

# Brevi cenni sulla legge italiana di autorizzazione alla ratifica della convenzione di budapest sulla cibercriminalita' (consiglio d'Europa)

**Autore:**

**In:** Diritto civile e commerciale

## Premessa

L'Italia, dopo la Francia, è stato il primo Paese europeo a mettere in piedi una legge organica per reprimere i delitti informatici, modificando il suo codice penale e di procedura penale. Si tratta della legge 23.12.1993, n. 547 alla quale si sono aggiunte successivamente altre leggi che, in settori particolari, tendevano a reprimere comportamenti illeciti relativamente alla c.d. pirateria informatica (decreto legislativo. 29.12.1992, n. 518, modificato con la legge 18.08.2000 n. 248 e, da ultimo, con la legge 22.5.2004 n. 128), alla protezione dei dati personali (legge 31.12.1996 n. 675 e in particolare il decreto legislativo n. 196 del 30.06.2003 e successive modifiche) alla c.d. pedofilia telematica (legge 3.8.1998 n. 269 modificata con la legge n. 11.8.2003 n. 228 e, da ultimo, con la legge 6 febbraio 2006 n. 38). Quest'ultima legge però contempla (art. 600 quater 1) soltanto la pornopedofilia virtuale e non anche quella c.d. putativa, prevista dall'art.9,2 comma,lett.b della Convenzione ( una persona che **appare** essere un minore.

) Il citato articolo 600 quater ,recante il titolo "Pornografia virtuale", infatti recita:..". 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".

Pertanto l'Italia, a mio avviso, al momento del deposito dello strumento di ratifica dovrebbe effettuare la riserva prevista dall'art. 42 della Convenzione con riferimento all'art. 9 par. 4....anche se,lo rilevo per inciso, della necessità di questa riserva non vi è cenno nella relazione al disegno di legge originario ( AC 2807 )

Per quanto riguarda la protezione dei minori, va ricordato ,incidentalmente,

che  
un disegno di legge governativo (AC. 3241 )  
in discussione al Parlamento prevede l'introduzione nel codice penale dell'art. 609 - undecies - intitolato "Adescamento di minorenni", secondo cui chiunque, allo scopo di abusare o sfruttare sessualmente un minore di anni sedici, intrattiene con lui, anche attraverso l'utilizzazione della rete internet o di altre reti o mezzi di comunicazione, una relazione tale da sedurlo, ingannarlo e comunque carpirne la fiducia, è punito con la reclusione da uno a tre anni". In tema di lotta al terrorismo e con riferimento ad Internet ricordo, infine, per inciso  
che il decreto legge 27 luglio 2005 n. 144, convertito in legge 31 luglio 2005 n. 155, relativo alle misure urgenti per il contrasto del terrorismo internazionale ha inserito l'articolo 2-bis nella legge 2.10.1967 n. 895, secondo cui: "Chiunque fuori dei casi consentiti da disposizioni di legge o di regolamento addestra taluno o fornisce istruzioni in qualsiasi forma, anche anonima, o per via telematica sulla preparazione o sull'uso di materiali esplosivi, di armi da guerra, di aggressivi chimici o di sostanze batteriologiche nocive o pericolose e di altri congegni micidiali è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a sei anni

E' da dire ora che nella seduta del 27 febbraio 2008 il Senato ha approvato definitivamente il disegno di legge n. 2012 di ratifica ed esecuzione della Convenzione: divenuta poi la legge n.48 del 18 marzo 2008 ..: La legge in questione, esaminata ed approvata con straordinaria premura, dopo più di un lustro di totale inerzia legislativa ( la sottoscrizione da parte dell'Italia era avvenuta il 23 novembre 2001 .... ) introduce alcune modifiche al sistema penale vigente sia sostanziale che processuale. In questa sede mi limiterò a brevi rilievi riguardanti essenzialmente le riforme di diritto sostanziale...".

1)

### **Attentati alla integrità dei dati e dei sistemi informatici o telematici (artt. 4 e 5 della Convenzione)**

La legge n.48 del 2008 ha

sostituito :l'articolo 635 bis  
del codice penale ..La rubrica  
attuale

è la seguente. : " Danneggiamento di informazioni, dati e programmi informatici"...Il testo è il seguente:

- " Salvo che il fatto costituisce 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".

A questo proposito è opportuno attirare l'attenzione sulle modiche intervenute a proposito dell'articolo 420 ( Attentato ad impianti di pubblica utilità ) nel testo introdotto con la legge n547 del 1993...Il testo dell'articolo recitava.."Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità,è punito,salvo che il fatto

costituisca  
più grave reato,con la reclusione da uno a quattro anni.

La pena di cui al primo comma si applica anche va chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità,ovvero dati,informazioni o programmi in essi contenuti o ad esso pertinenti.

Se dal fatto  
deriva la  
distruzione o il danneggiamento dell'impianto o del sistema,dei dati,delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è della reclusione  
da tre ad otto anni.

L'articolo in questione distingueva,quindi nettamente gli impianti, di pubblica utilità ,consistenti in complessi di strutture,,apparecchiature,congegni, ecc.coordinati  
e concorrenti ad un unico scopo  
idonei a soddisfare esigenze di pubblica utilità::,dagli altri sistemi ed oggetti informatici..

L'articolo 6

della legge di ratifica,senza che nella relazione al disegno di legge originario siano  
fornire  
idonee spiegazioni.,ha soppresso  
il secondo e terzo comma del citato articolo 420,collocato nell'ambito dei delitti contro l'ordine pubblico,,  
spostando  
le ipotesi di danneggiamento,distruzione,interruzione,ecc dei sistemi informatici pubblici o di pubblica utilità  
e dei dati,informazioni e programmi

ad essi pertinenti, nell'ambito dei reati contro il patrimonio ( cfr.artt.635-ter,635-quinquies. (1)  
)...Da questa  
operazione di maldestra  
chirurgia

giuridica, sono derivate due  
importanti conseguenze...La prima, per così dire di politica criminale,  
è stata quella di  
inquadrare gli attacchi, anche gravi, ai sistemi  
e beni informatici pubblici o di pubblica utilità, come  
fatti idonei a turbare l'ordine pubblico, cioè la pacifica vita della collettività.....il che  
indubbiamente fa a pugni con la realtà, dato che ormai l'intera vita sociale dipende dai sistemi informatici  
ed anche una semplice interruzione di un servizio pubblico, inteso il termine in senso lato, gestito da  
elaboratori  
è idoneo a creare, quanto meno, diffusi disagi nella collettività.....La seconda, forse più grave, è quella che  
è derivata dalla eliminazione pure e semplice del terzo comma dell'articolo 420. Cioè, attualmente, il delitto  
aggravato dall'evento, consistente nel danneggiamento e distruzione del **semplice impianto**  
di pubblica utilità o nell'interruzione del suo funzionamento, già previsto dal citato comma, sembra  
scomparso  
dal codice penale...

---

...

1)“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

2)

### **Abuso di dispositivi (Art. 6 della Convenzione)**

Un'altra modifica ha interessato l'articolo 615-quinquies che, in aderenza al testo della Convenzione è stato sostituito dall'altro

recante il titolo "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico" e che recita. " 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".

Come si ricava dalla relazione al disegno di legge, originario ( AC 2807 )...all'estensione della portata della norma originaria sotto il profilo oggettivo ha fatto riscontro la riformulazione dell'elemento soggettivo richiesto nei termini del dolo specifico...".

3)

### **Falsificazione informatica (Art. 7 della Convenzione)**

Nel sistema penale italiano l'ipotesi era prevista dall'articolo 491 bis del codice penale, come introdotto dalla legge n. 547 del 1993, avente come titolo: "Documenti informatici".

Con l'articolo in questione era stato inserito, nel capo III del titolo II del libro II del c.p., relativo alla falsità in atti, una nuova previsione che estendeva alle falsità riguardanti un documento informatico, le disposizioni in tema di falso in atto pubblico o in scrittura privata (artt. da 476 a 491 c.p.). La seconda parte dell'articolo in questione conteneva la definizione di documento informatico valevole nel settore penale: trattavasi di un "qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".

Per la migliore comprensione delle modifiche apportate dall'articolo 3. della

legge di ratifica al sopracitato articolo, è necessario riprodurre il testo originario che recitava:

491-bis. (Documenti informatici).- Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".

L'articolo 3

legge in questione ha modificato parzialmente il sopracitato articolo. Più precisamente nel primo periodo, dopo la parola "privato" sono state aggiunte le parole "aventi efficacia probatoria" mentre è stato soppresso il secondo periodo

sino

alle parole” destinati ad elaborarli...

Ciò è avvenuto, come si ricava dalla relazione al disegno di legge originario (n. 2807 ).

“...in considerazione della sopravvenuta inadeguatezza della definizione di documento informatico, inteso come “supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi destinati ad elaborarli”, si è deciso di accogliere, anche ai fini penali, la più ampia e corretta nozione di documento informatico, già contenuta nel regolamento di cui al decreto del Presidente della Repubblica 10 novembre 1997, n. 513, come “rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”

A

proposito .però, di definizione di documento informatico il patrio legislatore non è sembrato molto

aggiornato...infatti l’ultima definizione è contenuta nell’articolo 1 ,lett.(p del decreto legislativo

n.82 del 7 marzo 2005 ,il c.d Codice dell’Amministrazione Digitale....

Nella stessa prospettiva è sembrata opportuno al legislatore l’introduzione dell’articolo 495 bis il cui testo è il seguente::

“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”.

4)

### **Frode informatica (art. 8 della Convenzione)**

Il codice penale attuale prevede la frode informatica all’articolo 640-ter. Si tratta di una speciale ipotesi di truffa, relativa alla alterazione del funzionamento di un sistema informatico o telematico o ad esso pertinente. Più particolarmente la norma riguarda il fatto di chi, 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 essi pertinenti,

procura a sé o ad altri un ingiusto profitto con altrui danno. Anche questa disposizione è speciale rispetto alla fattispecie di truffa comune (art. 640).

La legge di ratifica prevede una ulteriore ipotesi di frode informatica, quella del certificatore. E così ,dopo l'articolo 640-quater del codice penale ,è stato inserito :

il . 640-quinquies.

il cui titolo è..” Frode informatica del soggetto che presta servizi di certificazione di firma elettronica”.. e che recita:. “ 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”.

Secondo la relazione al disegno di legge: la disposizione è apparsa necessaria in quanto, sebbene l'articolo 640-ter del codice penale incrimini già la frode informatica, per la ricorrenza di questo specifico reato appaiono necessarie condotte di alterazione del funzionamento di un sistema informatico ovvero di intervento senza diritto su dati, informazioni o programmi, che potrebbero non ricorrere nel caso dell'attività di certificazione. Peraltro, la nuova incriminazione appare incentrata non solo sulla semplice violazione degli obblighi del certificatore qualificato e accreditato (già sanzionata civilmente dalla lettera d) del comma 1 dell'articolo 30 del citato codice dell'amministrazione digitale), ma anche sulla effettiva ricorrenza di un ingiusto profitto con altrui danno.

A titolo di cronaca rilevo che il solito patrio legislatore è stato impreciso

in quanto la rubrica avrebbe dovuto indicare che il fatto si riferiva al certificatore

**qualificato**

,cioè al certificatore che presta servizi di certificazione qualificata.in relazione agli articoli 19e 32 del Codice dell'Amministrazione Digitale...

5)

**Responsabilità delle persone giuridiche (art. 12 della Convenzione)**

La responsabilità amministrativa delle persone giuridiche è prevista in Italia dal decreto legislativo 8



giugno 2001 n. 231 che stabilisce, tra l'altro, all'articolo 24 la responsabilità dell'ente per frode informatica in danno dello Stato o di un ente pubblico.

L'articolo in questione, dal titolo "Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico" recita: "In relazione alla commissione dei delitti di cui agli articoli 316-bis, 316-ter, 640, comma 2, n. 1, 640-bis e 640-ter se commesso in danno dello Stato o di altro ente pubblico, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote".

"Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità; si applica la sanzione pecuniaria da duecento a seicento quote".

"Nei casi previsti dai commi precedenti, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

Con il disegno di legge di ratifica si è introdotta nel decreto legislativo n. 231 una nuova norma che estende la responsabilità amministrativa delle persone giuridiche e degli enti alla quasi totalità dei delitti informatici.

Si tratta dell'articolo 24 bis, recante come titolo "Delitti informatici e trattamento illecito di dati" e che recita:; 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)".

A questo punto non può non rilevarsi un'ulteriore svariazione del patrio legislatore che, al momento di inserire nel corpo dell'articolo il necessario riferimento all'articolo 167 del decreto legislativo n.196 del .2003...( c.d Codice della Privacy) che prevede ,appunto il reato di trattamento illecito

dei dati, richiamato in rubrica ....,ahimè.. si è distratto...per cui il riferimento della rubrica all'ipotesi di cui al citato articolo 167

appare assolutamente incomprensibile...Inoltre appare implicitamente escluso dall'elenco dei reati per cui è prevista la responsabilità amministrativa ,il delitto di frode informatica

previsto dall'articolo 640 ter ,non in danno dello Stato o di altre ente pubblico..Nessuna spiegazione di tale omissione si ricava dal testo della relazione al disegno di legge originario.....

6)

### **Le modifiche di natura processuale**

Non è possibile in questa sede e indicare in dettaglio le modifiche introdotte nel codice di diritto processuale per adeguare la normativa esistente alle previsioni della Convenzione, anche se si tratta di modifiche importanti... alcune delle quali riguardano la ricerca dei mezzi di prova in relazione ai sistemi informatici e telematici. Tali modifiche riguardano l'art. 244 relativo

ai

casi ed

alle forme delle ispezioni ambientali e personali, l'art. 248 riguardante la richiesta di consegna di cosa determinata in sede di perquisizione, l'art. 254 (in tema di doveri di esibizione di atti e documenti e di segreti di ufficio, professionale o di stato...In tema di sequestro è stato inserito un nuovo articolo, il 254 bis, intitolato "Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni....Altre modifiche riguardano l'art. 259 in tema di custodia delle cose sequestrate e l'art. 260 ,relativo all'apposizione di sigilli alle cose sequestrate.

Altre innovazioni sono state introdotte in relazione all'attività ad iniziativa della polizia giudiziaria E' stato così modificato l'art. 352 relativo alle perquisizioni, l'art. 354 relativo all'acquisizione di plichi e di corrispondenza, l'art. 354 relativo agli accertamenti urgenti

sui luoghi, sulle cose e sulle persone ed al sequestro.

Una importante modifica riguarda l'introduzione nell'art. 132 del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003 n. 196 del comma 4-ter che consente al Ministro dell'Interno, o su sua delega, ai responsabili degli uffici centrali specialistici in materia informatica o telematica delle Forze dell'Ordine, di ordinare, anche in relazione alle eventuali richieste avanzate da Autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici, di conservare o proteggere per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico ai fini delle investigazioni previste all'art. 226 del decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento è prorogabile per motivate esigenze, per una durata complessiva non superiore a 6 mesi, e 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. Il comma quater prevede che 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 ed 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 costituisce più grave reato, le disposizioni dell'articolo 326 del codice penale.

Il comma 4 quinquies, a sua volta, stabilisce che i provvedimenti adottati ai sensi del comma 4-ter sono comunicanti 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".

Passando ad altro argomento, molto importante è la disposizione dell'articolo 11 della legge di ratifica che riguarda la competenza, e che aggiunge all'articolo 51 del codice di rito un ulteriore comma, il 3 quinquies, secondo cui .quando si tratta di procedimenti

per i delitti, consumati o tentati, di cui agli articoli 600 bis, 600 ter, 600 quater, 600 quinquies, 615 ter, 615 quater, 615 quinquies, 617 bis, 617 ter, 617 quater, 617 quinquies, 617 sexies, 635 bis, 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 del capoluogo e del distretto nel cui ambito ha sede il giudice competente...

Infine l'articolo 13 della legge di ratifica prevede norme di adeguamento in relazione alla individuazione delle autorità dello Stato competenti per le attività previste dagli articoli 24, 27 e 35 della Convenzione precisando che si tratta, rispettivamente, del Ministro della Giustizia e di

quello dell'Interno .

<https://www.diritto.it/brevi-cenni-sulla-legge-italiana-di-autorizzazione-alla-ratifica-della-convenzione-di-budapest-sulla-cibercriminalita-consiglio-d-europa/>