

LEGGE 18 marzo 2008, n. 48 ⁽¹⁾.

Ratifica ed esecuzione della [Convenzione del Consiglio d'Europa sulla criminalità informatica](#), fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno ⁽²⁾.

⁽¹⁾ Pubblicata nella Gazz. Uff. 4 aprile 2008, n. 80, S.O.

⁽²⁾ Il Ministero degli affari esteri, con [Comunicato 8 novembre 2008](#) (Gazz. Uff. 8 novembre 2008, n. 262), ha reso noto che in data 5 giugno 2008 si è provveduto al deposito dello strumento di ratifica previsto per l'entrata in vigore della Convenzione qui allegata; di conseguenza la suddetta Convenzione, a norma dell'articolo 36, paragrafo 4, della stessa, è entrata in vigore il 1° ottobre 2008.

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

Promulga

la seguente legge:

Capo I

RATIFICA ED ESECUZIONE

Art. 1 (*Autorizzazione alla ratifica*)

1. Il Presidente della Repubblica è autorizzato a ratificare la [Convenzione del Consiglio d'Europa sulla criminalità informatica](#), fatta a Budapest il 23 novembre 2001, di seguito denominata «Convenzione».

Art. 2 (*Ordine di esecuzione*)

1. Piena e intera esecuzione è data alla [Convenzione](#), a decorrere dalla data della sua entrata in vigore in conformità a quanto disposto dall'[articolo 36 della Convenzione](#) stessa.

Capo II

MODIFICHE AL CODICE PENALE E AL [DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231](#)

Art. 3 (*Modifiche al titolo VII del libro secondo del codice penale*)

1. All'articolo 491-bis del codice penale sono apportate le seguenti modificazioni:

- a) al primo periodo, dopo la parola: «privato» sono inserite le seguenti: «avente efficacia probatoria»;
- b) il secondo periodo è soppresso.

2. Dopo l'articolo 495 del codice penale è inserito il seguente:

«Art. 495-bis. - (Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri). - Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno».

Art. 4 (*Modifica al titolo XII del libro secondo del codice penale*)

1. L'articolo 615-quinquies del codice penale è sostituito dal seguente:

«Art. 615-quinquies. - (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico). - 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».

Art. 5 (*Modifiche al titolo XIII del libro secondo del codice penale*)

1. L'articolo 635-bis del codice penale è sostituito dal seguente:

«Art. 635-bis. - (Danneggiamento di informazioni, dati e programmi informatici). - Salvo che il fatto costituisca più grave reato, 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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero 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».

2. Dopo l'articolo 635-bis del codice penale sono inseriti i seguenti:

«Art. 635-ter. - (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità). - Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare,

cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 635-quater. - (Danneggiamento di sistemi informatici o telematici). - Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero 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.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 635-quinquies. - (Danneggiamento di sistemi informatici o telematici di pubblica utilità). - 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.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

3. Dopo l'articolo 640-quater del codice penale è inserito il seguente:

«Art. 640-quinquies. - (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica). - 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».

Art. 6 (*Modifiche all'articolo 420 del codice penale*)

1. All'articolo 420 del codice penale, il secondo e il terzo comma sono abrogati.

Art. 7 (*Introduzione dell'[articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231](#)*)

1. Dopo l'[articolo 24 del decreto legislativo 8 giugno 2001, n. 231](#), è inserito il seguente:
«Art. 24-bis. - (Delitti informatici e trattamento illecito di dati). - 1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione

pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)».

Capo III

MODIFICHE AL CODICE DI PROCEDURA PENALE E AL CODICE DI CUI AL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196

Art. 8 (*Modifiche al titolo III del libro terzo del codice di procedura penale*)

1. All'articolo 244, comma 2, secondo periodo, del codice di procedura penale sono aggiunte, in fine, le seguenti parole: «, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

2. All'articolo 247 del codice di procedura penale, dopo il comma 1 è inserito il seguente: «1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

3. All'articolo 248, comma 2, primo periodo, del codice di procedura penale, le parole: «atti, documenti e corrispondenza presso banche» sono sostituite dalle seguenti: «presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici».

4. All'articolo 254 del codice di procedura penale sono apportate le seguenti modificazioni:

a) il comma 1 è sostituito dal seguente:

«1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato»;

b) al comma 2, dopo le parole: «senza aprirli» sono inserite le seguenti: «o alterarli».

5. Dopo l'articolo 254 del codice di procedura penale è inserito il seguente:

«Art. 254-bis. - (Sequestro di dati informatici presso fornitori di servizi informatici,

telematici e di telecomunicazioni). - 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

6. All'articolo 256, comma 1, del codice di procedura penale, dopo le parole: «anche in originale se così è ordinato,» sono inserite le seguenti: «nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto,».

7. All'articolo 259, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria».

8. All'articolo 260 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole: «con altro mezzo» sono inserite le seguenti: «, anche di carattere elettronico o informatico,»;

b) al comma 2 è aggiunto, in fine, il seguente periodo: «Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria».

Art. 9 *(Modifiche al titolo IV del libro quinto del codice di procedura penale)*

1. All'articolo 352 del codice di procedura penale, dopo il comma 1 è inserito il seguente: «1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previste, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi».

2. All'articolo 353 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 2 sono aggiunte, in fine, le seguenti parole: «e l'accertamento del contenuto»;

b) al comma 3, primo periodo, le parole: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza» sono sostituite dalle seguenti: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica,» e dopo le parole: «servizio postale» sono inserite le seguenti: «, telegrafico, telematico o di telecomunicazione».

3. All'articolo 354, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «In relazione ai dati, alle informazioni e ai programmi informatici o ai

sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

Art. 10 (*Modifiche all'[articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196](#)*)

1. Dopo il comma 4-bis dell'[articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196](#), sono inseriti i seguenti:

«4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al [decreto legislativo 28 luglio 1989, n. 271](#), possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al [decreto legislativo n. 271 del 1989](#), ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale.

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia».

Art. 11 (*Competenza*)

1. All'articolo 51 del codice di procedura penale è aggiunto, in fine, il seguente comma:
«3-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il

tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente».

1-bis. Le disposizioni di cui al comma 3-quinquies dell'articolo 51 del codice di procedura penale, introdotto dal comma 1 del presente articolo, si applicano solo ai procedimenti iscritti nel registro di cui all'articolo 335 del codice di procedura penale successivamente alla data di entrata in vigore della presente legge. ⁽³⁾

(3) Comma aggiunto dall'[art. 12-bis, comma 1, D.L. 23 maggio 2008, n. 92](#), convertito, con modificazioni, dalla [L. 24 luglio 2008, n. 125](#).

Art. 12 *(Fondo per il contrasto della pedopornografia su internet e per la protezione delle infrastrutture informatiche di interesse nazionale)*

1. Per le esigenze connesse al funzionamento del Centro nazionale per il contrasto della pedopornografia sulla rete INTERNET, di cui all'[articolo 14-bis della legge 3 agosto 1998, n. 269](#), e dell'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione per le esigenze relative alla protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, di cui all'[articolo 7-bis del decreto-legge 27 luglio 2005, n. 144](#), convertito, con modificazioni, dalla [legge 31 luglio 2005, n. 155](#), è istituito, nello stato di previsione del Ministero dell'interno, un fondo con una dotazione di 2 milioni di euro annui a decorrere dall'anno 2008.

2. Agli oneri derivanti dal presente articolo, pari a 2 milioni di euro annui a decorrere dall'anno 2008, si provvede mediante corrispondente riduzione dello stanziamento iscritto, ai fini del bilancio triennale 2008-2010, nell'ambito del fondo speciale di parte corrente dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2008, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero della giustizia.

3. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

Capo IV

DISPOSIZIONI FINALI

Art. 13 *(Norma di adeguamento)*

1. L'autorità centrale ai sensi degli [articoli 24](#), paragrafo 7, e [27](#), paragrafo 2, della Convenzione è il Ministro della giustizia.

2. Il Ministro dell'interno, di concerto con il Ministro della giustizia, individua il punto di contatto di cui all'[articolo 35 della Convenzione](#).

Art. 14 (*Entrata in vigore*)

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica Italiana. E' fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

[Convenzione del Consiglio d'Europa sulla criminalità informatica](#)