]. In base alla Convenzione l'obbligo di cooperazione deve essere adeguato e proporzionato. La rivelazione di una password su richiesta delle autorità può, per esempio, essere appropriata in un caso e sproporzionata in un altro[127].

120 Per esempio nell'ambito di indagini condotte dalla polizia e dal giudice istruttore nella lotta alla pedopornografia.
121 Art. 246 segg. e 263 segg. CPP.
122 N. 190 del rapporto esplicativo (cfr. nota 1).
123 Questa situazione è simile a quella di un invio postale che gode di tutela analoga grazie al segreto postale, mentre, il giorno dopo, la stessa lettera, p. es. come parte della conta bilità del destinatario, può essere sequestrata con una perquisizione domiciliare e quindi vagliata ai fini dell'inchiesta.
124 Per determinate reti, a seconda del caso, l'autorità inquirente sarà a mala pena consapevole di questa circostanza.
125 «*Where lawfully accessible*».
126 Art. 14 cpv. 4 e art. 15 cpv. 8 LSCPT.
127 Cfr. n. 202 del rapporto esplicativo (nota 1), nonché l'art. 15 della Convenzione.

Sorge la domanda se tali obblighi posti dalla Convenzione vadano oltre il normale obbligo di testimoniare o l'obbligo di edizione di terzi[128] stabiliti dal diritto processuale penale svizzero. Il diritto in vigore soddisfa i requisiti della Convenzione, la quale limita ai soli casi idonei l'obbligo d'informazione, che sorge solo dietro richiesta da parte dell'autorità investigativa, autorizzata a emettere decisioni di edizione. Dal rapporto esplicativo si evince in particolare che la disposizione è rivolta agli amministratori di sistema o a persone con simili funzioni di vigilanza su un sistema informatico. Tuttavia, in casi del genere può essere necessario verificare sul piano nazionale l'esistenza di un'eventuale funzione di garante dell'interessato che, violando una decisione di edizione, potrebbe incorrere in una pena ai sensi dell'articolo 305 CP[129].

Articolo 20 Raccolta in tempo reale di dati relativi al traffico informatico

L'articolo 20 disciplina l'acquisizione in tempo reale, da parte delle autorità competenti, dei dati relativi al traffico informatico e ai collegamenti, e prevede la possibilità, per le Parti, di riconoscere a tali autorità la facoltà di ordinare ai fornitori di servizi la raccolta o la registrazione in tempo reale dei dati relativi ai collegamenti. La Convenzione consente alle Parti di introdurre un elenco di reati che giustifichino la raccolta di dati e di presentare una riserva in merito[130].

Il diritto svizzero vigente prevede che i dati relativi ai collegamenti (come anche quelli relativi al contenuto) possano essere raccolti ricorrendo alla sorveglianza in tempo reale purché si tratti di reati elencati nella LSCPT[131]. Tale elenco è stato inserito nel Codice di procedura penale anche per i dati relativi al contenuto. Il CPP prevede un'ulteriore estensione per i dati relativi al traffico e alla fatturazione, nonché i dati relativi ai collegamenti, riconoscendo alle autorità il diritto di esigere informazioni in merito in caso di crimini o delitti[132]. Avanzando una riserva ai sensi dell'articolo 14 paragrafo 3 della Convenzione, non sussiste alcuna necessità di adeguare la normativa in materia.

Articolo 21 Intercettazione di dati relativi al contenuto

L'articolo 21 disciplina la raccolta in tempo reale dei dati relativi al contenuto, che le autorità competenti possono effettuare od ordinare per una serie di reati gravi, determinabili autonomamente dalle Parti, per esempio stilando un elenco di reati. La legislazione svizzera prevede che la sorveglianza e la raccolta in tempo reale di dati relativi al contenuto possano essere ordinate per i reati elencati all'articolo 3 LSCPT. Non sussiste alcuna necessità di adeguare il diritto vigente.

Articolo 22 Competenza

La Convenzione attua una distinzione tra competenza obbligatoria e facoltativa delle Parti nel perseguimento dei reati descritti nella Convenzione. Il paragrafo 1 obbliga ogni Parte a fondare la propria competenza quando il reato avviene sul territorio

128 Che di norma non implica alcun ulteriore obbligo di collaborare attivamente nell'acquisizione di mezzi di prova; cfr. art. 265 CPP.
129 Fattispecie del favoreggiamento; cfr. DTF **120** IV 106.
130 Art. 14 par. 3 in combinato disposto con l'art. 42 della Convenzione.
131 Art. 3 LSCPT.
132 Art. 273 CPP, indipendentemente dall'elenco dei reati.

dello Stato (principio della territorialità; par. 1 lett. a) oppure, in via opzionale, quando viene commesso a bordo di una nave battente bandiera di tale Stato (principio della bandiera; lett. b) o a bordo di un aeromobile immatricolato in tale Stato (lett. c). La competenza dei giudici svizzeri è sancita dal diritto vigente e si evince dall'articolo 3 CP, dall'articolo 4 capoverso 2 della legge sulla navigazione[133] e dall'articolo 97 capoverso 1 della legge sull'aviazione[134].

Ai sensi del paragrafo 1 lettera d, lo Stato fonda la propria competenza quando il reato viene compiuto da un proprio cittadino e l'infrazione è punibile nel luogo in cui è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato. In questi casi la competenza dei giudici svizzeri si evince dall'articolo 7 capoverso 1 lettera a CP (principio della personalità attiva). Non è quindi necessario ricorrere alla riserva prevista dall'articolo 22 paragrafo 2 (riferito alle lett. b–d).

Ai sensi del paragrafo 3, la Parte deve stabilire la propria competenza per i reati fissati dalla Convenzione[135] anche nel caso in cui l'autore presunto del reato si trovi nel proprio territorio e non venga estradato solamente perché cittadino di tale Stato. La Svizzera adempie a questo obbligo di perseguimento penale in caso di mancata estradizione (*aut dedere aut iudicare*) grazie all'articolo 6 CP. L'articolo 7 AIMP[136] stabilisce che nessun cittadino svizzero può essere estradato senza il suo consenso per essere perseguito penalmente. La Convenzione Europea di estradizione del 13 dicembre 1957[137] disciplina l'estradizione di propri cittadini nell'articolo 6, imponendo lo stesso obbligo della Convenzione sulla cibercriminalità. Le regole per il perseguimento in via sostitutiva da parte della Svizzera sono stabilite negli articoli 85 e segg. AIMP. L'efficienza di tale azione penale dipende però essenzialmente dagli atti forniti e dai mezzi di prova messi a disposizione.

2.3 Capitolo III: Cooperazione internazionale

Principi generali

La Convenzione del Consiglio d'Europa mira a istituire un sistema rapido ed efficace di collaborazione giudiziaria internazionale in materia penale[138]. Fatte salve espresse disposizioni contrarie, si applicano gli accordi internazionali stipulati tra le Parti, nonché il diritto nazionale dei singoli Paesi. Per determinate misure, la Convenzione contiene tuttavia norme particolari, che possono discostarsi dalle disposi-

133 Legge federale del 23 settembre 1953 sulla navigazione marittima sotto bandiera svizzera; RS **747.30**.
134 Legge federale del 21 dicembre 1948 sulla navigazione aerea; RS **748.0**.
135 In questo caso il reato deve essere punito con una pena detentiva di almeno un anno; cfr. art. 24 par. 1 della Convenzione.
136 RS **351.1**
137 RS **0.353.1**
138 Al di fuori della procedura di assistenza giudiziaria, la Svizzera dispone di varie possibilità di cooperazione, soprattutto per quanto riguarda lo scambio di informazioni nell'ambito di Schengen, dell'Interpol e degli accordi bilaterali di collaborazione tra forze di polizia, nonché la cooperazione nell'ambito dell'Europol, a cui la Svizzera è legata dal 2004 grazie a un trattato. Le possibilità a disposizione della Svizzera per lo scambio di informazioni superano già le relative misure richieste dalla Convenzione.

zioni in vigore nei singoli Stati aderenti[139]. La ragione va ricercata soprattutto nell'obbligo di attuare rapidamente le misure, che difficilmente si concilia con la normale durata della procedura di assistenza. Considerando l'attuale normativa sulla cooperazione giudiziaria internazionale in materia penale, l'attuazione della Convenzione richiede una modifica dell'AIMP (art. 30 della Convenzione).

Articolo 23 Principi generali della cooperazione internazionale

In base all'articolo 23, le Parti devono cooperare tra loro «nella misura più ampia possibile», per cui gli ostacoli che impediscono la circolazione rapida e semplice delle informazioni e dei mezzi di prova tra gli Stati vanno rimossi nella misura del possibile. Questa disposizione, di uso comune negli accordi sulla lotta alla criminalità, nell'ambito della cibercriminalità comprende un aspetto particolare: le informazioni devono essere scambiate più velocemente rispetto alle normali procedure di collaborazione giudiziaria internazionale in materia penale[140]. L'obbligo di cooperazione fissato nell'articolo 23 si riferisce a tutti i reati collegati a sistemi e dati informatici[141] e all'acquisizione di prove elettroniche di un reato[142]. Le disposizioni del capitolo III valgono quindi sia per i reati commessi con un sistema informatico, sia per i casi in cui sia necessario raccogliere in forma elettronica le prove di un reato tradizionale, non compiuto con sistemi informatici[143].

Articolo 24 Estradizione

Ai sensi dell'articolo 24, che costituisce una disposizione di uso comune, l'obbligo di estradizione sussiste solamente per i reati definiti negli articoli 2–11 della Convenzione. Per l'obbligo di estradizione di cui all'articolo 24 devono essere soddisfatte contemporaneamente due condizioni, formulate nell'articolo 2 paragrafo 1 dell'Accordo di estradizione europeo: il reato deve essere punito in base alla legge di entrambi i Paesi[144] e deve essere prevista una pena privativa della libertà di una durata massima di almeno un anno. La comminatoria necessaria per concedere l'estradizione è specificata più in dettaglio nel commento agli articoli 2–11. Anche la legislazione svizzera prevede, all'articolo 35 AIMP, le due condizioni menzionate. Per quanto riguarda l'articolo 24 paragrafi 1–4 della Convenzione, la Svizzera non vincola l'estradizione all'esistenza di un trattato[145].

In base all'articolo 24 paragrafo 5, l'estradizione è soggetta alle condizioni previste dal diritto interno. Per la Svizzera si tratta degli articoli 32 e segg. AIMP. Come Parte richiesta, il nostro Paese non è tenuto all'estradizione se non ritiene che siano

139 Nel caso della Svizzera si tratta dell'art. 30 della Convenzione, che prevede la trasmissione rapida all'autorità richiedente di dati informatici conservati *prima* della conclusione del procedimento, nonché dell'art. 33 della Convenzione, che stabilisce l'assistenza nella raccolta in tempo reale di dati relativi al traffico informatico.
140 N. 6, 20 e 242 del rapporto esplicativo (nota 1).
141 Ossia i reati ai sensi dell'art. 14 par. 2 lett. a e b della Convenzione.
142 Art. 14 par. 2 lett. c.
143 N. 243 del rapporto esplicativo (nota 1).
144 Secondo le pertinenti disposizioni di legge di entrambe le Parti.
145 Art. 1 cpv. 1 lett. a AIMP.

rispettate le condizioni previste dalla Convenzione o dal diritto nazionale[146]. La collaborazione si fonda, infatti, sui trattati in vigore tra i due Stati interessati, nonché sulla Convenzione europea di estradizione del 13 dicembre 1957 con i due protocolli addizionali[147].

Nell'articolo 24 paragrafo 6 viene statuito il principio «*aut dedere aut iudicare*» (estradizione o perseguimento penale). I cittadini svizzeri non possono essere estradati senza il loro consenso scritto[148]. L'interessato che rifiuta il proprio consenso viene processato dalla Svizzera[149] su domanda dello Stato richiedente in ottemperanza all'articolo 24 paragrafo 6 della Convenzione e dell'articolo 7 capoverso 1 CP. La Svizzera informa la Parte richiedente del risultato del procedimento. Se la Parte la cui domanda di estradizione è stata respinta non richiede l'indagine o il perseguimento penale da parte delle autorità competenti, la Svizzera non è tenuta ad attivarsi in tal senso[150].

In base all'articolo 24 paragrafo 7, la Svizzera comunica al Segretario generale del Consiglio d'Europa che l'Ufficio federale di giustizia è responsabile delle richieste di estradizione o di arresto provvisorio[151]. Questa disposizione si applica soltanto se le due Parti interessate non hanno stipulato alcun accordo tra di loro[152]. In ogni caso, la designazione di un'autorità non esclude la possibilità di adire le vie diplomatiche[153].

Articolo 25 Principi generali dell'assistenza giudiziaria

L'articolo 25 obbliga le Parti a collaborare per un'ampia serie di reati, requisito che si desume anche dall'articolo 23[154]. Ai sensi dell'articolo 25 paragrafo 2, la Svizzera deve definire le basi legali che le permettano di garantire l'espletamento delle particolari forme di cooperazione stabilite della Convenzione, soprattutto quelle menzionate negli articoli 27 e 29–35. Tali disposizioni sono indispensabili per una cooperazione penale efficace in materia di reati informatici[155]. Gli adeguamenti della legislazione sono descritti nel dettaglio al capitolo relativo all'attuazione dell'articolo 30 della Convenzione.

146 L'art. 37 AIMP prevede, tra l'altro, che l'estradizione possa essere negata se la domanda si basa su una sentenza contumaciale e il procedimento non ha rispettato i diritti minimi della difesa riconosciuti a ogni imputato. In base a tale disposizione, l'estradizione può essere negata se lo Stato richiedente non offre garanzia che la persona perseguita non sarà condannata a morte o giustiziata né sottoposta a un trattamento pregiudizievole per la sua integrità fisica.

147 RS **0.353.1** (CEEstr), **0.353.11** e **0.353.12**

148 Art. 7 AIMP.

149 Le indagini e il perseguimento penale devono svolgersi rapidamente e con la stessa cura impiegata per qualsiasi altro reato simile.

150 Se non è stata presentata alcuna domanda di estradizione o se l'estradizione è stata rifiutata per un motivo diverso dalla cittadinanza, la Svizzera non è obbligata a incaricare le proprie autorità di procedere al perseguimento penale (n. 251 del rapporto esplicativo, nota 1).

151 Art. 17 cpv. 2 AIMP.

152 Se, invece, tra le Parti sussiste un trattato di estradizione bilaterale o multilaterale, come la menzionata CEEstr, esse sanno già a chi indirizzare la domanda di estradizione o di arresto provvisorio, rendendo superflua la tenuta di un registro.

153 N. 252 del rapporto esplicativo (nota 1).

154 Gli art. 33 e 34 permettono di modificare l'ambito di applicazione di queste misure; cfr. quanto esposto in merito a tali articoli.

155 N. 254 del rapporto esplicativo (nota 1).

L'articolo 25 paragrafo 3 della Convenzione introduce una misura di assistenza giudiziaria rapida, che tiene conto della labilità dei dati informatici e dei termini di conservazione, in parte limitati. Le richieste devono essere presentate velocemente e altrettanto rapidamente deve poter essere comunicata la risposta. L'articolo 25 paragrafo 3 permette di ricorrere a una forma di assistenza accelerata per impedire che informazioni o mezzi di prova essenziali vadano persi. Questo scopo viene raggiunto, da un lato, permettendo alle Parti, in casi d'urgenza, di presentare una domanda di cooperazione servendosi di mezzi di comunicazione veloce[156], e dall'altro, sollecitando la Parte richiesta a rispondere con gli stessi mezzi. Ogni Parte deve creare le condizioni necessarie per l'applicazione di tali misure[157]. In casi particolarmente delicati le Parti possono concordare misure di sicurezza speciali come la cifratura[158]. La Parte richiesta può esigere che successivamente le venga trasmessa una conferma formale utilizzando le vie di trasmissione tradizionali, procedura che corrisponde alla prassi svizzera.

L'articolo 25 paragrafo 4 della Convenzione sancisce il principio generale secondo cui l'assistenza giudiziaria è soggetta alle condizioni previste dai trattati di assistenza giudiziaria applicabili e dal diritto nazionale[159]. Questa disposizione di uso comune vale in particolare per misure incisive quali la perquisizione o il sequestro, attuate solo se la Parte richiesta ha la certezza che siano soddisfatte le condizioni necessarie per ordinarle, ma non vale se gli articoli del capitolo III dispongono espressamente altrimenti. La Convenzione contiene svariate deroghe a questo principio generale[160], in particolare per quanto riguarda i motivi di rifiuto dell'assistenza giudiziaria[161]. Ai sensi dell'articolo 25 paragrafo 4, la collaborazione per i reati di cui agli articoli 2–11 non può essere rifiutata adducendo il semplice motivo che il reato in questione è considerato di natura fiscale. Tale divieto non pone difficoltà, poiché i reati fissati dalla Convenzione non rappresentano di per sé reati fiscali.

Il paragrafo 5 contiene una disposizione di uso comune sulla doppia incriminazione[162].

156 E non dei tradizionali mezzi di trasmissione, ossia lettera sigillata inviata con corriere diplomatico o per posta.

157 Telefax e posta elettronica sono menzionati solo a titolo esemplificativo. È possibile utilizzare qualsiasi mezzo di comunicazione veloce idoneo al caso.

158 N. 256 del rapporto esplicativo (nota 1).

159 A tutela dei diritti di chi soggiorna nel territorio della Parte richiesta e può essere oggetto di una domanda di assistenza giudiziaria.

160 N. 258 del rapporto esplicativo (nota 1): una deroga simile si evince dall'art. 25 par. 2 della Convenzione, secondo cui ogni Parte deve garantire le forme di collaborazione descritte negli altri articoli del capitolo (conservazione, raccolta di dati in tempo reale, perquisizione e sequestro, partecipazione alla rete 24/7), indipendentemente dal fatto che tali misure siano già fissate nei trattati internazionali di assistenza giudiziaria adottati o nella legislazione nazionale in materia. Un'ulteriore deroga si trova nell'art. 27, sempre applicabile al disbrigo delle domande e prioritario rispetto a una normativa nazionale della Parte richiesta che disciplini la collaborazione internazionale, a meno che non esista un trattato di assistenza giudiziaria o altro accordo simile tra la Parte richiedente e la Parte richiesta.

161 Cfr. anche quanto esposto in merito all'art. 27 par. 4.

162 N. 259 del rapporto esplicativo (nota 1): a causa dei diversi ordinamenti giuridici dei singoli Stati, vi sono differenze nella terminologia e nella classificazione dei comportamenti criminali. Se un comportamento è considerato reato in entrambi gli ordinamenti, queste differenze puramente giuridiche non dovrebbero impedire la concessione dell'assistenza giudiziaria. Il principio della doppia incriminazione, qualora applicabile, andrebbe utilizzato con flessibilità per facilitare la concessione della mutua assistenza.

Articolo 26 Trasmissione spontanea di informazioni

L'articolo 26 estende all'assistenza giudiziaria una disposizione tratta dalla Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato dell'8 novembre 1990[163] e dall'articolo 28 della Convenzione penale sulla corruzione del 27 gennaio 1999[164]. Disposizioni simili si trovano anche nella maggior parte dei trattati bilaterali in vigore in materia di assistenza giudiziaria penale, nonché nell'articolo 11 del Secondo protocollo addizionale dell'8 novembre 2001[165] alla Convenzione europea di assistenza giudiziaria in materia penale che, come l'articolo 26 della Convenzione, prevede anche una clausola di confidenzialità. L'articolo 26 (disposizione potestativa) riconosce alle due Parti la possibilità, senza preventiva richiesta ed eventualmente, secondo il paragrafo 2, a determinate condizioni[166], di trasmettere all'altra Parte informazioni su indagini o procedimenti utili alla comune lotta contro la criminalità[167]. Lo scambio di informazioni è disciplinato dal diritto nazionale. Per la Svizzera valgono le condizioni stabilite dall'articolo 67*a* AIMP (Trasmissione spontanea di mezzi di prova e di informazioni).

Articolo 27 Procedure di assistenza giudiziaria in assenza di accordi internazionali applicabili

Nell'articolo 27 sono stati trasposti i principi di altri trattati stipulati dalla Svizzera. Il paragrafo 1 prevede che l'assistenza giudiziaria si svolga secondo le regole stabilite dai pertinenti accordi e trattati in materia, come la Convenzione europea di assistenza giudiziaria in materia penale del 20 aprile 1959[168] o il citato Protocollo addizionale. Le misure di assistenza giudiziaria per i reati informatici disciplinate negli articoli 29–35 della Convenzione presuppongono, però, la predisposizione delle necessarie basi legali laddove il diritto in vigore nei singoli Stati aderenti non sia sufficiente.

I paragrafi 2–10 contengono disposizioni da applicare in assenza di un trattato di assistenza giudiziaria e disciplinano la designazione di un'autorità centrale, la determinazione di eventuali condizioni, i motivi per la sospensione o il rifiuto dell'assistenza giudiziaria, nonché la relativa procedura, la confidenzialità delle domande e la trasmissione diretta di informazioni. Tali norme hanno la precedenza rispetto a quelle del diritto nazionale. L'articolo 27 non disciplina altri punti[169].

163 RS **0.311.53**
164 RS **0.311.55**; n. 260 del rapporto esplicativo (nota 1).
165 RS **0.351.12**
166 La Parte ricevente assume un obbligo nei confronti della Parte trasmittente solo se accetta le informazioni trasmesse spontaneamente: in tal modo accetta infatti automaticamente di attenersi alle condizioni legate alla trasmissione. L'articolo 26 della Convenzione prevede la possibilità di scegliere se accettare o respingere quanto offerto.
167 La criminalità non si arresta di fronte ai confini nazionali e le informazioni ottenute da una Parte nel corso delle sue indagini sono spesso di interesse anche per le autorità dell'altra Parte.
168 CEAG; RS **0.351.1**.
169 Non vi si trova, per esempio, alcuna disposizione relativa alla forma e al contenuto della domanda, all'audizione dei testimoni presso la Parte richiesta o richiedente, all'emissione di documenti ufficiali, al trasferimento dei testimoni detenuti o all'assistenza nei sequestri. Quanto a questi aspetti, dall'art. 25 par. 4 si evince che la concessione di questo tipo di assistenza è disciplinato dal diritto nazionale della Parte richiesta, fatte salve disposizioni contrarie stabilite nel capitolo III. In Svizzera si applica l'AIMP. N. 264 del rapporto esplicativo (nota 1).

Ai sensi dell'articolo 27 paragrafo 2, in assenza di trattati internazionali la Svizzera comunica al Segretario generale del Consiglio d'Europa l'autorità centrale competente per la trasmissione e le risposte alle domande di assistenza giudiziaria. Come per la dichiarazione relativa alla CEAG, è necessario precisare che l'Ufficio federale di giustizia (UFG) è l'autorità centrale per la trasmissione e la ricezione delle domande di assistenza giudiziaria. In questo contesto rientra anche l'articolo 27 paragrafo 9 lettera e, secondo cui le Parti possono dichiarare che, per ragioni di efficienza, le richieste effettuate in base a tale paragrafo dovranno essere indirizzate alla propria autorità centrale. In applicazione di questa disposizione tutte le richieste devono essere indirizzate all'UFG, il che implica un maggiore carico di lavoro e un maggiore fabbisogno di personale. Le domande di assistenza giudiziaria non riguardano infatti solo il perseguimento dei reati informatici, ma anche l'acquisizione di mezzi di prova elettronici per altri reati[170]. Si prevede anche che l'UFG sarà consultato regolarmente da autorità svizzere e straniere per ottenere pareri e raccomandazioni in merito alla procedura applicabile. Nel trattare le domande di assistenza indirizzate alla Svizzera, l'UFG, oltre a fornire informazioni, dovrà anche verificare più spesso le decisioni adottate dalle autorità d'esecuzione svizzere.

L'articolo 27 paragrafo 3 obbliga la Parte richiesta a eseguire le domande di assistenza giudiziaria in conformità con le procedure specificate dalla Parte richiedente, purché compatibili con la propria legislazione. Tale disposizione, che si trova anche in altri trattati internazionali[171], è volta a garantire il rispetto dei requisiti probatori in essere[172].

In base al paragrafo 4, l'assistenza può essere rifiutata per i motivi di cui all'articolo 25 paragrafo 4 della Convenzione[173], per i reati che la Parte richiesta considera politici o connessi con un reato politico, e in casi in cui possano essere lesi la sovranità, la sicurezza, l'ordine pubblico o altri interessi essenziali della Parte richiesta[174]. L'articolo 27 paragrafo 5, una disposizione di uso comune, permette alla Parte richiesta di sospendere (e non di rifiutare) l'esecuzione di una domanda di assistenza, quando l'immediata attuazione delle misure indicate potrebbe pregiudicare indagini o procedimenti penali condotti dalle proprie autorità[175]. Secondo il paragrafo 6, nei casi in cui normalmente rifiuterebbe o sospenderebbe l'assistenza, la Parte richiesta può invece porre delle condizioni per l'esecuzione della domanda. Se la Parte richiedente non può rispettare tali condizioni, la Parte richiesta può modifi-

170 Art. 25 par. 1.

171 Soprattutto l'art. V dell'Accordo del 10 settembre 1998 tra la Svizzera e l'Italia che completa la Convenzione europea di assistenza giudiziaria in materia penale del 20 aprile 1959 e ne agevola l'applicazione (RS **0.351.945.41**) e l'art. 9 del Trattato del 25 maggio 1973 fra la Confederazione Svizzera e gli Stati Uniti d'America sull'assistenza giudiziaria in materia penale (RS **0.351.933.6**).

172 Si tratta di garantire che vengano rispettate le disposizioni di legge vigenti nello Stato richiedente in materia di ammissibilità dei mezzi di prova, in modo che le prove acquisite possano essere utilizzate in giudizio. Cfr. n. 267 del rapporto esplicativo (nota 1).

173 Vale a dire per i motivi previsti dal diritto nazionale della Parte richiesta.

174 In base al principio sovraordinato, secondo cui l'assistenza giudiziaria deve essere garantita nella misura più ampia possibile, i motivi di rifiuto stabiliti dalla Parte richiesta vanno limitati e applicati con moderazione. Di conseguenza, fatta eccezione per quanto previsto dall'art. 28 della Convenzione, l'assistenza può essere rifiutata per motivi di protezione dei dati soltanto in casi eccezionali.

175 La sospensione dell'assistenza giudiziaria è giustificata se, per esempio, i mezzi di prova o le dichiarazioni di testimoni di cui la Parte richiedente necessita per indagini o procedimenti sono indispensabili per un procedimento imminente sul territorio della Parte richiesta (n. 270 del rapporto esplicativo, nota 1).

carle oppure rifiutare o sospendere l'assistenza. Secondo l'articolo 27 paragrafo 7 della Convenzione, la Parte richiesta è obbligata a informare la Parte richiedente del seguito che intende dare alla domanda e a motivare il rifiuto o la sospensione dell'assistenza. Ai sensi dell'articolo 27 paragrafo 8, la Parte richiedente può imporre alla Parte richiesta l'obbligo di confidenzialità in merito alla domanda e al suo contenuto[176]. La Svizzera ha aderito a una clausola analoga nel Secondo protocollo addizionale alla CEAG[177].

L'articolo 27 paragrafo 9 pone le basi per garantire una comunicazione rapida: le autorità centrali di cui all'articolo 27 paragrafo 2 comunicano direttamente tra loro. Le domande di assistenza giudiziaria possono essere trasmesse anche tramite l'Interpol[178]. Le richieste devono essere indirizzate direttamente all'autorità centrale svizzera (UFG).

Articolo 28 Confidenzialità e limitazioni di utilizzo

L'articolo 28 limita l'utilizzo delle informazioni o della documentazione, affinché la Parte richiesta possa avere la certezza che eventuali informazioni o documenti particolarmente delicati saranno impiegati esclusivamente per gli scopi per cui viene concessa l'assistenza giudiziaria. Come l'articolo 27, anche l'articolo 28 della Convenzione può essere applicato solo se non vi è alcun trattato in essere tra le Parti[179].

L'articolo 28 paragrafo 2 permette allo Stato richiesto di porre due condizioni: le informazioni o i documenti devono rimanere confidenziali se la domanda di assistenza giudiziaria non può essere soddisfatta in mancanza di tale condizione[180]; le informazioni o i documenti trasmessi non possono essere utilizzati per indagini o procedimenti diversi da quelli indicati nella domanda. In Svizzera il principio della specialità, che trova il suo fondamento nell'articolo 67 AIMP, riveste grande importanza pratica. In base ad esso i documenti e le informazioni trasmessi non possono essere usati nello Stato richiedente né a scopo d'indagine né come mezzi di prova in

176 Può infatti succedere che una Parte presenti una domanda di assistenza giudiziaria in un caso particolarmente delicato o in cui la divulgazione prematura dei fatti alla base della domanda avrebbe gravi conseguenze. La richiesta di confidenzialità può, però, essere avanzata solo nella misura in cui ciò non impedisca alla Parte richiesta di acquisire i mezzi di prova o le informazioni desiderate. Questa condizione è rilevante, ad esempio, quando occorre rendere pubbliche alcune informazioni per ottenere la decisione giudiziale indispensabile all'esecuzione della domanda oppure quando occorre mettere al corrente della domanda privati che sono in possesso di mezzi di prova, in modo da poter procedere all'esecuzione (n. 273 del rapporto esplicativo, nota 1).

177 Qualora la Parte richiesta non possa adeguarsi al requisito di confidenzialità, deve informare la Parte richiedente, che può ritirare o modificare la propria domanda.

178 Art. 27 par. 9 lett. b. In questo contesto si menziona anche l'Accordo di cooperazione tra la Svizzera ed Eurojust non ancora entrato in vigore, che sostiene gli Stati nella gestione veloce delle domande di assistenza giudiziaria (messaggio del Consiglio federale del 4 dicembre 2009, FF **2010** 23 segg.).

179 A meno che le Parti non stabiliscano altrimenti. In tal modo si evitano sovrapposizioni con altri trattati bilaterali o multilaterali di assistenza giudiziaria e accordi simili in vigore, permettendo ai responsabili di continuare ad attenersi alle regole attualmente applicate, senza dover conciliare l'applicazione di due accordi analoghi o addirittura contraddittori. Cfr. n. 276 del rapporto esplicativo (nota 1).

180 Come nel caso dell'identità di un informatore che deve rimanere confidenziale.

procedimenti vertenti su fatti per cui l'assistenza è inammissibile[181]. La limitazione dell'utilizzo delle informazioni e dei documenti trasmessi vale solo se espressamente voluta dalla Parte richiesta. In caso contrario, la Parte richiedente non è tenuta a rispettare alcuna restrizione del genere. Tale limitazione garantisce che le informazioni e i documenti siano utilizzati solo per gli scopi indicati nella domanda, escludendo un loro impiego per altri fini senza il consenso della Parte richiesta. La Convenzione del Consiglio d'Europa sulla cibercriminalità prevede tuttavia due eccezioni rispetto alla possibilità di limitare l'utilizzo delle informazioni e dei documenti[182]. Se uno Stato richiedente non può rispettare una delle condizioni deve prontamente informare lo Stato richiesto, che decide se vuole mettere comunque a disposizione le informazioni[183]. È poi possibile esigere dalla Parte richiedente che fornisca indicazioni sull'uso fatto delle informazioni o dei documenti ricevuti alle condizioni di cui al paragrafo 2, in modo che la Parte richiesta possa verificare il rispetto di tali condizioni[184]. In base al principio della specialità di cui all'articolo 67 AIMP, in determinati casi la Svizzera sarà tenuta a verificare se le condizioni legate alla trasmissione siano state rispettate.

Articolo 29 Conservazione rapida di dati informatici memorizzati

Ai sensi dell'articolo 29 paragrafo 1, una Parte può richiedere che i dati memorizzati attraverso un sistema informatico situato sul territorio della Parte richiesta siano conservati rapidamente e, ai sensi del paragrafo 3, ogni Parte è tenuta a creare le condizioni legali per l'applicazione di tale misura. In questo modo si intende evitare che i dati possano essere modificati, rimossi o cancellati durante il tempo necessario per elaborare, trasmettere ed eseguire una domanda di assistenza giudiziaria volta a reperire dati. La conservazione è una misura di portata limitata e provvisoria. I dati informatici sono estremamente labili e questa procedura garantisce che rimangano disponibili fino alla conclusione della lunga e complicata procedura di esecuzione di una domanda formale di assistenza giudiziaria. Questo provvedimento è più rapido di una normale procedura e ha effetto limitato. In questa fase non si richiede ai soggetti competenti per l'assistenza della Parte richiesta di farsi consegnare i dati in questione da chi li ha in custodia. Piuttosto la Parte richiesta deve assicurarsi che il custode dei dati (spesso un fornitore di servizi o un terzo) li conservi, ossia non li cancelli, finché non viene ordinata la loro successiva consegna[185]. Nel diritto svizzero questo requisito è soddisfatto da misure provvisionali, che possono essere ordinate dall'autorità d'esecuzione svizzera secondo l'articolo 18 AIMP. Per esempio, a un fornitore di servizi può essere intimato di effettuare una copia di sicurezza (*backup*),

181 Questo divieto si riferisce in particolare a reati che la Svizzera ritiene abbiano carattere politico, militare o fiscale. Cfr. art. 2 cpv. 1 e 3 AIMP: viene considerato di carattere fiscale un reato che sembra volto a una decurtazione di tributi fiscali o viola disposizioni in materia di provvedimenti di politica monetaria, commerciale o economica. I documenti e le informazioni trasmessi nel quadro dell'assistenza giudiziaria possono però essere utilizzati anche in un procedimento per truffa (qualificata) in materia fiscale.

182 Se il materiale messo a disposizione scagiona un imputato, viene portato a conoscenza della difesa o dell'autorità giudiziaria. Se il materiale messo a disposizione nel quadro di un trattato sull'assistenza giudiziaria viene utilizzato in sede di dibattimento, diviene accessibile a chiunque. In questi casi non è possibile garantire la confidenzialità delle indagini e dei procedimenti per cui è stata richiesta l'assistenza (n. 278 del rapporto esplicativo, nota 1).

183 Art. 28 par. 3.

184 Art. 28 par. 4.

185 N. 282 del rapporto esplicativo (nota 1).

su un supporto elettronico separato, dei dati rilevanti per le autorità straniere, proteggendoli da una successiva cancellazione da parte dell'utente o del fornitore stesso. L'autorità straniera deve presentare una domanda formale di assistenza giudiziaria entro il termine stabilito dalla legge. In caso contrario, la copia di sicurezza può essere distrutta. La procedura stabilita nell'articolo 29 della Convenzione può essere eseguita rapidamente e rispetta il diritto dell'interessato alla tutela della sfera privata, poiché i dati vengono trasmessi solo quando sono rispettati i criteri per la completa divulgazione ai sensi dei trattati sull'assistenza giudiziaria. Tale disposizione garantisce una procedura estremamente rapida, che impedisce la perdita irrecuperabile dei dati, conservati finché non possono essere trasmessi. Questi provvedimenti sono però applicabili solo quando il fornitore di servizi non è a sua volta coinvolto nel reato perseguito all'estero. In tal caso per attuare le misure provvisorie è necessario ricorrere a una perquisizione.

Il paragrafo 2 stabilisce il contenuto della domanda di conservazione, che va redatta e trasmessa rapidamente. Per tale motivo le informazioni riportate devono essere concise e limitarsi alle indicazioni necessarie per la conservazione dei dati[186]. In un momento successivo, la Parte richiedente deve presentare una domanda per la consegna dei dati.

L'articolo 29 paragrafo 4 prevede la possibilità di una riserva limitativa in merito alla doppia incriminazione, di cui la Svizzera si avvarrà, poiché il nostro Paese la considera un presupposto inderogabile per tutti i provvedimenti incisivi. La Svizzera si riserva quindi il diritto, per reati diversi da quelli descritti negli articoli 2–11 della Convenzione[187], di rifiutare di espletare una domanda di conservazione ai sensi dell'articolo 29, volta a ottenere la perquisizione o un'altra misura di accesso simile[188], il sequestro o un altro provvedimento di conservazione simile o la trasmissione dei dati memorizzati, se ha ragione di ritenere che, al momento della divulgazione, la condizione della doppia incriminazione non sia soddisfatta. La riserva avanzata dalla Svizzera ricalca quella in merito all'articolo 5 CEAG.

L'articolo 29 paragrafo 5 della Convenzione fissa le uniche condizioni che giustificano il rifiuto di una domanda di conservazione[189]. La loro applicazione pratica si fonda sull'interpretazione degli articoli 29 e 30, contemplanti misure provvisorie che, in quanto tali, precedono una domanda formale di assistenza giudiziaria. Secondo l'articolo 29, un'autorità straniera può richiedere la conservazione rapida di dati memorizzati e, ai sensi dell'articolo 30, la loro rapida trasmissione. Tuttavia, la Svizzera interpreta in modo diverso l'articolo 29 paragrafo 5 e l'articolo 30 paragrafo 2: se, nel momento di decidere in merito alla disposizione di misure provvisorie, è

186 Oltre all'indicazione dell'autorità richiedente e del reato, la domanda deve contenere una breve esposizione dei fatti, nonché le indicazioni necessarie per individuare i dati da conservare. Occorre inoltre indicare il nesso tra i dati e le indagini e illustrare i motivi che rendono necessaria la conservazione. N. 284 del rapporto esplicativo (nota 1).

187 La condizione della doppia incriminazione è soddisfatta per i reati di cui agli articoli 2–11 della Convenzione nella misura in cui le Parti non si siano avvalse di una riserva prevista dalla Convenzione per tali reati.

188 Cfr. la corrispondente riserva della Svizzera nel quadro della CEAG.

189 La Parte richiesta può rifiutare la domanda di conservazione solo se l'esecuzione potrebbe arrecare pregiudizio alla sua sovranità, alla sua sicurezza, al suo ordine pubblico e ad altri suoi interessi essenziali oppure se riguarda un reato considerato di carattere politico o legato a un reato politico. Questa misura è necessaria per garantire un'indagine e un perseguimento efficaci dei reati informatici, per cui non è possibile far valere altri motivi per rifiutare una domanda di conservazione (cfr. n. 287 del rapporto esplicativo, nota 1).

evidente che la domanda di assistenza per la trasmissione dei dati non può essere eseguita, la Svizzera dovrebbe rinunciarvi. L'articolo 31 permette infatti di rifiutare l'assistenza sulla base del diritto nazionale vigente e dei trattati applicabili. Se la Svizzera intende rifiutare una domanda di assistenza, non vi è motivo di conservare i dati a cui si riferisce tale richiesta.

Se la Parte richiesta ha motivo di credere che il custode dei dati potrebbe pregiudicare le indagini[190], deve prontamente informare la Parte richiedente[191], che può decidere se affrontare il rischio legato all'esecuzione della domanda di conservazione oppure scegliere un'altra forma di assistenza più incisiva, ma anche più sicura. Ai sensi dell'articolo 29 paragrafo 7 della Convenzione, i dati devono essere conservati per almeno 60 giorni fino al ricevimento della domanda formale di trasmissione e continuare ad essere conservati dopo il suo ricevimento[192]. Questo requisito non pone problemi alla Svizzera, dal momento che la legge non prevede alcun termine minimo per la conservazione dei dati e l'autorità d'esecuzione può stabilire a sua discrezione la durata del provvedimento. Le sue decisioni sono soggette al controllo dell'UFG, che può impugnarle se necessario.

Articolo 30 Trasmissione rapida di dati memorizzati relativi al traffico informatico

Modifiche necessarie del diritto vigente

Per far fronte in modo efficace alla criminalità informatica è necessario trasmettere rapidamente le informazioni acquisite. A differenza dei mezzi di prova tradizionali, caratterizzati da una certa persistenza temporale e spaziale e utilizzabili anche in caso di procedimenti di lunga durata, i dati informatici possono essere trasferiti in brevissimo tempo da un Paese all'altro e vengono di rado salvati per più di due mesi, rivelandosi estremamente labili. La semplice esecuzione di rapide misure provvisorie (sequestro dei dati rilevanti) non è sufficiente. I dati devono anche essere trasmessi quanto prima all'autorità richiedente, onde evitare che diventino inutilizzabili. Questo requisito costituisce l'oggetto dell'articolo 30 della Convenzione.

Il diritto svizzero non garantisce la corretta attuazione dell'articolo 30 della Convenzione. Su domanda di una Parte sul cui territorio è stato commesso un reato, la Parte richiesta spesso provvede alla conservazione dei dati relativi alla trasmissione di una comunicazione per mezzo di computer situati sul suo territorio. In tal modo si possono ripercorrere le tappe della comunicazione fino alla sua origine, individuare l'autore del reato o acquisire mezzi di prova decisivi. Nel corso delle indagini, la Parte richiesta può scoprire, dai dati relativi al traffico rintracciati sul proprio territorio, che la comunicazione è partita da un fornitore di servizi di uno Stato terzo o da un provider della Parte richiedente. In tal caso la Parte richiesta deve mettere rapidamente a disposizione della Parte richiedente una quantità sufficiente di dati relativi al traffico informatico per individuare il fornitore di servizi dello Stato terzo e il percorso della comunicazione. Se la comunicazione è stata trasmessa da uno Stato terzo, la Parte richiedente può, sulla base delle informazioni disponibili, inviare a tale Stato una domanda di conservazione e presentare una domanda di assistenza accelerata per individuare il fornitore di servizi e il percorso della comunicazione.

190 P. es. quando i dati da conservare sono custoditi da un fornitore di servizi indagato.
191 Art. 29 par. 6.
192 N. 289 del rapporto esplicativo (nota 1).

L'articolo 30 richiede la rapida trasmissione all'estero dei dati relativi al traffico informatico, resi accessibili grazie a un ordine di sorveglianza ai sensi della LSCPT. Tale obbligo è praticamente inconciliabile con il sistema di assistenza giudiziaria attualmente adottato in Svizzera, in base al quale, prima di trasmettere informazioni facenti parte della sfera privata[193], al detentore di tali informazioni va sempre presentata una decisone finale impugnabile[194]. Solo al termine di questa procedura, che dura vari mesi, è possibile trasmettere i dati all'autorità straniera, la quale tuttavia non potrà farne uso perché non sono più attuali. Inoltre, i lunghi tempi richiesti danno agli interessati, informati dalle autorità svizzere, la possibilità di far sparire mezzi di prova incriminanti[195]. Il diritto svizzero deve essere pertanto modificato per soddisfare i requisiti dell'articolo 30.

Il nuovo articolo 18*b* permette la trasmissione all'autorità straniera dei dati relativi al traffico informatico facenti parte della sfera privata prima della conclusione della procedura di assistenza giudiziaria nei due casi seguenti:

- capoverso 1 lettera a (disposizione per l'attuazione dell'articolo 30): le misure provvisionali adottate dimostrano che la comunicazione oggetto della domanda ha origine in un altro Stato;
- capoverso 1 lettera b (disposizione per l'attuazione dell'articolo 33): i dati vengono acquisiti dall'autorità d'esecuzione sulla base di un ordine di sorveglianza in tempo reale autorizzata in precedenza.

Le nuove condizioni di trasmissione si discostano dall'attuale sistema di assistenza, ragion per cui l'interessato gode di una maggiore tutela giurisdizionale, garantita dai capoversi 2 e 3 dell'articolo 18*b*, qualora l'assistenza venga successivamente negata. A tal fine sono previste tre misure di tutela: il provvedimento di sorveglianza deve essere autorizzato da un giudice indipendente ai sensi dell'articolo 272 CPP (cfr. nuovo art. 18*b* cpv. 1 lett. b *in fine* AIMP); i dati trasmessi non possono essere utilizzati come mezzi di prova prima che la procedura di assistenza giudiziaria sia conclusa per garantire la possibilità di far rimuovere dagli atti stranieri le informazioni trasmesse se l'impugnazione dovesse essere accolta (cfr. nuovo art. 18*b* cpv. 2 AIMP); e la trasmissione è soggetta all'immediato controllo dell'UFG (cfr. nuovo art. 18*b* cpv. 3 AIMP).

L'UFG provvede al rispetto della legge e può intervenire sia presso le autorità svizzere sia presso quelle straniere se la disposizione è stata applicata indebitamente o non rispettata. Questo articolo costituisce una novità nel sistema svizzero dell'assistenza giudiziaria, poiché permette di trasmettere all'autorità straniera informazioni facenti parte della sfera privata, senza che l'interessato ne sia prima informato e abbia avuto la possibilità di far valere le proprie argomentazioni. Tale procedura è

193 Art. 9 AIMP e art. 69 della legge federale del 15 giugno 1934 sulla procedura penale (RS **312.0**).

194 Art. 80*e* AIMP. Una tale procedura non è necessaria se la comunicazione oggetto d'indagine costituisce di per sé un reato commesso usando Internet. In tal caso l'Internet provider è tenuto a fornire, nell'ambito di una procedura semplificata, tutte le indicazioni che consentono di identificare l'autore del reato (art. 14 cpv. 4 LSCPT).

195 Il rischio di inquinamento delle prove giustifica la trasmissione tempestiva, p. es. opportuna quando l'autorità straniera vuole identificare una persona che utilizza servizi Internet svizzeri per scambiare materiale pedopornografico. Ad oggi i dati che permettono di identificare l'utente di un tale servizio non possono essere trasmessi all'autorità straniera prima che l'utente sia stato informato della decisione emessa a suo carico e abbia avuto la possibilità di impugnarla entro un termine di trenta giorni.

necessaria per soddisfare quanto stabilito dalla Convenzione, che tiene conto delle necessità assolute del perseguimento penale. Il nuovo articolo riduce la possibilità dell'interessato di opporsi tempestivamente alla trasmissione all'estero di informazioni facenti parte della sua sfera privata, tuttavia vi sono altre misure che continuano a garantirne la tutela. La domanda di assistenza giudiziaria non viene infatti verificata soltanto dall'autorità d'esecuzione, ma anche dall'UFG. Inoltre, anche l'autorità che autorizza la sorveglianza[196] deve verificare che la domanda soddisfi una serie di criteri, i quali sostanzialmente coincidono in larga misura con quelli della procedura di assistenza giudiziaria[197]. La persona coinvolta non viene privata di tutti i suoi diritti: non appena la situazione lo consente[198], deve essere informata dell'avvenuta trasmissione e può impugnare sia la decisione finale sia l'ordine di sorveglianza. Se il ricorso viene accolto, l'autorità straniera deve rimuovere le informazioni dai propri atti e attestarlo alle autorità svizzere. Fino al momento in cui l'interessato può far valere i propri diritti, le informazioni che lo riguardano non possono essere usate come mezzi di prova, ma solo a scopo d'indagine[199]. In tal modo la normativa proposta risponde ai requisiti del perseguimento penale, garantendo al contempo un'adeguata tutela degli interessi legittimi dell'interessato. Inoltre, questa modifica è utile anche per l'individuazione dei sospettati nella procedura di estradizione.

Dal punto di vista formale, l'autorità competente, cui viene indirizzata la domanda di sorveglianza in tempo reale dei dati relativi al traffico informatico, deve emettere una decisione di entrata nel merito e ottenere le autorizzazioni eventualmente necessarie ai sensi dell'articolo 272 CPP. In questa decisione o in una decisione incidentale l'autorità d'esecuzione ordina anche la trasmissione anticipata, vincolata a determinate condizioni, dei dati acquisiti sulla base dell'ordine di sorveglianza. La decisione deve essere inoltrata immediatamente all'UFG, che può opporvisi[200] se non sono rispettate le condizioni legali. Anche l'ordine e l'autorizzazione della sorveglianza devono essere comunicati all'UFG per permettergli di verificare che siano rispettate le condizioni dell'articolo 18*b*.

Vista la loro natura, le misure di sorveglianza in tempo reale non dovrebbero essere portate a conoscenza della persona sorvegliata. Nella cooperazione internazionale tale requisito è difficile da conciliare con il principio dell'AIMP, in base al quale nessuna informazione facente parte della sfera privata di una persona può essere trasmessa all'estero senza che tale persona abbia prima avuto la possibilità di opporsi all'attuazione di tale misura. Si riscontrano, dunque, interessi diversi non solo per quanto riguarda la trasmissione dei dati relativi al traffico informatico, disciplinata nell'articolo 33 della Convenzione, ma anche per quanto riguarda la trasmissione del contenuto delle comunicazioni intercettate. La dottrina ha riconosciuto questo possi-

196 Art. 7 cpv. 1 LSCPT.

197 Vale per la doppia incriminazione (art. 3 LSCPT), la proporzionalità (sussidiarietà delle misure; art. 3 cpv. 1 lett. a–c LSCPT) e la separazione dei documenti (art. 8 LSCPT).

198 In ogni caso al più tardi prima che si concluda l'inchiesta penale o venga sospesa la procedura (art. 10 cpv. 2 LSCPT).

199 Cfr. a tale proposito il messaggio del Consiglio federale del 1° ottobre 2004 per quanto riguarda l'art. 30 dell'Accordo di collaborazione tra l'Unione europea e i suoi Stati membri da un lato e la Confederazione Svizzera dall'altro per la lotta alla frode e altri atti illeciti che pregiudicano i suoi interessi finanziari; FF **2004** 5273, pag. 5495. Nel diritto svizzero viene applicato lo stesso criterio; cfr. p. es. l'art. 10 cpv. 3 AIMP e l'art. 22 della legge federale del 20 giugno 2003 sull'inchiesta mascherata (LFIM).

200 Art. 80*e*, 80*h* e 80*l* AIMP.

bile conflitto indicando gli attuali problemi nell'esecuzione delle domande di assistenza giudiziaria legati alla sorveglianza in tempo reale delle telecomunicazioni[201]. La revisione si limita però a soddisfare le condizioni per l'attuazione dell'articolo 33 e riguarda esclusivamente i dati relativi al traffico informatico e non quelli relativi al contenuto. L'articolo 18*b* AIMP non costituisce quindi una normativa ad ampio raggio, che consenta l'attuazione delle misure di sorveglianza nell'ambito dell'assistenza giudiziaria e includa sia i dati relativi al traffico informatico sia quelli relativi al contenuto.

Il nuovo articolo 18*b* capoverso 1 lettera b AIMP è illustrato anche nel commento all'articolo 33 della Convenzione.

Ulteriori spiegazioni relative all'articolo 30

Ai sensi dell'articolo 30 paragrafo 2, la Parte richiesta può rifiutarsi di trasmettere i dati relativi al traffico informatico solo se ritiene che questo potrebbe arrecare pregiudizio alla sua sovranità, alla sua sicurezza, al suo ordine pubblico o ad altri suoi interessi essenziali, oppure se si tratta di un reato considerato di carattere politico o legato a un reato politico. Come per l'articolo 29, anche in questo caso le informazioni sono ritenute talmente importanti per individuare l'autore o reperire mezzi di prova decisivi che si è voluto limitare i motivi che giustificano il rifiuto della trasmissione[202].

Articolo 31 Assistenza giudiziaria per l'accesso a dati informatici memorizzati

L'articolo 31 riconosce alle Parti la possibilità di perquisire per conto di un altro Stato aderente alla Convenzione i dati salvati attraverso un sistema informatico situato sul proprio territorio o di accedervi in altro modo, di sequestrarli o acquisirli in altro modo e di trasmetterli, come consentito per scopi nazionali in base all'articolo 19 della Convenzione. Non costituisce un problema il fatto che la presente disposizione non permetta di restringere le misure a una determinata categoria di reati e non riconosca la possibilità di avanzare riserve[203], poiché in base all'articolo 31 paragrafo 2 lettera f la cooperazione viene eseguita in applicazione dei trattati e delle disposizioni normative nazionali vigenti di cui all'articolo 23.

In base all'articolo 31 paragrafo 1, ogni Stato aderente può richiedere una delle forme di assistenza ivi previste, mettendo la Parte richiesta nella condizione di fornire tale assistenza. Ai sensi dell'articolo 31 paragrafo 3 una tale domanda deve essere espletata tempestivamente, quando vi è motivo di ritenere che i dati in questione siano particolarmente a rischio di perdita o di alterazione, oppure i trattati, gli accordi o la legislazione applicabili prevedano una cooperazione rapida[204].

201 Thomas Hansjakob, BÜPF / VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, San Gallo 2006; Robert Zimmermann, La coopération judiciaire internationale en matière pénale, Berna, 2004, n. 246-13 segg., pag. 285 segg.
202 N. 291 del rapporto esplicativo (nota 1).
203 Art. 42.
204 N. 292 del rapporto esplicativo (nota 1).

Articolo 32 Accesso transfrontaliero a dati informatici memorizzati, con consenso o quando sono pubblicamente disponibili

L'articolo 32 della Convenzione disciplina l'accesso transfrontaliero a dati pubblicamente disponibili[205] e a dati per cui la persona autorizzata a divulgarli ha fornito il consenso all'accesso. La disposizione si riferisce alle situazioni in cui è ammessa una procedura intrapresa da una Parte senza che l'abbia prima concordata con l'altra Parte[206], nel pieno rispetto della sovranità della Parte non avvertita. Dal punto di vista legale, la disposizione della Convenzione fa riferimento a due modi di reperire dati all'estero di cui gli Stati si avvalgono nella pratica. Nel corso delle trattative non è stato possibile raggiungere un consenso su misure di più ampia portata, che consentissero a una Parte di accedere per decisione unilaterale ai dati situati in un altro Stato aderente alla Convenzione senza il consenso di quest'ultimo[207].

Nell'articolo 32 viene disciplinato, da un lato, il caso in cui una Parte può accedere a dati pubblicamente disponibili in altri Paesi: nel caso di dati pubblicamente accessibili sulla pagina Internet di un'azienda o di un'amministrazione, ad esempio, la Parte non è obbligata a ottenere il consenso dello Stato in cui si trovano tali dati prima di poterli consultare e utilizzare. Dall'altro lato, la Parte può accedere o ricevere dati che si trovano in un altro Stato aderente se dispone del consenso legale e volontario di una persona legalmente autorizzata a divulgare i dati a un'autorità di perseguimento penale interna. Se si tratta di materiale confidenziale di un terzo che non ha prestato il proprio consenso alla divulgazione, non sussiste alcuna autorizzazione ai sensi dell'articolo 32 della Convenzione.

La disposizione dell'articolo 32 della Convenzione va quindi interpretata in senso restrittivo, soprattutto per quanto riguarda la seconda parte, per evitare il rischio di abuso sotto forma di elusione dell'assistenza giudiziaria oppure di violazione della sfera privata di terzi[208]. La facoltà legale di una persona di disporre dei dati e di divulgarli a un'autorità statale dipende in primo luogo dal diritto nazionale dello Stato in cui tale persona agisce. Sussiste, per esempio, nel caso di una persona che ha salvato proprie e-mail presso un fornitore di servizi straniero e trasmette questi dati a un'autorità di tale Paese[209]. All'atto pratico significa che la persona all'estero che ha salvato i dati in Svizzera potrà continuare a metterli volontariamente a disposizione di autorità straniere senza prima doverne informare le autorità svizzere, purché disponga dell'autorizzazione legale a tal fine e non venga intaccata la sfera privata di terzi.

Articolo 33 Assistenza giudiziaria per la raccolta in tempo reale di dati relativi al traffico informatico

Ai sensi dell'articolo 33, ogni Parte deve acquisire in tempo reale i dati relativi al traffico informatico per conto di un'altra Parte e gli Stati sono tenuti a collaborare in

205 *Open source data*.
206 Rapporto esplicativo, n. 293 (cfr. nota 1).
207 E senza rispettare la normale procedura di assistenza giudiziaria e amministrativa. La Convenzione (art. 39 par. 3) non autorizza altre modalità di accesso.
208 Questa concezione viene condivisa dalla Germania nel quadro della sua procedura di attuazione, cfr. quanto illustrato nel disegno di legge del Governo federale tedesco del 16 novembre 2007 sulla Convenzione sulla cibercriminalità, stampato 16/7218, pag. 55, consultabile all'indirizzo: http://dip21.bundestag.de/dip21/btd/16/072/1607218.pdf.
209 Il luogo in cui i dati sono salvati può trovarsi all'estero anche all'insaputa della persona autorizzata, poiché è difficilmente individuabile.

questo ambito. Le disposizioni e le condizioni valide per la cooperazione sono stabilite nelle convenzioni e nelle leggi applicabili in materia di assistenza giudiziaria penale. Spesso gli inquirenti non possono garantire che si possa risalire all'origine di una comunicazione seguendo le trasmissioni registrate in precedenza, perché è possibile che alcuni dati essenziali relativi al traffico informatico siano stati cancellati da un fornitore di servizi lungo il percorso, prima che potessero essere messi al sicuro. Per tale motivo gli inquirenti di tutte le Parti devono assolutamente avere la possibilità di acquisire dati relativi al traffico trasmessi attraverso un sistema informatico situato in un altro Stato aderente[210]. Secondo l'articolo 33 paragrafo 2, l'assistenza deve essere fornita almeno per i reati «per i quali la raccolta in tempo reale dei dati relativi al traffico informatico sarebbe possibile a livello nazionale in una situazione analoga». In base al diritto svizzero in vigore, i dati relativi al traffico informatico facenti parte della sfera privata vengono acquisiti mantenendo il relativo segreto e non possono essere trasmessi prima che sia stata emessa una decisione finale. Il nuovo articolo 18*b* AIMP sancisce la possibilità di trasmettere tempestivamente i dati all'estero senza che tale decisione debba essere notificata alla persona residente in Svizzera[211]. In tal modo anche le indagini straniere sono tutelate.

L'articolo 33 della Convenzione non contempla alcuna restrizione in termini di gravità del reato per l'applicazione delle misure di sorveglianza. Il nuovo articolo 273 CPP[212] permetterà la sorveglianza in tempo reale dei dati relativi al traffico informatico esclusivamente per le indagini su delitti e crimini. L'articolo 15 paragrafo 1 della Convenzione prevede tuttavia il principio della proporzionalità per i poteri e le procedure, stabilendo che ogni Parte deve applicare tale principio in sintonia con i principi vigenti nel proprio diritto nazionale[213]. Le Parti possono quindi non dare corso a domande che violano il principio della proporzionalità. Questo permette alla Svizzera di rifiutare la propria collaborazione se la condotta perseguita all'estero è considerata una semplice contravvenzione in base al diritto svizzero[214].

Articolo 34 Assistenza giudiziaria per l'intercettazione di dati relativi al contenuto

L'articolo 34 limita l'obbligo di assistenza giudiziaria per l'acquisizione di dati relativi al contenuto, poiché l'intercettazione di tali dati costituisce una profonda ingerenza nella sfera privata. Questa forma di assistenza viene concessa solo nella misura in cui i trattati applicabili e il diritto interno lo permettono. La prassi in materia di assistenza giudiziaria in merito è solo agli inizi, per cui la legislazione esistente e il diritto interno in materia fungono da punti di riferimento per la portata e le restrizioni dell'obbligo di collaborazione[215]. In base al nuovo articolo 18*b* AIMP, prima della conclusione della procedura possono essere trasmessi all'estero solo i dati relativi al traffico informatico, non quelli relativi al contenuto. Pertanto,

210 N. 295 del rapporto esplicativo (nota 1).
211 Art. 80*m* AIMP.
212 Il nuovo diritto processuale penale consente la sorveglianza retroattiva quando la gravità del reato la giustifica ed è necessaria per l'inchiesta (art. 273 e 269 cpv. 1 lett. b e c CPP), anche se tale reato non figura nell'elenco dei reati dell'art. 269 CPP.
213 N. 146 del rapporto esplicativo (nota 1).
214 A questa categoria appartengono anche le scommesse via Internet (art. 42 della legge federale dell'8 giugno 1923 concernente le lotterie e le scommesse professionalmente organizzate; RS **935.51**).
215 N. 297 del rapporto esplicativo (nota 1).

secondo l'articolo 30 capoverso 1 AIMP[216], le autorità svizzere non si possono nemmeno rivolgere a un altro Stato per la consegna anticipata di dati relativi al contenuto.

Articolo 35 Rete 24/7

Secondo l'articolo 35 della Convenzione, le Parti devono designare un punto di contatto disponibile 24 ore su 24 sette giorni su sette, che fornisca supporto alle indagini penali nazionali e internazionali nei casi di criminalità informatica. Il punto di contatto non è tenuto ad adottare provvedimenti diretti in materia di consulenza legale, di assistenza giudiziaria, di acquisizione delle prove, di conservazione dei dati o di indagini penali in generale[217]. Per soddisfare i requisiti della Convenzione, deve fungere da servizio di riferimento con il compito di facilitare i contatti tra le autorità straniere e quelle nazionali coinvolte nel caso.

Tale funzione può essere attribuita alla centrale operativa dell'Ufficio federale di polizia (fedpol), mentre l'UFG, con il suo servizio di picchetto, si assumerà i compiti relativi all'assistenza giudiziaria e all'estradizione (in particolare la decisione sull'ammissibilità di un provvedimento), stabiliti dall'articolo 35 paragrafo 1 lettere a–c della Convenzione.

Il lavoro aggiuntivo per espletare i casi di assistenza giudiziaria e le domande presentate nel quadro della Convenzione dipende dal numero di Stati aderenti, dalla complessità dei singoli casi e dallo sviluppo tecnologico, sia riguardo alla delinquenza nei vari Stati sia in riferimento agli strumenti di perseguimento penale[218]. L'UFG reputa che il lavoro supplementare dovuto all'attuazione e alla ratifica della Convenzione del Consiglio d'Europa (servizio di picchetto e normale gestione dei casi[219]) giustifichi l'assunzione di una persona a tempo pieno. Anche per fedpol, la cui centrale operativa riceverà le richieste 24 ore su 24, l'implementazione dei requisiti della Convenzione richiede l'assunzione di un'ulteriore persona a tempo pieno.

2.4 Capitolo IV: Disposizioni finali

Le disposizioni finali della Convenzione del Consiglio d'Europa sulla cibercriminalità corrispondono – eccettuate alcune lievi peculiarità – a quelle previste da altre convenzioni del Consiglio d'Europa.

Ai sensi dell'*articolo 36* della Convenzione possono aderirvi sia gli Stati membri del Consiglio d'Europa sia gli Stati che non ne fanno parte, ma che hanno partecipato all'elaborazione della Convenzione[220]. Possono inoltre essere invitati ad aderire anche altri Stati[221].

216 Le autorità svizzere non possono inoltrare a un altro Stato una domanda che esse stesse non possono soddisfare per legge.
217 Cfr. art. 35 par. 1 della Convenzione e il n. 298 segg. del rapporto esplicativo (nota 1).
218 Risorse ed equipaggiamento per la sorveglianza, la conservazione e il controllo del traffico di dati elettronici.
219 Cfr. anche n. 2.3.6.
220 Canada, Giappone, Stati Uniti d'America e Sud Africa.
221 *Art. 37* della Convenzione. Attualmente (gennaio 2010) sono stati invitati Cile, Costa Rica, Repubblica dominicana, Messico e le Filippine.

La Convenzione è entrata in vigore il 1° luglio 2004, dopo che almeno cinque Stati avevano siglato la ratifica come previsto[222]. Attualmente gli Stati aderenti sono 26 e l'unico firmatario non membro del Consiglio d'Europa sono gli Stati Uniti.

Nell'elaborare la Convenzione, la possibilità di formulare dichiarazioni e riserve è stata prevista come parte integrante del testo mantenuto volutamente semplice[223]. L'*articolo 40* elenca le sei disposizioni in merito alle quali le Parti possono rilasciare dichiarazioni restrittive. Come già spiegato nel commento alle singole disposizioni, si propone che la Svizzera rilasci dichiarazioni in merito agli articoli 2, 3, 7, 9 numero 3, nonché 27 numero 9 lettera e.

In base all'*articolo 41* (clausola federale), uno Stato può avvalersi di una riserva per dichiarare che, a causa della sua struttura, non può adempiere alle obbligazioni derivanti dal capitolo II[224] della Convenzione[225]. Tale riserva non deve tuttavia scalfire la cooperazione internazionale[226]. Dato che in Svizzera la legiferazione in materia penale è prerogativa della Confederazione e che il nuovo Codice di procedura penale del 5 ottobre 2007 entrerà presto in vigore, non è necessario avanzare una tale riserva.

Una particolarità della Convenzione è costituita dal numero predefinito di possibili riserve fissato dall'*articolo 42*, in base al quale le Parti possono avanzare riserve esclusivamente in merito alle nove disposizioni ivi riportate. Si prevede che la Svizzera si avvalga di quattro riserve in relazione agli articoli 6 numero 3, 9 numero 4, 14 numero 3 e 29 numero 4. Per i dettagli si rimanda al commento delle singole disposizioni.

Le riserve e le dichiarazioni svizzere riportate nel decreto federale devono essere comunicate al Segretario generale del Consiglio d'Europa in occasione del deposito del documento di ratifica.

In caso di controversie in merito all'interpretazione o all'applicazione della Convenzione, le Parti interessate devono adoperarsi per trovare una soluzione bonaria intavolando negoziati (*art. 45*). A differenza di altre più recenti Convenzioni del Consiglio d'Europa, la presente Convenzione non prevede alcun meccanismo di sorveglianza o valutazione reciproche.

La Convenzione può essere denunciata in qualsiasi momento con un termine di preavviso di tre mesi mediante notifica al Segretario generale del Consiglio d'Europa (*art. 47*).

222 *Art. 36 par. 3* della Convenzione.
223 Cfr. rapporto esplicativo del Consiglio d'Europa, n. 49 e 50 (nota 1).
224 Misure interne.
225 Si tratta di una clausola poco usuale, inserita nel testo in seguito all'intervento determinante degli Stati Uniti.
226 Cap. III della Convenzione.

2.5 Ulteriori aspetti della procedura di consultazione

In occasione della procedura di consultazione, vari partecipanti[227] hanno richiesto di estendere l'articolo 18*b* AIMP ai dati relativi al contenuto al fine di migliorare il perseguimento penale[228]. Tuttavia, il Consiglio federale ha optato per una «revisione circoscritta» dell'AIMP, dal momento che la Convenzione non impone[229] un'estensione ai dati relativi al contenuto e che la maggioranza dei partecipanti non ha auspicato una tale modifica. Le possibilità di cooperazione secondo l'articolo 18*a* AIMP restano immutate, sebbene il significato della cooperazione nella raccolta in tempo reale di dati informatici relativi al contenuto rimanga piuttosto limitata.

È stato inoltre proposto di ancorare nella legge la definizione di «dati relativi al traffico informatico» ripresa dall'articolo 1 lettera d della Convenzione. Tale richiesta non è stata accolta, ma si è tenuto conto dei possibili fraintendimenti con l'articolo 2 lettera g OSCPT, introducendo espressamente la nozione di «traffico informatico» nell'articolo 18*b* AIMP. La sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni è già disciplinata dall'art. 18*a* AIMP; l'articolo 18*b* AIMP non si riferisce alla sorveglianza della telefonia. La nozione di dati relativi al traffico informatico è descritta in modo esaustivo dalla dottrina e dalla pratica[230].

Infine, nella procedura di consultazione è stato proposto di istituire l'obbligo di utilizzare esclusivamente dispositivi sicuri per la trasmissione veloce delle domande. Tuttavia è possibile garantire una sicurezza sufficiente dei dati anche adottando misure di sicurezza nel singolo caso[231].

2.6 Il Protocollo addizionale del 28 gennaio 2003 contro il razzismo e la xenofobia

Il Protocollo addizionale del 28 gennaio 2003 alla Convenzione sulla cibercriminalità relativo all'incriminazione di atti di natura razzista e xenofoba commessi attraverso sistemi informatici obbliga gli Stati firmatari a rendere punibili la discriminazione e l'istigazione all'odio e alla violenza contro una persona a causa della razza, del colore della pelle, della discendenza, della provenienza o della religione. Inoltre vengono dichiarate applicabili le disposizioni della Convenzione contro la cibercriminalità. Il Protocollo è entrato in vigore il 1° marzo 2006 e finora è stato ratificato da 15 Paesi, tra cui quattro Stati membri dell'UE[232].

227 I Cantoni SG, VD, NE, FR, BS, BL, JU, AR, nonché la Conferenza delle autorità inquirenti della Svizzera e la Conferenza svizzera dei procuratori.
228 Cfr. n. 1.4.
229 Art. 34 della Convenzione.
230 I dati relativi al traffico informatico comprendono in particolare indicazioni sull'indirizzo, il periodo in cui avviene la connessione, i dati utilizzati per la procedura di autentificazione (login) e il tipo di connessione (S. Bondallaz: *La protection des personnes et de leurs données dans les télécommunications*, n. 1821 e 1823, pag. 518).
231 L'applicazione della Convenzione del Consiglio d'Europa non implica un trattamento diverso delle domande di assistenza giudiziaria. Di norma non vengono adottate misure di sicurezza per le domande ordinarie. Modificare questa prassi comporterebbe notevoli complicazioni.
232 Stato: gennaio 2010.

La Svizzera ha sottoscritto il Protocollo il 9 ottobre 2003. L'ordinamento giuridico svizzero soddisfa i requisiti obbligatori del Protocollo. Sebbene la disposizione contro il razzismo dell'articolo 261bis CP non specifichi i criteri del colore della pelle, della discendenza e della provenienza nazionale indicati nel Protocollo, tali varianti della fattispecie vengono di fatto coperte dai concetti di razza ed etnia.

Il diritto svizzero applicabile supera quanto stabilito dal Protocollo in vari ambiti. Ad esempio, a differenza dei requisiti del Protocollo, l'elemento della religione costituisce un criterio a sé stante e il diritto penale svizzero non riduce il concetto di etnia alla provenienza etnica, particolarità significativa all'atto pratico.

Nonostante l'ampia compatibilità del nostro ordinamento giuridico con il Protocollo addizionale, il progetto in discussione propone solamente la ratifica della Convenzione sulla cibercriminalità. L'attuazione del Protocollo, che verte su una materia essenzialmente diversa, dovrà essere verificata a parte in un secondo tempo. In tal modo è possibile concentrarsi sulle questioni di diritto sostanziale legate alla cibercriminalità, al diritto processuale penale in materia di prove elettroniche e alle problematiche dell'assistenza giudiziaria in questo settore. Inoltre, si devono attendere i risultati dei lavori in corso nel DFGP sulla punibilità dell'uso di simboli razzisti[233], poiché vanno tenuti in considerazione nell'esame di una possibile attuazione del Protocollo addizionale.

2.7 Rapporto con altre revisioni in materia penale

Il 5 ottobre 2007 le Camere federali hanno approvato il Codice di diritto processuale penale svizzero (CPP), che sostituirà i vari ordinamenti cantonali, nonché la procedura penale federale. L'entrata in vigore del CPP è prevista per il 1° gennaio 2011. Il presente messaggio rimanda a varie riprese alle disposizioni del CPP[234], essenziali per l'attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità o garanti di una corrispondenza integrale e accertabile nel diritto svizzero. L'entrata in vigore della Convenzione presuppone quindi per la Svizzera l'entrata in vigore del CPP. Il presente progetto non rischia ritardi per questo.

Un gruppo di lavoro della Confederazione ha iniziato la revisione della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT). Il coordinamento delle due pratiche è garantito dal DFGP.

3 Ripercussioni

3.1 Ripercussioni finanziarie e sull'effettivo del personale della Confederazione

A causa delle trasformazioni sociali derivanti dall'impiego delle moderne tecnologie dell'informazione e della connessa diffusione della criminalità informatica, si preve-

233 Cfr. a tale proposito il comunicato stampa del DFGP del 1° luglio 2009 relativo all'avvio della consultazione sulla corrispondente integrazione del CP, consultabile sul sito http://www.bj.admin.ch. La punibilità di tali simboli non è richiesta dal protocollo addizionale.

234 Cfr. in particolare quanto esposto in merito agli art. 16–21 nonché 23, 25, 30 e 33 della Convenzione.

de un maggiore carico di lavoro per le autorità di polizia e di perseguimento penale, nonché per il servizio annesso al DFGP incaricato della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, indipendentemente dalla Convenzione del Consiglio d'Europa. Dato che nella maggior parte dei casi i reati compiuti per mezzo di Internet superano i confini nazionali, anche gli uffici preposti all'esecuzione delle domande di assistenza giudiziaria saranno più sollecitati.

L'attuazione e la ratifica della Convenzione comporta una maggiore pressione, in termini qualitativi e quantitativi, sulla sezione responsabile dell'assistenza giudiziaria in seno all'UFG e richiede un'ulteriore funzione di coordinamento all'interno della Centrale operativa della Polizia giudiziaria federale. Si calcola che il maggiore carico di lavoro (servizio di picchetto e normale gestione dei casi) giustifichi un nuovo posto a tempo pieno presso l'UFG[235]. Anche per fedpol, la cui centrale operativa riceverà le richieste 24 ore su 24, l'implementazione dei requisiti della Convenzione richiede l'assunzione di un'ulteriore persona a tempo pieno. Le spese connesse saranno compensate internamente.

Questa non è la sede adatta per decidere in merito a un eventuale maggiore fabbisogno di personale e risorse negli Uffici interessati, per esempio per la lotta contro la pedofilia in rete, che supera i requisiti cogenti della Convenzione del Consiglio d'Europa. Alla luce degli sviluppi della criminalità informatica e sulla base dei futuri dati empirici, per raggiungere gli obiettivi posti dalla Convenzione, in determinati casi potrebbe rivelarsi necessario istituire servizi specializzati negli uffici competenti, il che costituirebbe un plusvalore pratico nella lotta alla criminalità informatica.

3.2 Ripercussioni sull'economia

Non si prevedono ripercussioni sull'economia derivanti dall'attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità.

3.3 Ripercussioni in ambito informatico

Non si prevedono ripercussioni in ambito informatico derivanti dall'attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità. L'attrezzatura informatica attualmente in dotazione alle autorità di perseguimento penale della Confederazione, al Tribunale federale e al Tribunale penale federale soddisfa le condizioni poste dalla Convenzione ed è sufficiente a garantire il corretto espletamento dei procedimenti penali e giudiziari.

3.4 Ripercussioni per i Cantoni

A causa del rapido sviluppo tecnologico e sociale nel settore delle moderne tecnologie della comunicazione, si prevede un aumento del numero di casi di cibercriminalità[236]. Tuttavia, non si presume che l'attuazione della Convenzione avrà ripercus-

235 Infatti, in virtù del nuovo art. 18*b* AIMP, un certo numero di decisioni finora impugnabili dall'UFG e dall'interessato sarà d'ora in avanti sottoposto al solo controllo dell'UFG.

236 Cfr. n. 3.1.

sioni dirette sui Cantoni. Sulla base delle esperienze maturate dagli Stati aderenti sin dall'entrata in vigore della Convenzione nel 2004, attualmente non si prevede un forte aumento né del numero di procedure di perseguimento penale per i reati definiti dalla Convenzione né delle domande di assistenza giudiziaria[237]. Il punto di contatto istituito dalla Convenzione sarà integrato in fedpol. L'UFG fungerà, invece, da centro di raccolta delle domande di assistenza giudiziaria e sarà responsabile delle relative risposte.

4 Programma di legislatura

Il progetto è inserito nel messaggio del 23 gennaio 2008 sul programma di legislatura 2007–2011[238].

5 Costituzionalità

La costituzionalità del decreto federale di approvazione e di attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità si fonda sull'articolo 54 capoverso 1 della Costituzione federale (Cost.)[239], che riconosce alla Confederazione la facoltà di stipulare trattati internazionali. L'articolo 184 capoverso 2 Cost. conferisce al Consiglio federale la facoltà di concludere e ratificare trattati internazionali. In base all'articolo 166 capoverso 2 Cost., l'Assemblea federale è competente per l'approvazione dei trattati internazionali.

I trattati internazionali sono soggetti a referendum facoltativo se sono di durata indeterminata e indenunciabili, se prevedono l'adesione a un'organizzazione internazionale oppure se comprendono disposizioni importanti contenenti norme di diritto o per l'attuazione delle quali è necessaria l'emanazione di leggi federali[240]. La Convenzione è stipulata a tempo indeterminato, ma può essere denunciata in qualsiasi momento e non prevede l'adesione a un'organizzazione internazionale. Tuttavia l'adesione alla Convenzione comporta modifiche del Codice di procedura penale e della legge sull'assistenza in materia penale. Il decreto di approvazione viene pertanto sottoposto a referendum facoltativo conformemente all'articolo 141 capoverso 1 lettera d numero 3 Cost.

I disegni di legge si fondano sull'articolo 54 capoverso 1 e 123 capoverso 1 Cost.

237 Cfr. anche n. 1.3: valutazione della Convenzione.
238 FF **2008** 587, in particolare pag. 665.
239 RS **101**
240 Art. 141 cpv. 1 lett. d Cost.