

Bruxelles, 12 agosto 2016
(OR. en)

9955/1/16
REV 1 DCL 1

GENVAL 71
CYBER 66

DECLASSIFICAZIONE

del documento: 9955/1/16 REV 1

data: 14 luglio 2016

nuovo status: Pubblico

Oggetto: Relazione di valutazione sul settimo ciclo di valutazioni reciproche
"Attuazione pratica e funzionamento delle politiche europee in materia di
prevenzione e lotta alla criminalità informatica"
- Relazione sull'Italia

Si allega per le delegazioni la versione declassificata del documento in oggetto.

Il testo del presente documento è identico a quello della versione precedente.



Consiglio
dell'Unione europea

Bruxelles, 14 luglio 2016
(OR. en)

9955/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 71
CYBER 66

RELAZIONE

Origine:	Segretariato generale del Consiglio
Destinatario:	delegazioni
Oggetto:	Relazione di valutazione sul settimo ciclo di valutazioni reciproche "Attuazione pratica e funzionamento delle politiche europee in materia di prevenzione e lotta alla criminalità informatica" - Relazione sull'Italia

DECLASSIFIED

Indice

1	Sintesi	5
2	Introduzione	7
3	Aspetti generali e strutture	10
3.1	Strategia nazionale per la cibersicurezza	10
3.2	Priorità nazionali per quanto riguarda la criminalità informatica	10
3.3	Statistiche sulla criminalità informatica	11
3.3.1	Principali tendenze in materia di criminalità informatica	11
3.3.2	Numero di casi di criminalità informatica registrati	12
3.4	Stanzamenti del bilancio nazionale destinati alla prevenzione e alla lotta contro la criminalità informatica e sostegno finanziario dell'UE	14
3.5	Conclusioni	15
4	STRUTTURE NAZIONALI	17
4.1	Magistratura (inquirente e giudicante)	17
4.1.1	Struttura interna	17
4.1.2	Capacità e ostacoli per un'efficace azione penale	17
4.2	Autorità di contrasto	19
4.3	Altre autorità/istituzioni/partenariato pubblico-privato	20
4.4	Cooperazione e coordinamento a livello nazionale	21
4.4.1	Obblighi giuridici o politici	22
4.4.2	Risorse destinate al miglioramento della cooperazione	22
4.5	Conclusioni	22
5	Aspetti giuridici	24
5.1	Diritto penale sostanziale concernente la criminalità informatica	24
5.1.1	Convenzione del Consiglio d'Europa sulla criminalità informatica	24

5.1.2	Descrizione della legislazione nazionale	24
	A/ Decisione quadro 2005/222/GAI del Consiglio relativa agli attacchi contro i sistemi d'informazione e direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione	29
	B/ Direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile.....	29
	C/ Frodi con carte on-line.....	31
5.2	Questioni procedurali.....	34
5.2.1	Tecniche investigative	34
5.2.2	Analisi forensi e cifratura	35
5.2.3	Prove elettroniche	35
5.3	Protezione dei diritti umani/delle libertà fondamentali	36
5.4	Competenza giurisdizionale.....	36
5.4.1	Principi applicati per indagare sulla criminalità informatica.....	36
5.4.2	Norme in caso di conflitto di competenza giurisdizionale e ricorso a Eurojust	38
5.4.3	Competenza giurisdizionale per atti di criminalità informatica commessi nella "nuvola informatica"	39
5.5	Conclusioni	39
6	Aspetti operativi.....	41
6.1	Attacchi informatici	41
6.1.1	Natura degli attacchi informatici	41
6.1.2	Meccanismo per rispondere agli attacchi informatici.....	41
6.2.	Contrasto della pedopornografia e degli abusi sessuali on-line.....	41
6.2.1	Banche dati per l'identificazione delle vittime e misure per evitare la rivittimizzazione	42
6.2.2	Misure per contrastare lo sfruttamento/l'abuso sessuale on-line, il sexting e il bullismo informatico.....	42
6.2.3	Azioni preventive contro turismo sessuale, spettacoli pedopornografici e altro	42
6.2.4	Soggetti e misure per il contrasto dei siti web che contengono o diffondono materiale pedopornografico	43
6.3	Frodi con carte on-line.....	43
6.3.1	Segnalazione on-line.....	43
6.3.2	Ruolo del settore privato.....	43
6.5	Conclusioni	45
7	Cooperazione internazionale	46
7.1	Cooperazione con le agenzie dell'UE	46
7.1.1	Requisiti formali per cooperare con Europol/EC3, Eurojust, ENISA	46

7.1.2	Valutazione della cooperazione con Europol/EC3, Eurojust, ENISA.....	51
7.1.3	Risultati operativi delle squadre investigative comuni e delle pattuglie digitali	51
7.2	Cooperazione tra le autorità italiane e Interpol.....	51
7.3	Cooperazione con Stati terzi	52
7.4	Cooperazione con il settore privato	52
7.5	Strumenti di cooperazione internazionale.....	54
7.5.1	Assistenza giudiziaria reciproca	54
7.5.2	Strumenti di riconoscimento reciproco.....	55
7.5.3	Consegna/estradizione	55
7.6	Conclusioni	60
8	Formazione, sensibilizzazione e prevenzione	61
8.1	Formazione specifica	61
8.2	Sensibilizzazione e prevenzione	62
8.2.1	Legislazione/politica e altre misure nazionali	62
8.2.2	Partenariato pubblico-privato (PPP)	62
8.3	Conclusioni	63
9	Osservazioni finali e raccomandazioni	64
9.1.	Suggerimenti dell'Italia.....	64
9.2	Raccomandazioni.....	64
9.2.1	Raccomandazioni all'Italia.....	65
9.2.2	Raccomandazioni all'Unione europea, alle sue istituzioni e agli altri Stati membri.....	67
9.2.3	Raccomandazioni a Eurojust/Europol/ENISA.....	68
	Annex A: Programme for the on-site visit and persons interviewed/met.....	69
	Annex B: List of abbreviations/glossary of terms	71

1 SINTESI

L'Italia ha approvato il suo Quadro strategico nazionale per la sicurezza dello spazio cibernetico nel 2013. La strategia mira prioritariamente a garantire i servizi critici, a combattere più efficacemente la criminalità informatica e a migliorare le capacità nazionali di difesa. Ulteriori attività di sostegno finalizzate alla realizzazione di questi obiettivi comprendono: l'istituzione dell'autorità per la sicurezza delle reti e dell'informazione (NIS), il miglioramento dei partenariati pubblico-privato, la promozione della cooperazione internazionale, il rafforzamento delle attività delle squadre di pronto intervento informatico (CERT) nazionali, il miglioramento della comprensione della cibersicurezza da parte del pubblico e la sua sensibilizzazione al riguardo.

L'Italia dispone di un solido quadro giuridico, il suo diritto penale sostanziale contempla l'intera gamma dei reati connessi alla criminalità informatica. Il codice penale è regolarmente riesaminato e modificato per adattarlo alle nuove tendenze emergenti. L'Italia ha attuato la decisione quadro sui provvedimenti di blocco dei beni, la decisione quadro relativa agli attacchi contro i sistemi di informazione e quella relativa alle decisioni di confisca, nonché la direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile. È parte della convenzione di Budapest ma non ha ratificato la convenzione del 2000 relativa all'assistenza giudiziaria tra gli Stati membri. Per l'assistenza giudiziaria reciproca fa affidamento piuttosto sulla Convenzione europea di assistenza giudiziaria in materia penale (CEAG) del 1959, l'accordo di Schengen, Interpol e i canali diplomatici.

L'attuazione degli aspetti della strategia relativi alle attività di contrasto è di competenza del Ministero dell'interno, che è responsabile della polizia, comprese le divisioni di polizia specializzate come la Polizia postale e delle comunicazioni. A quest'ultima fanno capo il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (C.N.A.I.P.I.C.) e il Centro nazionale per il contrasto alla pedopornografia online (CNCPO).

La Polizia postale e delle comunicazioni dispone di notevoli poteri e tecniche investigative per indagare sui reati informatici e per gestire le prove elettroniche e i sistemi di cifratura. Le prove elettroniche sono considerate ammissibili se acquisite secondo le migliori prassi dell'informatica forense, che sono stabilite in larga misura conformemente alla Convenzione del Consiglio d'Europa sulla criminalità informatica.

Le imprese del settore privato che forniscono servizi critici non hanno l'obbligo di segnalare alle autorità italiane gli attacchi informatici e gli incidenti di sicurezza, sebbene il quadro strategico preveda la condivisione delle informazioni tra operatori pubblici e privati e C.N.A.I.P.I.C.. Per quanto riguarda la prevenzione dello sfruttamento sessuale dei minori, l'Italia blocca l'accesso ai siti web contenenti pedopornografia fornendo regolarmente liste nere ai fornitori di servizi Internet (ISP).

L'Italia mantiene contatti con Europol ed Eurojust e fa buon uso delle squadre investigative comuni (SIC); compie inoltre sforzi considerevoli per facilitare i collegamenti con gli altri partner internazionali, ad esempio gli Stati Uniti.

L'Italia prevede programmi di sensibilizzazione e prevenzione per informare il pubblico e l'industria sui rischi della criminalità informatica e promuovere l'uso sicuro di Internet. In particolare, le campagne e le presentazioni organizzate dalla Polizia postale e delle comunicazioni sono considerate di ampia portata ed efficaci.

In generale, i valutatori potrebbero concludere che l'Italia si impegna nella lotta contro la criminalità informatica e ha adottato a tal fine una serie di misure. Il gruppo di valutazione è stato positivamente impressionato dal numero di iniziative chiave attuate e ritiene che molte di queste potrebbero servire da modello di buone prassi e potrebbero essere utilizzate dagli altri Stati membri per rendere più incisive le loro strategie di lotta alla criminalità informatica. Meritano di essere citati, in particolare, la stazione di polizia on-line, le vaste campagne di sensibilizzazione del pubblico e il blocco dei siti web illegali.

Il gruppo di valutazione ha tuttavia individuato alcuni ambiti in cui sono necessari ulteriori miglioramenti e ha rivolto all'Italia raccomandazioni al riguardo (cfr. capitolo 9). Invita l'Italia ad attuare tali raccomandazioni al fine di potenziare ulteriormente i suoi sforzi nella lotta alla criminalità informatica.

2 INTRODUZIONE

In seguito all'adozione dell'azione comune 97/827/GAI del 5 dicembre 1997¹ è stato istituito un meccanismo di valutazione dell'applicazione e dell'attuazione a livello nazionale degli impegni internazionali in materia di lotta alla criminalità organizzata. Conformemente all'articolo 2 dell'azione comune, il 3 ottobre 2013 il gruppo per le questioni generali, valutazione compresa (GENVAL) ha deciso di dedicare il settimo ciclo di valutazioni reciproche all'attuazione pratica e al funzionamento delle politiche europee in materia di prevenzione e lotta alla criminalità informatica.

La scelta della criminalità informatica come oggetto del settimo ciclo di valutazioni reciproche è stata accolta con favore dagli Stati membri. Tuttavia, vista l'ampia gamma di reati rientranti nella nozione di criminalità informatica, è stato convenuto di incentrare la valutazione sui reati considerati meritevoli di particolare attenzione dagli Stati membri. La valutazione riguarda pertanto tre settori specifici - attacchi informatici, abuso sessuale su minori/pedopornografia on-line e frodi con carte on-line - e dovrebbe fornire un esame esauriente degli aspetti giuridici e operativi della lotta alla criminalità informatica, della cooperazione transfrontaliera e della cooperazione con le competenti agenzie dell'UE. La direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile² (data di recepimento: 18 dicembre 2013) e la direttiva 2013/40/UE³ relativa agli attacchi contro i sistemi di informazione (data di recepimento: 4 settembre 2015) rivestono particolare importanza in questo contesto.

¹ Azione comune del 5 dicembre 1997 (97/827/GAI), GU L 344 del 15.12.1997, pagg. 7 - 9.

² GU L 335 del 17.12.2011, pag. 1.

³ GU L 218 del 14.8.2013, pag. 8.

Inoltre, le conclusioni del Consiglio sulla strategia dell'UE per la cibersicurezza, del giugno 2013⁴, ribadiscono l'obiettivo di ratificare al più presto la convenzione del Consiglio d'Europa sulla criminalità informatica (convenzione di Budapest)⁵, del 23 novembre 2001, e sottolineano, nel preambolo, che "l'UE non chiede la creazione di un nuovo strumento giuridico internazionale relativo alle questioni riguardanti la cibersicurezza". Detta convenzione è integrata da un protocollo sugli atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici⁶.

L'esperienza maturata con le passate valutazioni mostra che le posizioni degli Stati membri riguardo all'attuazione degli strumenti giuridici pertinenti variano; in tale contesto l'attuale esercizio di valutazione potrebbe fornire un utile contributo anche agli Stati membri che eventualmente non abbiano attuato tutti gli aspetti dei vari strumenti. Tuttavia, la valutazione si vuole ampia e interdisciplinare, e non è incentrata soltanto sull'attuazione dei vari strumenti di lotta alla criminalità informatica, ma piuttosto sugli aspetti operativi negli Stati membri.

Pertanto, oltre alla cooperazione con i servizi preposti all'azione penale, si esaminerà anche il modo in cui le autorità di polizia cooperano con Eurojust, con l'ENISA e con Europol/EC3, e il modo in cui il feedback fornito dai vari attori è trasmesso ai competenti servizi sociali e di polizia. La valutazione è incentrata sull'attuazione delle politiche nazionali di lotta contro gli attacchi e le frodi informatici e la pedopornografia. Esamina inoltre le prassi operative degli Stati membri in materia di cooperazione internazionale e il sostegno offerto alle vittime della criminalità informatica.

⁴ 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633. JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87. CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

⁵ STCE n. 185; aperta alla firma il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004.

⁶ STCE n. 189; aperto alla firma il 28 gennaio 2003 ed entrato in vigore il 1° marzo 2006.

L'ordine delle visite negli Stati membri è stato deciso dal gruppo GENVAL il 1° aprile 2014. L'Italia è stata il decimo Stato membro ad essere valutato nel corso di questo ciclo di valutazioni. Conformemente all'articolo 3 dell'azione comune, la presidenza ha elaborato l'elenco degli esperti designati per le valutazioni da svolgere. Gli Stati membri hanno designato esperti che vantano conoscenze pratiche approfondite nel settore, in seguito a una richiesta scritta in tal senso rivolta dal presidente del gruppo GENVAL alle delegazioni il 28 gennaio 2014.

I gruppi di valutazione si compongono di tre esperti nazionali, coadiuvati da due membri del personale del Segretariato generale del Consiglio e da osservatori. Per il settimo ciclo di valutazioni reciproche, il gruppo GENVAL ha approvato la proposta della presidenza di invitare in qualità di osservatori la Commissione europea, Eurojust, ENISA ed Europol/EC3.

Gli esperti incaricati di effettuare la valutazione in Italia erano Gilles Herrmann (Lussemburgo), Matthew Roach (Regno Unito) e Savin Svet (Slovenia). Erano presenti anche tre osservatori: Hari Tiesmaa (Eurojust), Sara Marcolla (Europol/EC3) e Michele Socco (Commissione europea), insieme a Nicola Murphy e Steven Cras del Segretariato generale del Consiglio.

La presente relazione è stata stilata dal gruppo di esperti con l'ausilio del Segretariato generale del Consiglio, sulla scorta delle risultanze della visita di valutazione in Italia, svoltasi dal 26 al 28 maggio 2015, e delle risposte particolareggiate fornite dall'Italia al questionario di valutazione ed ai quesiti che ne sono conseguentemente scaturiti.

3 ASPETTI GENERALI E STRUTTURE

3.1 Strategia nazionale per la cibersecurity

La strategia nazionale dell'Italia per la cibersecurity è contenuta nel "Quadro strategico nazionale per la sicurezza dello spazio cibernetico"⁷, adottato dalla presidenza del Consiglio dei ministri nel dicembre 2013.

La lotta contro la criminalità informatica è una delle azioni stabilite dal piano nazionale, che prevede che ogni dipartimento governativo predisponga strutture e procedure per prevenire e contrastare gli attacchi informatici. In tale contesto, il Ministero dell'interno assicura la supervisione del ruolo delle divisioni di polizia incaricate dell'applicazione della legge e di quelle specializzate, come la Polizia postale e delle comunicazioni.

Il quadro strategico comprende sei indirizzi strategici, a loro volta sviluppati ulteriormente in undici indirizzi operativi.

3.2 Priorità nazionali per quanto riguarda la criminalità informatica

Il piano nazionale prevede l'istituzione di un sistema integrato di scambio delle informazioni attraverso partenariati pubblico-privato al fine di coinvolgere le strutture tecniche (CERT), le strutture militari (CERT DIFESA) e le strutture preposte all'applicazione della legge nella creazione di capacità e nella formazione. Il governo italiano ha dato priorità alla creazione di strutture che facilitino la condivisione delle informazioni e il reciproco scambio tra il mondo accademico, l'industria e la pubblica amministrazione. Nel complesso, le priorità nazionali sono in linea con le disposizioni dell'UE in materia di lotta alla criminalità informatica.

⁷ http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/piano-nazionale-cyber_0.pdf

L'articolo 7 bis della legge n. 155 recante "misure urgenti per il contrasto del terrorismo internazionale", conferisce alla Polizia postale e delle comunicazioni - in quanto organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione - la competenza esclusiva di assicurare i servizi di protezione informatica delle infrastrutture critiche operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

Per l'attuazione delle disposizioni del suddetto articolo 7 bis, il 9 gennaio 2008 il Ministero dell'interno ha emanato un decreto che prevede l'istituzione del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (C.N.A.I.P.I.C.). Il Centro è stato integrato nel servizio di Polizia postale e delle comunicazioni con un decreto del Capo della polizia - direttore generale della pubblica sicurezza - del 7 agosto 2008⁸. Si tratta di una struttura di analisi e di coordinamento investigativo che coopera con le altre istituzioni, con i settori militare e dell'intelligence e con la CERT nazionale.

3.3 Statistiche sulla criminalità informatica

3.3.1 Principali tendenze in materia di criminalità informatica

Il Servizio di analisi criminale della Direzione centrale della polizia criminale esamina i reati di cui agli articoli 615, 617, 623 bis, 635 e 640 del codice penale italiano. Per quanto riguarda le tendenze emergenti, l'Italia ha registrato un progressivo aumento di attacchi informatici sempre più sofisticati contro infrastrutture critiche, siti governativi e i settori economico e bancario, oltre ad attacchi di terrorismo informatico perpetrati, in particolare, da jihadisti.

⁸ Il DPCM 24 gennaio 2013 definisce l'architettura istituzionale per la protezione della sicurezza informatica e nazionale, e affida alla CERT nazionale la funzione di sostegno al NISP (nucleo interministeriale situazione e pianificazione), che agisce come centro per il coordinamento informatico interministeriale a livello nazionale. www.certnazionale.it

Le statistiche indicano che il numero di reati commessi è aumentato di circa il 50% tra il 2012 e il 2013, e che nel 2014 i casi risolti sono stati poco più di 34 000, in leggero calo rispetto agli anni precedenti. Anche il numero di persone segnalate per reati informatici nel 2013 è aumentato di circa il 15% rispetto al 2012, passando a oltre 4 500 persone. [1. Questi dati dovrebbero essere integrati, ove possibile, con quelli sulle violazioni dell'articolo 600 del codice penale e dell'articolo 130 del codice sulla privacy, nonché sulle violazioni di cui al decreto legislativo n. 64 dell'11 aprile 2011 (furto d'identità). 2. Dovrebbe essere indicata la percentuale dei reati informatici rispetto al totale dei reati, e si dovrebbe distinguere tra persone segnalate e arrestate].

3.3.2 Numero di casi di criminalità informatica registrati

Le uniche statistiche disponibili riguardano i reati segnalati alle autorità di contrasto. La Polizia postale e delle comunicazioni compila statistiche sulle attività istituzionali svolte su tutto il territorio nazionale.

La tabella di seguito riportata contiene le statistiche concernenti il numero di persone segnalate alle autorità giudiziarie e i reati all'origine della segnalazione.

Descrizione del reato	2012		2013		2014	
	Reati comm.	Persone arr.	Reati comm.	Persone arr.	Reati comm.	Persone arr.
Accesso non autorizzato a computer/sistemi TIC	6310	1097	8051	889	9490	893
Possesso illegale/diffusione di codici di accesso a sistemi TIC	700	253	1105	197	800	254
Diffusione di programmi destinati a danneggiare o alterare un sistema informatico	59	29	63	30	80	35
Falsificazione/alterazione o cancellazione del contenuto di comunicazioni	19	4	22	14	30	9
Intercettazione illegale, ostacolo a o interruzione di comunicazioni informatiche/TIC	154	134	257	175	229	74
Installazione di dispositivi destinati a intercettare/ostacolare o interrompere computer/TIC	269	254	251	329	170	149
Falsificazione, alterazione o compromissione del contenuto di comunicazioni elettroniche	142	18	150	22	153	30
Altre comunicazioni e conversazioni	37	14	28	10	38	19
Danneggiamento di sistemi TIC/informatici	277	49	202	39	180	49
Frode informatica	17669	2088	29089	2835	22936	2936
Danneggiamento di sistemi informatici o sistemi TIC	136	34	136	64	92	35

Danneggiamento di sistemi informatici o sistemi TIC	128	29	146	20	132	14
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato	89	47	86	56	96	52

3.4 Stanziamenti del bilancio nazionale destinati alla prevenzione e alla lotta contro la criminalità informatica e sostegno finanziario dell'UE

Per la lotta contro lo sfruttamento sessuale di minori on-line e per la protezione delle infrastrutture critiche sono previsti appositi stanziamenti di bilancio. I fondi sono assegnati direttamente alla Polizia postale e delle comunicazioni.

Il quadro strategico nazionale stabilisce che siano stanziare risorse adeguate per l'amministrazione pubblica direttamente responsabile della realizzazione degli obiettivi in esso indicati siano destinate.

Inoltre, vari progetti, come quello attualmente in corso per migliorare l'analisi delle immagini al fine di contrastare lo sfruttamento sessuale di minori on-line e i progetti destinati a lavorare con le vittime di questi reati, sono in parte finanziati dall'UE.

3.5 Conclusioni

- I valutatori hanno avuto la chiara impressione che l'Italia abbia un approccio serio alla cibersicurezza e il gruppo di valutazione ha espresso apprezzamento per il quadro strategico, che stabilisce le priorità nazionali al riguardo. Il gruppo ha constatato tuttavia che la strategia non definisce chiaramente compiti o obiettivi particolari per i soggetti interessati, e quindi il ruolo di ciascuno di essi non è chiaro. Ciò potrebbe comportare una duplicazione delle risorse, che potrebbe essere evitata se le funzioni di ciascun soggetto fossero precisate nel quadro nazionale⁹.
- Analogamente, non esistono stanziamenti specifici per l'attuazione del quadro strategico né esiste una stima dei relativi costi¹⁰. A parere del gruppo di valutazione, sarebbe utile elaborare un piano d'azione che individui azioni specifiche per ciascun soggetto implicato nella cibersicurezza e nella lotta contro la criminalità informatica, corredato da stime finanziarie. Il gruppo ha inoltre segnalato l'esigenza di riesaminare periodicamente gli investimenti in corso per tenere conto delle tendenze globali in materia di criminalità informatica, e di adattarli per rispondere all'aggravarsi delle minacce.
- L'Italia compila ed aggiorna statistiche sulla criminalità informatica, sebbene non sia chiaro in che misura tali statistiche siano complete e come siano effettuati il monitoraggio e la mappatura delle tendenze rilevate. I dati forniti sembrano suggerire una segnalazione incompleta dei casi di criminalità informatica, carenza di cui tener conto al momento di stabilire le risorse da destinare nell'ambito della strategia nazionale. Ciò detto, è apparso chiaramente che le autorità italiane sono consapevoli delle nuove minacce emergenti e vi rispondono attivamente con azioni mirate o con l'introduzione di nuove leggi.

⁹ Successivamente alla visita di valutazione, l'Italia ha informato il gruppo in merito alla valutazione del primo programma del quadro strategico nazionale e del piano strategico nazionale per la cibersicurezza (entrambi di durata biennale). Il primo esercizio si è concluso lo scorso dicembre 2015 e, secondo le autorità italiane, ha determinato innegabili progressi per quanto riguarda le azioni eseguite dall'Italia nella risposta globale alla minaccia informatica e l'introduzione di un sistema nazionale efficace e resiliente. Il prossimo programma terrà conto dei risultati delle azioni pianificate, anche in funzione dell'esito degli audit interni, che già prevedono obiettivi specifici e un sistema di misurazione per valutare le attività svolte dai dipartimenti competenti.

¹⁰ In seguito alla visita di valutazione, le autorità italiane hanno informato il gruppo in merito all'adozione di una nuova legge (Legge 208 del 28 dicembre 2015), che prevede uno specifico bilancio per la cibersicurezza con un importo totale pari a 150 milioni di EUR a livello nazionale. Il 10% di tale importo sarà assegnato alla Polizia postale e delle comunicazioni.

- Inoltre, il gruppo ha constatato l'esistenza di notevoli discrepanze tra i dati statistici forniti dalla polizia e quelli forniti dalla procura. Il gruppo ha riconosciuto che c'era da attendersi qualche discrepanza, dovuta all'esistenza di banche dati diverse utilizzate dalle varie autorità e gestite secondo criteri diversi, in particolare per quanto riguarda i campi utilizzati.

DECLASSIFIED

4 STRUTTURE NAZIONALI

4.1 Magistratura (inquirente e giudicante)

4.1.1 Struttura interna

I casi comuni di criminalità informatica sono gestiti dai magistrati ordinari, ossia magistrati inquirenti e giudici. I giudici possono essere selezionati nell'ambito del corpo giudicante sulla base della loro esperienza o formazione specifica per trattare casi informatici o concernenti le TIC.

Vi sono alcuni magistrati inquirenti che sono formalmente designati in qualità di magistrati inquirenti specializzati nel campo della criminalità informatica. Va rilevato che la competenza in materia non è attribuita agli uffici del pubblico ministero presso i giudici di primo grado (140), come avviene per la maggior parte dei reati, bensì alle procure distrettuali (29) (cfr. articolo 51, comma 3-quinquies, del codice di procedura penale). L'attribuzione della competenza per i reati informatici agli uffici del pubblico ministero presso il tribunale del capoluogo del distretto e la conseguente concentrazione delle indagini, che sono assegnate a un numero ridotto di magistrati inquirenti, consentono di fatto a questi ultimi di acquisire un alto grado di specializzazione.

4.1.2 Capacità e ostacoli per un'efficace azione penale

Capacità

L'Italia vanta un solido quadro legislativo in materia di criminalità informatica, che viene periodicamente riesaminato per tenere conto delle tendenze e delle minacce emergenti. Ad esempio, è attualmente all'esame del Parlamento una legge contenente "Disposizioni per la prevenzione e il contrasto del bullismo e del bullismo informatico".

- Inoltre, un decreto-legge antiterrorismo emanato di recente (n. 7 del 2015), modificato e convertito in legge dalla legge n. 43 del 17 aprile 2015 (Gazzetta ufficiale n. 91 del 20 aprile 2015), ha aggiornato gli strumenti intesi a contrastare l'uso di Internet a fini di proselitismo nonché di complicità e favoreggiamento di gruppi terroristici. Sono previste, in particolare, le seguenti disposizioni:
 - i)* aggravamenti delle pene stabilite per i reati di istigazione a delinquere o di istigazione al terrorismo perpetrati attraverso strumenti telematici o informatici;
 - ii)* possibilità per le autorità giudiziarie di ordinare ai fornitori di servizi Internet di inibire l'accesso ai siti utilizzati per commettere i reati di terrorismo inseriti nell'elenco costantemente aggiornato dal servizio di Polizia postale e delle comunicazioni della polizia nazionale italiana. In caso di mancato adempimento al suddetto ordine, le autorità giudiziarie vietano l'accesso ai pertinenti siti Internet.
- Ratifica ed esecuzione del protocollo sulla criminalità informatica (disegno di legge). Il 27 marzo 2015 il Consiglio dei ministri ha approvato un disegno di legge di ratifica ed esecuzione del "Protocollo addizionale alla convenzione del Consiglio d'Europa sulla criminalità informatica, riguardante la criminalizzazione degli atti di razzismo e xenofobia commessi a mezzo di sistemi informatici".

Ostacoli

A giudizio dell'Italia, il principale ostacolo a un'efficace lotta contro la criminalità informatica è la difficoltà di ottenere rapidamente informazioni dai server stranieri (in particolare dai server statunitensi di Google, Microsoft, Yahoo e Facebook). Anche una volta ottenuti, i dati possono essere limitati e pertanto risultare spesso inutili ai fini investigativi, dato che il loro periodo di conservazione (da parte dei suddetti fornitori di servizi Internet) è al massimo di 90 giorni.

4.2. Autorità di contrasto

Polizia postale e delle comunicazioni

La Polizia postale e delle comunicazioni, in quanto divisione della polizia nazionale italiana specializzata nella prevenzione e lotta alla criminalità informatica, garantisce il rispetto dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione. È presente su tutto il territorio nazionale attraverso 20 compartimenti con competenza regionale e 81 sezioni con competenza provinciale, coordinati a livello centrale dal servizio Polizia delle comunicazioni. Pertanto, la Polizia postale e delle comunicazioni è l'organo incaricato dalla legge di lottare contro fenomeni criminali quali lo sfruttamento sessuale di minori on-line e di proteggere le infrastrutture critiche. Svolge le suddette attività e le altre attività investigative riguardanti la criminalità informatica a livello centrale e coordinando i compartimenti e le sezioni di Polizia postale presenti su tutto il territorio nazionale.

All'interno del servizio di Polizia postale e delle comunicazioni si trova il punto di contatto per le emergenze tecnico-operative connesse alla criminalità informatica transnazionale previsto dalla convenzione di Budapest sulla criminalità informatica.

Il punto di contatto è attivo 24 ore su 24, 7 giorni su 7 nell'ambito della Rete per la criminalità ad alta tecnologia istituita nel quadro del G8 e successivamente estesa al Consiglio d'Europa. È situato presso il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (C.N.A.I.P.I.C.). L'obiettivo principale della rete è rispondere rapidamente alle richieste di congelamento dei dati in attesa della pertinente formalizzazione attraverso rogatorie o attraverso il trattato di mutua assistenza giudiziaria.

Il punto di contatto funge anche da punto di collegamento centrale nazionale (National Central Reference Point - NCRP) nel quadro dei canali Interpol per far fronte alle richieste urgenti provenienti dai punti di contatto operativi 24 ore al giorno.

Stazione di polizia on-line

La stazione di polizia on-line è stata lanciata nel 2006 con l'obiettivo primario di fornire un migliore servizio al pubblico. È stata la prima stazione di questo tipo creata nell'UE e nel 2007 ha ricevuto il premio "E-gov" come buona prassi più stimolante in Europa. Opera 24 ore su 24, 7 giorni su 7.

La stazione riceve fra le 100 e le 200 segnalazioni al giorno, di cui 30-35 durante l'orario notturno. Esistono due tipi di segnalazione: come testimone o come vittima. Gli utenti devono registrarsi per segnalare un reato e utilizzare il servizio, ma alcune informazioni immediate sono disponibili sulla home page. Pertanto, le segnalazioni possono essere fatte in primo luogo on-line ed essere successivamente formalizzate presso una stazione di polizia entro le 48 ore necessarie. È attualmente allo studio la possibilità di utilizzare la firma elettronica al momento della segnalazione, il che eviterebbe la necessità di formalizzare ulteriormente la segnalazione.

Le segnalazioni concernenti reati di criminalità informatica sono trasmesse al C.N.A.I.P.I.C. o, a seconda dei casi, alla sezione della Polizia postale e delle comunicazioni che si occupa di pedopornografia.

4.3. Altre autorità/istituzioni/partenariato pubblico-privato

Il DPCM (decreto del presidente del Consiglio dei ministri) del 27 gennaio 2014 con il quale è stato adottato il quadro strategico nazionale prevede un coordinamento tra CERT nazionale, CERT Difesa e pubblica amministrazione.

Il quadro strategico nazionale per la sicurezza dello spazio cibernetico attribuisce un ruolo centrale al partenariato pubblico-privato. In particolare, gli operatori pubblici e privati che forniscono reti e servizi di comunicazioni al pubblico sono tenuti a:

- comunicare all'unità preposta alla ciber sicurezza qualsiasi violazione significativa della sicurezza e dell'integrità dei loro sistemi informatici;
- adottare tutte le misure e le migliori prassi necessarie per garantire la ciber sicurezza;
- condividere informazioni con le agenzie di intelligence e sicurezza e consentire l'accesso alle banche dati pertinenti per la ciber sicurezza;
- collaborare alla gestione delle crisi informatiche ripristinando la funzionalità delle loro reti e dei loro sistemi.

I partenariati pubblico-privato sono pertanto considerati una componente essenziale per il successo della strategia. La cooperazione in questo contesto è stata assicurata mediante accordi ad hoc intesi a rafforzarla ulteriormente. Nella prospettiva di compiere ulteriori progressi, il quadro strategico incoraggia a potenziare le sinergie con il settore privato per coinvolgere nei partenariati tutte le entità che, indipendentemente dalle dimensioni, sono d'importanza strategica per l'avanzamento scientifico, tecnologico, industriale ed economico del paese.

Un progetto che merita di essere menzionato è il progetto OF2CEN, una piattaforma che riunisce banche e polizia e rende anonimi i dati permettendo alle banche di segnalare alla polizia le operazioni sospette mediante un canale sicuro. OF2CEN è diventato pienamente operativo nel 2013 dopo una fase pilota che ha coinvolto 15 banche. Esistono inoltre memorandum d'intesa con banche e infrastrutture critiche, con i servizi finanziari e con l'Associazione bancaria italiana (ABI).

4.4. Cooperazione e coordinamento a livello nazionale

Tale cooperazione è illustrata nel quadro strategico nazionale per la sicurezza dello spazio cibernetico¹¹.

¹¹ http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf

4.4.1 Obblighi giuridici o politici

4.4.2 Risorse destinate al miglioramento della cooperazione

Il quadro strategico nazionale per la sicurezza dello spazio cibernetico non prevede finanziamenti mirati, ma l'indirizzo operativo n. 10, relativo alle risorse, è incentrato sulla valutazione dei costi associati agli eventi cibernetici e sull'eventualità di reclutare personale specializzato. Le risorse per l'attuazione del quadro strategico provengono dal bilancio ordinario della pubblica amministrazione.

4.5 Conclusioni

- Il gruppo di valutazione ha constatato con soddisfazione che l'attribuzione della competenza per i reati informatici agli uffici del pubblico ministero presso il tribunale del capoluogo del distretto e la conseguente concentrazione delle indagini, che sono assegnate a un numero ridotto di magistrati inquirenti, consentono di fatto a questi ultimi di acquisire un alto grado di specializzazione.
- In base alla struttura e all'organizzazione della polizia, la formazione di operatori "di prima linea" per le indagini sulla criminalità informatica nonché la partecipazione ad esercitazioni di cibersicurezza a livello nazionale dovrebbero essere estese a specifici operatori a livello di compartimenti di polizia, creando così un più forte nucleo di competenze per le indagini sulla criminalità informatica ed ampliare la disponibilità e il sostegno forense. Il conferimento di competenze a livello regionale seguirebbe a tempo debito.

- Inoltre, il gruppo di valutazione suggerisce che in futuro la sezione incaricata della criminalità informatica partecipi insieme alla CERT alle esercitazioni europee sulla sicurezza informatica, al fine di sviluppare procedure standard, sensibilizzare, individuare le lacune e mettere a punto buone prassi.
- Il gruppo ha constatato con soddisfazione che vi è piena comprensione del ruolo della Polizia postale e delle comunicazioni nella lotta alla criminalità informatica. Nell'ambito del servizio viene operata una chiara distinzione di ruoli e responsabilità tra le varie sezioni.
- Il gruppo ha espresso apprezzamento per il commissariato di polizia on-line, ritenendolo innovativo, di facile impiego e di grande aiuto nella lotta contro la criminalità on-line, e che rende l'attività di contrasto più efficace e l'assistenza più accessibile al pubblico. Ha inoltre espresso apprezzamento per l'intenzione d'introdurre in futuro la firma elettronica.
- Anche il progetto OF2CEN è stato considerato utile dal gruppo, che incoraggia l'Italia a prendere in esame la sua introduzione ed estensione a un maggior numero di istituzioni finanziarie del settore privato al fine di migliorarne l'efficacia e la portata.
- Il gruppo ha constatato con soddisfazione che il quadro strategico prevede esplicitamente la promozione del partenariato pubblico-privato; ad eccezione del progetto OF2CEN, tuttavia, il gruppo non è convinto che tale partenariato stia operando nella misura prevista da detto quadro, e incoraggia pertanto a proseguire i lavori al riguardo.

5 ASPETTI GIURIDICI

5.1 Diritto penale sostanziale concernente la criminalità informatica

5.1.1 Convenzione del Consiglio d'Europa sulla criminalità informatica

L'Italia è parte della convenzione del Consiglio d'Europa sulla criminalità informatica e ha modificato la sua legislazione per darle applicazione.

5.1.2 Descrizione della legislazione nazionale

Il codice penale italiano contiene le seguenti norme in materia di reati informatici:

1. Accesso abusivo ad un sistema informatico o telematico (articolo 615-ter del codice penale)

Il codice prevede la pena della reclusione fino a tre anni per chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La pena è della reclusione da uno a cinque anni:

- 1) se il fatto è commesso *i)* da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, *ii)* da chi esercita anche abusivamente la professione di investigatore privato, o *iii)* con abuso della qualità di operatore del sistema;
- 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

2. Danneggiamento di sistemi informatici o telematici (articolo 635-quater del codice penale)

Chiunque, attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

3. Danneggiamento di sistemi informatici o telematici di pubblica utilità (articolo 635-quinquies del codice penale)

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

4. Danneggiamento di informazioni, dati e programmi informatici (articolo 635-bis del codice penale)

Chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

5. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (articolo 635-ter del codice penale)

La distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, sono puniti con la reclusione da tre a otto anni. Se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

6. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (articolo 617-quater del codice penale)

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. La stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

- 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- 3) da chi esercita anche abusivamente la professione di investigatore privato.

7. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (articolo 615-quinquies del codice penale)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

8. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (articolo 617-quinquies del codice penale)

L'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punita con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

9. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (articolo 615-quater del codice penale)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

10. Denaro virtuale

Al gruppo è stato riferito che il trattamento del denaro virtuale non è disciplinato da disposizioni specifiche della legislazione italiana.

Le autorità italiane hanno confermato che la legislazione interna non contempla disposizioni specifiche riguardanti il denaro virtuale, ma hanno rilevato che questa apparente lacuna è colmata dalla possibilità di ampliare, per via interpretativa, il campo d'azione delle misure previste dal codice di procedura penale. In tale contesto hanno fatto riferimento all'articolo 253 del codice di procedura penale, che prevede la possibilità di procedere al sequestro del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti. Il secondo comma di tale articolo precisa che *"sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo"*. Inoltre, l'articolo 321 del codice di procedura penale prevede la possibilità di disporre il sequestro preventivo delle cose di cui è consentita la confisca nonché delle cose pertinenti al reato quando vi è pericolo che la loro libera disponibilità possa aggravare o protrarre le conseguenze del reato ovvero agevolare la commissione di altri reati. Secondo le autorità italiane, laddove il denaro virtuale costituisca il prodotto, il profitto o il prezzo di un reato, o fosse comunque pertinente a un reato, non vi sarebbe alcun ostacolo all'applicazione ad esso di misure restrittive, né alla sua ammissione in un procedimento penale.

Le autorità italiane hanno riconosciuto, per contro, che non esistono norme sostanziali riguardanti specificamente i *bitcoin* o strumenti analoghi e questa lacuna non può essere colmata applicando per analogia le disposizioni in materia di falsificazione di monete, spendita e introduzione nello Stato di monete falsificate, in ragione dell'esplicito divieto di applicazione per analogia in materia penale. In ogni caso, la necessità di ampliare il campo d'azione di tali disposizioni appare difficilmente prospettabile, essendo esse chiaramente dirette a tutelare la fede pubblica e relative a monete nazionali o straniere aventi corso legale.

A/ Decisione quadro 2005/222/GAI del Consiglio relativa agli attacchi contro i sistemi d'informazione e direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione

La direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio è stata inclusa nella "Delega al governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2014" (A.S. 1758, pag. 66, punto 4).

B/ Direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile

La direttiva 2011/93/UE, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile è stata recepita con il decreto legislativo 4 marzo 2014 n. 39.

- Atti riguardanti i contenuti, in particolare sfruttamento sessuale dei minori on-line e pedopornografia

1. Pornografia minorile (articolo 600-ter)

Chiunque,

- 1) utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico;
- 2) recluta o induce minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli trae altrimenti profitto,

è punito con la reclusione da sei a dodici anni e con la multa da euro 24.000 a euro 240.000. Alla stessa pena soggiace chi fa commercio del materiale pornografico.

- Chiunque, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 24.000 a euro 240.000.
- Chiunque offre o cede ad altri, anche a titolo gratuito, il materiale pornografico, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164.
- Chiunque assiste a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto è punito con la reclusione fino a tre anni e con la multa da euro 1.500 a euro 6.000.

Ai fini della legislazione, per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

2. Detenzione di materiale pornografico (articolo 600-quater del codice penale)

Chiunque consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità.

3. Pornografia virtuale (articolo 600-quater.1)

- (1) Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.

Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

C/ Frodi con carte on-line

- **Atti in cui i sistemi informatici/di informazione costituiscono lo strumento o il bersaglio, in particolare le frodi con carte on-line**

1. Frode informatica (articolo 640-ter del codice penale)

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

2. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (articolo 640-quinquies)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

Per quanto riguarda l'istigazione, il favoreggiamento e il concorso legati alla criminalità informatica, si applicano le seguenti regole generali:

- **Concorso:** quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita, salve le disposizioni degli articoli seguenti.
- **Istigazione:** se il reato è stato commesso, l'istigazione equivale a partecipazione. Secondo la legislazione italiana, l'istigazione non è punita se il reato non è stato commesso.
- **Favoreggiamento personale:** chiunque, dopo che fu commesso un delitto per il quale la legge stabilisce l'ergastolo o la reclusione, e fuori dei casi di concorso nel medesimo, aiuta taluno a eludere le investigazioni dell'autorità, comprese quelle svolte da organi della Corte penale internazionale, o a sottrarsi alle ricerche effettuate dai medesimi soggetti, è punito con la reclusione fino a quattro anni.

- Quando il delitto commesso è quello previsto dall'art. 416-bis, si applica, in ogni caso, la pena della reclusione non inferiore a due anni.
 - Se si tratta di delitti per i quali la legge stabilisce una pena diversa, ovvero di contravvenzioni, la pena è della multa fino a euro 516.
 - Le disposizioni di questo articolo si applicano anche quando la persona aiutata non è imputabile o risulta che non ha commesso il delitto.
- **Favoreggiamento reale:** chiunque aiuta taluno ad assicurare il prodotto o il profitto o il prezzo di un reato, è punito con la reclusione fino a cinque anni se si tratta di delitto, e con la multa da euro 51 a euro 1.032 se si tratta di contravvenzione.
 - **Delitto tentato:** chi compie atti idonei, diretti in modo non equivoco a commettere un delitto, risponde di delitto tentato, se l'azione non si compie o l'evento non si verifica. Il colpevole del delitto tentato è punito: con la reclusione non inferiore a dodici anni, se la pena stabilita è l'ergastolo; e, negli altri casi con la pena stabilita per il delitto, diminuita da un terzo a due terzi.
 - Se il colpevole volontariamente desiste dall'azione, soggiace soltanto alla pena per gli atti compiuti, qualora questi costituiscano per sé un reato diverso.
 - Se volontariamente impedisce l'evento, soggiace alla pena stabilita per il delitto tentato, diminuita da un terzo alla metà.

5.2 Questioni procedurali

- È consentito procedere alla perquisizione e al sequestro di sistemi di informazione/dati informatici secondo quanto previsto agli articoli 254, 254-bis, 352 e 354 del codice di procedura penale quale modificato dalla Convenzione del Consiglio d'Europa sulla criminalità informatica.
- È consentito procedere all'intercettazione/raccolta in tempo reale di dati di traffico/contenuto secondo quanto previsto all'articolo 266-bis del codice di procedura penale.
- La conservazione di dati informatici è prevista all'articolo 132 del codice della privacy.
- L'ordinanza relativa alla conservazione di dati di traffico/contenuto e alle informazioni sugli utenti è prevista all'articolo 132 del codice della privacy.
- Le disposizioni in materia di accesso a dati informatici, dati di contenuto, dati di traffico, ordinanza di perquisizione/sequestro di sistemi di informazione, reti gestite o controllate da indiziati di reati informatici sono previste dal decreto Frattini.¹²

5.2.1 Tecniche investigative

È consentito procedere al sequestro di apparecchiature informatiche (hardware e software) durante le operazioni. Tali apparecchiature sono acquisite attraverso sistemi che non alterano le prove e ne consentono la copia forense. Se per motivi tecnici non è possibile ripetere queste operazioni, si procede ad un esame incrociato delle parti coinvolte. La successiva analisi è finalizzata alla ricerca di prove elettroniche che vengono segnalate e trasmesse agli organi investigativi insieme alle relative copie forensi.

¹² http://www.interlex.it/testi/dlg08_109.htm

Per le attività d'indagine relative alla criminalità informatica è possibile ricorrere a tecniche investigative speciali quali intercettazioni, attività sotto copertura e ricerche OSINT. Le autorità di contrasto possono anche avvalersi di malware, ma il loro uso deve essere autorizzato da un magistrato inquirente e non sempre ciò accade. Il gruppo è stato informato dell'esistenza di linee guida nazionali, ma poiché i magistrati hanno la discrezionalità finale tali linee guida non sono attuate in modo uniforme a livello nazionale. Le prove raccolte per mezzo di malware/intrusione legale possono essere utilizzate in sede giudiziaria se ne è stato autorizzato l'uso mediante provvedimento giurisdizionale. Il gruppo è stato altresì informato del fatto che la Polizia postale e delle comunicazioni ha chiesto di prevedere la capacità di creare, se necessario, un trojan della polizia, ma questo suggerimento non è stato accolto e pertanto le forze di contrasto continueranno ad avvalersi di metodi investigativi più tradizionali.

5.2.2 Analisi forensi e cifratura

L'Italia è anche in grado di usare strumenti speciali per decifrare file cifrati (ad esempio zip e office), nonché per trattare contenitori cifrati (pgp, drivecrypt, truecrypt) e per la cifratura totale del disco. Non vi sono centri forensi istituzionali, ma centri privati specializzati usati esclusivamente per il recupero dei dati da supporti/dispositivi danneggiati. In Italia non vi sono società che provvedono alla decifratura per conto delle autorità di contrasto.

Le autorità interessate cooperano l'una con l'altra sulla base di accordi con i paesi dell'UE e del G8 come pure di accordi bilaterali con paesi terzi.

5.2.3 Prove elettroniche

In Italia le prove elettroniche sono considerate ammissibili se acquisite secondo le migliori prassi dell'informatica forense, che sono stabilite in larga misura conformemente alla Convenzione del Consiglio d'Europa sulla criminalità informatica. I criteri di ammissibilità si applicano anche alle prove elettroniche acquisite al di fuori dell'Italia grazie alla cooperazione con Stati membri o all'assistenza giudiziaria reciproca internazionale.

5.3. Protezione dei diritti umani/delle libertà fondamentali

In generale i diritti e le libertà fondamentali sono protetti dalla Costituzione italiana (articoli 2, 3, 13, 15, 19, 21 e 33) e dal diritto primario. In ordine alla protezione della vita privata e dei dati personali il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il codice contiene anche disposizioni che disciplinano, segnatamente, il trattamento dei dati con sistemi informatici. Queste disposizioni prevedono l'adozione di specifiche misure minime di sicurezza per la protezione dei sistemi in questione (articolo 34). Inoltre il Garante per la protezione dei dati personali promuove la sottoscrizione di codici di deontologia e di buona condotta per il trattamento dei dati personali effettuato da fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica (articolo 133).

5.4 Competenza giurisdizionale

5.4.1 Principi applicati per indagare sulla criminalità informatica

Tutti i reati (non solo la criminalità informatica) - anche se commessi parzialmente al di fuori del territorio nazionale - si considerano commessi interamente nel territorio nazionale ai fini dell'applicazione della legge penale italiana.

L'articolo 6 del codice penale dispone che chiunque commetta un reato nel territorio dello Stato è punito secondo la legge italiana. Il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione o dell'omissione.

Tutti i reati (non solo la criminalità informatica) commessi al di fuori del territorio dello Stato sono puniti secondo la legge italiana nei casi seguenti:

- a) reati contro lo Stato italiano;
- b) reati previsti da convenzioni internazionali;
- c) altri casi minori.

L'articolo 7 del codice penale dispone che è punito secondo la legge italiana il cittadino italiano o lo straniero che commette in territorio estero taluno dei seguenti reati:

- 1) delitti contro la personalità dello Stato italiano;
- 2) delitti di contraffazione del sigillo dello Stato e di uso di tale sigillo contraffatto;
- 3) delitti di falsità in monete aventi corso legale nel territorio dello Stato, o in valori di bollo o in carte di pubblico credito italiano;
- 4) delitti commessi da pubblici ufficiali a servizio dello Stato, abusando dei poteri o violando i doveri inerenti alle loro funzioni;
- 5) ogni altro reato per il quale speciali disposizioni di legge o convenzioni internazionali stabiliscono l'applicabilità della legge penale italiana.

Fatta eccezione per i casi anzidetti la punibilità dei reati commessi all'estero dipende:

- a) dalla gravità del reato e relativa pena;
- b) dalla presenza in Italia dell'autore del reato;
- c) dalla richiesta del Ministro della giustizia.

Inoltre l'articolo 8 del codice penale dispone che il cittadino italiano o lo straniero, che commette in territorio estero un delitto politico non compreso tra quelli indicati nel numero 1 dell'articolo 7, è punito secondo la legge italiana, a richiesta del Ministro della giustizia.

Se si tratta di un delitto punibile a querela della persona offesa, occorre, oltre a tale richiesta, anche la querela.

Agli effetti della legge penale, è delitto politico ogni delitto, che offende un interesse politico dello Stato, ovvero un diritto politico del cittadino. È altresì considerato delitto politico il delitto comune determinato, in tutto o in parte, da motivi politici.

L'articolo 9 del codice penale dispone che il cittadino italiano che commette in territorio estero un delitto per il quale la legge italiana stabilisce l'ergastolo o la reclusione non inferiore nel minimo a tre anni, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato. Se si tratta di delitto per il quale è stabilita una pena restrittiva della libertà personale di minore durata, il colpevole è punito a richiesta del Ministro della giustizia, ovvero a istanza o a querela della persona offesa.

L'articolo 10 del codice penale dispone che lo straniero che commette in territorio estero, a danno dello Stato o di un cittadino italiano, un delitto per il quale la legge italiana stabilisce l'ergastolo, o la reclusione non inferiore nel minimo a un anno, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato, e vi sia richiesta del Ministro della giustizia, ovvero istanza o querela della persona offesa.

5.4.2 Norme in caso di conflitto di competenza giurisdizionale e ricorso a Eurojust

In Italia vige il principio di obbligatorietà dell'azione penale poiché l'articolo 112 della Costituzione dispone che il pubblico ministero ha l'obbligo di esercitare l'azione penale.

Per questa ragione, se sussistono le condizioni per l'applicazione della legge italiana, l'autorità giudiziaria dà avvio all'azione penale anche se indagini analoghe sono in corso in altri Stati. La sola eccezione all'esercizio dell'azione penale si ha quando una persona sia stata giudicata con sentenza definitiva o assolta per i medesimi fatti in un altro Stato aderente alla convenzione Schengen (articolo 54).

Al momento della visita di valutazione, l'Italia non aveva ancora recepito la decisione quadro 2009/948/GAI sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali. Tuttavia, dopo la visita di valutazione l'Italia ha comunicato al gruppo che la decisione quadro 2009/948/GAI è stata ora recepita nell'ordinamento giuridico italiano mediante il decreto legislativo n. 29 del 15 febbraio 2016, che è entrato in vigore il 22 marzo 2016. In particolare, l'articolo 11 di tale decreto dispone che nel caso di accordo sulla concentrazione dei procedimenti in altro Stato membro, il giudice dichiara la sopravvenuta improcedibilità. Secondo l'Italia, tale disposizione risolve il problema in virtù del principio dell'obbligatorietà dell'azione penale e dell'assenza di una disposizione specifica che consenta di risolvere casi di conflitti di competenza giurisdizionale.

5.4.3. Competenza giurisdizionale per atti di criminalità informatica commessi nella "nuvola informatica"

Non è nota alcuna sentenza della Corte di cassazione al riguardo; tuttavia, in forza della legge italiana sulla competenza giurisdizionale (articolo 6 del codice penale), se file elettronici illegali nella nuvola (ad esempio un'immagine pedopornografica) sono visibili da un computer in Italia, vale la competenza giurisdizionale italiana ed è possibile intervenire mediante rogatoria; può inoltre essere richiesta la cancellazione del file illegale residente su un server all'estero.

5.5 Conclusioni

- Il diritto penale sostanziale è esauriente e flessibile. La normativa italiana contempla tutta una gamma di reati e disciplina il tentativo, la partecipazione, l'istigazione e il concorso, la negligenza e la responsabilità giuridica.
- La Polizia postale e delle comunicazioni dispone di notevoli poteri e strumenti di indagine. Il gruppo ha accertato che, in Italia, i diritti fondamentali sono rispettati e che nel caso di sorveglianza o altre tecniche investigative speciali è esercitato l'opportuno controllo giudiziario. Non di meno ha rilevato che, nonostante gli orientamenti nazionali al riguardo, il ricorso a talune forme di sorveglianza speciale è limitato a causa della discrezionalità dei magistrati.

- Il gruppo ha riconosciuto che la legge italiana sulla competenza giurisdizionale (articolo 6 del codice penale) facilita il trattamento di dati presenti nella nuvola, sebbene le norme giurisdizionali possano comportare, in caso di criminalità informatica, complicazioni dovute alla probabile concorrenza di elementi transfrontalieri.
- L'impressione avuta nel corso della visita è che le autorità giudiziarie italiane non considerino "denaro" la moneta virtuale; ne consegue che parecchi elementi dell'ordinamento giuridico non si applicherebbero a questo tipo di denaro. Al gruppo è stato ad esempio comunicato che non sarebbero disponibili poteri per la confisca di denaro virtuale, il che sembra cozzare con la realtà del mondo informatizzato, in cui esistono molte forme di denaro virtuale, ampiamente utilizzate dai criminali, e avverso i quali l'azione legale dovrebbe essere possibile. Pare dunque opportuno che l'Italia adatti legislazione e prassi al riguardo.¹³

DECLASSIFIED

¹³ Successivamente alla visita di valutazione, le autorità italiane hanno informato il gruppo che è in via di realizzazione un centro di studi cibernetici, in collaborazione con il mondo accademico (Università di Modena e Reggio Emilia e Università "La Sapienza" di Roma), che si propone di indagare e analizzare i fenomeni emergenti riguardanti l'uso (e l'abuso) di Bitcoin e suoi "parenti stretti", come Ripple, Litecoin ecc. In tale centro si procederà allo studio delle varie tecniche di deanonimizzazione per percorrere a ritroso la *blockchain* e ottenere un alto impatto nell'affrontare le nuove sfide investigative.

6 ASPETTI OPERATIVI

6.1 Attacchi informatici

6.1.1 Natura degli attacchi informatici

6.1.2 Meccanismo per rispondere agli attacchi informatici

Come detto nel primo capitolo, il ministro dell'interno ha emanato il 9 gennaio 2008 un decreto che prevede l'istituzione del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (C.N.A.I.P.I.C.). Il Centro è stato integrato nel servizio di Polizia postale e delle comunicazioni con un decreto del Capo della polizia - direttore generale della pubblica sicurezza - del 7 agosto 2008.

Si tratta di una struttura di analisi e di coordinamento investigativo che coopera con le altre istituzioni, con i settori militare e dell'intelligence e con il CERT.

6.2. Contrasto della pedopornografia e degli abusi sessuali on-line

La direttiva 2011/93/UE, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile è stata recepita con il decreto legislativo 4 marzo 2014 n. 39. Inoltre il decreto prevede circostanze aggravanti specifiche quando siano usati mezzi atti ad impedire l'identificazione dei dati nei tipi di reato connessi alla circolazione e produzione di materiale pedopornografico.

Il Centro nazionale per il contrasto della pedopornografia online (CNCPO) della Polizia postale e delle comunicazioni mantiene elenchi aggiornati di siti web contenenti materiale illegale in cui siano coinvolti minori e incarica gli ISP di rimuovere e bloccare questi contenuti su servizi situati in Italia. Se il server è situato al di fuori dell'Italia viene avviata la procedura Notice & Takedown (Notifica e rimozione), se e quando possibile, attraverso il National Centre for Missing and Exploited Children - NCMEC (Centro nazionale per i minori scomparsi e sfruttati) poiché questo garantisce il sequestro e la trasmissione dei dati investigativi alle agenzie investigative competenti sul territorio.

6.2.1 Banche dati per l'identificazione delle vittime e misure per evitare la rivittimizzazione

L'Italia non dispone di banche dati nazionali per l'identificazione delle vittime, ma si serve della banca dati ICSE di Interpol. Le autorità di contrasto italiane possono accedere direttamente all'ICSE attraverso il Centro nazionale per il contrasto alla pedopornografia online (CNCPO) della Polizia postale e delle comunicazioni.

6.2.2 Misure per contrastare lo sfruttamento/l'abuso sessuale on-line, il sexting e il bullismo informatico

Quando ONG o cittadini comunicano che un sito web veicola contenuti illegali il CNCPO provvede alle necessarie verifiche. Se l'informazione è confermata, il centro inserisce il sito nella lista nera e ne ordina la rimozione.

6.2.3 Azioni preventive contro turismo sessuale, spettacoli pedopornografici e altro

La legislazione italiana contiene disposizioni specifiche per la sanzione del turismo sessuale. La legge n. 269/1988 contiene un articolo (Iniziative turistiche volte allo sfruttamento della prostituzione minorile) secondo cui chiunque organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tali attività è punito con la reclusione da sei a dodici anni e con la multa da lire trenta milioni a lire trecento milioni.

L'Italia ricorre ad indagini on-line sotto copertura per contrastare lo sfruttamento sessuale dei minori sul web in tempo reale. Ritiene questo strumento efficace, in particolare nell'ambito della cooperazione internazionale di polizia.

6.2.4 Soggetti e misure per il contrasto dei siti web che contengono o diffondono materiale pedopornografico

La mancata cancellazione di immagini/video può verificarsi se la circolazione del materiale è avvenuta su Internet e la rimozione non risulta possibile, oppure il materiale si trova su server stranieri dai quali è impossibile ottenere la cancellazione.

Al riguardo l'Italia partecipa all'iniziativa mondiale denominata "Global Alliance", che si prefigge di rimuovere il materiale all'origine.

6.3 Frodi con carte on-line

6.3.1 Segnalazione on-line

Le sezioni locali della Polizia postale e delle comunicazioni ricevono regolarmente segnalazioni sia da cittadini titolari di carte di pagamento sia da agenzie private (emittenti/acquirenti).

6.3.2 Ruolo del settore privato

Pedopornografia

Il CNCPO agisce di propria iniziativa stilando relazioni sulle operazioni svolte e/o condotte dagli ISP (o dai fornitori di contenuti) su richiesta. Informa inoltre l'autorità giudiziaria qualora il caso sia di competenza nazionale.

Come detto al punto 6.2 i fornitori di servizi Internet hanno l'obbligo e la responsabilità di filtrare i contenuti indicati dall'autorità giudiziaria e dal CNCPO.

Se il materiale si trova su siti web italiani l'autorità giudiziaria dispone il sequestro del sito. Per i siti stranieri le procedure di filtraggio (liste nere) competono al CNCPO di concerto con l'autorità giudiziaria, che può chiederne il ripristino e pertanto renderli nuovamente visibili.

Nel caso di reti sociali o servizi ad ampia diffusione, sono utilizzate piattaforme dedicate per le agenzie di contrasto che spesso devono essere autorizzate dall'autorità giudiziaria nazionale.

Se il server è situato al di fuori dell'Italia viene avviata la procedura Notice & Takedown (Notifica e rimozione), se e quando possibile, attraverso il National Centre for Missing and Exploited Children - NCMEC (Centro nazionale per i minori scomparsi e sfruttati) poiché questo garantisce il sequestro e la trasmissione dei dati investigativi alle agenzie investigative competenti sul territorio. Le richieste della polizia possono essere trasformate in rogatorie; è possibile anche usare altri canali stabiliti in virtù della convenzione di Budapest sulla criminalità informatica.

Frodi con carte di credito

La cooperazione è assicurata attraverso lo scambio di informazioni ed esperienze tra industria, settore privato e agenzie di contrasto in relazione ad attacchi criminali contro strumenti di pagamento elettronici.

L'Italia si serve di una gamma di prodotti software e hardware per l'analisi dei dati ottenuti durante le indagini su operazioni fraudolente con o senza presenza fisica della carta.

La disamina quotidiana delle tecniche criminali usate nelle frodi con carte consente uno scambio costante di informazioni tra gli organismi interessati e, pertanto, i sistemi di difesa fisici e virtuali risultano potenziati ai fini del contrasto dell'accesso fraudolento a dati sensibili e le risposte investigative vengono adattate grazie a un'idonea attività di prevenzione basata sulle informazioni.

La cooperazione stretta e intensa con Europol e il progetto EMPACT "Cibercryme Card Fraud", in cui l'Italia è rappresentata dalla Polizia postale e delle comunicazioni, permette - attraverso riunioni periodiche - uno scambio efficace tra le agenzie di contrasto impegnate nel settore. In queste riunioni sono pianificate operazioni congiunte, esaminate proposte di soluzione a problemi legislativi, logistici o strumentali e, se necessario, sono organizzate riunioni operative per uno scambio diretto di opinioni tra gli investigatori coinvolti nelle indagini. Anche Eurojust partecipa a questo gruppo di lavoro, fungendo da collegamento tra autorità giudiziarie e autorità di contrasto degli Stati membri.

6.5 Conclusioni

- Il gruppo si compiace dell'istituzione del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (C.N.A.I.P.I.C.) e ne incoraggia l'ulteriore coordinamento e cooperazione con la CERT nazionale.
- Il gruppo è rimasto impressionato dal lavoro del CNCPO e dal monitoraggio puntuale dei siti web che ha portato alla creazione di liste nere in base alle quali i siti devono essere filtrati e bloccati.
- Il gruppo ha altresì constatato con soddisfazione che l'eliminazione e il blocco dei siti sono, secondo la legislazione nazionale, obbligatori per gli ISP e che, inoltre, si provvede a notificare alle autorità straniere i siti al di fuori dell'Italia con materiale che costituisce un abuso sui minori.
- Il gruppo si è anche compiaciuto della specifica legislazione italiana sul turismo sessuale e del fatto che vengano notificate all'ICSE le immagini rinvenute per ridurre la rivittimizzazione.

7 COOPERAZIONE INTERNAZIONALE

7.1 Cooperazione con le agenzie dell'UE

7.1.1 Requisiti formali per cooperare con Europol/EC3, Eurojust, ENISA

L'Italia vanta una buona cooperazione con Europol/EC3 a vari livelli.

A livello UE attraverso il Centro europeo per la lotta alla criminalità informatica (EC3)

- L'Italia partecipa alla priorità "Criminalità informatica"¹⁴ dell'EMPACT¹⁵ definita nel quadro del ciclo programmatico dell'UE per il periodo 2014-2017¹⁶. In linea con quest'ultimo, gli obiettivi strategici sono definiti nei MASP¹⁷ e gli obiettivi operativi sono attuati tramite OAP¹⁸.
- L'Italia è associata a tutti i punti focali dedicati alla criminalità informatica, che sono progetti operativi sviluppati da Europol/EC3 a sostegno delle indagini degli Stati membri dell'UE e di terzi.

¹⁴ Obiettivo: lottare contro i reati informatici perpetrati da gruppi della criminalità organizzata e che generano ingenti profitti illegali come la frode on-line e la frode con carte di pagamento, i reati informatici che provocano gravi danni alle vittime come lo sfruttamento sessuale di minori, e gli attacchi informatici che colpiscono le infrastrutture critiche e i sistemi informativi dell'UE.

¹⁵ Piattaforma multidisciplinare europea di lotta alle minacce della criminalità.

¹⁶ Conclusioni del Consiglio sull'elaborazione e attuazione di un ciclo programmatico dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale, doc. 15358/10.

¹⁷ Piani strategici pluriennali.

¹⁸ Piani d'azione operativi.

- L'Italia partecipa alla task force di azione congiunta contro la criminalità informatica (J-CAT) varata il 1° settembre 2013, che mira a rafforzare ulteriormente la lotta contro la criminalità informatica dentro e fuori dai confini dell'UE. Un "cyber agente" italiano della Polizia postale e delle comunicazioni ha partecipato alla J-CAT sin dall'inizio di questa iniziativa.
- Attualmente, tre dei 68 funzionari in servizio presso l'EC3 sono cittadini italiani, e di questi uno è agente temporaneo (punto focale Terminal) e due sono agenti contrattuali (uno nell'Outreach team e uno nello Strategy team).
- Dal 2013 l'Italia è membro dell'organo direttivo della task force dell'Unione europea sulla criminalità informatica (EUCTF) composta dai responsabili delle unità nazionali di criminalità informatica designate di tutti gli Stati membri dell'UE e da Europol. L'EUCTF è un gruppo interforze costituito per consentire ai responsabili delle unità di criminalità informatica, con la partecipazione di Europol, della Commissione europea, della CEPOL e di Eurojust, e con INTERPOL, Norvegia, Svizzera e Islanda in qualità di osservatori, di discutere le questioni strategiche ed operative legate alle indagini e azioni penali contro la criminalità informatica dentro e fuori dai confini dell'UE.
- L'Italia partecipa alla coalizione europea contro la criminalità informatica finanziaria (EFC) istituita per promuovere le relazioni tra i servizi di contrasto e il settore finanziario nella lotta allo sfruttamento sessuale commerciale di minori on-line.
- OF2CEN dell'UE - Tra il 2010 e il 2013 la Polizia postale e delle comunicazioni ha portato a buon fine un progetto finanziato dall'UE (OF2CEN) per la creazione di una piattaforma di scambio di informazioni per le banche e i servizi di contrasto ai fini della lotta contro i reati informatici e le frodi on-line. Sulla scia di tale successo, è in atto un nuovo progetto volto ad estendere la portata del precedente OF2CEN a livello europeo, con l'obiettivo di rafforzare la cooperazione tra tutte le banche e tutti i servizi di contrasto europei.

Attacchi informatici

Partecipazione dell'Italia alla sottopriorità "Attacchi informatici" dell'EMPACT

L'Italia partecipa alla priorità G3 in materia di criminalità, "Attacchi informatici", nell'ambito delle seguenti azioni operative:

- elaborazione della valutazione della minaccia della criminalità organizzata su Internet (iOCTA 2015);
- individuazione di importanti minacce informatiche, attuali ed emergenti, che gravano su due o più Stati membri;
- sviluppo di un insieme comune di strumenti per colpire i principali distributori, sistemi e servizi di malware che interessano due o più Stati membri ed interromperne le attività;
- individuazione di obiettivi di alto valore che si prestano ad una risposta collaborativa con la partecipazione di due o più Stati membri;
- consolidamento del gruppo di coordinamento delle ricerche operative su Internet dell'Unione europea istituito nel 2014;
- raccolta di contributi malware relativi agli attacchi attuali presso il settore bancario nell'ambito dell'EC3 e loro immissione nel sistema di analisi dei malware di Europol (EMAS). Raccolta di contributi attraverso la J-CAT e altri canali Europol;
- individuazione degli obiettivi e coordinamento degli arresti di gruppi o individui dediti alla criminalità informatica a più basso livello (che si avvalgono dei servizi di gruppi di criminalità organizzata dediti alla criminalità informatica);
- sostegno agli Stati membri e ai partner operativi per rendere le tecniche di riciclaggio di denaro e di recupero dei beni parte integrante delle azioni operative dell'OAP e sfruttare al massimo le piste delle indagini finanziarie contro obiettivi individuati nelle azioni operative dell'OAP;
- scambio di migliori prassi ed esperienze nella cooperazione con paesi terzi, indirettamente tramite l'EUCTF (azione operativa 3.1);
- creazione di una tassonomia comune per la criminalità informatica tra i servizi di contrasto degli Stati membri e le CERT;
- creazione e/o adozione di un formato comune per la segnalazione di casi di criminalità informatica all'EC3 di Europol, ai servizi di contrasto e alle CERT;
- creazione di un software automatico di analisi delle statistiche relative ai casi di criminalità informatica segnalati, indirettamente tramite l'EUCTF;
- sviluppo e attuazione di una soluzione per la verifica incrociata di dati e la risoluzione di conflitti di dati pseudonomizzati e per l'eliminazione delle interferenze indesiderate fra i dati (data deconfliction).

Partecipazione dell'Italia al punto focale CYBORG¹⁹

L'Italia partecipa al punto focale Cyborg. Nella maggior parte delle recenti operazioni riguardanti attacchi con malware e rimozioni di botnet, l'Italia ha svolto un ruolo importante o in qualità di paese colpito o perché parte dell'infrastruttura criminale era situata nel suo territorio. Europol ha ricevuto un puntuale sostegno operativo in tutte le operazioni e, quando necessario, la Polizia di Stato ha messo a disposizione agenti sul posto. L'eccellente cooperazione con i Carabinieri è assicurata dalla presenza di un rappresentante nell'organo direttivo dell'EUCTF.

Frodi nei pagamenti

Partecipazione dell'Italia alla sottopriorità "Frodi con carte di pagamento" dell'EMPACT

L'Italia partecipa alle seguenti azioni operative:

- incremento della partecipazione e dei contributi alla piattaforma di esperti Europol (EPE SPACE);
- svolgimento di attività di formazione e scambio di migliori prassi in materia di frodi con carte di credito;
- miglioramento della conoscenza dell'impatto delle frodi con carte di credito a livello europeo e nazionale;
- inclusione delle frodi con mezzi di pagamento diversi dai contanti nel programma degli eventi di sensibilizzazione rivolti ai cittadini;
- incremento dell'interazione con il settore privato a livello nazionale per aiutare indagini nazionali/internazionali;
- innalzamento del livello di scambio di informazioni tra Europol e gli Stati membri;
- agevolazione dello scambio di informazioni nei paesi dell'Unione europea, compresi i paesi non appartenenti all'UE;

¹⁹ Questo punto focale mira a prevenire e contrastare le forme di criminalità rientranti nel mandato di Europol associate alla criminalità organizzata legata ad Internet e alle TIC (tecnologie dell'informazione e della comunicazione). Più in particolare, sarà incentrato sui reati definiti agli articoli da 2 a 8 della Convenzione sulla criminalità informatica.

- organizzazione e coordinamento di un'azione negli aeroporti volta a colpire i truffatori on-line che effettuano e agevolano l'acquisto di biglietti aerei.

Partecipazione dell'Italia al punto focale TERMINAL²⁰

L'Italia partecipa al punto focale Terminal svolgendo un ruolo in numerose operazioni internazionali, compresa la giornata d'azione "Aeroporti" (Airport Action Day).

Sfruttamento sessuale di minori

Partecipazione dell'Italia al punto focale TWINS²¹

L'Italia partecipa al punto focale Twins. Si rileva un buon livello di cooperazione e partecipazione alle attività operative. La cooperazione ha luogo principalmente con la Polizia postale²².

²⁰ Questo punto focale mira a colpire le reti di individui dediti ad attività fraudolente legate a frodi con carte di pagamento.

²¹ Questo punto focale ha ad oggetto le reti pedopornografiche su Internet: mira a colpire le reti criminali dedite alla produzione, alla vendita e alla distribuzione di materiale relativo ad abusi sui minori.

²² Successivamente alla visita di valutazione, le autorità italiane hanno fornito le seguenti informazioni.

Per quanto riguarda le attività di contrasto volte a combattere i reati sessuali su minori on-line in un'ottica di rafforzamento degli obiettivi della "Global Alliance", come già indicato nel documento di valutazione riteniamo utile esaminare attentamente la questione delle indagini sulle *darknet*, ben conosciute per la loro capacità di consentire all'utente di mantenere l'anonimato durante la navigazione su Internet. Tali attività d'indagine, che vedono la piena partecipazione del Centro nazionale per il contrasto alla pedopornografia online (CNCPO), rappresentano la sfida attuale e una priorità per le indagini in detto settore criminale e per questo motivo sono state svolte congiuntamente e nel quadro della cooperazione internazionale tra servizi di contrasto, ad esempio il punto focale Twins/Centro per la lotta alla criminalità informatica EC3 di Europol.

Sono stati sviluppati vari progetti tesi a cercare soluzioni investigative e forensi in grado di migliorare le tecniche d'indagine necessarie per contrastare il dilagare dei sistemi di anonimizzazione nonché i canali utilizzati per la moneta virtuale "bitcoin", già colpiti dal Centro nazionale per il contrasto alla pedopornografia online (CNCPO) con un ingente numero di sequestri di portafogli virtuali. I risultati di tali attività di ricerca potrebbero essere disponibili prossimamente e condivisi nel quadro dei progetti EMPACT, oltre che formare oggetto di attività di formazione per investigatori a livello europeo.

7.1.2 Valutazione della cooperazione con Europol/EC3, Eurojust, ENISA

L'Italia valuta questa cooperazione positivamente. Il gruppo è stato informato del fatto che l'Italia esplora anche modi per rafforzare ulteriormente questa cooperazione, ad esempio nelle relazioni con Stati terzi²³.

7.1.3 Risultati operativi delle squadre investigative comuni e delle pattuglie digitali

È attualmente in corso un'indagine svolta in cooperazione con Europol che fornirà ad altri servizi di polizia di paesi UE informazioni su casi di rilevanza penale.

7.2 Cooperazione tra le autorità italiane e Interpol

La Divisione III (Interpol) del Servizio per la cooperazione internazionale di polizia fa parte di un efficace sistema di lotta contro la cosiddetta "criminalità informatica".

L'Ufficio centrale nazionale Interpol dell'Italia fa parte del Servizio per la cooperazione internazionale di polizia (SCIP). Lo SCIP fa parte della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza e coordina le indagini e operazioni che richiedono assistenza internazionale. È diretto, secondo un sistema di rotazione, da un alto funzionario della Polizia di Stato, dei Carabinieri o della Guardia di Finanza.

L'Italia sostiene inoltre la rete di ufficiali di collegamento, la quale:

- consente l'acquisizione di conoscenze sul fenomeno criminale comparando le diverse leggi di altri paesi;
- fornisce regolari aggiornamenti sui "modi operandi" e sulle tecniche utilizzati all'estero per combattere il fenomeno;
- individua rapidamente punti di riferimento esteri al fine di promuovere forme più dirette di cooperazione anche al di fuori dei consueti canali di polizia.

²³ In seguito alla visita di valutazione, l'Italia ha informato il gruppo del fatto che la Polizia postale e delle comunicazioni è ora l'unico punto di contatto per l'IRU di Europol.

Altre iniziative

- Il Servizio per la cooperazione internazionale di polizia è un servizio interforze per la cooperazione internazionale operativa di polizia. Comprende anche l'Ufficio centrale nazionale Interpol, l'Unità nazionale Europol italiana e la Divisione SIRENE.
- L'Italia partecipa anche al gruppo del G8 per la lotta alla criminalità ad alta tecnologia (Gruppo Roma-Lione).

7.3 Cooperazione con Stati terzi

Come molti altri Stati membri, l'Italia ritiene che la cooperazione con i paesi terzi sia variabile e ha incontrato difficoltà nel ricevere tempestivamente da alcuni Stati terzi, come gli Stati Uniti, informazioni richieste a fini di indagine. Il gruppo è stato informato del fatto che l'Italia valuta la possibilità di fare un uso migliore di Europol/EC3 per i rapporti con Stati terzi nell'ambito di operazioni congiunte o al fine di avvicinare nuovi paesi partner suscettibili di contribuire ad un ampliamento della portata delle attività operative nel settore della criminalità informatica.

7.4 Cooperazione con il settore privato

Le disposizioni contenute nel codice di procedura penale non contemplano il coinvolgimento del settore privato. Consulenti tecnici, spesso del settore privato, possono essere nominati nel quadro di procedimenti penali particolarmente complessi in relazione ad indagini sulla criminalità informatica (ad esempio, per analizzare il contenuto di un disco rigido sequestrato).

I gruppi di lavoro costituiti presso la Polizia postale e delle comunicazioni spesso vedono la partecipazione del settore privato. La partecipazione a tali gruppi dipende, tuttavia, dalla volontà dei singoli fornitori di servizi (fornitori di servizi Internet, compagnie telefoniche, banche, ecc.).

Gli articoli da 14 a 16 del decreto legislativo n. 70/2003 (recante attuazione della direttiva europea sul commercio elettronico) disciplinano la responsabilità dei cosiddetti prestatori intermediari operando una distinzione tra:

- attività di semplice trasporto dati (mere conduit);
- memorizzazione intermedia e temporanea di informazioni effettuata allo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta (caching);
- memorizzazione di informazioni fornite da un destinatario del servizio, compresa la messa a disposizione di uno spazio di memorizzazione su un server per siti e pagine web (hosting).

Tuttavia, tali disposizioni si applicano principalmente in un contesto di diritto civile. In un contesto di diritto penale, la responsabilità dei fornitori di servizi Internet può essere ricavata dai principi generali in materia di concorso nel reato (articolo 110 del codice penale) o di mancato impedimento di un evento (laddove la legge preveda espressamente l'obbligo di intervenire per impedire l'evento; articolo 40, secondo comma, del codice penale). In base alla legislazione italiana, le richieste di bloccare l'accesso a siti web o di rimuovere contenuti da siti web sono presentate al giudice per le indagini preliminari, che provvede mediante specifico decreto (sequestro preventivo ai sensi dell'articolo 321 del codice di procedura penale). Nel campo della prevenzione del terrorismo, la legge n. 43 del 17 aprile 2015 (che converte in legge il decreto-legge sul contrasto al terrorismo) ha introdotto un meccanismo più rapido per l'inibizione/rimozione di contenuti. Più in particolare:

- il Ministero dell'interno fornisce un elenco aggiornato dei siti utilizzati per le attività e le condotte di cui agli articoli 270-bis e 270-sexies del codice penale nel quale confluiscono le segnalazioni effettuate dagli organi di polizia giudiziaria;
- i fornitori di connettività, su richiesta dell'autorità giudiziaria procedente, devono inibire l'accesso ai siti inseriti nell'elenco secondo le modalità, i tempi e le soluzioni tecniche individuati e definiti per legge;
- quando si procede per delitti commessi con finalità di terrorismo e sussistono concreti elementi che consentano di ritenere che alcuno compia dette attività per via telematica, il pubblico ministero può ordinare la rimozione del contenuto ad esse relativo. In caso di contenuti generati dagli utenti e ospitati su piattaforme riconducibili a soggetti terzi, è disposta la rimozione dei soli specifici contenuti illeciti;

- i destinatari devono adempiere all'ordine immediatamente e comunque non oltre 48 ore dal ricevimento della notifica. In caso di mancato adempimento, si dispone l'interdizione dell'accesso al dominio Internet nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale.

7.5 Strumenti di cooperazione internazionale

7.5.1 Assistenza giudiziaria reciproca

Per la criminalità informatica non vi sono norme specifiche di assistenza giudiziaria reciproca. Si applicano le convenzioni internazionali, bilaterali o multilaterali di carattere generale o, se i necessari requisiti preliminari sono soddisfatti, le convenzioni relative a reati specifici (ossia la convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale del 2000).

L'Italia non ha ratificato la convenzione relativa all'assistenza giudiziaria in materia penale del 2000. Essa ha tuttavia fatto presente che la Camera dei deputati ha ora approvato un progetto di legge delega relativa al recepimento di tale convenzione che è attualmente all'esame del Senato; al fine di accelerare il recepimento, il ministro della giustizia ha formalizzato la nomina di una commissione tecnica incaricata di elaborare le relative norme. Alla stessa commissione è stato anche affidato il compito di elaborare un insieme di norme finalizzate al recepimento della direttiva relativa all'ordine europeo di indagine penale, recepimento per il quale sono stati già conferiti poteri al governo. È dunque molto probabile che nel corso di quest'anno si proceda al recepimento della direttiva relativa all'ordine europeo di indagine penale e alla ratifica della convenzione relativa all'assistenza giudiziaria in materia penale del 2000.

Nel frattempo si applicano (altre) norme generali, comprese le pertinenti convenzioni internazionali (poiché la criminalità informatica non è disciplinata da alcuna legislazione specifica). Ad esempio la convenzione europea di assistenza giudiziaria in materia penale del 1959 prevede che durante le indagini, o nei casi urgenti, una richiesta possa essere inviata direttamente dall'autorità giudiziaria italiana (procedura attiva) o all'autorità giudiziaria italiana (procedura passiva), che è altresì competente a decidere su tali richieste.

Per gli Stati che, come l'Italia, aderiscono alla convenzione Schengen è inoltre possibile inviare direttamente le richieste alle autorità giudiziarie che sono anche competenti a decidere sulle richieste di assistenza giudiziaria reciproca.

In altri casi una richiesta di assistenza giudiziaria reciproca può essere inviata attraverso l'autorità centrale per la cooperazione giudiziaria internazionale (ministero della giustizia). Nei casi non specificamente previsti da accordi, ovvero se così indicato negli accordi, il canale di comunicazione utilizzato è quello diplomatico, qualora non si segua il canale diretto o il tramite delle autorità centrali.

Ove possibile l'Italia stabilisce anche contatti diretti informali con le forze di polizia o le autorità giudiziarie in altre giurisdizioni. Sono utilizzabili molteplici canali (telefono, mail, teleconferenze, visite personali, ecc.).

Molte di richieste di assistenza giudiziaria reciproca sono inviate agli Stati Uniti (ad esempio per conoscere i contenuti di un conto Facebook). In questo caso ci si avvale del trattato bilaterale vigente tra Italia e Stati Uniti, integrato dal trattato Unione europea-Stati Uniti. A volte gli Stati Uniti respingono una richiesta a causa dell'assenza della cosiddetta "probabile causa" ovvero perché il caso è considerato di rilevanza minima.

7.5.2 Strumenti di riconoscimento reciproco

L'Italia ha recepito la decisione quadro 2002/584 relativa al mandato d'arresto europeo e la decisione quadro 2008/909 sull'esecuzione delle pene detentive. È pertanto possibile attuare il riconoscimento reciproco delle sentenze e delle misure privative della libertà personale al fine di dare direttamente esecuzione a una sentenza o alla consegna di una persona ricercata.

7.5.3 Consegna/estradizione

Relativamente al mandato d'arresto europeo (procedura passiva), tutti i reati informatici possono dar luogo a consegna in forza della normativa in questione, senza verifica della doppia incriminazione. La pertinente legislazione italiana prevede che ogni reato informatico sanzionabile con una pena privativa della libertà personale della durata massima pari o superiore a tre anni può dar luogo a consegna.

Un mandato d'arresto europeo può dare luogo a consegna purché sia stata inflitta una pena privativa della libertà personale non inferiore a quattro mesi (mandato d'arresto europeo emesso ai fini dell'esecuzione di una pena), o se il reato è sanzionabile con una pena privativa della libertà personale della durata massima non inferiore a dodici mesi (mandato d'arresto europeo emesso al fine di perseguire penalmente) (articolo 7, commi 3 e 4 della legge 69/2005).

Quanto alla procedura attiva del mandato d'arresto europeo, per rispettare il principio di proporzionalità è necessario che il reato informatico sia stato sanzionato con una pena privativa della libertà personale superiore a dodici mesi (mandato d'arresto europeo emesso ai fini dell'esecuzione di una pena) o che il mandato d'arresto sia stato emesso per un reato informatico sanzionabile con una pena privativa della libertà personale non inferiore nel massimo a cinque anni (mandato d'arresto europeo emesso al fine di perseguire penalmente).

Per l'estradizione passiva si applicano le convenzioni internazionali vigenti. Nel caso di estradizione attiva il ministro della giustizia, conformemente al principio di proporzionalità e fatta eccezione per casi specifici, presenta una richiesta di estradizione soltanto per condanne superiori a quattro anni di pena privativa della libertà (estradizione ai fini dell'esecuzione di una pena), o se è stato emesso un mandato d'arresto per un reato informatico sanzionabile con una pena privativa della libertà non inferiore nel massimo a cinque anni (estradizione al fine di perseguire penalmente).

Si veda la tabella seguente:

1) Frode informatica;				
Reato	Pena		Consegna	Estrad.
	Min	Max		
Articolo 640-ter. ("Frode informatica") Phishing o Dialer				
Comune	6 mesi di reclusione	3 anni di reclusione	Solo con ord. esec.	SÌ
Aggravato	1 anno	5 anni	SÌ	SÌ
Articolo 640 ("Truffa")	1 anno	5 anni	SÌ	SÌ

RESTREINT UE/EU RESTRICTED

2) Falsità materiale;				
Reato	Pena		Consegna	Estrad.
	Min	Max		
Articolo 491-bis, ("Documenti informatici")				
Compresso dal privato	8 mesi	4 anni	Solo con ord. esec.	Sì
Compresso dal pubblico ufficiale	1 anno	6 anni	Sì	Sì
	1 anno	5 anni	Sì	Sì

3) Integrità dei dati e dei sistemi informatici;				
Reato	Pena		Consegna	Estrad.
	Min	Max		
Articolo 635-bis ("Danneggiamento di sistemi informatici e telematici")	6 mesi	3 anni	Solo con ord. esec.	Sì
Articolo 420 ("Attentato a impianti di pubblica utilità")	1 anno	4 anni	Solo con ord. esec.	Sì
Articolo 392 ("Esercizio arbitrario delle proprie ragioni con violenza sulle cose") In relazione ai sistemi informatici comprende l'alterazione, la modifica o la cancellazione in tutto o in parte di un programma al fine di impedirne il regolare funzionamento.	Pena Multa		NO	NO
Articolo 615-quinquies ("Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico")	fino a 2 anni		Solo con ord. esec.	Sì

4) Riservatezza dei dati e delle comunicazioni informatiche.				
Reato	Pena		Consegna	Estrad.
	Min	Max		
Articolo 615-ter ("Accesso abusivo ad un sistema informatico o telematico")				
Comune	fino a 3 anni		Solo con ord. esec.	Sì
Casi specifici previsti dall'articolo	1 anno	5 anni	Sì	Sì

RESTREINT UE/EU RESTRICTED

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico. Casi generali	1 anno		Sì	Sì
Casi specifici	3 anni	5 anni 8 anni		
Articolo 615-quater ("Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici")	fino a 1 anno		Solo con ord. eseg.	Sì
Articolo 621 ("Rivelazione del contenuto di documenti segreti")	fino a 3 anni		Solo con ord. eseg.	Sì
Articolo 617-quater ("Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche")				
Comune	6 mesi	4 anni	Solo con ord. eseg.	Sì
Casi specifici previsti dall'articolo	1 anno	5 anni	Sì	Sì
Articolo 617-quinquies ("Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche")	1 anno	4 anni	Solo con ord. eseg.	Sì
Articolo 617-sexies ("Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche")	1 anno	4 anni	Solo con ord. eseg.	Sì

Per la criminalità informatica non vi sono norme specifiche. Pertanto si applicano le norme generali.

Nei casi di estradizione attiva il ministro della giustizia presenta direttamente la richiesta, anche su istanza dell'autorità giudiziaria. La richiesta può essere trasmessa direttamente all'autorità centrale straniera o per il tramite del ministero degli affari esterni e della cooperazione internazionale (in base alle convenzioni internazionali vigenti).

Nei casi di estradizione passiva la richiesta è presentata, direttamente o attraverso i canali diplomatici, al ministro italiano della giustizia. La competenza decisionale sull'extradizione passiva incombe al ministro della giustizia, previo parere favorevole all'extradizione dell'organo giurisdizionale competente. Se quest'ultimo ritiene che non sia possibile concedere l'extradizione, il ministro della giustizia non può concederla. Per contro se l'organo giurisdizionale ritiene che possa essere concessa, la decisione di concederla o di rifiutarla è a discrezione del ministro.

Consegna per mezzo del cosiddetto mandato d'arresto europeo passivo

Un mandato d'arresto europeo emesso da un'autorità giudiziaria straniera è inviato, per il tramite del ministero della giustizia, alla Corte d'appello giurisdizionalmente competente (in base al luogo in cui si trova la persona di cui è richiesta la consegna).

L'emissione di un mandato d'arresto europeo spetta al giudice per le indagini preliminari (GIP) che ha emesso un'ordinanza di custodia cautelare, o al pubblico ministero che ha emesso l'ordine di esecuzione della pena detentiva o della misura di sicurezza definitiva prevista dalla sentenza. L'invio della richiesta allo Stato estero rientra nella competenza del ministero della giustizia.

I canali di comunicazione usati sono SIRENE e SIS II per il mandato d'arresto europeo e INTERPOL (I 24/7). Può essere inoltre consultata la banca dati ASF.

Il mandato d'arresto europeo, passivo o attivo, comporta sempre l'arresto temporaneo ed è in genere eseguito entro i limiti stabiliti dalla decisione quadro (90 giorni al massimo) una volta che la persona ricercata è stata localizzata. Il tempo medio di esecuzione è comunque più breve.

Le richieste di estradizione, passive e attive, sono in genere corredate di una richiesta di arresto provvisorio. Le procedure di estradizione, passive e attive, richiedono generalmente più tempo.

Ad ogni emissione di mandato d'arresto europeo, viene seguita la procedura standard per i paesi che non aderiscono alla convenzione Schengen, i cosiddetti paesi associati (Norvegia e Islanda comprese). In tal caso si applica la procedura di estradizione.

7.6 Conclusioni

- L'Italia non ha ratificato la convenzione relativa all'assistenza giudiziaria in materia penale del 2000 e, pertanto, per agevolare l'assistenza giudiziaria reciproca fa riferimento a strumenti precedenti, ad esempio la convenzione del 1959 e la convenzione Schengen. Poiché la convenzione del 2000 ha semplificato le procedure di assistenza giudiziaria reciproca secondo il gruppo sarebbe estremamente utile per l'Italia ratificarla.
- L'Italia non partecipa alla sottopriorità sullo sfruttamento sessuale dei minori dell'EMPACT 2015: dovrebbe essere incoraggiata a farlo²⁴.

DECLASSIFIED

²⁴ In seguito alla visita di valutazione, l'Italia ha informato il gruppo del fatto che ora partecipa alla sottopriorità sullo sfruttamento sessuale dei minori.

8 FORMAZIONE, SENSIBILIZZAZIONE E PREVENZIONE

8.1 Formazione specifica

Formazione per la magistratura: la Scuola superiore della magistratura organizza corsi sulla criminalità informatica, sotto forma sia di formazione iniziale - per i magistrati in tirocinio - sia di formazione permanente - per i magistrati ordinari. Parte della formazione prevede un modulo dedicato ai protocolli di indagine e di analisi incentrati sugli aspetti principali della criminalità informatica e dei reati collegati alle tecnologie telematiche, nonché il corso P15089 di formazione permanente dedicato al diritto penale del web, un modulo di apprendimento a distanza per il 2014. Inoltre è impartita una formazione specifica ai funzionari impiegati in attività operative nelle rispettive unità.

Formazione per la polizia: per la Polizia postale e delle comunicazioni è prevista una formazione di base, unitamente a studi regolari di livello universitario per i gradi direttivi medi e superiori e parte dell'istruzione standard per gli agenti di polizia. Per tutte le unità specializzate nella criminalità informatica sono inoltre previsti corsi di aggiornamento. La durata dei corsi di formazione dipende dall'anzianità di servizio degli agenti, ossia sei settimane se l'agente è in servizio da meno di tre anni, e una settimana se è in servizio da più di tre anni. La formazione è impartita da formatori interni.

Inoltre la Scuola di polizia di Cesena ha messo a punto un corso di tre giorni per la formazione dei formatori, con l'ausilio dell'FBI e dei servizi di intelligence statunitensi. La scuola superiore di Polizia di Roma ha iniziato a impartire una formazione per l'alta dirigenza, che prevede un modulo sulla criminalità informatica e che si colloca tra i corsi di base e quelli di aggiornamento.

8.2 Sensibilizzazione e prevenzione

Negli ultimi anni la Polizia postale e delle comunicazioni ha realizzato progetti di informazione sulla prevenzione dei rischi di Internet per i minori e gli educatori, in cooperazione con soggetti pubblici e privati impegnati nella protezione dei minori.

La campagna, che è arrivata al quinto anno, è rivolta ai minori di età compresa tra i 7 e 18 anni. Solo lo scorso anno ha interessato 400.000 studenti: si tratta quindi di uno strumento ad ampia diffusione. Prevede sessioni dedicate con insegnanti e genitori in cui sono sottolineati rischi e vantaggi dell'uso di Internet.

Dal 2013 la Polizia postale e delle comunicazioni sta anche portando avanti una campagna d'informazione itinerante con presentazioni effettuate da membri della polizia, del ministero dell'istruzione, da psicologi e da privati. All'evento partecipano anche celebrità e noti sportivi per aumentare l'attrattiva a beneficio del pubblico bersaglio e vengono inoltre presentate storie vere di vittime di reati. Nell'ambito della campagna per le scuole è stato inoltre realizzato uno spettacolo teatrale in cui veniva descritto un caso autentico di cyberbullismo che ha condotto al suicidio di un diciassettenne.

Anche il Garante della protezione dei dati è impegnato dal 2005 in campagne di sensibilizzazione nelle scuole per sensibilizzare i minori ai rischi insiti nella condivisione dei dati su Internet.

8.2.1 Legislazione/politica e altre misure nazionali

8.2.2 Partenariato pubblico-privato (PPP)

Le autorità italiane sono efficacemente sostenute dal settore privato nelle campagne di sensibilizzazione pubblica, ad esempio con contributi finanziari al centro stampa dell'evento itinerante nonché alla partecipazione di celebrità e noti sportivi.

8.3 Conclusioni

- Il gruppo è stato impressionato dal livello di formazione impartito agli operatori, in particolare la polizia impegnata nella lotta alla criminalità informatica; ritiene tuttavia che possa essere prevista maggiore formazione per i magistrati, parallelamente a quella per gli agenti di polizia almeno a livello di specifici distretti, creando in tal modo sinergie positive tra operatori della giustizia e agenti di polizia e, di conseguenza, realizzando un'autentica collaborazione in rete. Un altro contributo efficace e positivo per ravvicinare magistrati, CERT e Polizia potrebbe derivare dall'uso di una tassonomia comune, sulla falsariga di quella usata dalle CERS europee e da EC3 (v. allegato della presente relazione).
- Sarebbe utile che l'Italia si avvallesse maggiormente delle opportunità offerte da Europol a tal fine; un certo numero di agenti di polizia almeno a livello di specifici distretti, potrebbe così partecipare alla piattaforma SPACE dell'EC3 di Europol e iscriversi ai corsi ECTEC e CEPOL. Andrebbe altresì valutata la possibilità di dare l'accesso a corsi di formazione esterna, ossia corsi di terzo livello per gli operatori impegnati nella lotta alla criminalità informatica.
- Il gruppo è rimasto impressionato dalle campagne di sensibilizzazione del pubblico realizzate dalla Polizia postale e delle comunicazioni e dal Garante. Ha rilevato tuttavia la possibilità di doppioni e suggerirebbe un miglior coordinamento tra le due autorità, ad esempio nell'ambito della strategia nazionale."

9 OSSERVAZIONI FINALI E RACCOMANDAZIONI

9.1. Suggerimenti dell'Italia

Le autorità italiane ritengono che la legislazione comune sulla conservazione dei dati debba essere messa a punto con l'obiettivo di acquisire i dati direttamente dai paesi partner nel quadro delle indagini sulla criminalità informatica e di introdurre misure di sicurezza più stringenti per le istituzioni private (ex Documenti programmatici).

9.2 Raccomandazioni

Per quanto riguarda l'attuazione pratica e il funzionamento della decisione quadro e delle direttive, il gruppo di esperti impegnato nella valutazione dell'Italia ha potuto esaminare in modo soddisfacente il sistema di tale paese.

L'Italia dovrebbe verificare il seguito riservato alle raccomandazioni formulate nella presente relazioni diciotto mesi dopo la valutazione e riferire sui progressi al gruppo GENVAL.

Il gruppo di valutazione ritiene opportuno sottoporre all'attenzione delle autorità italiane alcuni suggerimenti. Inoltre, in base alle diverse migliori prassi, vengono formulate raccomandazioni correlate anche all'UE e alle sue istituzioni ed agenzie, in particolare Europol.

9.2.1 Raccomandazioni all'Italia

- 1) Il gruppo ha constatato con soddisfazione che l'Italia dispone di una strategia in materia di criminalità informatica, il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", e di indirizzi operativi a corredo; ritiene tuttavia che la strategia debba essere più mirata e contenere obiettivi specifici e misurabili cosicché risulti chiaro il ruolo di ogni soggetto implicato nella strategia stessa. In tal modo sarebbe anche garantito un miglior coordinamento dei ruoli dei diversi soggetti evitando duplicazione degli sforzi. Sarebbe inoltre utile disporre della stima dei costi di ciascuna azione.
- 2) Relativamente all'approvazione di tecniche investigative speciali, pur rilevando l'esistenza di linee guida regionali sull'uso di queste misure, al gruppo è stato riferito che vi sono differenze in tali linee guida. Il gruppo raccomanda che l'Italia consideri di affrontare quest'incoerenza per migliorare la capacità investigativa della polizia riguardo alla criminalità informatica.
- 3) L'Italia sembra dotata di un consistente quadro legislativo ma al gruppo è stato riferito che il trattamento del denaro virtuale non è disciplinato da disposizioni specifiche. Si invita l'Italia a considerare se la legislazione o le procedure giuridiche possano o debbano essere adattate per affrontare meglio la questione del denaro virtuale.

- 4) Sviluppare la cooperazione pubblico-privato rappresenta una priorità fondamentale della strategia. Il gruppo raccomanda che l'Italia adotti ulteriori misure per promuovere questa cooperazione i) ricorrendo all'esperienza e alle competenze dei fornitori di servizi/esperti dell'industria, ii) migliorando la cooperazione con il settore finanziario tramite l'ampliamento del progetto OF2CEN²⁵, e iii) vagliando se la segnalazione obbligatoria da parte del settore privato di attacchi informatici possa essere utile.
- 5) È fortemente raccomandato che l'Italia porti a termine la ratifica della convenzione relativa all'assistenza giudiziaria in materia penale del 2000 per rafforzare l'assistenza giudiziaria tra Stati membri. Ne deriverebbe una maggiore capacità di affrontare efficacemente la criminalità informatica e una migliore cooperazione con altri Stati membri. Ne beneficerebbero altresì le indagini penali con elementi transfrontalieri.

²⁵ Successivamente alla visita di valutazione, le autorità italiane hanno osservato che, per quanto riguarda il settore della criminalità informatica finanziaria, nel periodo 2016-2017 l'Italia si concentrerà sul rafforzamento dei partenariati pubblico-privato in relazione al progetto OF2CEN dell'UE. La Polizia postale e delle comunicazioni italiana è a capo del progetto OF2CEN dell'UE, al quale partecipano le autorità di contrasto di Ungheria, Francia e Spagna e che prevede la partecipazione attiva della Federazione bancaria europea, che fornirà sostegno e divulgherà l'iniziativa tra le sue banche associate. Nel contempo, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, in qualità di punto focale della lotta dell'UE contro la criminalità informatica, contribuirà a coinvolgere nel progetto Stati membri in tutta l'UE e si avvantaggerà di una migliore capacità di individuare nuove tendenze in materia di criminalità. Per quanto riguarda la partecipazione all'attuale ciclo programmatico (2014-2017), la Polizia postale e delle comunicazioni ha aderito ad entrambe le priorità relative a "Attacchi informatici" e "Frodi con carte": in particolare, per la prima volta, nell'ambito del piano d'azione operativo 2016 (priorità "Attacchi informatici"), l'Italia è responsabile di azione per l'azione operativa 1.3, relativa ai "Prestaconto", che consiste in un piano operativo PPP finalizzato a raccogliere e condividere informazioni sulla criminalità informatica finanziaria.

- 6) Si raccomanda inoltre all'Italia di diffondere maggiore consapevolezza tra gli operatori riguardo all'assistenza giudiziaria reciproca in generale, segnatamente ragguagliandoli sui canali più appropriati per l'emissione di rogatorie e la richiesta di informazioni sulla criminalità informatica ad autorità di contrasto e autorità giudiziarie straniere. È evidente che agli operatori non è chiaro dove devono trasmettere i casi e quali sono le persone da contattare. Al riguardo si raccomanda che l'Italia rafforzi la cooperazione con Europol ed Eurojust.
- 7) Si raccomanda all'Italia di integrare i programmi di formazione interni sulla criminalità informatica valendosi delle opportunità formative offerte dagli organismi dell'UE (ad esempio EC3, ECTEG e CEPOL) e di quelle offerte da istituzioni accademiche e società private.²⁶ In particolare il gruppo ritiene che possa essere potenziata la formazione per la magistratura.
- 8) Il gruppo raccomanda di migliorare la raccolta e la collazione di statistiche, sia a livello di applicazione della legge sia a quello dell'azione penale. In tal modo si contribuirebbe a migliorare, tra l'altro, l'allocazione delle risorse, il raffronto dei casi e la classificazione dei reati in base a categorie quali il modus operandi e le attività criminali.

9.2.2 Raccomandazioni all'Unione europea, alle sue istituzioni e agli altri Stati membri

- 1) Il gruppo ritiene che il modello italiano di registrazione dei dati di identificazione personale al punto vendita delle carte SIM sia una prassi che dovrebbe essere adottata, ove possibile, dagli altri Stati membri. Questa prassi fornirebbe alle autorità di contrasto informazioni utili che potrebbero essere di ausilio nelle indagini su una serie di attività criminali quali la criminalità informatica, la criminalità organizzata e il terrorismo.

²⁶ Successivamente alla visita di valutazione, le autorità italiane hanno informato il gruppo che l'Italia sta integrando la formazione interna avvalendosi anche di opportunità offerte da agenzie dell'UE come la CEPOL. Per il 2016 l'Italia parteciperà al programma di scambi della CEPOL, con particolare attenzione per i settori relativi agli attacchi informatici e alle frodi con carte. Le autorità italiane hanno altresì chiesto alla CEPOL di essere incluse in vari corsi.

- 2) Nelle raccomandazioni del gruppo viene espressa la necessità di un rinnovato sforzo europeo per affrontare la criminalità informatica. A livello dell'UE occorre prendere ulteriormente in esame questioni inerenti, tra l'altro, alla raccolta di prove elettroniche, alla competenza giurisdizionale, al miglioramento dell'assistenza giudiziaria reciproca e all'accesso ai dati conservati nella "nuvola".
- 3) Il gruppo raccomanda di considerare uno sviluppo della legislazione dell'UE che incarichi gli ISP di bloccare/rimuovere i siti web con contenuti fraudolenti. Nel sistema italiano questa prassi è già utilizzata con risultati soddisfacenti e potrebbe essere replicata nell'intera UE.

9.2.3 Raccomandazioni a Eurojust/Europol/ENISA

- 1) Il gruppo raccomanda a Eurojust di fornire informazioni agli Stati membri, mediante manuali utente/elenchi dei servizi, su come contattare le altre autorità per le diverse attività di assistenza giudiziaria reciproca in ogni Stato membro (ad esempio ricorrendo a taluni strumenti o procedure).
- 2) Eurojust ed Europol dovrebbero promuovere i servizi e le risorse da essi forniti agli Stati membri che possono migliorare la capacità nazionale in ordine all'assistenza giudiziaria reciproca.

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

Agenda dei lavori

Monday, 25 May 2015

Time to be defined

arrival at the Rome – Fiumicino Airport
transfer to the Hotel

Tuesday, 26 May 2015

09:00

arrival at Polo Tuscolano

09:15

welcome to the SGAE by Dr. Roberto Sgalla
Central Director of Highway, Railway, Postal
and Communication and Special Units of State
Police

10:00 to 12:30:

Postal and Communication Police Service

- introduction by Mr. Antonio Apruzzese Director of Postal and Communication Police Service
- general presentation of the Italian contrast and prevention strategies against cybercrime

12:30 to 13:45: lunch

14:00 to 15:30: visit to CNAIPC, CNCPO, COMMISSARIATO di P.S. on line

- CNAIPC: overview of the operational procedures in relation to the protection of critical infrastructures
- CNCPO: introduction to infrastructures tools in preventing and combating on line pedophilia.
Multidisciplinary approach, International Cooperation
- COMMISSARIATO DI P.S. ON LINE: presentation of the on line Police Office

17:00 National Security Agencies DIS, AISI e AISE

- New National cyber security system
- D.P.C.M. 24 gennaio 2013

20:00 dinner

Wednesday, 27 May 2015

09:00 visit to data protection Authority

- introduction to the Authority's tasks
- cybercrime contrast vs rights of privacy (Decreto Legislativo n. 196/2003)
- cooperation at governmental level

12:30 to 13:45: lunch

14:15 transfer to Procura della Repubblica di Roma

15:00

- meeting with the cybercrime task force set up by the Prosecution Office: strategies, operational procedures
- ratification law of Budapest Convention n. 48/2008
- International cooperation

17:00 arrival in Hotel

Thursday, 28 May 2015

09:00 departure to Milan

- security protocols implemented by CNAIPC for Expo

Time to be defined departure to Rome

Friday, 29 May 2015

09:30 arrival at Polo Tuscolano

- wrap up meeting - closing remarks

10:45 transfer to the Ministry of the Interior

12:00 welcome to the SGAE by the Chief of Police, General Director of Public Security

Time to be defined: transfer to the Rome Fiumicino Airport

ANNEX B: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ITALY OR ACRONYM IN ORIGINAL LANGUAGE	ITALIAN OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
CERT	-	-	Computer Emergency Response Team
CSE	-	-	Child Sexual Exploitation
NIS		-	Network and Information Security Authority
CNCPO	-	-	National Centre for the Fight against Online Child Pornography
EC3	-	-	European Cybercrime Center at Europol
CNAIPIC		-	National Anti-Cybercrime Centre for the Protection of Critical Infrastructure
EMPACT	-	-	European Multidisciplinary Platform against Criminal Threats
ENISA	-	-	European Network and Information Security Agency
EUROJUST	-	-	The European Union's Judicial Cooperation Unit
EUROPOL		-	The European Police Office

GENVAL	GENVAL	<i>Groupe de travail "Questions Générales y compris l'Evaluation"</i>	Working Party "General Questions including Evaluation"
NCRPs			National Centre Reference Point
JIT	-	-	Joint Investigation Team
ABI			Association of Italian Banks
MLA	-	-	Mutual Legal Assistance
EUCTF	-	-	European Union Cybercrime Task Force
EFC	-	-	European Financial Cybercrime Coalition
LEAs	-	-	Law Enforcement Authorities
PCF	-	-	Payment Card Fraud
FP TWINS	-	-	Child pornography networks on the internet
EAW	-	-	European Arrest Warrants