Procedura di consultazione

Dipartimento federale di giustizia e polizia

Approvazione e attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità

Avamprogetto e rapporto esplicativo

Ufficio di giustizia
Berna, marzo 2009

Compendio

L'Assemblea federale sarà invitata ad approvare la Convenzione del Consiglio d'Europa del 23 novembre 2001 sulla cibercriminalità (o criminalità informatica), entrata in vigore il 1° luglio 2004. Si tratta del primo, e finora unico, trattato internazionale sulla criminalità informatica e in rete. La Convenzione obbliga gli Stati aderenti 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 leggere modifiche al Codice penale e alla legge sull'assistenza in materia penale, nonché presentare alcune riserve e dichiarazioni all'atto della ratifica.

La prima parte della 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 la raccolta 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, consente di attuare le disposizioni procedurali della Convenzione in modo uniforme su scala nazionale. Il 27 febbraio 2008 il Consiglio federale ha proposto di accogliere la mozione Glanzmann-Hunkeler (07.3629) concernente 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 Codice penale). A tal fine si propone di ampliare la gamma di atti passibili di pena, in modo da rendere perseguibili anche coloro che mettono a disposizione programmi e 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, fortemente criticata dalla dottrina, dell'assenza di fini di lucro.

Dal punto di vista procedurale, il Codice di procedura penale approvato dal Parlamento (cfr. sopra) adempie i presupposti della Convenzione.

Nell'ambito della cooperazione internazionale, per l'attuazione degli articoli 30 e 33 della Convenzione, è indispensabile introdurre una nuova disposizione (nuovo art. 18b della legge federale sull'assistenza internazionale in materia penale), che attribuisca all'autorità d'esecuzione svizzera la facoltà di ordinare la trasmissione dei dati relativi al traffico informatico prima della conclusione della procedura di assistenza giudiziaria. Questa misura è giustificata dalla labilità di alcuni 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.

Indice

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. Tale sviluppo ha permesso, 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 immagazzinate nei sistemi informatici possono essere consultate, richiamate e scaricate da una cerchia di persone difficile da determinare.

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 notevoli benefici, permette al contempo di compiere nuovi tipi di 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 in seno al Consiglio d'Europa, 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 23 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 sono tenuti 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 pornografia infantile in Internet e la sua diffusione (art. 9). Vanno inoltre rese punibili le violazioni del diritto dei beni immateriali commesse per via elettronica

[1] Stato: dicembre 2008. Il testo della Convenzione e del rapporto esplicativo del Consiglio d'Europa (a cui si farà più volte riferimento in seguito) è consultabile alla pagina internet: http://conventions.coe.int/Treaty/ITA/v3DefaultITA.asp (STCE n. 185).

(art. 10) e le imprese devono essere obbligate a rispondere dei reati stabiliti dalla Convenzione (art. 12).

Nella seconda parte vengono fissate le norme per la procedura penale. Sono prevalentemente contemplate le questioni legate alla raccolta 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. In base alla Convenzione, le Parti devono cooperare tra loro nella misura più ampia possibile.

1.3 Valutazione della Convenzione

La Convenzione del Consiglio d'Europa sulla cibercriminalità risponde alle nuove sfide poste dalle tecnologie informatiche[2] che gli Stati e la comunità internazionale si trovano a dover affrontare, e riconosce la necessità di combattere e prevenire non solo all'interno del Paese, ma anche al di fuori dei confini nazionali, la criminalità che agisce in rete su scala internazionale. L'invito della Convenzione ad armonizzare le legislazioni nazionali in Europa e non solo e a rafforzare la collaborazione internazionale va accolto favorevolmente. Gli Stati che hanno già attuato la Convenzione 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.

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 reputano limitati gli effetti pratici della Convenzione, non da ultimo perché manca un sistema di monitoraggio e le Parti si scambiano poche informazioni.

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

2.1 Capitolo I: Uso dei termini

2.1.1 Articolo 1 – Definizioni

L'articolo 1 definisce i concetti di «sistema informatico», «dati informatici», «fornitore di servizi» (*service provider*) e «dati relativi al traffico elettronico» ai fini dell'applicazione della Convenzione. Dai dati relativi al traffico elettronico 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 Conven-

[2] Cfr. cap. 1.1.

zione si discosta dall'articolo 2 lettera g dell'ordinanza del 31 ottobre 2001 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT)[3], in cui si fa riferimento ai dati che i fornitori di servizi registrano per certificare gli invii. Il concetto viene analizzato più in dettaglio nella parte della Convenzione dedicata al diritto processuale[4]. Tuttavia, all'atto pratico, le definizioni dei termini della Convenzione non si differenziano in modo sostanziale dai concetti utilizzati in Svizzera.

2.2 Capitolo II: Provvedimenti da adottare a livello nazionale

2.2.1 Articolo 2 – Accesso illegale a un sistema informatico

L'articolo 2 della Convenzione intende uniformare la punibilità dell'attività di hacking su scala internazionale. Devono essere puniti tutti coloro che accedono illecitamente e senza autorizzazione a un sistema informatico o a parte di esso. Le Parti possono presentare una dichiarazione[5], 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)[6] 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[7]. 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[8], che contesta il fatto che ai sensi di tale articolo un soggetto che agisce per curiosità è passibile di sanzione, mentre, in determinate circostanze, un soggetto che agisce a fine di lucro rimane impunito. Questa concezione non tiene conto del fatto che l'accesso a un sistema di elaborazione di dati con intento di lucro è spesso finalizzato a procurare dati elettronici per l'utilizzo in proprio o da parte di terzi. In questo caso, la punibilità è garantita dal-

3 RS **780.11**
4 Art. 14 segg.
5 Cfr. art. 40 della Convenzione.
6 RS **311**
7 Una dichiarazione di uguale o simile tenore in merito all'art. 2 è già stata rilasciata da alcuni 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 volutamente semplice (cfr. n. 49 e 50 del rapporto esplicativo della Convenzione, nota 1).
8 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.

l'articolo 143 CP[9], che prevede una pena addirittura superiore rispetto all'articolo 143bis[10]. 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 un'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[11]. 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 l'intento di lucro[12]. Inoltre, il criterio dell'assenza dell'intento di lucro entra inevitabilmente in conflitto con la proposta di ampliare la gamma di atti passibili di pena[13], 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, nel contesto dell'attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità, si propone di cassare la caratteristica dell'assenza dell'intento di lucro nell'articolo 143bis CP (per la dicitura cfr. esposizione relativa all'articolo 6 della Convenzione[14]). 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 tiene conto delle critiche mosse in relazione a questo punto. Non è possibile escludere del tutto il rischio di una lacuna dell'articolo 143bis in termini di punibilità, ma tale pericolo può essere arginato: se un soggetto, con intento di lucro, 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) in quanto compie un reato ai sensi dell'articolo 143bis.

2.2.2 Articolo 3 – Intercettazione illecita

Ai sensi dell'articolo 3 della Convenzione, commette un reato chi con strumenti tecnici intercetta deliberatamente 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[15]. 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 doloso.

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

9 Acquisizione illecita di dati.
10 Questa concezione è stata difesa anche nell'ambito dei dibattiti parlamentari, cfr. boll. sten. del Consiglio Nazionale, 1993, pag. 935 segg.
11 Cfr. p. es. l'art. 156 (estorsione) oppure l'art. 181 CP (coazione).
12 Nel disegno di legge originario del Consiglio federale le due norme contenute negli art. 143 e 143bis 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.
13 Cfr. ibid.
14 Cap. 2.2.5.
15 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, ma la norma non tutela i dispositivi di trasmissione come tali, se non quando costituiscono impianti informatici ai sensi dell'articolo stesso[16].

In base all'articolo 143 CP[17], 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[18]. 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[19].

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 raggiunto utilizzando sistemi di cifratura, codici di accesso, chiavi biometriche oppure password. La protezione deve essere *normalmente sufficiente* a impedire l'accesso non autorizzato[20]. Non è per esempio necessario che vengano adottate altre misure di sicurezza specifiche[21] 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[22] non rientra nella fattispecie di reato in questione.

L'articolo 3 della Convenzione si riferisce, tuttavia, solo all'intercettazione indebita di *trasmissioni* di dati informatici, in relazione alle quali di norma si possono imporre solo limitati requisiti di sicurezza[23]. In questi casi, la punibilità ai sensi dell'articolo 143 CP non va, in linea di massima, vincolata alla presenza di una protezione come l'utilizzo di tecniche di cifratura. In questo senso l'articolo 143 CP rispetta quindi le disposizioni dell'articolo 3 della Convenzione. Come già spiegato, il traffico non pubblico di dati non può 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.

In base al rapporto esplicativo della Convenzione[24], anche il flusso di informazioni all'interno di un computer costituisce una trasmissione di dati ai sensi dell'articolo 3.

16 N. Schmid, *Computerkriminalität*, Zurigo 1994, § 5 n. 16.
17 Acquisizione illecita di dati.
18 Eventualmente, senza però effettivamente farne uso (N. Schmid, op. cit., § 4 n. 40 s.).
19 N. Schmid, loc. cit., § 4 n. 30 e n. 51.
20 Cfr. Weissenberger, op. cit., n. 18 ad art. 143.
21 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.
22 P. es. in caso di computer utilizzato da più utenti oppure di uso illecito di dati affidati in custodia.
23 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.
24 N. 55; cfr. nota 1.

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). Ammesso che si disponga dell'attrezzatura tecnica e delle conoscenze adeguate, questi dati sono relativamente facili da intercettare; ciononostante sono considerati particolarmente 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 notevoli provvedimenti per accedere a tali trasmissioni. L'articolo 143 CP può essere applicato anche in questo caso. Non è necessario ricorrere a una modifica della legislazione in aggiunta alla dichiarazione menzionata in precedenza.

2.2.3 Articolo 4 – Attentato all'integrità dei dati

L'articolo 4 della Convenzione punisce il danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici commessi senza autorizzazione e illecitamente. Una Parte può riservarsi il diritto di stabilire il verificarsi di un danno considerevole come presupposto per la punibilità[25].

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 secondo un modo simile. Rende inservibili i dati chiunque impedisca – anche solo temporaneamente – alla persona che ne ha diritto di utilizzare i dati[26]. 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 della modifica/inservibilità. Il requisito della punibilità è garantito dall'articolo 144bis CP.

2.2.4 Articolo 5 – Attentato 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. Per *impedimento serio* si intende in particolare l'invio di dati in forma, quantità o frequenza tali da ostacolare seriamente il funzionamento di un computer[27]. L'invio di e-mail di massa[28] non richiesto non è coperto dalla disposizione[29].

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[30].

25 Art. 42 della Convenzione. Alcuni Stati hanno già fatto ricorso alla possibilità di avanzare tale riserva, cfr. http://conventions.coe.int/.

26 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).

27 Blocco doloso di un computer, cfr. n. 67 del rapporto esplicativo (nota 1).

28 «Spamming». Il 1° aprile 2007 è entrata in vigore una disposizione corrispondente (art. 3 lett. o della legge federale contro la concorrenza sleale; RS **241**, FF **2003** 6883).

29 N. 69 del rapporto esplicativo (cfr. nota 1).

30 Per esempio inviando pacchetti di dati modificati di grandi dimensioni a server, il cui funzionamento viene così bloccato (cfr. Weissenberger, op. cit., n. 35 in relazione all'art. 144bis, e riferimenti menzionati.

2.2.5 Articolo 6 – Abuso di apparecchiature

2.2.5.1 Disposizioni della Convenzione

L'articolo 6 della Convenzione punisce chiunque illecitamente e intenzionalmente produca, fornisca, procuri per l'uso, introduca, distribuisca o metta a disposizione in altro modo apparecchiature, programmi[31], codici di accesso e password utilizzati per commettere un reato ai sensi dei precedenti articoli[32]. Oltre che l'atto in sé, dev'essere intenzionale anche il compimento dei reati di cui agli articoli 2-5[33]. 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[34].

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 capoverso 3 dell'articolo 6 le Parti possono avvalersi di una riserva generale[35], che però non può inficiare la punibilità di chiunque venda, distribuisca o metta a disposizione password, codici o altri dati simili che permettono di accedere a un sistema informatico.

2.2.5.2 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[36].

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[37] in combinato disposto con gli articoli 143 e 143bis CP.

Sulla base di quanto affermato dalla dottrina e dalla giurisprudenza in merito al tentativo (incompiuto) ai sensi dell'articolo 22 capoverso 1 CP[38], in determinate circostanze la produzione o il possesso di dispositivi, programmi o elementi simili 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).

31 P. es. programmi virus, cfr. n. 72 del rapporto esplicativo (nota 1).
32 Art. 6 cpv. 1 lett. a.
33 Art. 6 cpv. 1 lett. a *in fine*.
34 Art. 6 cpv. 1 lett. b.
35 Art. 42 della Convenzione.
36 Cfr. DTF **129** IV 230.
37 Art. 22 e art. 25 CP.
38 Cfr. DTF **114** IV 114, **119** IV 227; S. Trechsel / P. Noll, *Schweizerisches Strafrecht, AT I*, Zurigo 1998, pag. 174 segg.

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[39]. Non è necessario che il complice conosca né la vittima né l'autore né le modalità del reato[40]. 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 viene punito nemmeno il favoreggiamento di un atto principale (ancora) intentato. Come già spiegato, devono sussistere un collegamento e un nesso in termini di contenuto e di tempo con un reato concretamente pianificato.

In base al principio dell'accessorietà effettiva[41], di norma non è punibile chi possiede o produce 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[42] 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[43] ed è quindi opportuno provvedere ad integrare l'articolo 143bis con la seguente disposizione, che contempla la diffusione illegale di codici d'accesso o dati simili e, analogamente all'articolo 144bis numero 2 CP (danneggiamento di dati), punisce determinate azioni preliminari al reato di hacking[44]:

> [1] *Chiunque~~, senza fine di lucro,~~ si introduce 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 è punito, a querela di parte, con una pena detentiva sino a tre anni o con una pena pecuniaria.*
>
> [2] ***Chiunque mette in circolazione o rende accessibili password, programmi o altri dati che sa o deve presumere destinati allo scopo di cui al capoverso 1** è punito con una pena detentiva sino a tre anni o con una pena pecuniaria.*

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.

Inoltre, si suggerisce di eliminare il requisito giuridico della mancanza dell'intento di lucro (cfr. quanto esposto in relazione all'art. 3 della Convenzione[45]), per rendere plausibile la punibilità degli «atti preliminari» anche dal punto di vista sistematico, indipendentemente dallo scopo di lucro.

39 Cfr. S. Trechsel, *Kurzkommentar*, Zurigo 1997, n. 1 ad art. 25.
40 Forster, in: *Basler Kommentar, StGB I*, 2003, n. 19 ad art. 25.
41 Cfr. S. Trechsel, *Kurzkommentar*, Zurigo 1997, n. 21 segg. avanti l'art. 24.
42 E non un programma ai sensi della legge.
43 Cfr. art. 6 cpv. 3.
44 Cfr. Schmid, op. cit., n. 31 ad art. 143bis.
45 Cap. 2.2.1.

L'integrazione proposta 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[46]. Saranno pertanto punibili il *rendere accessibili* e il *mettere in circolazione* 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'altra fattispecie di reato[47].

2.2.6 Articolo 7 – Falsificazione informatica

L'articolo 7 dichiara punibili l'inserimento, la modifica, la cancellazione e la soppressione intenzionale e illecita di dati, da cui risultano dati non autentici, con l'intento di farli apparire autentici a fini legali. Le Parti possono rilasciare una dichiarazione[48] 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[49]. Se invece l'autore interviene su un processo di elaborazione di dati con conseguente danno o trasferimento patrimoniale, si applica l'articolo 147 CP[50]. Del resto, la fattispecie della falsificazione di documenti o del relativo tentativo si applica anche nel caso di documenti e dati elettronici[51]. 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 profitto.

2.2.7 Articolo 8 – Frode informatica

L'articolo 8 della Convenzione considera punibile chiunque cagioni intenzionalmente e illecitamente un danno patrimoniale ad altra persona con l'intento fraudolento o illegale di procurare a sé o a un altro un beneficio patrimoniale. Il danno patrimoniale deve essere provocato inserendo, modificando, 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»[52], il trasferimento patrimoniale non è dovuto a un errore umano provocato dall'autore del reato, ma è ottenuto manipolando semplicemente i dati[53]. Si ha utilizzo di dati falsi ai sensi del 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.

46 In particolare per quanto riguarda la produzione e l'introduzione di dati.
47 In particolare art. 143 e 143bis CP.
48 Art. 40 della Convenzione.
49 Art. 144bis n. 1 CP.
50 Abuso di un impianto per l'elaborazione di dati.
51 Art. 251 in combinato disposto con l'art. 110 cpv. 4 CP.
52 Ai sensi dell'art. 146 CP.
53 Cfr. a questo proposito anche N. Schmid, op. cit., n. 1 in relazione al § 7.

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 precedenza sulla disposizione penale in discussione[54].

2.2.8 Articolo 9 – Pornografia infantile

Ai sensi dell'articolo 9 della Convenzione è passibile di pena chi, servendosi di un sistema informatico, intenzionalmente offre, rende accessibile, diffonde, trasmette, si procura, possiede oppure produce per la diffusione tramite computer pornografia infantile.

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 capoverso 2 lettera c della Convenzione[55]. Non occorre avvalersi di riserve.

L'articolo 9 capoverso 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 si tratta 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 che sembra un minore, l'immagine non è soggetta a sanzione secondo il diritto svizzero in vigore. È vero che tali rappresentazioni possono avere un effetto degenerante su chi le guarda, ma il loro potenziale pericoloso e il loro significato reale sono notevolmente ridotti rispetto agli effetti fatali della rappresentazione pedopornografica «effettiva», sia per i soggetti coinvolti che per gli spettatori. Estendere la punibilità non appare quindi opportuno; si suggerisce di inserire una riserva in merito all'applicazione in Svizzera della lettera b del capoverso 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[56], ossia all'età protetta ai sensi dell'articolo 187 CP[57]. 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. Nell'ambito dell'implementazione e della ratifica della Convenzione vi è la possi-

54 Cfr. N. Schmid, loc. cit., n. 161 in relazione al § 7.
55 Cfr. messaggio concernente la modifica del CP e del CPM del 10 maggio 2000, FF **2000** 2609.
56 Cfr. Schwaibold/Meng, *Basler Kommentar*, loc. cit., n. 21 segg. ad art. 197.
57 Atti sessuali con fanciulli.

bilità di dichiarare[58] l'intenzione di applicare il limite di età di 16 anni anche in riferimento all'articolo 9 capoverso 3. La Svizzera dovrebbe ricorrere 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 necessità e l'opportunità di modificare il limite d'età per la punibilità degli atti sessuali con minori e delle corrispondenti raffigurazioni vanno verificate più in dettaglio nel contesto di un'eventuale attuazione della Convenzione del Consiglio d'Europa per la protezione dei bambini contro lo sfruttamento e gli abusi sessuali del 15 ottobre 2007.

2.2.9 Articolo 10 – Reati contro la proprietà intellettuale e diritti collegati

La terminologia utilizzata nella versione francese di questa disposizione della Convenzione si discosta da quella comunemente utilizzata in Svizzera[59]. 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[60];
- Convenzione internazionale per la protezione degli artisti, interpreti ed esecutori, produttori di fonogrammi e organismi di radiodiffusione del 26 ottobre 1961[61];
- Accordo sugli aspetti commerciali dei diritti sulla proprietà intellettuale[62];
- Trattato OMPI sulla proprietà intellettuale del 20 dicembre 1996[63];
- Trattato OMPI sull'interpretazione e l'esecuzione e i fonogrammi del 20 dicembre 1996[64].

Con la revisione parziale della legge sul diritto d'autore (LDA)[65], 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.

Come precisato nel rapporto esplicativo del Consiglio d'Europa, con l'aggiunta dell'espressione «tenendo fede agli obblighi che ha assunto» in tutti e due i capoversi dell'articolo 10, si chiarisce che le Parti della presente Convenzione non sono obbligate ad applicare gli accordi elencati a cui non aderiscono[66]. 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 Con-

58 Art. 40 della Convenzione.
59 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*).
60 RS **0.231.15**.
61 Convenzione di Roma; RS **0.231.171**.
62 Accordo TRIPS, Allegato 1C all'accordo del 15 aprile 1994 che istituisce l'Organizzazione mondiale del commercio; RS **0.632.20**.
63 WCT; RS **0.231.151**.
64 WPPT; RS **0.231.171.1**.
65 RS **231.1**.
66 N. 110 *in fine* del rapporto esplicativo (nota 1).

venzione di Berna, alla Convenzione di Roma, all'Accordo TRIPS e ai Trattati WCT e WPPT. È dunque necessario verificare quali obblighi derivanti da queste convenzioni sia tenuta ad adempiere in seguito all'adesione alla Convenzione del Consiglio d'Europa sulla cibercriminalità.

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 «attraverso l'utilizzo di 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.

2.2.10 Articolo 11 – Tentativo, istigazione e complicità

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

2.2.11 Articolo 12 – Responsabilità delle persone giuridiche

Ai sensi dell'articolo 12 della Convenzione, una persona giuridica deve poter essere ritenuta responsabile dei reati stabiliti dalla Convenzione commessi a suo vantaggio da una persona fisica che eserciti un potere di direzione all'interno dell'impresa (cpv. 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 agisca sotto la sua direzione, se viene dimostrata una mancanza di controllo da parte di una persona con potere di direzione (cpv. 2).

La responsabilità può essere di natura civile, amministrativa o penale (cpv. 3) e non deve pregiudicare l'eventuale responsabilità della persona fisica che ha commesso il reato (cpv. 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[67], per esempio, prevede la responsabilità delle imprese, senza tuttavia affrontare espressamente l'aspetto civile, amministrativo o penale[68]. La Convenzione salvaguarda il principio ancora ampiamente diffuso, nonostante una tendenza internazionale contraria, secondo cui una persona giuridica non può essere punita. Tuttavia, le Parti devono assicurarsi che anche le persone giuridiche siano assoggettate ad adeguate sanzioni o misure, incluse quelle pecuniarie[69].

67 STCE 173, art. 18; RS **0.311.55**.
68 Nel rapporto esplicativo (n. 86) viene tuttavia sottolineato che gli Stati non sono obbligati a introdurre la responsabilità delle persone giuridiche.
69 Cfr. art. 13 della Convenzione.

La responsabilità penale delle persone giuridiche è stata introdotta nel diritto svizzero il 1° ottobre 2003[70]. Una responsabilità primaria dell'impresa sussiste per un numero ridotto di categorie di reato, quando l'impresa può essere accusata di non aver preso tutte le misure ragionevoli e indispensabili per impedire il reato[71]. I reati previsti dalla Convenzione[72] non rientrano nelle categorie di reato menzionate[73].

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[74]. 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[75] 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 rappresentante 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 capoverso 4 della Convenzione stabilisce che la responsabilità della persona giuridica non deve pregiudicare la responsabilità dell'autore del reato. Sorge quindi la domanda se le Parti sono tenute a introdurre 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 capoverso 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, dopo la condanna dell'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 la persona giuridica[76].

Oltre alla responsabilità penale, è a disposizione lo strumento della responsabilità amministrativa con 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

70 Oggi art. 102 e 102*a* CP.
71 Art. 102 cpv. 2 CP.
72 Art. 2-9 della Convenzione.
73 Nell'elenco sono riportate soprattutto fattispecie di corruzione e il reato di riciclaggio di denaro.
74 Art. 102 cpv. 1 CP.
75 Reati puniti con una pena detentiva o con una pena pecuniaria; cfr. art. 10 CP.
76 Cfr. Niggli/Gfeller, *Basler Kommentar*, Basilea 2007, n. 113 ad art. 102.

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 bancario che non soddisfa più i presupposti per l'autorizzazione o che viola in modo grave i propri obblighi legali[77].

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[78]. 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 sia venuto meno ai suoi obblighi di sorveglianza permettendo a un altro dipendente di compiere il reato in questione.

Nel complesso si può quindi affermare che il diritto svizzero è risponde ai presupposti 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. Per di più la responsabilità sussidiaria dell'impresa assume maggiore importanza proprio nel caso dei reati in discussione, poiché è altamente probabile che le persone fisiche che compiono reati in rete non possano essere individuate. Non è quindi necessario inserire i reati previsti dalla Convenzione nell'elenco di reati determinanti una responsabilità primaria delle imprese nel diritto svizzero o ampliare genericamente tale elenco[79].

2.2.12 Articolo 13 – Sanzioni e misure

Il capoverso 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 capoverso 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[80], 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.

2.2.13 Articolo 14 – Ambito di applicazione delle disposizioni procedurali

Il capoverso 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

77 Art. 23^{quinquies} della legge sulle banche dell'8 novembre 1934; RS **952.0**.
78 Art. 52 e art. 57 cpv. 2 CC.
79 A differenza delle convenzioni penali internazionali contro la corruzione, dove il collegamento tra i reati delle convenzioni e l'attività economica delle imprese è notevolmente maggiore.
80 Cfr. sopra, art. 12.

sistema informatico. Inoltre, il capoverso 2 lettera c stabilisce che le disposizioni si applicano anche all'insieme delle prove elettroniche di un reato[81]. 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[82].

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 ordinamenti 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[83] e dalla sua ordinanza[84]. La LSCPT rimarrà valida anche dopo l'entrata in vigore del Codice di procedura penale del 5 ottobre 2007[85] (esecuzione della sorveglianza). Le norme di procedura penale[86] saranno invece inserite nel CPP. Nel caso presente 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 capoverso 3 lettera b è dedicato ai cosiddetti «gruppi definiti di utenti», come ad esempio quelli delle reti elettroniche interne alle aziende. Ai sensi dell'articolo 1 capoverso 4 e dell'articolo 15 capoverso 8 LSCPT, gli esercenti 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[87].

2.2.14 Articolo 15 – Condizioni e tutele

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.

2.2.15 Articolo 16 – Conservazione rapida di dati informatici immagazzinati

L'articolo 16 della Convenzione obbliga le Parti ad assicurarsi che le autorità inquirenti competenti possano ordinare o ottenere che i dati informatici immagazzinati vengano messi al sicuro velocemente[88]. Se l'ordine di conservazione è indirizzato 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.

81 «*De toute infraction pénale*».
82 Cfr. n. 141 del rapporto esplicativo.
83 LSCPT; RS **780.1**.
84 OSCPT; RS **780.11**.
85 CPP; FF **2007** 6327, entrata in vigore programmata per il 01.01.2011.
86 Art. 3-10 LSCPT.
87 A condizione che i dati siano disponibili.
88 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.

I vari codici di procedura penale 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[89], i supporti e i documenti elettronici rientrano nel concetto di mezzi di prova materiali e di conseguenza possono essere messi agli atti[90] o sequestrati in seguito a perquisizione[91].

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*»[92]. È sufficiente che i dati vengano messi al sicuro dalle autorità.

Il diritto svizzero in vigore risponde almeno in parte all'invito della Convenzione e precisamente 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[93]. 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.

2.2.16 Articolo 17 – Conservazione e divulgazione rapide di dati relativi al traffico informatico

L'articolo 17 della Convenzione impone che la conservazione dei dati sul traffico informatico[94] prevista dall'articolo 16 venga garantita anche nel caso in cui in una comunicazione siano coinvolti più fornitori di servizi (cpv. 1 lett. a).

L'ordinamento giuridico svizzero rispetta quanto stabilito dal capoverso 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 cpv. 2). Il fatto che diversi fornitori di servizi siano coinvolti in una comunicazione non pregiudica quindi la conservazione rapida dei dati sul traffico informatico.

Il capoverso 1 lettera b prevede che il fornitore di servizi destinatario dell'ordine di mettere al sicuro i dati sul traffico informatico fornisca alle autorità competenti i dati

89 Cfr. quanto esposto in merito all'art. 14 della Convenzione.
90 Art. 192 segg. CCP.
91 Art. 246 segg. CCP.
92 Cfr. n. 160 del rapporto esplicativo (nota 1).
93 Art. 15 cpv. 3 LSCPT: conservazione di dati necessari all'identificazione degli utenti nonché dati relativi al traffico e alla fatturazione. L'estensione del termine a un anno è plausibile (ma non è richiesta dalla Convenzione; cfr. n. 161 *in fine* del rapporto esplicativo).
94 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).

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 fase non consiste nell'individuare per nome l'autore o il destinatario dei messaggi[95].

Con l'entrata in vigore del Codice di procedura penale del 5 ottobre 2007[96], 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[97], 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[98], 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»[99] e si riferisce sia a indirizzi IP statici che dinamici[100]. 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 richiesta direttamente al servizio competente, indipendentemente dal reato fatto valere[101].

2.2.17 Articolo 18 – Ingiunzione di produrre

Ai sensi dell'articolo 18 capoverso 1 lettera a della Convenzione, l'autorità inquirente competente può obbligare chiunque a fornire dati informatici immagazzinati, 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[102]. In caso di rifiuto vi è la possibilità di applicare misure coercitive.

Inoltre, i fornitori di servizi (cpv. 1 lett. b) sono obbligati, su ordine dell'autorità competente, a fornire i dati dei clienti[103], ma non quelli riguardanti il collegamento o il contenuto. L'articolo 18 della Convenzione[104] non disciplina quindi l'identifica-

95 N. 169 del rapporto esplicativo (cfr. nota 1).
96 Prevista per il 01.01.2011.
97 Art. 15 della Convenzione.
98 Questo termine può rappresentare una restrizione rispetto ai reati «commessi tramite l'utilizzo di un sistema informatico».
99 Cfr. decisione della Commissione di ricorso DATEC del 27.04.2007, J-2003-162, consultabile all'indirizzo www.reko-inum.admin.ch.
100 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.
101 L'elenco dell'art. 3 LSCPT non è applicabile.
102 Cfr. art. 263 segg. CPP, soprattutto art. 265: obbligo di consegna.
103 «*Subscriber information*», p. es. identità del cliente, informazioni sui pagamenti.
104 Cpv. 1 lett. b.

zione 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[105]. Come già esposto in merito all'articolo 17 della Convenzione, l'autorità inquirente può richiedere informazioni concernenti collegamenti e dati sul traffico e la fatturazione per tutti i crimini e i delitti[106]. 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[107]. Vanno forniti in particolare il nome e l'indirizzo del partecipante, nonché altri elementi dell'indirizzo ai sensi della legge del 30 aprile 1997 sulle telecomunicazioni[108].

L'articolo 18 capoverso 1 lettera b della Convenzione si limita ai dati conservati dal provider e non prescrive in che misura e per quanto tempo le informazioni debbano essere immagazzinate 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 se si tiene conto delle disposizioni contenute nel Codice di procedura penale.

2.2.18 Articolo 19 – Perquisizione e sequestro di dati informatici immagazzinati

L'articolo 19 capoversi 1 e 3 della Convenzione 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 le cose mobili, anche i dati informatici devono poter essere sequestrati e resi accessibili. Deve inoltre essere possibile sequestrare anche i computer[109]. I presupposti per tali perquisizioni devono essere essenzialmente gli stessi di quelli per la ricerca di mezzi di prova «tradizionali».

Nel presente caso non si tratta essenzialmente di questioni inerenti al diritto delle telecomunicazioni o della sorveglianza di tale traffico. Trovano quindi applicazione le normative nazionali sulla raccolta e la conservazione delle prove. Numerosi esempi pratici degli ultimi anni[110] 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[111].

L'articolo 19 si riferisce ai dati informatici immagazzinati e, in linea di massima, può essere applicato nei confronti di chiunque. Sorge la domanda sulla misura in cui questa facoltà di accesso dell'autorità di perseguimento penale valga anche per i dati immagazzinati dai provider (per es. dati dei clienti relativi al contenuto) e se ne derivi una limitazione della protezione offerta dal segreto delle telecomunicazioni. Il

105 L'elenco di reati dell'art. 3 LSCPT non può essere applicato nemmeno in questo caso.
106 Art. 273 CPP.
107 Cfr. sopra.
108 LTC; RS **784.10**.
109 N. 187 del rapporto esplicativo (cfr. nota 1).
110 Per esempio nell'ambito di indagini condotte dalla polizia e dal giudice istruttore nella lotta alla pedopornografia.
111 Art. 246 segg. e 263 segg. CPP.

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 salvato temporaneamente da un provider e non ancora visualizzato dal mittente può essere considerato parte della comunicazione[112], godendo così della relativa protezione. Di conseguenza, può essere comunicato dal fornitore del servizio solo sulla base di una decisione e a determinate condizioni. Ad ogni modo, i dati non sono più protetti dal segreto delle telecomunicazioni nel momento in cui vengono immagazzinati nel supporto di salvataggio del destinatario, dove possono essere messi sotto sequestro[113]. Pertanto, l'articolo 19 della Convenzione non scalza i principi nazionali esistenti in materia di segreto delle telecomunicazioni.

Il capoverso 2 prevede che le autorità, dopo aver avuto accesso a un primo sistema informatico, possano accedere, laddove legalmente consentito, anche a un ulteriore sistema collegato per perquisirlo. Tale facoltà ampliata può quindi 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 nazionale offre la possibilità di accedere, nell'ambito di una perquisizione, a un altro sistema di dati collegato[114]. Ciò presuppone che la facoltà dell'autorità si estenda anche al contesto allargato, circostanza riconosciuta dalla formulazione della disposizione della Convenzione[115].

Il capoverso 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[116]. 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[117].

Sorge la domanda se tali obblighi posti dalla Convenzione vadano oltre il normale obbligo di testimoniare o l'obbligo di edizione di terzi[118] stabiliti dal diritto processuale penale svizzero. Il diritto in vigore soddisfa i requisiti della Convenzione, vista la limitazione ai casi idonei sancita per l'obbligo d'informazione, che sorge solo dietro richiesta da parte dell'autorità investigativa, la quale ha la facoltà di emettere decisioni di edizione. Dal rapporto esplicativo[119] si evince in particolare che la disposizione è rivolta agli amministratori di sistema o a persone con funzioni di vigilanza simili su un sistema informatico. Tuttavia, in casi del genere può essere necessario verificare sul piano nazionale l'esistenza di un'eventuale funzione di

112 N. 190 del rapporto esplicativo (cfr. nota 1).
113 Questa situazione è simile a quella di un invio postale che gode di corrispondente tutela grazie al segreto postale, mentre il giorno dopo la stessa lettera, p. es. come parte della contabilità del destinatario, può essere sequestrata con una perquisizione domiciliare e quindi vagliata ai fini dell'inchiesta.
114 Per determinate reti, a seconda del caso, l'autorità inquirente sarà a mala pena consapevole di questa circostanza.
115 «*Where lawfully accessible*».
116 Art. 14 cpv. 4 e art. 15 cpv. 8 LSCPT (obbligo dei proprietari di reti interne alle aziende e di centralini privati di garantire l'accesso e rilasciare le necessarie informazioni).
117 Cfr. n. 202 del rapporto esplicativo (nota 1), nonché l'art. 15 della Convenzione.
118 Che di norma non implica alcun ulteriore obbligo di collaborare attivamente nella ricerca di mezzi di prova; cfr. art. 265 CPP.
119 N. 200 segg. del rapporto esplicativo (nota 1).

garante dell'interessato che, violando una decisione di edizione, potrebbe incorrere in una pena ai sensi dell'articolo 305 CP[120].

2.2.19 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 sul traffico informatico e i 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 sui 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[121].

Il diritto svizzero vigente prevede che i dati sui collegamenti (come anche quelli relativi al contenuto) possano essere raccolti ricorrendo alla sorveglianza in tempo reale per i reati elencati nella LSCPT[122]. Per quanto riguarda i dati sul contenuto, tale elenco è stato inserito nel Codice di procedura penale. Il CPP prevede un'ulteriore estensione riguardo ai dati sul traffico e sulla fatturazione, nonché ai dati sui collegamenti, riconoscendo alle autorità il diritto di esigere informazioni in merito in caso di crimini o delitti[123]. Avanzando una riserva ai sensi dell'articolo 14 capoverso 3 della Convenzione, non sussiste alcuna ulteriore necessità di adeguare la normativa in materia.

2.2.20 Articolo 21 – Intercettazione di dati relativi al contenuto

L'articolo 21 disciplina la raccolta in tempo reale dei dati sul contenuto, che le autorità competenti possono effettuare o 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 sul contenuto possano essere ordinate per i reati elencati all'articolo 3 LSCPT. Non sussiste alcuna necessità di adeguare il diritto vigente.

2.2.21 Articolo 22 - Competenza

La Convenzione attua una distinzione tra competenza obbligatoria e facoltativa delle Parti nel perseguimento dei reati descritti nella Convenzione. Il capoverso 1 obbliga ogni Parte a fondare la propria competenza quando il reato avviene nel territorio dello Stato (principio della territorialità, cpv. 1 lett. a; disposizione cogente) 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[124] e dall'articolo 97 capoverso 1 della legge sull'aviazione[125].

Ai sensi del capoverso 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 capo-

120 Fattispecie del favoreggiamento; cfr. DTF **120** IV 106.
121 Art. 14 cpv. 3 in combinato disposto con l'art. 42 della Convenzione.
122 Art. 3 LSCPT.
123 Art. 273 CPP, indipendentemente dall'elenco dei reati.
124 Legge federale del 23 settembre 1953 sulla navigazione marittima sotto bandiera svizzera; RS **747.30**.
125 Legge federale del 21 dicembre 1948 sulla navigazione aerea; RS **748.0**.

verso 1 lettera a CP (principio della personalità attiva). Non è quindi necessario ricorrere alla riserva prevista dall'articolo 22 capoverso 2 (riferito alle lett. b-d).

Ai sensi del capoverso 3, la Parte deve stabilire la propria competenza in merito ai reati fissati dalla Convenzione[126] 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 della legge federale sull'assistenza internazionale in materia penale[127] 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[128] disciplina l'estradizione di cittadini propri 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'esito di tale azione penale dipende essenzialmente dagli atti forniti e dai mezzi di prova messi a disposizione.

2.3 Capitolo III: Cooperazione internazionale

2.3.1 Principi generali

La Convenzione del Consiglio d'Europa sulla cibercriminalità mira a istituire un sistema rapido ed efficace di collaborazione giudiziaria internazionale in materia penale. 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 disposizioni in vigore nei singoli Stati aderenti[129]. La ragione va ricercata soprattutto nell'obbligo di eseguire 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 (cfr. cap. 2.3.9.1).

2.3.2 Articolo 23 – Principi generali relativi alla 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[130]. L'obbligo di cooperazione fissato nell'articolo 23 si riferisce a tutti i reati collegati a sistemi e dati informatici[131] e alla raccolta di prove di un reato in forma elettronica [132]. 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 le prove in forma elettronica di un reato tradizionale, non compiuto con sistemi informatici[133].

2.3.3 Articolo 24 – Estradizione

Ai sensi dell'articolo 24, che costituisce una disposizione di uso comune, l'obbligo di estradizione sussiste solamente[134] 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 capoverso 1 dell'Accordo di estradizione europeo: il reato deve essere punito in base alla legge di entrambi i Paesi[135] 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. La legislazione svizzera coincide con la Convenzione perché, in base all'articolo 35 AIMP, l'estradizione è ammissibile se, secondo i documenti a sostegno della domanda, il reato è passibile di una sanzione restrittiva della libertà per un massimo di almeno un anno o di una sanzione più severa, sia secondo il diritto svizzero sia secondo quello dello Stato richiedente. Per quanto riguarda l'articolo 24 capoversi 1-4 della Convenzione, la Svizzera non subordina l'estradizione all'esistenza di un trattato[136].

In base all'articolo 24 capoverso 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 rispettate le condizioni previste dalla Convenzione o dal diritto nazionale[137]. La collaborazione si fonda, infatti, sui trattati in vigore tra i due Stati interessati, nonché sulla Convenzione europea di estradizione del 13 dicembre 1957 (CEEstr) con i due protocolli addizionali[138].

126 In questo caso il reato deve essere punito con una pena detentiva di almeno un anno; cfr. art. 24 cpv. 1 della Convenzione.
127 Assistenza in materia penale, AIMP; RS **351.1.**
128 RS **0.353.1**.
129 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 sul traffico informatico.
130 N. 6, 20 e 242 del rapporto esplicativo (nota 1).
131 Ossia i reati ai sensi dell'art. 14 cpv. 2 lett. a e b della Convenzione.
132 Art. 14 cpv. 2 lett. c.
133 N. 243 del rapporto esplicativo (nota 1).
134 Si fa rilevare la differenza rispetto alla collaborazione nell'ambito dell'assistenza giudiziaria, il cui campo di applicazione ai sensi dell'art. 23 è notevolmente più ampio: l'obbligo di cooperazione vale sia per i reati collegati a sistemi e dati informatici sia per la raccolta di mezzi di prova di un reato in forma elettronica.
135 Secondo le pertinenti disposizioni di legge di entrambe le Parti.
136 Art. 1 cpv. 1 lett. a AIMP.
137 L'art. 37 AIMP prevede, tra l'altro, che l'estradizione possa essere negata se la domanda si basa su una sentenza contumaciale e la procedura giudiziale non ha rispettato i diritti minimi della difesa riconosciuti a ogni persona imputata di reato, eccetto quando lo Stato richiedente offre garanzie ritenute sufficienti per assicurare alla persona perseguita il diritto a un nuovo processo che salvaguardi i diritti della difesa. 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.
138 RS **0.353.1**, **0.353.11** e **0.353.12**.

Nell'articolo 24 capoverso 6 viene applicato il principio «*aut dedere aut iudicare*» (estradizione o perseguimento penale). I cittadini svizzeri non possono essere estradati senza il loro consenso scritto[139]. L'interessato che rifiuta il proprio consenso viene processato dalla Svizzera[140] su domanda dello Stato richiedente in ottemperanza all'articolo 24 capoverso 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[141].

In base all'articolo 24 capoverso 7, la Svizzera deve comunicare al Segretario Generale del Consiglio d'Europa che l'Ufficio federale di giustizia (UFG) è responsabile delle richieste di estradizione o di arresto provvisorio[142]. Questa disposizione si applica soltanto se le due Parti interessate non hanno stipulato alcun accordo tra loro[143]. In ogni caso, la designazione di un'autorità non esclude la possibilità di procedere per via diplomatica[144].

2.3.4 Articolo 25 – Principi generali relativi alla mutua assistenza

L'articolo 25 obbliga le Parti a collaborare in una serie molto ampia di reati, requisito che si desume anche dall'articolo 23[145]. Ai sensi dell'articolo 25 capoverso 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[146]. Gli adeguamenti della legislazione sono descritti nel dettaglio al capitolo 2.3.9.1.

L'articolo 25 capoverso 3 della Convenzione introduce una misura di assistenza rapida. I dati informatici sono estremamente labili: è sufficiente premere alcuni tasti o lanciare un programma automatico per cancellarli, rendendo pertanto impossibile identificare l'autore del reato o eliminando le prove della sua colpevolezza. Alcuni tipi di dati vengono salvati solo per breve tempo prima di essere cancellati. In questi casi urgenti la richiesta deve essere presentata velocemente e altrettanto rapidamente deve essere comunicata la risposta. L'articolo 25 capoverso 3 prevede, di conseguenza, una forma di assistenza accelerata per impedire che informazioni o mezzi di prova essenziali vadano persi perché cancellati prima che fosse possibile redigere e trasmettere una domanda di assistenza e ricevere la risposta. Questo scopo viene raggiunto, da un lato, permettendo alle Parti, in casi d'urgenza, di presentare una

139 Art. 7 AIMP.
140 Le indagini e il perseguimento penale devono svolgersi rapidamente e con la stessa cura impiegata per qualsiasi altro reato simile.
141 Se non è stata presentata alcuna richiesta 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).
142 Art. 17 cpv. 2 AIMP.
143 Se, invece, tra le Parti sussiste un trattato di estradizione bilaterale o multilaterale, come la menzionata CEEstr, esse sanno già a chi indirizzare la richiesta di estradizione o di arresto provvisorio, rendendo superflua la tenuta di un registro.
144 N. 252 del rapporto esplicativo (nota 1).
145 Gli art. 33 e 34 permettono di modificare l'ambito di applicazione di queste misure; cfr. quanto esposto in merito a tali articoli.
146 N. 254 del rapporto esplicativo (nota 1).

domanda di cooperazione servendosi di mezzi di comunicazione veloce[147], e dell'altro, sollecitando la Parte richiesta a rispondere con gli stessi mezzi. Ogni Parte deve creare le condizioni necessarie all'applicazione di tali misure[148]. In casi delicati le Parti possono concordare particolari misure di sicurezza come la cifratura[149]. 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 capoverso 4 della Convenzione sancisce il principio generale secondo cui l'assistenza giudiziaria è soggetta alle condizioni previste dai trattati di mutua assistenza applicabili e dal diritto nazionale[150]. 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[151], ma non vale se gli articoli del capitolo III prevedono espressamente altrimenti. La Convenzione contiene svariate deroghe a questo principio generale[152], in particolare per quanto riguarda i motivi di rifiuto dell'assistenza giudiziaria[153]. Ai sensi dell'articolo 25 capoverso 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, anche se i metodi descritti nella Convenzione possono essere utilizzati per commettere reati di natura fiscale. Non si può escludere che alcuni Stati possano tentare di utilizzare i mezzi di comunicazione veloce introdotti dalla Convenzione sulla cibercriminalità per ottenere informazioni che la Svizzera non desidera fornire, con il pretesto di un reato informatico o del reperimento di dati informatici che costituiscono prove.

Il capoverso 5 contiene una disposizione di uso comune sulla doppia incriminazione[154].

147 E non dei tradizionali mezzi di trasmissione, ossia lettera sigillata inviata con corriere diplomatico o per posta, che richiedono molto più tempo.

148 Telefax e posta elettronica sono menzionati solo a titolo esemplificativo. È possibile utilizzare qualsiasi mezzo di comunicazione veloce idoneo al caso. Con lo sviluppo tecnologico possono essere introdotti ulteriori mezzi di comunicazione veloce, utili per la presentazione di domande di assistenza.

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

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

151 N. 257 del rapporto esplicativo (nota 1).

152 N. 258 del rapporto esplicativo (nota 1): una deroga simile si evince dall'art. 25 cpv. 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 disposizione nazionale della Parte richiesta che disciplini la collaborazione internazionale, a meno che non esista un trattato di mutua assistenza o altro accordo simile tra la Parte richiedente e la Parte richiesta (condizioni e motivi per rifiutare l'assistenza giudiziaria).

153 Cfr. anche quanto esposto in merito all'art. 27 cpv. 4.

154 N. 259 del rapporto esplicativo (nota 1): a causa dei diversi ordinamenti giuridici dei singoli Stati, vi sono differenze nella terminologia e nella classificazione delle condotte criminali. Se una condotta è considerata un 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.

2.3.5 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 [155] e dall'articolo 28 della Convenzione penale sulla corruzione del 27 gennaio 1999[156]. 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 alla Convenzione europea di assistenza giudiziaria in materia penale[157] 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 capoverso 2, a determinate condizioni[158], di trasmettere all'altra Parte informazioni su indagini o procedimenti utili alla comune lotta contro la criminalità[159]. Lo scambio di informazioni è disciplinato dal diritto nazionale. Per la Svizzera valgono le condizioni stabilite dall'articolo 67*a* AIMP[160].

2.3.6 Articolo 27 – Procedure relative alle richieste di mutua assistenza in assenza di accordi internazionali applicabili

Nell'articolo 27 sono stati trasposti i principi di altri trattati stipulati dalla Svizzera. Il capoverso 1 prevede che l'assistenza giudiziaria si svolga secondo le regole stabilite dai pertinenti accordi e trattati sulla mutua assistenza, come la Convenzione europea di assistenza giudiziaria in materia penale del 20 aprile 1959[161] 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 capoversi 2-10 contengono disposizioni da applicare in assenza di un trattato di mutua assistenza 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 richiese e la trasmissione diretta di informazioni. Tali norme hanno la precedenza rispetto a quelle del diritto nazionale. L'articolo 27 non disciplina altri punti[162].

Ai sensi dell'articolo 27 capoverso 2, in assenza di trattati internazionali la Svizzera deve comunicare al Segretario Generale del Consiglio d'Europa l'autorità centrale

155 RS **0.311.53**.
156 RS **0.311.55**; n. 260 del rapporto esplicativo (nota 1).
157 RS **0.351.12**.
158 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.
159 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.
160 Trasmissione spontanea di mezzi di prova e di informazioni.
161 CEAG; RS **0.351.1**.
162 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 cpv. 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).

competente per la trasmissione delle domande di assistenza giudiziaria e le risposte. Come per la dichiarazione relativa alla CEAG, è necessario precisare che l'Ufficio federale di giustizia del Dipartimento federale di giustizia e polizia di Berna è responsabile della ricezione di tutte le domande di assistenza giudiziaria provenienti dall'estero e della trasmissione di tutte le domande di assistenza giudiziaria della Svizzera. In questo contesto rientra anche l'articolo 27 capoverso 9 lettera e, secondo cui le Parti possono dichiarare che, per ragioni di efficienza, le richieste effettuate in base a tale capoverso dovranno essere indirizzate alla propria autorità centrale. Nel caso della Svizzera le richieste vanno indirizzate all'UFG, il che implica un maggiore carico di lavoro e un maggiore fabbisogno di personale[163]. Le domande di assistenza giudiziaria non riguardano infatti solo il perseguimento dei reati informatici, ma anche la raccolta di mezzi di prova in forma elettronica per conto di altri Stati[164]. Tali domande di assistenza sono di norma più complesse e prioritarie rispetto alle richieste che pervengono solitamente. Vista la complessità della tematica, si prevede che in futuro l'UFG sarà consultato regolarmente da autorità svizzere e straniere e dovrà rilasciare pareri e raccomandazioni in merito alla procedura applicabile. Sbrigando le domande di assistenza indirizzate alla Svizzera, l'UFG, oltre a fornire informazioni, dovrà anche verificare maggiormente le decisioni adottate dalle autorità svizzere. In base al nuovo articolo 18*b* AIMP[165], infatti, una parte delle decisioni fino ad ora impugnabili dall'Ufficio o dall'interessato sarà soggetta esclusivamente al controllo dell'UFG, che dovrà garantire la credibilità del sistema introdotto con questa nuova disposizione. I nuovi compiti prevedono anche l'obbligo di illustrare alle autorità straniere le condizioni stabilite nell'articolo 18*b* AIMP e di assicurarsi che vengano rispettate. Per soddisfare i dettami della Convenzione, è necessario istituire un gruppo specializzato in cibercriminalità all'interno dell'UFG. I compiti da svolgere (incluso servizio di picchetto) dovrebbero giustificare l'assunzione a tempo pieno di un'ulteriore persona. In questo modo la Svizzera sarà in grado assicurare una risposta rapida alle richieste, fattore estremamente importante per la lotta alla criminalità informatica. Anche i Cantoni devono agire velocemente, reperendo gli specialisti necessari e predisponendo l'infrastruttura informatica necessaria.

L'articolo 27 capoverso 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[166], è volta a garantire il rispetto dei requisiti in essere in materia di prove[167]. In base al capoverso 4, l'assistenza può essere rifiutata: per i motivi di cui all'articolo 25 capoverso 4 della Convenzione[168], 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 essen-

163 Soprattutto per il servizio di picchetto e la formazione.
164 Art. 25 cpv. 1.
165 Cfr. cap. 2.3.9.1.
166 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**).
167 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).
168 Vale a dire per i motivi previsti dal diritto nazionale della Parte richiesta.

ziali della Parte richiesta[169]. L'articolo 27 capoverso 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[170]. Secondo il capoverso 6, nei casi in cui normalmente rifiuterebbe o sospenderebbe l'assistenza, la Parte richiesta può invece porre delle condizioni per l'esecuzione della richiesta. Se la Parte richiedente non può rispettare tali condizioni, la Parte richiesta può modificarle oppure rifiutare o sospendere l'assistenza. Secondo l'articolo 27 capoverso 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[171]. Ai sensi dell'articolo 27 capoverso 8, la Parte richiedente può imporre alla Parte richiesta l'obbligo di confidenzialità in merito alla domanda e al suo oggetto[172]. La Svizzera ha aderito a una clausola analoga nel Secondo protocollo addizionale alla CEAG[173].

L'articolo 27 capoverso 9 pone le basi per garantire una comunicazione rapida. Di norma le autorità centrali di cui all'articolo 27 capoverso 2 comunicano direttamente tra loro. In casi urgenti, tuttavia, giudici e avvocati della Parte richiedente possono trasmettere le domande di assistenza direttamente ai giudici e agli avvocati della Parte richiesta, inviandone copia all'autorità centrale del proprio Paese, che provvederà a inoltrarla all'autorità centrale della Parte richiesta. Le domande possono essere trasmesse anche tramite l'Interpol[174]. Le autorità della Parte richiesta che ricevono una domanda non di loro competenza devono trasmetterla all'autorità competente della Parte richiesta oppure darne comunicazione alle autorità della Parte richiedente[175]. Le domande possono essere trasmesse direttamente senza coinvolgere l'autorità centrale anche in casi non urgenti, se l'autorità della Parte richiesta può espletare la richiesta senza l'impiego di misure coercitive. Uno Stato aderente alla Convenzione può comunicare agli altri Stati tramite il Segretario Generale del Consiglio d'Europa che, per ragioni di efficienza, le richieste devono essere

169 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. N. 268 e 269 del rapporto esplicativo (nota 1).

170 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 nel territorio della Parte richiesta. N. 270 del rapporto esplicativo (nota 1).

171 L'obbligo della Parte richiesta di comunicare i propri motivi è tesa a migliorare l'efficienza dell'assistenza giudiziaria e a permettere alla Parte richiedente di accedere a informazioni a lei sconosciute sulla presenza di testimoni o la disponibilità di mezzi di prova e le relative circostanze. N. 272 del rapporto esplicativo (nota 1).

172 Può infatti succedere che una Parte presenti una richiesta di assistenza giudiziaria in un caso particolarmente delicato o in cui la divulgazione prematura dei fatti alla base della richiesta 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 richiesta oppure quando occorre mettere al corrente della richiesta privati che sono in possesso di mezzi di prova, in modo da poter procedere all'esecuzione. N. 273 del rapporto esplicativo (nota 1).

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

174 Art. 27 cpv. 9 lett. b.

175 Art. 27 cpv. 9 lett. c.

indirizzate direttamente alla propria autorità centrale[176]. La Svizzera ha deciso di seguire tale procedura.

2.3.7 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[177].

L'articolo 28 capoverso 2 permette allo Stato richiesto di porre due condizioni: le informazioni o i documenti devono rimanere confidenziali se la richiesta di assistenza giudiziaria non può essere soddisfatta in mancanza di tale condizione[178]; le informazioni o i documenti trasmessi non possono essere utilizzati per indagini o procedimenti diversi da quelli indicati nella richiesta. 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 procedimenti vertenti su fatti per cui l'assistenza è inammissibile[179]. 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 richiesta, 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[180]. 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[181]. È poi possibile esigere dalla Parte richiedente che fornisca indicazioni sull'uso fatto delle informazioni o dei documenti ricevuti alle condizioni di cui al capoverso 2, in modo che la Parte richiesta possa verificare il

176 Art. 27 cpv. 9 lett. e; cfr. quanto esposto in merito all'art. 27 cpv. 2.

177 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).

178 Come nel caso dell'identità di un informatore che deve rimanere confidenziale. Cfr. n. 277 del rapporto esplicativo (nota 1).

179 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 in materia fiscale.

180 a) Il materiale messo a disposizione che scagiona un imputato viene portato a conoscenza della difesa o dell'autorità giudiziaria. b) Se il materiale messo a disposizione nel quadro di un trattato sull'assistenza giudiziaria viene utilizzato prevalentemente in sede di dibattimento, spesso in procedimenti pubblici, in cui la rivelazione è obbligatoria, 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).

181 Art. 28 cpv. 3.

rispetto di tali condizioni[182]. In base al principio della specialità di cui all'articolo 67 AIMP, in determinati casi la Svizzera sarà tenuta verificare se le condizioni legate alla trasmissione siano state rispettate.

2.3.8 Articolo 29 – Conservazione rapida di dati informatici immagazzinati

Ai sensi dell'articolo 29 capoverso 1, una Parte può richiedere che i dati immagazzinati a mezzo di un sistema informatico nel territorio della Parte richiesta siano conservati rapidamente e, ai sensi del capoverso 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 periodo di tempo necessario per elaborare, trasmettere ed eseguire una richiesta 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 richiesta formale di assistenza giudiziaria. Questo provvedimento è più rapido di una normale procedura e rappresenta un intervento dall'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[183]. 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*), 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 richiesta 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 divulgazione completa ai sensi dei trattati sull'assistenza giudiziaria. Tale disposizione garantisce una procedura estremamente rapida, che impedisce la perdita irrecuperabile dei dati, i quali vengono conservati finché non possono essere successivamente 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 capoverso 2 stabilisce il contenuto della richiesta 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[184]. In un momento successivo, la Parte richiedente deve presentare una richiesta per la consegna dei dati.

182 Art. 28 cpv. 4.
183 N. 282 del rapporto esplicativo (nota 1).
184 Oltre all'indicazione dell'autorità che richiede la conservazione e del reato alla base della richiesta, sono essenziali una breve esposizione dei fatti, nonché le indicazioni necessarie per determinare e localizzare i dati da conservare. Occorre inoltre indicare il nesso tra i dati e le indagini o il procedimento avviati in seguito al reato, e illustrare i motivi che rendono necessaria la conservazione. N. 284 del rapporto esplicativo (nota 1).

La doppia incriminazione non è una condizione essenziale per adottare provvedimenti di conservazione dei dati[185], poiché in questo caso l'applicazione di tale criterio sarebbe controproducente[186]. L'articolo 29 capoverso 4 prevede, tuttavia, la possibilità di una riserva limitativa in merito. La Svizzera si avvarrà di tale strumento, poiché il nostro Paese considera la doppia incriminazione 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 richiesta 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 immagazzinati, 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:

«La Svizzera si riserva il diritto di subordinare alla condizione prevista dall'articolo 29 capoverso 4 l'esecuzione di una domanda di assistenza giudiziaria che richieda l'applicazione di una misura coercitiva.»

L'articolo 29 capoverso 5 della Convenzione fissa le uniche condizioni che giustificano il rifiuto di una richiesta 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 richiesta formale di assistenza giudiziaria. Secondo l'articolo 29, un'autorità straniera può richiedere la conservazione rapida di dati immagazzinati e, ai sensi dell'articolo 30, la loro rapida trasmissione. Tuttavia, la Svizzera interpreta in modo diverso l'articolo 29 capoverso 5 e l'articolo 30 capoverso 2: se, nel momento di decidere in merito alla disposizione di misure provvisorie, è evidente che la richiesta 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 richiesta 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

185 Art. 29 cpv. 3.

186 La conservazione non è infatti una misura particolarmente incisiva, poiché i dati rimangono in possesso del custode che è legalmente autorizzato a custodirli e vengono trasmessi o verificati dai responsabili della Parte richiesta solamente quando viene accolta la formale domanda di assistenza giudiziaria che ne richiede la consegna.

187 La condizione della doppia incriminazione è comunque 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 per tali reati. In questo caso le Parti possono esigere l'adempimento della condizione della doppia incriminazione solo per reati diversi da quelli descritti nella Convenzione.

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 propria sovranità, alla sicurezza, all'ordine pubblico e ad altri 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 richiesta di conservazione. Cfr. n. 287 del rapporto esplicativo (nota 1).

190 P. es. quando i dati da conservare sono custoditi da un fornitore di servizi controllato da un'organizzazione criminale o soggetto a indagini.

191 Art. 29 cpv. 6.

oppure scegliere un'altra forma di assistenza più incisiva, ma anche più sicura[192]. Ai sensi dell'articolo 29 capoverso 7 della Convenzione, i dati devono essere conservati per almeno 60 giorni fino al ricevimento della richiesta formale di trasmissione e continuare ad essere conservati dopo il suo ricevimento[193]. 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.

2.3.9 Articolo 30 – Trasmissione rapida di dati sul traffico informatico conservati

2.3.9.1 Modifiche necessarie del diritto vigente

Lo sviluppo estremamente rapido delle tecnologie dell'informazione ha profondamente modificato la nostra società. A causa della necessità di scambiare ingenti quantità di dati[194], le nuove tecnologie si sono affermate in tutti gli ambiti dell'attività umana e hanno comportato innumerevoli trasformazioni economiche e sociali e anche nuove forme di criminalità. Hanno messo in dubbio gli esistenti principi del diritto e reso necessaria l'adozione di misure tecniche a tutela dei sistemi informatici e di provvedimenti legali volti a prevenire la criminalità, fungendo al contempo da deterrente. 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[195] 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 richiesta di una Parte nel cui territorio è stato commesso un reato, la Parte richiesta spesso provvede alla conservazione dei dati sulla trasmissione di una comunicazione per mezzo di computer situati nel 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 sul traffico rintracciati nel 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 di dati sul traffico informatico sufficiente 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

192 Come l'ordine di consegna, la perquisizione o il sequestro. N. 288 del rapporto esplicativo (nota 1).

193 N. 289 del rapporto esplicativo (nota 1).

194 Il facile accesso alle informazioni contenute nei sistemi informatici, la ricerca semplice, nonché le pressoché illimitate possibilità di scambio e di divulgazione di tali informazioni, indipendentemente dalla lontananza geografica, hanno fatto aumentare vertiginosamente la quantità di informazioni disponibili e le conoscenze che se ne possono ricavare.

195 Una banca deve p. es. conservare la propria documentazione contabile per dieci anni.

richiesta di conservazione e presentare una domanda di assistenza accelerata per individuare il fornitore di servizi e il percorso della comunicazione. 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[196], al detentore di tali informazioni va sempre presentata una decisone finale impugnabile[197]. Solo al termine di questa procedura, che dura diversi 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[198]. Il diritto svizzero deve essere pertanto modificato per soddisfare quanto stabilito dall'articolo 30. Questo è lo scopo del capoverso 1 lettera a del nuovo articolo 18*b* AIMP, il cui capoverso 1 lettera b adempie anche i requisiti per l'attuazione dell'articolo 33:

> ***Art. 18b Dati relativi al traffico informatico***
>
> *[1] L'autorità federale o cantonale incaricata della domanda può ordinare la trasmissione all'estero di dati relativi al traffico informatico prima della conclusione della procedura di assistenza giudiziaria, se:*
>
> *a. le misure provvisionali adottate dimostrano che la comunicazione oggetto della domanda ha origine in un altro Stato; oppure se*
>
> *b. tali dati sono stati acquisiti dall'autorità d'esecuzione sulla base di un ordine di sorveglianza in tempo reale autorizzata in precedenza (art. 269-281 CPP).*
>
> *[2] Tali dati non possono essere utilizzati come prove prima che la decisione in merito alla concessione e alla portata dell'assistenza giudiziaria sia passata in giudicato.*
>
> *[3] La decisione di cui al capoverso 1, ed eventualmente l'ordine e l'autorizzazione della sorveglianza, devono essere tempestivamente comunicati all'Ufficio federale.*

Il nuovo articolo 18*b* permette la trasmissione all'autorità straniera dei dati sul traffico informatico facenti parte della sfera privata prima della conclusione della procedura di assistenza giudiziaria nei due casi seguenti: le misure provvisionali adottate dimostrano che la comunicazione oggetto della domanda ha origine in un altro Stato (cpv. 1 lett. a; disposizione per l'attuazione dell'articolo 30); i dati vengono acquisiti dall'autorità d'esecuzione sulla base di un ordine di sorveglianza in tempo reale autorizzata in precedenza (cpv. 1 lett. b; disposizione per l'attuazione dell'artico-

196 Art. 9 AIMP e art. 69 della legge federale sulla procedura penale (RS **312.0**).

197 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).

198 Il rischio di inquinamento delle prove giustifica la trasmissione tempestiva, che è p. es. idonea 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. Questo lasso di tempo gli permette di cancellare tutti i dati incriminanti salvati sul suo computer.

lo 33). 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:

a) 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);
b) i dati trasmessi non possono essere utilizzati come mezzi di prova prima che la procedura di assistenza giudiziaria non 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
c) la trasmissione è soggetta all'immediato controllo dell'UFG (cfr. nuovo art. 18*b* cpv. 3 AIMP).

Possono essere trasmessi solo i dati acquisiti sulla base di un ordine di sorveglianza autorizzata. In tal modo si garantisce che i dati siano stati acquisiti in conformità con il diritto svizzero e che la richiesta di assistenza sia stata verificata non solo dall'autorità d'esecuzione, ma anche da un giudice indipendente[199]. Tale controllo è ulteriormente rafforzato dall'obbligo di comunicare tempestivamente all'UFG ogni decisione di trasferimento dei dati. 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 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 garantire la sua 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[200] deve verificare che la richiesta soddisfi una serie di criteri, i quali sostanzialmente coincidono in larga misura con quelli della procedura di assistenza giudiziaria[201]. La persona coinvolta non viene privata di tutti i suoi diritti: non appena la situazione lo consente[202], 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

199 La verifica giudiziale non riguarda l'assistenza in sé, ma si avvale di molti dei criteri applicati all'assistenza giudiziaria.
200 Art. 7 cpv. 1 LSCPT.
201 Vale per la doppia incriminazione (secondo art. 3 LSCPT), per la proporzionalità (sussidiarietà delle misure; art. 3 cpv. 1 lett. a-c LSCPT) e per la separazione dei documenti (art. 8 LSCPT).
202 In ogni caso al più tardi prima che si concluda l'inchiesta penale o venga sospesa la procedura (art. 10 cpv. 2 LSCPT).

scopo d'indagine[203]. In tal modo la normativa proposta rispetta i 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 richiesta di sorveglianza in tempo reale dei dati sul 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[204] 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 sul 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 possibile conflitto indicando gli attuali problemi nell'esecuzione delle domande di assistenza giudiziaria legati alla sorveglianza in tempo reale delle telecomunicazioni[205]. La revisione si limita però a soddisfare le condizioni per l'attuazione dell'articolo 33 e riguarda esclusivamente i dati sul 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 sul 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.

2.3.9.2 Ulteriori spiegazioni relative all'articolo 30

Ai sensi dell'articolo 30 capoverso 2, la Parte richiesta può rifiutarsi di trasmettere i dati sul traffico informatico solo se ritiene che questo potrebbe arrecare pregiudizio alla propria sovranità, alla sicurezza, all'ordine pubblico o ad altri 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

203 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).

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

205 Thomas Hansjakob, LSCPT / OSCPT, *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.

talmente importanti per individuare l'autore o reperire mezzi di prova decisivi che si è deciso di limitare i motivi che giustificano il rifiuto della trasmissione[206].

2.3.10 Articolo 31 – Mutua assistenza concernente l'accesso a dati informatici immagazzinati

L'articolo 31 riconosce alle Parti la possibilità di perquisire per conto di un altro Stato aderente alla Convenzione i dati salvati per mezzo di un sistema informatico situato nel proprio territorio o di accedervi in altro modo, di sequestrarli o conservarli in altro modo e di trasmetterli, come consentito per scopi nazionali in base all'articolo 19[207] della Convenzione[208]. Non costituisce un problema il fatto che l'articolo 31 non permetta di limitare le misure a una determinata categoria di reati e non riconosca la possibilità di avanzare riserve[209], poiché l'articolo 31 viene attuato in applicazione dei trattati e delle disposizioni normative nazionali vigenti di cui all'articolo 23.

In base all'articolo 31 capoverso 1 ogni Stato aderente può richiedere una delle forme di assistenza ivi previste, mettendo la Parte richiesta nella condizione di fornire tale assistenza. L'articolo 31 capoverso 2 prevede che la cooperazione si fondi sulle condizioni stabilite nei trattati, negli accordi e nella legislazione nazionale applicabili. Ai sensi dell'articolo 31 capoverso 3 una tale richiesta deve essere espletata tempestivamente, quando vi è motivo di ritenere che i dati in questione siano particolarmente a rischio di perdita o di modificazione, oppure i trattati, gli accordi o la legislazione applicabili prevedano una cooperazione rapida.

2.3.11 Articolo 32 – Accesso transfrontaliero a dati informatici immagazzinati con il consenso o pubblicamente disponibili

L'articolo 32 della Convenzione disciplina l'accesso transfrontaliero a dati pubblicamente disponibili[210] 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 incontestabilmente ammessa una procedura intrapresa da una Parte, senza che l'abbia prima concordata con l'altra Parte[211], 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[212].

Nell'articolo 32 viene disciplinato, da un lato, il caso in cui una Parte può accedere a dati pubblicamente disponibili in altri Paesi: ad esempio, nel caso di dati pubblicamente accessibili in Internet nel dominio di un'azienda, 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

206 N. 291 del rapporto esplicativo (nota 1).
207 Perquisizione e sequestro di dati informatici immagazzinati.
208 N. 292 del rapporto esplicativo (nota 1).
209 Art. 42.
210 *Open source data*.
211 Rapporto esplicativo, n. 293 (cfr. nota 1).
212 E senza rispettare la normale procedura dell'assistenza giudiziaria e amministrativa. La Convenzione non autorizza altre modalità di accesso; cfr. art. 39 cpv. 3 della Convenzione.

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 però 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[213]. 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[214]. All'atto pratico significa che la persona all'estero che ha immagazzinato 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.

2.3.12 Articolo 33 – Mutua assistenza nella raccolta in tempo reale di dati relativi al traffico informatico

Ai sensi dell'articolo 33, ogni Parte deve acquisire in tempo reale i dati sul traffico informatico per conto di un'altra Parte e gli Stati sono tenuti a collaborare in 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 sul traffico informatico siano stati cancellati da un fornitore di servizi lungo il percorso, prima che potessero essere conservati. Per tale motivo gli inquirenti di tutte le Parti devono assolutamente avere la possibilità di acquisire dati sul traffico trasmessi attraverso un sistema informatico situato in un altro Stato aderente[215]. Secondo l'articolo 33 capoverso 2, l'assistenza deve essere fornita almeno per i reati «per i quali la raccolta in tempo reale dei dati sul traffico sarebbe possibile, in ambito interno, in una situazione analoga». In base al diritto svizzero in vigore, i dati sul traffico informatico facenti parte della sfera privata vengono acquisiti mantenendo il relativo segreto, e prima che vengano trasmessi deve essere stata emessa una decisione finale. Il nuovo articolo 18*b* AIMP, proposto nel capitolo 2.3.9.1, crea la possibilità di trasmettere tempestivamente i dati all'estero, senza che tale decisione debba essere notificata alla persona residente in Svizzera[216]. 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 artico-

213 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 concernente la Convenzione sulla cibercriminalità, stampato 16/7218, pag. 55, consultabile all'indirizzo Internet: http://dip21.bundestag.de/dip21/btd/16/072/1607218.pdf .

214 Il salvataggio all'estero, essendo difficile da individuare, può verificarsi anche all'insaputa persona autorizzata.

215 N. 295 del rapporto esplicativo (nota 1).

216 Art. 80*m* AIMP.

lo 273 CPP[217] permetterà la sorveglianza in tempo reale dei dati sul traffico informatico esclusivamente per le indagini su delitti e crimini. L'articolo 15 capoverso 1 della Convenzione prevede, tuttavia, il principio della proporzionalità per le facoltà e le procedure, stabilendo che ogni Parte deve applicare tale principio in sintonia con i principi vigenti nel proprio diritto nazionale[218]. Le Parti possono quindi non dare corso a richieste che violano il principio della proporzionalità. Questo permette alla Svizzera di rifiutare la propria collaborazione se la condotta perseguita all'estero è considerata una contravvenzione in base al diritto svizzero. La situazione potrebbe rivelarsi più complicata per le scommesse in Internet con grandi somme in palio, dal momento che la Svizzera le considera semplici contravvenzioni[219].

2.3.13 Articolo 34 – Mutua assistenza in materia di intercettazione di dati relativi al contenuto

L'articolo 34 limita l'obbligo di assistenza giudiziaria nell'acquisizione di dati sul 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 permettano. La prassi in materia di assistenza giudiziaria in merito è solo agli inizi, per cui l'esistente legislazione e il diritto interno in materia fungono da punti di riferimento per la portata e le restrizioni dell'obbligo di collaborazione[220]. In base al nuovo articolo 18*b* AIMP, di cui al capitolo 2.3.9.1, prima della conclusione della procedura possono essere trasmessi all'estero solo i dati sul traffico informatico, non quelli relativi al contenuto. Pertanto, secondo l'articolo 30 capoverso 1 AIMP[221], le autorità svizzere non si possono rivolgere a un altro Stato per l'intercettazione di dati sul contenuto.

2.3.14 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[222]. Per soddisfare i requisiti della Convenzione, il punto di contatto deve solo 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 di assistenza giudiziaria e di estradizione (in particolare la decisione sull'ammissibilità di un provvedimento), stabiliti dall'articolo 35 capoverso 1 lettere a-c della Convenzione.

217 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 art. 269 cpv. 1 lett. b e c CPP), anche se tale reato non figura nell'elenco dei reati dell'art. 269 CPP.

218 N. 146 del rapporto esplicativo (nota 1).

219 Art. 42 della legge federale dell'8 giugno 1923 concernente le lotterie e le scommesse professionalmente organizzate (LLS; RS **935.51)**.

220 N. 297 del rapporto esplicativo (nota 1).

221 Le autorità svizzere non possono inoltrare a un altro Stato una richiesta che esse stesse non possono soddisfare per legge.

222 Cfr. art. 35 cpv. 1 della Convenzione in combinato disposto con il n. 298 segg. del rapporto esplicativo (nota 1).

Il lavoro aggiuntivo per espletare i casi di assistenza giudiziaria e le richieste presentate nel quadro della Convenzione è difficile da valutare e dipende dal numero di Stati aderenti alla Convenzione, dalla complessità dei singoli casi e dallo sviluppo tecnologico, sia riguardo alla delinquenza nei vari Stati sia in riferimento agli strumenti di perseguimento penale[223]. 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) 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 minimi della Convenzione richiede l'assunzione di un'ulteriore persona.

A prescindere da quanto stabilito direttamente dalla Convenzione, i servizi coinvolti in seno a fedpol ritengono appropriato e auspicabile aumentare ulteriormente le risorse disponibili. Affinché l'istituzione del punto di contatto apporti un valore aggiuntivo nella lotta alla cibercriminalità rispetto allo *status quo*, oltre alle mansioni minime previste dalla Convenzione, si potrebbero attribuire a questo servizio anche altri compiti di più ampia portata. In particolare le mansioni indicate nell'articolo 35 capoverso 1 lettere a-c potrebbero essere espletate servendosi del supporto tecnico e legale immediato di un'unità specializzata. Per garantire un perseguimento penale rapido ed efficiente, il punto di contatto dovrebbe stabilire anche i contatti e le procedure per l'interazione tra le autorità di perseguimento e i provider di servizi Internet[224].

La cooperazione tra i provider di servizi Internet e le autorità di perseguimento penale presuppone un costante scambio tra gli attori coinvolti e richiede l'organizzazione di corsi di formazione tecnica e legale. Se il punto di contatto viene strutturato nel modo suggerito, questi compiti verrebbero assegnati, in termini organizzativi e tecnici, al Servizio nazionale di coordinazione contro la criminalità su Internet della Confederazione e dei Cantoni (SCOCI[225]), già in contatto con gli inquirenti informatici della polizia cantonale e i vari fornitori di servizi Internet. L'aggregazione dei due nuovi posti necessari secondo le conoscenze attuali permetterebbe di sfruttare più proficuamente le sinergie[226].

Per garantire un rapido supporto nei casi di assistenza giudiziaria o di procedimenti penali di competenza della Confederazione, nell'istituire un punto di contatto efficiente sarebbe sensato e appropriato organizzare un servizio di picchetto anche all'interno del Commissariato indagini IT della Polizia giudiziaria federale, che potrebbe fornire maggiore assistenza alle autorità di perseguimento penale cantonali, dal momento che, in materia di cibercriminalità e in generale nel campo delle indagini informatiche, i Cantoni non dispongono dello stesso livello di conoscenze necessarie all'esecuzione dell'assistenza richiesta. Questo servizio giustificherebbe altri due posti di lavoro.

223 Risorse ed equipaggiamento per la sorveglianza, la conservazione e il controllo del traffico di dati elettronici.

224 Cfr. a tale proposito le linee guida per la cooperazione tra autorità di perseguimento penale e provider di servizi Internet del Consiglio d'Europa (*Guidelines for the cooperation between law enforcement and internet service providers*): http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_FR.asp.

225 Cfr. www.cybercrime.ch.

226 A causa della struttura del SCOCI, i nuovi posti non potrebbero esservi integrati, ma solo aggregati dal punto di vista organizzativo.

La decisione in merito alla richiesta di risorse e alla possibilità di effettuare una compensazione senza ripercussioni sul preventivo del DFGP dovrà essere presa nel contesto del messaggio indirizzato al Parlamento.

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 alla sua elaborazione[227]. Possono inoltre essere invitati ad aderire alla Convenzione anche altri Stati[228].

La Convenzione è entrata in vigore il 1° luglio 2004, dopo che almeno cinque Stati avevano siglato la ratifica come previsto[229]. Attualmente gli Stati aderenti sono 23 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 volutamente semplice[230]. 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[231] della Convenzione[232]. Tale riserva non deve tuttavia scalfire la cooperazione internazionale[233]. 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.

227 Canada, Giappone, Stati Uniti d'America e Sud Africa.
228 *Art. 37* della Convenzione. Attualmente (novembre 2008) sono stati invitati Costa Rica, Messico e le Filippine.
229 *Art. 36 cpv. 3* della Convenzione.
230 Cfr. le quanto illustrato nel rapporto esplicativo del Consiglio d'Europa relativo alla Convenzione, n. 49 e 50 (nota 1).
231 Misure interne.
232 Si tratta di una clausola poco usuale, che è stata inserita nel testo in seguito all'intervento determinante degli Stati Uniti.
233 Capitolo III della Convenzione.

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*).

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

Il Protocollo addizionale alla Convenzione sulla cibercriminalità relativo all'incriminazione di atti di natura razzista e xenofoba commessi a mezzo di sistemi informatici del 28 gennaio 2003 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 13 Paesi, tra cui tre Stati membri dell'UE.

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 che può risultare significativa nella pratica.

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[234], poiché vanno tenuti in considerazione nell'verifica esamina sull'attuazione del Protocollo addizionale.

2.6 Rapporto con altre revisioni in materia penale

Il 5 ottobre 2007 le Camere federali hanno licenziato 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

[234] Cfr. il documento di lavoro dell'UFG per l'indagine conoscitiva sulla norma penale in materia di razzismo del maggio 2007, consultabile in francese all'indirizzo: http://www.bj.admin.ch/etc/medialib/data/kriminalitaet/gesetzgebung/rassismus.Par.0002.File.tmp/F_Bericht_15%205%2007.pdf

presente rapporto, rimanda a varie riprese alle disposizioni del CPP[235], essenziali per l'attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità o garanti di una copertura completa nel diritto svizzero. L'entrata in vigore della Convenzione presuppone quindi per la Svizzera l'entrata in vigore del CPP. Tuttavia, 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). In caso di ripercussioni sul progetto in discussione, il coordinamento delle due pratiche è garantito.

3 Ripercussioni

3.1 Ripercussioni finanziarie e sul personale della Confederazione

A causa dell'aumento dei casi di criminalità informatica, si prevede un maggiore carico di lavoro per le autorità di perseguimento penale, nonché per il servizio annesso al DFGP incaricato della sorveglianza del traffico postale e 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 maggiormente sollecitati in futuro.

L'attuazione e la ratifica della Convenzione può comportare 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. Sulla corrispondente richiesta di risorse umane e sul’eventuale compensazione interna al Dipartimento si dovrà decidere nel quadro del messaggio indirizzato al Parlamento.

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 delle procedure di perseguimento e di giudizio.

3.4 Ripercussioni sui 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. Tuttavia, l'attuazione della Convenzione non dovrebbe avere ripercussioni significative sui Cantoni. In particolare non si prevede un forte aumento né del numero di procedure di perseguimento penale per i reati di cui alla Convenzione né

[235] Cfr. in particolare quanto esposto in merito agli art. 16-21 nonché 23, 25, 30 e 33 della Convenzione.

delle domande di assistenza giudiziaria[236]. Il punto di contatto stabilito 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 Rapporto con il programma di legislatura

Il progetto è inserito nel messaggio sul programma di legislatura 2007-2011[237].

5 Aspetti giuridici

5.1 Rapporto con l'Unione europea

L'attuazione della Convenzione del Consiglio d'Europa sulla cibercriminalità non comporta problemi in termini di compatibilità del diritto svizzero con quello dell'Unione europea (UE). Tra gli Stati aderenti alla Convenzione vi sono già alcuni Stati membri dell'UE, e in altri Stati membri è in corso la procedura di attuazione.

5.2 Costituzionalità

La costituzionalità del decreto federale per l'approvazione della Convenzione del Consiglio d'Europa sulla cibercriminalità si fonda sull'articolo 54 capoverso 1 della Costituzione federale (Cost.)[238], 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[239]. 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 va 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 della Costituzione federale.

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

Allegato

Decreto federale di approvazione e attuazione della convenzione del Consiglio d'Europa sulla cibercriminalità (avamprogetto)