11. sollecita gli Stati membri a seguire la recente iniziativa della Norvegia e a non avvalersi dei «pozzi di carbonio» per soddisfare l'obiettivo di Kyoto, come contemplato nell'accordo finale di Bonn;

12. ritiene che l'acquisto nell'Unione europea di diritti di emissione («hot air») debba essere subordinato all'utilizzo di finanziamenti verdi in Russia e in Ucraina e che tutti i finanziamenti raccolti mediante la vendita di diritti di emissione debbano essere utilizzati per progetti utili per l'ambiente;

13. ribadisce che il processo di Kyoto rappresenta unicamente la base di un ulteriore lavoro volto a combattere il cambiamento climatico; esorta pertanto le parti contraenti, e in particolare i paesi industrializzati, ad adottare ulteriori obiettivi ambiziosi di riduzione delle emissioni;

14. sottolinea che la cooperazione con il Parlamento europeo, la Commissione e il Consiglio si è rivelata costruttiva ed auspica che la conferenza di Marrakech rafforzi tale cooperazione e il ruolo del Parlamento europeo nel quadro di questo processo;

15. incarica la sua Presidente di trasmettere la presente risoluzione alla Commissione, al Consiglio, ai governi e ai Parlamenti degli Stati membri e al segretariato della Convenzione quadro delle Nazioni Unite sui cambiamenti climatici.

---

8. Lotta alla criminalità informatica

A5-0284/2001

Raccomandazione del Parlamento europeo sulla strategia intesa a creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica (2001/2070(COS))

Il Parlamento europeo,

— visto l'articolo 39, paragrafo 3, del trattato sull'Unione europea, che consente al Parlamento europeo di formulare raccomandazioni al Consiglio,

— vista la comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni «Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica» (COM(2000) 890),

— viste le sue precedenti risoluzioni sulle tecnologie dell'informazione, segnatamente le sue risoluzioni sul copyright e il commercio elettronico,

— visti i recenti lavori e risultati ottenuti in questo settore dal G8, dall'OSCE, dalle Nazioni Unite, dal Consiglio d'Europa, dai rappresentanti dell'industria, dai servizi di polizia e dagli organismi preposti alla protezione della privacy,

— visto l'articolo 107 del Regolamento,

— vista la relazione della commissione per le libertà e i diritti dei cittadini, la giustizia e gli affari interni e i pareri della commissione giuridica e per il mercato interno e della commissione per l'industria, il commercio estero, la ricerca e l'energia (A5-0284/2001),

A. preoccupato per le dispute giuridiche che potrebbero insorgere in sede di applicazione della Convenzione del Consiglio d'Europa sul crimine informatico, della legislazione degli Stati membri e delle norme della Comunità europea e dell'Unione europea,

B. visto che un'adeguata protezione dei dati costituisce una condizione indispensabile per ottenere la fiducia dei consumatori e assicurare un flusso affidabile e libero dell'informazione,

Giovedì 6 settembre 2001

C. considerando che le nuove tecnologie dell'informazione e della comunicazione stanno avendo un impatto rivoluzionario e fondamentale per la crescita dell'Europa, la competitività e le opportunità occupazionali, oltre che profonde implicazioni economiche, sociali e giuridiche, e stanno diventando un elemento cruciale delle nostre economie,

D. consapevole pertanto del fatto che la società dell'informazione potrebbe essere sfruttata da criminali per mettere a repentaglio non soltanto il corretto funzionamento del software, dell'hardware e dei network, ma anche per perpetrare reati di tipo tradizionale grazie a tecniche computerizzate, attaccando per esempio:

— i diritti fondamentali, la dignità e la privacy dei cittadini (violazioni della privacy, comportamenti razzisti e xenofobi, pornografia infantile, traffico di esseri umani, traffico illecito di droghe, organi ed armi, ecc.),

— il corretto funzionamento della vita quotidiana nella nostra società, perturbando servizi di interesse generale (attacchi alle reti computerizzate dei servizi di trasporto e comunicazione, alle forniture di energia e di acqua, alle attività economiche e ai servizi ambientali),

— il corretto funzionamento della nostra economia attraverso minacce all'industria (copyright, telemarketing, trasferimenti di conti) e ai servizi finanziari (frodi finanziarie, rapine alle banche, riciclaggio di denaro sporco, frodi sulle carte di credito),

— la sicurezza interna ed esterna degli Stati membri attraverso la minaccia del terrorismo,

E. consapevole del fatto che le tecniche tradizionali o le procedure tradizionali di applicazione della legge utilizzate dai servizi di polizia non sempre sono sufficienti per fronteggiare questi tipi di reato a causa delle difficoltà che si incontrano nel definire in modo coerente ed efficace:

— l'autore di un reato, nel caso di un'associazione a delinquere su scala mondiale, e la responsabilità di terzi,

— il luogo in cui si è verificato l'evento,

— i criteri di valutazione dell'elemento doloso (*dolus directus aut dolus eventualis*),

— l'impatto dei danni reali o potenziali collegati all'attività,

— il luogo in cui è stato commesso il reato visto che il contesto è esso stesso senza frontiere,

— le competenze dell'autorità giudiziaria e gli strumenti di mutua assistenza giuridica,

— le modalità della lotta contro il crimine informatico che, per definizione, è un fenomeno in evoluzione, sotto il profilo formale e contenutistico,

F. preoccupato per il fatto che, malgrado gli sforzi delle organizzazioni internazionali e sopranazionali, i vari ordinamenti giuridici nazionali, persino all'interno degli Stati membri, mostrano tuttora notevoli divergenze specie per quanto riguarda:

— le norme penali relative all'attività di «hacking», alla tutela della segretezza commerciale e all'elemento oggettivo del reato,

— i poteri coercitivi degli organismi di investigazione (specie per quanto riguarda i dati criptati e le indagini nelle reti internazionali),

— l'ambito di applicazione, relativamente alla responsabilità dei provider di servizi intermedi, da una parte, e i fornitori di contenuto dall'altro, della giurisdizione penale che implica l'attuazione della direttiva sul commercio elettronico in modo da raggiungere l'armonizzazione,

G. convinto che tali divergenze indeboliscano la capacità degli Stati membri di lottare contro la criminalità informatica e che gli Stati membri e le istituzioni europee debbano definire un quadro giuridico coerente per le indagini e le sanzioni penali con riferimento alla criminalità ad alta tecnologia e ai reati connessi ai sistemi informatici, come proposto dalla Commissione nella sua comunicazione, per proteggere i cittadini europei, il mercato interno e la sicurezza interna dell'Unione stessa e dei suoi Stati membri,

H. consapevole che la lotta contro la criminalità informatica è già stata presa in considerazione dal Consiglio europeo di Tampere quale priorità nello sviluppo dell'Unione come spazio di libertà, sicurezza e giustizia (articolo 2 del trattato UE), che deve essere fondato su:

— i principi della democrazia, dello stato di diritto e della protezione dei diritti fondamentali (articolo 6, paragrafo 2, del trattato UE),

— il controllo giurisdizionale della Corte di giustizia sulle iniziative delle istituzioni europee, anche quando queste operano nel settore della cooperazione di polizia e giudiziaria in materia penale (articolo 46, lettera d), del trattato UE),

— il reciproco rafforzamento tra le politiche della Comunità e dell'Unione, tenendo conto che il trattato UE non pregiudica il trattato CE (articolo 47 del trattato UE),

— l'obbligo per gli Stati membri di cooperare lealmente fra loro e con le istituzioni europee all'atto di introdurre misure interne ed esterne per una società europea dell'informazione più sicura, preservando allo stesso tempo i diritti dell'Unione e della Comunità, in particolare mediante l'introduzione nelle convenzioni internazionali di opportune clausole di accesso/sconnessione conformi alla giurisprudenza della Corte di giustizia (causa «AETR») [1],

— la necessità di associare il Parlamento europeo, con l'obiettivo di assicurare il controllo democratico in sede di adozione della legislazione interna dell'Unione e degli accordi internazionali (come le convenzioni del Consiglio d'Europa),

I. ricordando che un futuro quadro regolamentare dell'Unione per quanto concerne la criminalità informatica deve assicurare che i requisiti dei singoli Stati membri e dell'Unione in materia di sicurezza siano compatibili con i principi della cittadinanza europea e che occorre trovare un giusto equilibrio tra le attività di lotta contro la criminalità informatica e i diritti fondamentali dell'individuo riguardanti la riservatezza e la protezione dei dati personali,

J. ricordando che il diritto fondamentale alla riservatezza e alla protezione dei dati personali in questi settori va interpretato sulla base dell'articolo 8 della Convenzione europea sui diritti dell'uomo (CEDU) e della giurisprudenza del Tribunale per i diritti dell'uomo, secondo cui ogni eccezione ai principi della riservatezza richiede una base giuridica, deve essere necessaria ai fini della protezione di un interesse pubblico e deve essere rigorosamente proporzionata all'obiettivo specifico previsto, per cui qualsiasi obbligo generalizzato concernente la conservazione dei dati e qualsiasi forma di intercettazione sistematica sono in contrasto con questo principio di proporzionalità [2],

K. ribadendo il parere del gruppo di lavoro istituito sulla base dell'articolo 29 della direttiva 95/46/CE [3] e le dichiarazioni dei responsabili nazionali della sicurezza informatica riuniti a Stoccolma e ad Atene,

---

[1] Una clausola generale di sconnessione è più efficace che non cercare di individuare per ogni aspetto di una Convenzione possibili incoerenze con il diritto comunitario. Si tratta inoltre di un'operazione difficile, in quanto le disposizioni della Convenzione sono generali e il diritto comunitario può evolvere. Essendo le disposizioni della Convenzione così generali, la loro attuazione a livello di diritto nazionale potrebbe risultare incompatibile con il diritto comunitario. Una clausola di sconnessione è utile anche per rassicurare tutti gli interessati che la Convenzione non usurperà gli strumenti giuridici comunitari esistenti.

[2] Secondo questa giurisprudenza, in particolare:
- l'obiettivo dell'articolo 8 è essenzialmente quello di proteggere l'individuo da interferenze arbitrarie da parte delle autorità pubbliche (CDU, sentenza del 23.7.1968), per cui un'eccezione al diritto alla protezione dei dati è ammissibile solo se necessaria o indispensabile in una società democratica;
- qualsiasi eccezione deve essere fondata sul diritto, che deve essere «accessibile» e «prevedibile» (sentenze CDU «Groppera Radio AG» del 28.3.1990, «Barthold» del 25.3.1985, «Kruslin» del 24.4.1990 e «Chappel» del 30.3.1989);
- la protezione giuridica deve essere assicurata in particolare quando viene esercitato in segreto un potere dell'esecutivo, come nel caso delle misure di sorveglianza segreta delle comunicazioni. In tali casi sarebbe contrario allo stato di diritto che la discrezionalità giuridica accordata all'esecutivo venisse espressa in termini di potere illimitato. Pertanto, la legge deve indicare con sufficiente chiarezza la portata della discrezionalità riconosciuta alle autorità competenti e le modalità del suo esercizio, tenuto conto dell'obiettivo legittimo della misura in questione, per fornire all'individuo una protezione adeguata contro un'interferenza arbitraria. (sentenze CDU «Malone» del 2.08.1984 e, nella stessa prospettiva, «Sunday Times» del 26.04.1979 e «Valenzuela Contreras» del 30.07.1998).

[3] GU L 281 del 23.11.1995, pag. 31.

Giovedì 6 settembre 2001

1. eprime le seguenti raccomandazioni:

Nella misura in cui la Comunità e l'Unione sono direttamente responsabili

a) invita il Consiglio e la Commissione ad avviare, a livello dell'Unione, una strategia coerente che consenta da una parte di preservare Internet (o qualsiasi altra rete di comunicazione internazionale) come un mercato globale e libero nonché la sicurezza dei servizi e delle infrastrutture dell'informazione in modo che ognuno possa portare avanti le sue diverse attività e, dall'altro, di prevenire, allo stesso tempo, le attività criminali lesive delle libertà e degli interessi dei cittadini e dell'interesse pubblico;

b) invita la Commissione a mettere a punto definizioni comuni e proposte per risolvere i conflitti di giurisdizione tra Stati membri (la non esclusione della nazionalità essendo una delle distinzioni principali) e per ravvicinare il diritto penale sostanziale nella misura ritenuta necessaria per raggiungere una coerenza a livello politico e giuridico tale da facilitare l'azione penale e l'irrogazione della pena nei confronti di coloro che si rendono responsabili di:

   — il traffico di esseri umani, il riciclaggio di denaro sporco, la pornografia infantile e il terrorismo;

   — i cosiddetti crimini high-tech, ad esempio diffusione di virus, diniego di servizi, accesso non autorizzato, con o senza dolo, o azioni e attività miranti ad eludere la protezione della proprietà intellettuale, come la vendita e pubblicizzazione di dispositivi di «hacking» per finalità illecite e la pubblicazione su Internet di codici o parole d'ordine;

   sottolinea pertanto che occorre sancire il principio che le attività criminali «off-line» devono essere criminali «on-line» e che, laddove vi sia una definizione comune dei reati, occorre garantire il riconoscimento reciproco delle ordinanze predibattimentali; chiede pertanto alla Commissione:

   — di proporre misure legislative e iniziative non legislative finalizzate alla definizione di un quadro globale di politica di lotta al crimine informatico al fine di garantire la sicurezza delle infrastrutture dell'informazione;

   — di fissare gli obiettivi per la lotta contro la criminalità informatica e i mezzi per conseguire tali obiettivi;

   — di valutare l'efficacia del quadro regolamentare esistente della succitata direttiva 95/46/CE e della direttiva 97/66/CE [1];

   — di consultare, in particolare, le società di carte di credito al fine di consentire una maggiore autoregolamentazione di Internet e di promuovere la sicurezza;

   — di considerare l'introduzione, su base volontaria, di un sistema europeo di certificazione (standard europeo) per far fronte alla criminalità informatica, in linea con le posizioni già espresse dal Parlamento europeo;

   — di avanzare proposte relative al ravvicinamento del diritto sostanziale e procedurale nel settore della tutela della proprietà intellettuale e all'introduzione di sanzioni realmente dissuasive nonché procedure calibrate sull'ambiente telematico mondiale;

c) invita il Consiglio e la Commissione a delineare misure per la raccolta delle prove da parte dei servizi di polizia, che devono essere:

   — chiaramente definite in relazione allo specifico comportamento criminale come definito al punto (b);

   — legittime in modo che, ad esempio, qualsiasi intercettazione rispetti le norme già definite nella Convenzione di assistenza legale reciproca e ottemperare comunque a una decisione giudiziaria;

   — proporzionate e limitate, nel tempo e nella portata, a ciò che è strettamente necessario per consentire, se del caso, prima del pronunciamento della Corte, una procedura finalizzata soprattutto al blocco delle informazioni pertinenti che essendo volatili, andrebbero altrimenti perse;

   — concepite in modo tale da evitare qualsiasi intrusione arbitraria nel settore della privacy;

d) invita il Cosiglio e la Commissione a far sì che queste misure assicurino un equilibrio tra un'efficace prevenzione e punizione del crimine ed il rispetto del diritto alla libertà di ogni individuo e alla tutela dei dati personali e rispettino la Convenzione europea sui diritti dell'uomo, la Carta UE dei diritti fondamentali (in particolare il diritto alla libertà di espressione, il rispetto della vita e delle comunicazioni private e alla protezione dei dati personali) e la legislazione UE nonchè a tener conto dei pareri

[1] GU L 24 del 30.1.1998, pag. 1.

del gruppo di lavoro istituito sulla base dell'articolo 29 della succitata direttiva 95/46/CE e del responsabile della protezione dei dati istituito dal regolamento (CE) n. 45/2001 [1]; in tale contesto, ricorda che il problema dell'anonimato dell'accesso a Internet va attentamente analizzato al fine di trovare le soluzioni più eque al problema della criminalità informatica senza pregiudicare gli interessi legittimi degli utilizzatori;

e) raccomanda alla Commissione di concentrare:

- a livello politico, le competenze in materia di protezione dei dati, attualmente disperse tra le Direzioni generali Mercato interno e Società dell'informazione, sotto la responsabilità del Commissario competente per i diritti fondamentali;
- a livello amministrativo, in una direzione specifica, tutte le unità della Commissione responsabili per l'attuazione delle politiche connesse alla privacy;
- a livello del responsabile europeo per la protezione dei dati, la segreteria di tutte le autorità di protezione dei dati operanti nell'ambito dell'Unione;

f) invita il Consiglio e la Commissione a confermare il principio in base al quale i costi per la lotta contro il crimine, derivanti da misure legislative, dovrebbero essere imputati ai servizi di polizia. Nei casi in cui, conformemente alla legislazione dell'Unione o a quella nazionale, occorra per lo stoccaggio di dati la loro salvaguardia e altre esigenze generatrici di costi aggiuntivi, la cooperazione di organismi privati come, ad esempio, i fornitori di servizio Internet e gli operatori di rete, le spese devono essere rimborsate; gli operatori di rete e i fornitori di servizi non devono essere ritenuti responsabili in caso di mancato rispetto degli obblighi contrattuali o di danni dovuti a richieste di controlli di polizia; in linea generale rileva che l'uso di Internet deve essere accessibile a tutti e che conseguentemente il suo costo deve essere mantenuto ad un livello quanto più basso possibile, in conformità delle conclusioni del Vertice di Lisbona;

g) chiede al Consiglio e alla Commissione di incoraggiare la cooperazione di quanti operano nell'industria informatica al fine di rendere efficace la prevenzione dei crimini informatici garantendo che le leggi non creino oneri eccessivi all'industria;

h) raccomanda al Consiglio e alla Commissione di istituire, a livello UE, un Foro del crimine informatico in cui i servizi di polizia, i provider, gli operatori delle telecomunicazioni, le organizzazioni per le libertà civili, i rappresentanti dei consumatori, le autorità preposte alla protezione dei dati ed altre parti interessate si incontrino al fine di trovare soluzioni giuridiche comuni per taluni problemi esistenti e di accrescere la comprensione reciproca e la cooperazione a livello UE; compito del Foro sarebbe di accrescere la consapevolezza dei cittadini circa i rischi creati dai criminali che si servono di Internet, di promuovere la miglior prassi per la sicurezza, di elaborare un codice etico, di individuare strumenti e procedure efficaci per contrastare il crimine informatico e incoraggiare l'ulteriore sviluppo dei meccanismi di gestione delle crisi e di allerta; chiede agli Stati membri che ancora non abbiano istituito simili strutture sul loro territorio di dare vita ad iniziative di questo genere;

i) invita il Consiglio a definire chiaramente il ruolo di Europol e Eurojust nella lotta contro il crimine informatico evitando la duplicazione delle banche dati interne, assicurando il coordinamento reciproco e garantendo che l'attività di questi organismi sia soggetta al controllo democratico e rispetti l'acquis comunitario sulla protezione dei dati personali; esorta pertanto gli Stati membri a sostenere le unità di polizia specializzate nella lotta contro il crimine informatico a livello nazionale;

j) chiede al Consiglio e alla Commissione di organizzare una conferenza di insigni giuristi degli Stati membri e dei paesi candidati:

- per discutere delle questioni e dei problemi della criminalità informatica che si pongono sotto il profilo della giurisdizione su Internet (ad esempio, le banche dati) e del reciproco riconoscimento delle decisioni giudiziarie in campo penale nonché dell'assistenza reciproca (ad esempio, clausola della duplice perseguibilità, riduzione della burocrazia, sostituzione delle rogatorie e dei trattati con procedure più rapide) e
- per esaminare i problemi relativi alla definizione dei reati, alle questioni correlate in materia di diritti umani, alle questioni probatorie e alle circostanze nelle quali si potrebbero eventualmente istituire «cibertribunali» specializzati;

[1] GU L 8 del 12.1.2001, pag. 1.

Giovedì 6 settembre 2001

k) raccomanda al Consiglio e alla Commisione di promuovere la ricerca europea nel campo delle tecnologie di protezione e prevenzione, quali le tecniche di trascrizione in codice per migliorare la possibilità di autotutela dell'utente e accrescere la consapevolezza degli utenti; ritiene che i consumatori, l'industria e gli altri soggetti dovrebbero quindi sviluppare e applicare misure di sicurezza e tecnologie preventive, in particolare:

   — rafforzando, in conformità con la legislazione comunitaria esistente, i «numeri verdi» *(hotlines)* che promuovono un'Internet più sicura, sistemi europei di valutazione per i fornitori di Internet e altre iniziative che assicurino messaggi sicuri, motori di ricerca di facile uso (con filtri), l'individuazione e il perseguimento di forum di discussione connessi alla pornografia infantile e promuovendo la cooperazione con le società che emettono carte di credito per individuare servizi illegali;

   — coordinando il trattamento dei reclami presentati da utenti di Internet in materia di trafficanti, pornografia infantile e xenofobia e collegandoli alla banca dati del G-8, per assicurare uno scambio di informazioni in tempo reale su una rete di punti di contatto funzionante 24 ore su 24;

   — facendo in modo che il CCR coordini la ricerca sulla sorveglianza della tecnologia «peer-to-peer», oltre alla ricerca in generale sull'informatica forense;

   — prendendo pienamente atto della priorità che il Parlamento accorda alla ricerca nel settore della sicurezza dell'informazione, come stabilito nella sua risoluzione del 3 maggio 2001 su «Internet di prossima generazione: la necessità di un'iniziativa di ricerca dell'UE» [1];

   — raccogliendo e analizzando i dati statistici disponibili sui vari tipi di reato informatico a sostegno del quadro di valutazione della Commissione volto a esaminare i progressi compiuti nella creazione di una zona di libertà, sicurezza e giustizia; invita gli Stati membri e quanti lavorano nell'industria informatica a cooperare in tale settore;

Nella misura in cui è necessaria l'iniziativa internazionale

l) raccomanda al Consiglio e alla Commissione di invitare gli Stati membri (e i paesi candidati) a coordinare i loro sforzi sulla scena internazionale e ad adottare un approccio comune alle attività svolte in materia di lotta contro la criminalità informatica nelle varie sedi internazionali (Consiglio d'Europa, G-8, Gruppo di Lione, OCSE e ONU) e in particolare a modificare il progetto di Convenzione del Consiglio d'Europa sul crimine informatico (cui aderiscono anche gli Stati Uniti, il Canada, il Giappone e il Sudafrica), in modo da salvaguardare un reale equilibrio tra gli interessi dei servizi di polizia e la necessità di proteggere i diritti fondamentali e le libertà dei cittadini, in particolare la privacy, la protezione dei dati e gli interessi commerciali. A tal fine è necessario che:

   — il principio di stoccaggio generalizzato dei dati venga vietato;

   — nessuno possa essere obbligato a incriminare se stesso rivelando codici o programmi di criptazione;

   — non possano essere liberamente trasferiti dati verso un paese terzo che non garantisca un livello di protezione dei dati equivalente a quello assicurato dall'articolo 8 della CEDU e dalla Convenzione n. 108 del Consiglio d'Europa;

   — i diritti comunitari e dell'Unione siano mantenuti, per consentire, da una parte, alla Comunità o all'Unione di aderire alla Convenzione, in rappresentanza degli Stati membri quando è in gioco la politica comunitaria o dell'Unione (clausola di collegamento) e, d'altra parte, per affermare che gli Stati membri sono vincolati dalle regole dell'Unione o della Comunità se emerge un conflitto con la Convenzione (clausola di distacco);

   ritiene pertanto che occorra rafforzare tali aspetti in una ulteriore nuova versione prima di firmare la Convenzione;

m) chiede al Consiglio e alla Commissione di sollecitare gli Stati membri a modificare immediatamente il progetto di Convenzione includendo una clausola di accesso e di sconnessione che tuteli i diritti della Comunità e dell'Unione così come sono stati definiti dalla Corte di giustizia;

---

[1] «Testi approvati» in tale data, punto 14.

n) raccomanda al Consiglio e alla Commissione di avviare un ampio dialogo e intensificare gli scambi esistenti con gli Stati Uniti allo scopo di individuare una strategia comune e di ridurre almeno le differenze che si constatano nelle metodologie di lotta contro il crimine informatico, così come sono state delineate nella presente raccomandazione; al riguardo va migliorato il dialogo transatlantico su questioni legislative ed esaminata la possibilità di inviare rappresentanti dell'UE presso organi informali statunitensi che lottano contro il crimine informatico, quali il Partenariato per la sicurezza delle infrastrutture essenziali (PCIS); occorrerebbe inoltre invitare rappresentanti statunitensi presso gli organismi corrispondenti dell'UE;

*

* *

2. incarica la sua Presidente di trasmettere la presente raccomandazione al Consiglio e alla Commissione.

---

9. Relazione annuale sull'attività del Mediatore europeo (2000)

A5-0280/2001

Risoluzione del Parlamento europeo concernente la relazione annuale sull'attività del Mediatore europeo (2000) (C5-0302/2001 − 2001/2043(COS))

Il Parlamento europeo,

− vista la relazione annuale per il 2000 del Mediatore europeo (C5-0302/2001),

− visto l'articolo 43 della Carta dei diritti fondamentali dell'Unione europea,

− visto il trattato che istituisce la Comunità europea, in particolare gli articoli 21 e 195,

− visto il trattato che istituisce la Comunità europea del carbone e dell'acciaio, in particolare l'articolo 20,

− visto il trattato che istituisce la Comunità europea dell'energia atomica, in particolare l'articolo 107,

− vista la sua risoluzione del 17 novembre 1993, in particolare la sezione concernente lo statuto e le condizioni generali per l'esercizio delle funzioni del Mediatore ([1]),

− vista la sua risoluzione del 9 marzo 1994 concernente lo statuto e le condizioni generali per l'esercizio delle funzioni del Mediatore, segnatamente l'articolo 3, paragrafo 8 ([2]),

− vista la sua risoluzione del 14 luglio 1995 sul ruolo del Mediatore europeo ([3]),

− vista la sua risoluzione del 6 luglio 2000 concernente la relazione annuale del Mediatore europeo relativa al 1999 ([4]),

− vista la sua risoluzione del 6 luglio 2000 sulle deliberazioni della commissione per le petizioni nell'anno parlamentare 1999-2000 ([5]),

− visto l'articolo 47, paragrafo 1, del suo regolamento,

− vista la relazione della commissione per le petizioni (A5-0280/2001),

([1]) GU C 329 del 6.12.1993, pag. 132.
([2]) GU L 113 del 4.5.1994, pag. 15.
([3]) GU C 249 del 25.9.1995, pag. 226.
([4]) GU C 121 del 24.4.2001, pag. 468.
([5]) GU C 121 del 24.4.2001, pag. 465.