UFFICIO SEGRETERIA ISTITUZIONALE
Depositato in Data 30 novembre 2020
IL DIRIGENTE
Rep. San Marino * UFFICIO SEGRETERIA ISTITUZIONALE

PROGETTO DI LEGGE
"DISPOSIZIONI IN MATERIA DI CRIMINI INFORMATICI"

TITOLO I
DISPOSIZIONI GENERALI

Articolo 1
(Definizioni)

1. Ai sensi della presente Legge si intende per:

a) "crimine di genocidio", "crimini contro l'umanità" e "crimini di guerra": gli atti di cui, rispettivamente, agli articoli 6, 7 e 8 dello statuto della Corte Penale Internazionale, la cui commissione sia stata accertata con sentenza passata in giudicato da un Tribunale internazionale alla cui giurisdizione la Repubblica è sottoposta;

b) "dato informatico": qualunque rappresentazione di fatti, informazioni o concetti in forma elettronica, suscettibile di essere utilizzata in un sistema informatico;

c) "dato relativo al traffico informatico": qualsiasi informazione computerizzata relativa a una comunicazione compiuta attraverso un sistema informatico che costituisce una parte della catena di comunicazione e ne indica l'origine, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio;

d) "documento informatico": qualunque rappresentazione in formato elettronico di atti, fatti o dati giuridicamente rilevanti;

e) "fornitore di servizi": i) qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico; ii) qualunque altra entità che elabora o memorizza dati informatici per conto di tale servizio di comunicazione o per gli utenti di questo servizio;

f) "sistema informatico": qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali effettuano l'elaborazione automatica di dati in base a un programma.

g) "programma informatico" o "software": sequenza di istruzioni o codici che possono essere eseguiti da un elaboratore;

h) "pornografia minorile": ogni rappresentazione, fatta 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 atta ad offendere il pudore sessuale;

i) "documento" la rappresentazione, su qualsiasi supporto, di atti, fatti o dati giuridicamente rilevanti.

TITOLO II
MODIFICHE AL CODICE PENALE

Articolo 2

1. L'art. 301 bis del Codice Penale è modificato come segue:

"Art. 301 bis

Segreteria di Stato per gli Affari Esteri, la Cooperazione Economica Internazionale e le Telecomunicazioni
REP SAN MARINO

(Documenti informatici)

1. Le disposizioni previste dal presente Capitolo si applicano altresì quando le falsità riguardano un documento informatico."

Articolo 3

1. L'articolo 182 bis del Codice Penale è modificato come segue:

"Art. 182 bis
(Accesso abusivo ad un sistema informatico o telematico)

"1. Chiunque abusivamente accede a un sistema informatico o telematico protetto da misure di sicurezza, o a parte di esso, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la prigionia di secondo grado.

2. La pena è della prigionia di terzo grado:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri di ufficio, o da chi anche abusivamente esercita la professione di investigatore privato, ovvero con abuso della qualità di amministratore di sistema o delle proprie credenziali di accesso".

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 informatico o telematico o l'interruzione del suo funzionamento, ovvero la distruzione o il danneggiamento delle informazioni, dei dati o programmi ivi contenuti.

3. Se i fatti di cui ai commi primo e secondo riguardano sistemi informatici o telematici di interesse pubblico, la pena è, rispettivamente, della prigionia di terzo e quarto grado.

4. Nel caso previsto dal primo comma il misfatto è punibile a querela della persona offesa. Negli altri casi si procede d'ufficio. Si procede d'ufficio, altresì, nel caso in cui il sistema informatico o telematico sia in uso allo Stato o ad altro pubblico ufficio o sia comunque ad essi pertinente."

Articolo 4

1. Dopo il comma 1 dell'art. 202 del Codice Penale sono aggiunti i seguenti commi:

"Art. 202
(Usurpazione di beni immateriali)

1. Chiunque, in qualsiasi forma, usurpa in tutto o in parte la paternità di un'opera dell'ingegno altrui ovvero, senza il consenso di chi ha il diritto di disporne e a scopo di lucro, la riproduce, diffonde o utilizza in tutto o in parte è punito con la prigionia e la multa a giorni di secondo grado.

2. Le pene sono aumentate di un grado se le condotte di cui ai commi precedenti sono commesse mediante utilizzo di mezzi di comunicazione di massa."

Articolo 5

1. L'art. 203 bis del Codice Penale è modificato come segue:

Segreteria di Stato per gli Affari Esteri, la Cooperazione Economica Internazionale e le Telecomunicazioni
REP SAN MARINO

"Articolo 203 bis
(*Danneggiamento di informazioni, dati e programmi informatici*)

1. Salvo che il fatto costituisca più grave reato, chiunque abusivamente cancella, rende indisponibili, danneggia, deteriora o altera informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la prigionia di secondo grado.

2. Salvo che il fatto costituisca più grave reato, si applica la pena di cui al comma 1 a chiunque commette un fatto idoneo a cancellare, rendere indisponibili, danneggiare, deteriorare o alterare informazioni, dati o programmi informatici in uso allo Stato o da altro pubblico ufficio, ad essi pertinenti o comunque di pubblica utilità. Se l'evento si verifica, la pena è della prigionia di terzo grado.

3. Le pene di cui ai commi precedenti sono aumentate di un grado se il fatto è commesso con abuso della qualità di operatore di sistema."

Articolo 6

1. Dopo l'articolo 203 bis del Codice Penale è inserito l'articolo seguente:

"Art. 203 ter
(*Danneggiamento di sistemi informatici e telematici*)

1. Salvo che il fatto costituisca più grave reato chiunque, al fine di procurare a sé o ad altri un profitto ingiusto alteri, in qualsiasi modo, il funzionamento di un sistema informatico o telematico ovvero intervenga abusivamente con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico è punito con la prigionia, l'interdizione e la multa a giorni di secondo grado.

2. Se il fatto di cui al comma 1 è idoneo a distruggere o danneggiare sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, si applica la pena della prigionia, l'interdizione e la multa a giorni di secondo grado. Se l'evento si verifica, la pena è della prigionia, interdizione e multa a giorni di terzo grado.

3. Le pene di cui ai commi precedenti sono aumentate di un grado se il fatto è commesso con abuso della qualità di operatore di sistema."

Articolo 7

1. Dopo l'articolo 182 bis del Codice Penale è inserito il seguente articolo:

"Art. 182 ter
(Detenzione e diffusione abusiva di codici di accesso)

1. Chiunque al fine di procurare a sé o ad altri un profitto ingiusto o di arrecare ad altri un danno detiene, si procura, riproduce, fornisce ad altri o comunque diffonde abusivamente codici o altri mezzi idonei ad accedere ad un sistema informatico o telematico protetto da misure di sicurezza, ovvero abusivamente fornisce istruzioni idonee al predetto scopo, è punito con la prigionia di primo grado e con la multa.

2. La pena è della prigionia di secondo grado e della multa, se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri di ufficio, o da chi anche abusivamente esercita la professione di investigatore privato, ovvero con abuso della qualità di operatore del sistema.

3. Si applica la pena della prigionia di terzo grado, l'interdizione di terzo grado e la multa, a chiunque abusivamente detiene, si procura, riproduce, fornisce ad altri o comunque diffonde applicazioni, apparecchiature o programmi informatici idonei a distruggere o danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, ovvero alterare il suo funzionamento.

REP SAN MARINO

4. Per i reati di cui al presente articolo si procede d'ufficio."

Articolo 8

1. L'articolo 204 ter del Codice Penale è modificato come segue:

"Art. 204 ter
(Frodi informatiche)

1.E' punito con la prigionia e l'interdizione di secondo grado nonché con la multa chiunque, al fine di procurare a sé o ad altri un ingiusto profitto, alteri, in qualsiasi modo, il funzionamento di un sistema informatico o telematico ovvero intervenga abusivamente, con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico.

2. Si applica la prigionia e l'interdizione di terzo grado nonché la multa se il fatto è commesso a danno dello Stato o di altro pubblico ufficio, o abbia comunque cagionato un danno di rilevante gravità, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

3. Si applica la pena della prigionia e dell'interdizione di quarto grado nonché della multa qualora la condotta fraudolenta abbia prodotto un trasferimento non autorizzato di denaro o valori in danno al titolare.

4. Si applica la pena della prigionia e dell'interdizione di terzo grado e della multa se il fatto è commesso con indebito utilizzo dell'identità digitale in danno di uno o più soggetti."

Articolo 9

1. L'art. 177 ter del Codice Penale è così sostituito:

"Art. 177 ter
(Pornografia minorile)

1. Chiunque utilizza un minore degli anni diciotto per realizzare esibizioni, spettacoli, opere o materiale di pornografia minorile è punito con la prigionia e l'interdizione di terzo grado.

2. Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma ovvero ne trae altrimenti profitto.

3. Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, divulga o pubblicizza il materiale pornografico di cui al primo comma, ovvero divulga informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la prigionia e l'interdizione di terzo grado.

4. Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, consapevolmente offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la prigionia e l'interdizione di secondo grado.

5. Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo, terzo e quarto, consapevolmente usufruisce del materiale di cui al comma primo, è punito con la prigionia e l'interdizione di primo grado.

6. La pena è aumentata di un grado se i fatti previsti nel presente articoli sono commessi ai danni di un minore degli anni quattordici, ovvero di un minore degli anni diciotto che si trovi in condizioni di infermità o deficienza psichica.

7. La pena è aumentate di un grado ove il materiale sia di ingente quantità.

8. In caso di condanna per i misfatti previsti dai commi precedenti è sempre ordinata la confisca del materiale pornografico ai sensi dell'articolo 147 del Codice Penale. A tal fine il Giudice può disporre nell'istruttoria il sequestro del materiale pornografico.

9. Fermo restando l'obbligo di procedere a confisca, non è punibile il minore che, per uso esclusivamente personale e senza scopo di lucro, compia talune delle azioni previste nel presente articolo."

Articolo 10

1. L'articolo 289 del Codice Penale è modificato come segue:

"Art. 289
(Istigazione a delinquere)

1. Chiunque pubblicamente istiga a commettere un misfatto è punito con la prigionia di primo grado.

2. Alla stessa pena soggiace chi pubblicamente, eccedendo i limiti della critica, fa l'apologia di un fatto che la Legge prevede come misfatto.

3. Si applica la pena della prigionia di secondo grado se l'istigazione o l'apologia riguardano la commissione crimini di genocidio, crimini contro l'umanità o crimini di guerra.

4. Le pene di cui ai commi precedenti sono aumentate di un ulteriore grado se il fatto è commesso servendosi delle comunicazioni sociali o di mezzi di comunicazione di massa.

Articolo 11

1. L'articolo 179 bis del Codice Penale è modificato come segue:

"Art. 179 bis
(Discriminazione, odio o violenza per motivi razziali, etnici, nazionali, religiosi o legati all'orientamento sessuale e all'identità di genere)

1. Chiunque diffonde in qualsiasi modo idee fondate sulla superiorità o sull'odio razziale o etnico, o incita a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali, religiosi o legati all'orientamento sessuale e all'identità di genere, ovvero incita a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali, religiosi o legati all'orientamento sessuale e all'identità di genere, è punito con la prigionia di secondo grado.

2. Le pene sono aumentate di un grado se la provocazione o l'istigazione si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave, sull'approvazione o sulla giustificazione della Shoah, ovvero di crimini di genocidio, di crimini contro l'umanità o di crimini di guerra.

3. Le pene di cui ai commi precedenti sono aumentate di un ulteriore grado se il fatto è commesso servendosi delle comunicazioni sociali o di mezzi di comunicazione di massa.

4. Per i reati aggravati dalla circostanza della discriminazione razziale, etnica, nazionale o religiosa, o legata all'orientamento sessuale e di genere, di cui all'articolo 90, comma 1, punto 1, si procede in ogni caso d'ufficio."

Articolo 12
(Cyber bullismo e Cyberstalking)

All'art. 181 bis del Codice Penale sono aggiunti i seguenti commi:

Segreteria di Stato per gli Affari Esteri, la Cooperazione Economica Internazionale e le Telecomunicazioni
REP. SAN MARINO

"Qualora le molestie o le minacce di cui al primo comma siano poste in essere in danno di un minore di anni 21, sotto forma di sistematiche e ripetute angherie e pratiche vessatorie, la pena è aumentata di un grado.
Se il fatto è commesso da persona cui, per ragioni di cura, di educazione, di istruzione, di vigilanza o di custodia, il minore è affidato ovvero nell'ambito di un luogo di istruzione o altro luogo di aggregazione giovanile, la pena è aumentata di un ulteriore grado.
Qualora le molestie o le minacce di cui al primo comma siano poste in essere da un soggetto legato alla vittima da stabili rapporti affettivi ancorché cessati, la pena è aumentata di un grado.
Qualora le molestie o le minacce di cui ai commi precedenti siano poste in essere avvalendosi di mezzi di comunicazione di massa, ovvero attraverso reti di telecomunicazione, la pena è aumentata di un grado.

Articolo 13

Dopo l'art. 181 bis del Codice Penale è aggiunto il seguente articolo:

Art. 181 ter
(Diffusione abusiva di immagini personali)

Chiunque, mediante diffusione, in qualsiasi forma, divulga abusivamente, allo scopo di arrecare un danno, immagini personali altrui è punito con la prigionia e la multa a giorni di secondo grado.

Qualora la condotta di cui al primo comma sia posta in essere da un soggetto legato alla vittima da stabili rapporti affettivi, ancorché cessati, la pena è aumentata di un grado.

Articolo 14

1. L'articolo 6 del Codice Penale è modificato come segue:

"Art. 6
(Reati commessi all'estero)

1. E' soggetto alle disposizioni del presente Codice Penale chiunque commette fuori territorio dello Stato uno dei misfatti previsti dagli articoli: 170, 185, 196, 204 bis, 204 ter, 284, 285, 305, 305 bis, 324, 325, 326, 328, 329, 331, 332, 333, 334, 337, 337 bis, 337 ter, 338, 339, 341, 342, 343, 344, 346, 347, 371, 372, 373, 374, 374 bis, 374 ter, 375, 376, 377, 378, 379, 380, 400, 401, 401 bis, 403, 403 bis, 403 ter, 403 quater, 405.

2. E' inoltre soggetto alla legislazione sammarinese:

1) chiunque commette fuori territorio dello Stato favoreggiamento in relazione ai misfatti di cui agli articoli 401, 401 bis, 403, 403 bis, 403 ter e 403 quater;

2) chiunque commette fuori territorio dello Stato i misfatti di cui agli articoli 167, 168, 244 e 268;

3) chiunque commette fuori territorio dello Stato i misfatti di cui agli articoli 237 e 239, se compiuti mediante dirottamento di aeromobili aventi per prima destinazione il territorio dello Stato ovvero da esso partiti;

4) il cittadino o il residente sul territorio della Repubblica che commette fuori territorio dello Stato i misfatti di cui all'articolo 179 bis comma 3, 182 bis, 182 ter, 190 bis, 202 comma 3, 203 bis, 203 ter, 301 bis, ovvero 177 ter se commesso attraverso un sistema informatico o telematico, nonché il concorso e il favoreggiamento dei misfatti elencati. Per i casi di cui al presente numero, la giurisdizione sammarinese si applica qualora il fatto sia previsto come reato anche nello Stato in cui il crimine è stato commesso o qualora sia stato commesso fuori dalla giurisdizione di uno Stato;

5) chiunque commette fuori territorio dello Stato ogni altro reato per il quale le convenzioni o i trattati internazionali obbligano la Repubblica alla repressione di fatti commessi all'estero.

3. La Legge sammarinese si applica inoltre a chiunque commette, fuori del territorio dello Stato a danno di un cittadino sammarinese, misfatto punibile con la prigionia di grado non inferiore al secondo. "

TITOLO III
DISPOSIZIONI SPECIALI NEL PROCESSO PENALE E INTEGRAZIONI ALLE DISPOSIZIONI DI PROCEDURA PENALE

CAPO I
ORDINI DELL'AUTORITÀ GIUDIZIARIA RELATIVI A DATI CONTENUTI IN SISTEMI INFORMATICI O TELEMATICI

Articolo 15
(Ordine di conservazione di dati contenuti in sistemi informatici o telematici)

1. Qualora vi sia il sospetto che dati o informazioni utili allo svolgimento di indagini penali siano contenuti in un sistema informatico o telematico, o in parte di esso, e vi sia fondato motivo di ritenere che possano essere dispersi o cancellati, il Giudice, con decreto motivato, ordina, al soggetto che ne ha la disponibilità o il controllo, l'adozione delle misure tecniche necessarie a garantire l'immediata protezione e conservazione dei dati nel loro stato originale. Il Giudice dispone altresì che il destinatario dell'ordine adotti ogni misura necessaria ad assicurare la riservatezza sul contenuto di tali dati.

2. Nei casi di cui al comma 1, il Giudice può ordinare la conservazione dei dati utili allo svolgimento delle indagini anche sulla base di una richiesta proveniente da un'Autorità giudiziaria estera ai sensi dell'articolo 23 della presente Legge.

3. Salvo quanto disposto dal comma precedente, qualora l'ordine di conservazione abbia ad oggetto dati relativi a comunicazioni telematiche contenuti in un sistema informatico o telematico presso un fornitore di servizi, il Giudice può ordinare che gli siano trasmessi dati sul traffico in misura sufficiente a consentire l'individuazione di altri fornitori di servizi coinvolti nelle comunicazioni telematiche rilevanti ai fini dell'indagine.

4. L'obbligo di conservazione dei dati perdura sino al momento dell'acquisizione da parte dell'Autorità giudiziaria e comunque non oltre novanta giorni dall'adozione del decreto con il quale è stata ordinata la conservazione. Nel caso in cui non sia possibile procedere all'acquisizione dei dati entro tale termine, o qualora sopraggiunga dall'estero la richiesta di cui all'articolo 23 della presente Legge, il Giudice può prorogare gli effetti dell'ordine di conservazione per un periodo massimo di ulteriori 60 giorni.

Articolo 16
(Ordine di produzione di dati contenuti in sistemi informatici o telematici)

1. Qualora vi sia il sospetto che dati o informazioni utili allo svolgimento di indagini penali siano contenuti in un sistema informatico o telematico, o in parte di esso, il Giudice, con decreto motivato, può ordinare al soggetto che ne ha la disponibilità o il controllo di trasmetterli all'Autorità giudiziaria.

2. Fuori dei casi di cui al comma 1, il Giudice, con decreto motivato, può altresì ordinare ai fornitori di servizi di trasmettere all'Autorità giudiziaria dati e informazioni utili allo svolgimento delle indagini relativi a specifici abbonati o ai servizi da questi utilizzati.

Segreteria di Stato per gli Affari Esteri, la Cooperazione Economica Internazionale e le Telecomunicazioni
REP SAN MARINO

Articolo 17
(Ordine di rimozione di dati e programmi informatici)

1. Al fine di evitare che le conseguenze del reato siano aggravate o protratte o che sia agevolata la commissione di altri reati, il Giudice ordina, con decreto motivato, che i dati o i programmi pertinenti al reato contenuti in un sistema informatico o telematico, o in parte di esso, siano resi inaccessibili o rimossi.

2. Nell'emettere l'ordine di cui al comma precedente, il Giudice dispone altresì che siano adottate le misure tecniche necessarie a garantire la conservazione dei dati resi inaccessibili o rimossi.

3. In caso di archiviazione, i dati conservati ai sensi del comma 2 sono restituiti all'avente diritto.

Articolo 18
(Modalità di esecuzione degli ordini dell'Autorità giudiziaria)

1. Chiunque riceve un ordine ai sensi dell'articolo 13, 14 o 15 della presente Legge è tenuto a ottemperarvi nei modi e nei termini stabiliti dal Giudice. Su richiesta motivata del destinatario dell'ordine, il Giudice può prorogare il termine concesso per adempiervi.

2. In ogni caso, le modalità di trasmissione devono garantire la conformità delle copie ai dati originali nonché la riservatezza sul loro contenuto.

3. Il destinatario dell'ordine è tenuto a mantenere il segreto sulle indagini in corso e sulle procedure intraprese in esecuzione dell'ordine ricevuto.

Articolo 19
(Sanzioni amministrative)

1. Il destinatario di un ordine adottato ai sensi degli articoli 13, 14 o 15 che, senza giustificato motivo, non vi ottemperi nei modi e nei termini stabiliti dal Giudice con decreto e in conformità a quanto disposto dall'articolo 16 della presente Legge è punito con la sanzione pecuniaria amministrativa pari ad Euro 5.000,00.

Articolo 20
(Sanzioni penali)

1. Salvo che il fatto costituisca più grave reato, alla violazione dell'obbligo di segreto di cui all'articolo 18, comma 3 si applicano le disposizioni dell'articolo 192 bis del Codice Penale.

CAPO II
PERQUISIZIONI E SEQUESTRI

Articolo 21

1. L'articolo 58 bis del Codice di Procedura Penale è modificato come segue:

"Art. 58 bis
(Sequestro probatorio)

1. Il Giudice, con decreto motivato, ordina il sequestro del corpo del reato e delle cose ad esso pertinenti che siano necessarie per l'accertamento dei fatti.

2. 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.

3. Il Giudice o il personale di polizia giudiziaria delegato dall'autorità giudiziaria, può esaminare ed acquisire copia di atti, documenti, corrispondenza, dati e informazioni contenuti in programmi informatici presso gli istituti finanziari nonché procedere al sequestro di atti, documenti e corrispondenza, titoli, valori, somme depositate e di ogni altra cosa, anche se contenuti in cassette di sicurezza, quando abbia fondato motivo di ritenere che siano pertinenti al reato, sebbene non appartengano all'imputato o non siano iscritti a suo nome.

4. Il decreto con il quale è disposta l'acquisizione presso gli istituti finanziari di copia della documentazione è notificato al Procuratore del Fisco e al soggetto finanziario presso il quale sono esaminati o acquisiti i documenti, i dati o le informazioni.

Articolo 22

1. Dopo l'articolo 58 ter del Codice di Procedura Penale è inserito il seguente articolo:

"Art. 58 quater
(Sequestri di dati o documenti informatici)

1. Fuori dei casi di cui al comma 3 dell'articolo 58 bis, le disposizioni di cui al comma 1, 2 e 4 del medesimo articolo nonché le disposizioni di cui all'articolo 58 ter si applicano altresì qualora il sequestro o l'acquisizione di copia abbia ad oggetto dati o documenti informatici ovunque contenuti.

2. Nel disporre che sia acquisita copia dei dati o dei documenti informatici utili per le indagini, il Giudice ordina l'adozione delle misure tecniche necessarie a garantirne la conservazione nella loro integrità sia in fase di acquisizione che per tutta la durata delle indagini.

3. Qualora non sia possibile effettuare copia dei dati o dei documenti, il Giudice dispone il sequestro del sistema informatico o telematico, o di parte di esso, in cui questi sono contenuti."

Articolo 23

1. L'articolo 68 del Codice di Procedura Penale è modificato come segue:

" Art. 68
(Perquisizioni)

1. Se la natura del reato è tale, che verosimilmente se ne possano acquistare le prove da scritti o effetti esistenti presso l'inquisito, o presso altre persone, od in luoghi ove si reputano occultati, ovvero da dati, documenti o programmi contenuti in sistemi informatici o telematici, o in parte di essi, può eseguirsi la perquisizione, che si riconosca opportuna per rinvenirli."

Articolo 24

1. L'articolo 74 del codice di procedura penale è modificato come segue:

"Art. 74

1. La perquisizione reale al domicilio dell'inquisito o di altri, non può farsi che con decreto Commissariale scritto nel processo, decreto la cui copia autenticata si trasmette al Capo della forza pubblica. Nel detto decreto si prescrivono le cautele da usarsi nella perquisizione, incluso, qualora si proceda a perquisizioni su sistemi informatici o telematici, le misure tecniche necessarie per garantire la conservazione dei dati nella

loro integrità. Della omissione di tali cautele e misure è responsabile il Capo della forza. Non è necessario il decreto per eseguirla al domicilio del prevenuto, quando questa si opera nell'atto dell'arresto del prevenuto stesso."

TITOLO IV
COOPERAZIONE INTERNAZIONALE

Articolo 25
(Richieste d'urgenza dall'estero)

1. Prima che sia effettuata formale richiesta di rogatoria internazionale, qualora vi sia il rischio che nel frattempo i dati contenuti in un sistema informatico o telematico e pertinenti al reato siano dispersi o cancellati, l'Autorità estera competente può richiedere all'Autorità giudiziaria sammarinese di ordinare la conservazione d'urgenza di tali dati al soggetto che ne ha la disponibilità o il controllo, inclusi dati sul traffico relativi a specifiche comunicazioni telematiche.

2. La richiesta, redatta in forma scritta, deve indicare:

a) l'autorità, dalla quale la domanda promana e, se differente, l'autorità competente per il procedimento penale;

b) il reato per il quale lo Stato richiedente procede e un breve riassunto dei fatti;

c) i dati informatici di cui è richiesta la conservazione e il loro legame con il reato;

d) tutte le informazioni utili a identificare il soggetto che detiene o controlla i dati informatici o il luogo dove si trova il sistema informatico interessato;

e) la necessità della conservazione;

f) l'intenzione di avanzare successiva rogatoria internazionale con riferimento ai dati di cui è richiesta la conservazione d'urgenza.

3. Il Giudice, verificata la completezza della domanda, con decreto motivato, ordina al soggetto che ha la disponibilità o il controllo dei dati oggetto della richiesta di adottare tutte le misure tecniche necessarie a garantirne la conservazione nella loro integrità.

4. Qualora il Giudice ritenga che l'esecuzione dell'ordine di conservazione non garantisca la futura disponibilità dei dati o possa comunque arrecare pregiudizio alle indagini in corso nello Stato richiedente, sospende l'esecuzione dell'ordine e ne dà immediata comunicazione a quest'ultimo.

5. L'ordine di conservazione produce effetti per un massimo di sessanta giorni, i quali, in caso di domande irregolari, iniziano a decorrere dalla ricezione delle modifiche e/o informazioni richieste per il perfezionamento della domanda. Se nel frattempo l'autorità giudiziaria riceve la rogatoria di cui al comma 2, lettera f), l'ordine produce effetti sino a quando il Giudice non abbia adottato il decreto di exequatur di cui all'articolo 8, comma 1, della Legge 30 luglio 2009 n. 104.

6. L'esecuzione della richiesta è negata se:

a) la domanda è avanzata sulla base di reati non punibili secondo la Legge dello Stato richiedente e secondo quella della Repubblica;

b) gli atti richiesti compromettono la sovranità, la sicurezza o altri interessi essenziali della Repubblica;

c) la domanda si riferisce a reati considerati dalla Repubblica come reati politici o come reati connessi con reati politici.

Articolo 26
(Trasmissione all'estero di dati sul traffico)

1. Nei casi in cui la richiesta di conservazione di cui all'articolo precedente abbia ad oggetto dati sul traffico relativi a comunicazioni telematiche, il Giudice che, nell'eseguire la richiesta, venga a conoscenza del coinvolgimento di fornitori di servizi stranieri ne dà immediata notizia allo Stato richiedente, trasmettendo dati sul traffico in misura sufficiente a consentire l'individuazione dei medesimi.

2. I dati di cui al comma 1 non sono trasmessi qualora ricorra una delle ipotesi di cui al comma 6, lettere b) e c) dell'articolo 23 della presente Legge.

Articolo 27
(Entrata in vigore)

1. La presente Legge entra in vigore il quindicesimo giorno successivo alla sua legale pubblicazione.