COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 22.5.2007
SEC(2007) 641

DOCUMENTO DI LAVORO DELLA COMMISSIONE

Documento di accompagnamento della

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO E AL COMITATO DELLE REGIONI

Verso una politica generale di lotta contro la cibercriminalità

SINTESI DELLA VALUTAZIONE D'IMPATTO

{COM(2007) 267 definitivo}
{SEC(2007) 642}

SINTESI

1. INTRODUZIONE

Negli ultimi anni l'uso di Internet è esploso e la comparsa di nuovi fenomeni e di nuove tecniche ha creato maggiore insicurezza.

Nel **programma legislativo e di lavoro per il 2007** la Commissione giudica che è ormai necessario aggiornare completamente la sua politica in materia di cibercriminalità e quindi prevede di mettere a punto una comunicazione su una politica europea di lotta contro la cibercriminalità.

Nella fase iniziale di consultazione è apparso chiaro che mancano dati e statistiche al riguardo; per questo motivo principale la Commissione ha commissionato (2006) uno **studio esterno**[1] (in seguito "studio esterno"), che ha costituito la base principale della valutazione d'impatto.

Durante la preparazione la Commissione ha anche analizzato una serie di misure legislative e non legislative, soprattutto in relazione a possibili "lacune" del quadro normativo vigente. Occorre sottolineare che la Commissione ha prestato particolare attenzione alla **convenzione del Consiglio d'Europa sulla cibercriminalità**[2] e alla **decisione quadro relativa agli attacchi contro i sistemi di informazione**[3], ritenendoli gli strumenti normativi più completi in termini di norme sostanziali e procedurali.

Sulla base di queste attività, la Commissione sta preparando una nuova iniziativa di politica generale, che include una comunicazione sulla lotta contro la cibercriminalità a livello dell'UE. Di conseguenza, la presente valutazione d'impatto verterà principalmente su questioni strategiche.

In questo contesto la Commissione desidera sottolineare il proprio impegno a garantire che la politica volta a combattere e perseguire la cibercriminalità sarà definita e attuata nel pieno rispetto dei diritti fondamentali, in particolare della libertà di espressione, del rispetto della vita privata e familiare e della protezione dei dati personali. A tal fine si procederà conformemente alla comunicazione della Commissione intitolata "Il rispetto della Carta dei diritti fondamentali nelle proposte legislative della Commissione" del 2005 [COM(2005) 172].

---

1 Studio d'impatto di una comunicazione sulla cibercriminalità, elaborato dalla società *Yellow Window Management Consulting* (contratto n. DG 2006/JLS D 2/03).

2 Convenzione del Consiglio d'Europa del 2001 sulla cibercriminalità: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3 Decisione quadro relativa agli attacchi contro i sistemi di informazione (2005/222/GAI).

2. PROBLEMI E OBIETTIVI

Il rapido sviluppo di Internet e di altri sistemi di informazione comporta l'emergere di un settore economico completamente nuovo e di nuovi e rapidi flussi di scambio di dati, prodotti e servizi attraverso le frontiere interne ed esterne dell'Unione. I consumatori e i cittadini ovviamente ne traggono numerosi vantaggi, tuttavia questo sviluppo apre anche molte nuove possibilità di illeciti, e si delineano chiaramente modelli di nuove attività criminali contro Internet o che comunque si avvalgono dei sistemi di informazione. Queste attività criminali sono in costante evoluzione e l'attività legislativa e quella operativa di contrasto difficilmente riescono a stare al passo. Il carattere intrinsecamente transnazionale di questo nuovo tipo di reato pone inoltre l'esigenza di una maggiore cooperazione transnazionale fra autorità di contrasto.

Per esaminare il problema generale in modo più approfondito, lo si è scisso in otto aspetti strategici problematici:

- crescente vulnerabilità della società, delle imprese e dei cittadini alla cibercriminalità;
- maggior frequenza e sofisticatezza dei reati informatici;
- mancanza, a livello dell'UE, di una politica e di una legislazione coerenti per combattere la cibercriminalità;
- difficoltà specifiche nella cooperazione operativa tra autorità di contrasto;
- esigenza di sviluppare competenze e strumenti tecnici, la formazione e la ricerca;
- mancanza di una struttura funzionale di cooperazione tra attori importanti dei settori pubblico e privato;
- ripartizione poco chiara delle responsabilità e degli obblighi;
- mancanza di consapevolezza dei rischi connessi alla cibercriminalità.

Va osservato che le consultazioni svolte in vista della presente relazione hanno rivelato una sorprendente convergenza di opinioni di tutte le parti interessate -autorità di contrasto o società private- in merito agli attuali problemi dell'UE in questo settore.

2.1. Chi sono gli interessati?

La cibercriminalità colpisce tutti i settori della società e la politica di lotta contro tale fenomeno sarà visibile praticamente ovunque. Considerato il numero elevatissimo di cittadini che usano computer privati, la maggior parte di essi può -proprio perchè vittime potenziali- essere interessata dalle iniziative di lotta alla cibercriminalità.

Alcuni elementi evidenziano tuttavia un aumento delle attività criminali contro gruppi specifici di vittime, per i quali una politica efficace di lotta contro la cibercriminalità potrebbe quindi avere indubbi vantaggi. Parimenti, l'industria della società dell'informazione, e la società dell'informazione in generale, potrebbero essere importanti attori in questo contesto, date le rilevanti ripercussioni economiche positive che deriverebbero da un rafforzamento della sicurezza o dall'instaurarsi di un clima di maggiore sicurezza.

2.2. L'UE ha il diritto di adottare misure?

Date l'entità e la gravità delle minacce alla sicurezza, è e sarà sempre più necessario rispondere alle minacce della cibercriminalità. Gli aspetti della sicurezza connessi alla cibercriminalità hanno una dimensione globale e pertanto non possono essere affrontati solo a livello nazionale. La minaccia è internazionale e tale deve essere anche la risposta, perlomeno in parte. È indubbio che la lotta contro la cibercriminalità continuerà ad essere importantissima e incisiva a livello nazionale, ma è anche chiaro che occorre coordinare gli sforzi nazionali ed eventualmente integrarli a livello europeo.

2.3. Obiettivi

Alla luce dei problemi esposti, l'obiettivo strategico generale della politica proposta può essere così sintetizzato:

Potenziare e coordinare meglio la lotta contro la cibercriminalità a livello nazionale, europeo e internazionale.

Questo obiettivo strategico generale può essere scisso in cinque sottobiettivi strategici, presentati di seguito in un ordine di priorità provvisorio:

- migliorare le azioni operative di contrasto transnazionali contro la cibercriminalità in generale e contro le forme gravi di cibercriminalità in particolare, e migliorare lo scambio di informazioni, intelligence e migliori pratiche tra autorità di contrasto degli Stati membri e di paesi terzi;

- individuare e creare strumenti operativi che permettano ai settori pubblico e privato di cooperare e di fissarsi obiettivi comuni, e migliorare lo scambio di informazioni, intelligence e migliori pratiche tra questi due settori per lottare contro la cibercriminalità a livello dell'UE;

- istituire una piattaforma e strutture politiche per elaborare una politica europea coerente di lotta alla cibercriminalità, in cooperazione con gli Stati membri e le organizzazioni competenti dell'UE e internazionali, e rendere più efficaci i quadri normativo e istituzionale esistenti, anche chiarendo le responsabilità e gli obblighi di tutti gli attori interessati;

- far fronte alla crescente minaccia di forme gravi di cibercriminalità promuovendo l'acquisizione di competenze, conoscenze e strumenti tecnici, incluse azioni per potenziare la formazione e la ricerca nel settore;

- fare opera di sensibilizzazione generale sulle minacce della cibercriminalità, soprattutto tra i consumatori e gli altri gruppi vulnerabili di vittime potenziali.

3. OPZIONI POLITICHE STRATEGICHE

Qualsiasi politica di lotta contro la cibercriminalità deve, per la natura stessa del suo oggetto, essere poliedrica. Per essere davvero efficace, deve combinare attività di contrasto tradizionali e altri strumenti, come elementi di autoregolamentazione e strutture di cooperazione tra le varie parti interessate. È stata esposta sopra una serie di problemi e obiettivi strategici per la presente iniziativa. Per conseguire tali obiettivi occorre combinare varie azioni. Sulla base delle ampie consultazioni svolte, la Commissione ha formulato quattro opzioni politiche generali, comportanti ciascuna una serie di azioni specifiche.

3.1. Opzione politica generale n. 1: status quo/nessuna nuova azione importante

Secondo questa opzione, la Commissione non intraprende alcuna azione orizzontale generale nel settore e di conseguenza:

- continuerebbe a valutare la necessità di strumenti normativi mirati o di iniziative strategiche intraprendendo, se necessario, le azioni opportune;
- seguirebbe i progetti di struttura già avviati a livello dell'UE e internazionale per la lotta contro la cibercriminalità;
- continuerebbe a lanciare nuovi progetti in settori mirati di interesse per la lotta contro la cibercriminalità, senza però prendere iniziative politiche orizzontali.

3.2. Opzione politica generale n. 2: legislazione generale

L'opzione prevede l'adozione di una strategia volta a introdurre gradualmente un quadro normativo generale di lotta alla cibercriminalità, che implicherebbe:

- che la Commissione proponga sistematicamente definizioni di reati armonizzate o uniformi per l'UE, ma anche a livello internazionale;
- che la Commissione proponga norme minime comuni per la configurazione di fattispecie di reato e sanzioni nell'UE;
- l'istituzione di piattaforme formali di cooperazione pubblico/privato e per la formazione e la ricerca;
- la creazione di una rete formale per le attività di contrasto.

3.3. Opzione politica generale n. 3: creazione di reti informali

La Commissione istituirebbe formalmente, da sola o con altre istituzioni, reti o gruppi di esperti in materia di cibercriminalità cui affiancherebbe un sistema volontario di certificazione di sicurezza per operatori, produttori e consumatori. Ciò comporterebbe:

- la creazione di un organo informale costituito da esperti in attività di contrasto della cibercriminalità;
- la creazione di una piattaforma o rete informale di esperti di cibercriminalità provenienti dai settori pubblico e privato.

3.4. Opzione politica generale n. 4: approccio strategico coerente

Questa opzione prevede l'introduzione, a livello dell'UE, di una strategia coerente di lotta contro la cibercriminalità, la cui caratteristica principale sarebbe quella di elaborare un quadro strategico di politica europea di lotta alla cibercriminalità, con lo scopo generale di formulare migliori orientamenti per azioni concrete e ottimizzare gli strumenti esistenti. Altri aspetti operativi importanti di questa strategia sarebbero:

- una maggiore cooperazione fra autorità di contrasto a livello dell'UE;
- l'introduzione di una struttura strategica di cooperazione pubblico/privato per la lotta alla cibercriminalità;
- la promozione della creazione di una rete di cooperazione internazionale globale nel settore interessato;
- l'adozione di misure legislative, se necessarie.

4. VALUTAZIONE DELLE OPZIONI POLITICHE E SCELTA DI UN'OPZIONE

4.1. Valutazione

Le opzioni politiche generali sono state valutate in base ai seguenti criteri:

- ripercussioni sociali;
- ripercussioni economiche;
- costi per la pubblica amministrazione;
- grado di coerenza con gli obiettivi politici;
- valore aggiunto e rispetto del principio di sussidiarietà;
- fattibilità.

Le conclusioni della valutazione sono riassunte come segue.

4.1.1. Opzione politica generale n. 1

È ritenuta chiaramente insufficiente in relazione alle sfide esistenti. In linea di principio, l'opzione "nessuna nuova azione" ha un impatto limitato, nella fattispecie però è difficile valutare se l'impatto non rischi invece di essere significativo dato che, per definizione, non sono noti i tipi di reato futuri. L'impatto negativo potenziale di questa opzione è molto elevato nel lungo termine, considerata l'importanza attuale e sempre maggiore dei reati informatici.

4.1.2. Opzione politica generale n. 2

Si è concluso che questa opzione può essere perseguita solo con molta cautela e in una prospettiva a lungo termine e richiederebbe studi approfonditi di fattibilità giuridica e lunghi negoziati politici. L'opzione può avere ripercussioni molto importanti ma, essendo poco probabile che si verifichino progressi reali nel breve periodo, diventa incerta nel breve periodo. Ci si può inoltre chiedere se, nell'attuazione pratica delle iniziative strategiche, gli obiettivi saranno raggiunti in modo così efficace come lo sono a livello politico e teorico. Scegliendo questa opzione, il rischio è che il livello operativo della lotta alla cibercriminalità non venga sufficientemente coinvolto nelle scelte e decisioni politiche strategiche. Tenuto conto dell'importanza delle ripercussioni connesse, sarebbe inoltre opportuno chiarire il ruolo della Commissione al riguardo. Si potrebbe poi sostenere che risultati analoghi sono raggiungibili anche con misure meno interventiste.

4.1.3. Opzione politica generale n. 3

Questa opzione è ritenuta molto interessante dal punto di vista strategico, anche se è difficile prevederne il valore aggiunto e le ripercussioni concrete. Il rischio è che le nuove strutture di rete ottengano pochi risultati concreti. La Commissione sarebbe nella posizione ideale per coordinare azioni di autoregolamentazione nel settore interessato, ma secondo questa opzione svolgerebbe un ruolo più di coordinamento e mediazione che di direzione strategica.

4.1.4. Opzione politica generale n. 4

Si ritiene che l'opzione contempli varie azioni strategiche molto pertinenti. Le ripercussioni negative o gli ostacoli di rilevo sembrano davvero pochi. Uno degli inconvenienti è che le ripercussioni dirette della politica saranno alquanto modeste. Ciò, tuttavia, vale solo nel breve periodo; una volta adottate misure di attuazione adeguate si dovrebbero avere ripercussioni molto importanti. È tuttavia difficile prevedere con esattezza le ripercussioni concrete, in quanto la fase strategica dovrà diventare operativa in un secondo momento e solo allora saranno valutate tutte le ripercussioni.

Occorre nuovamente sottolineare che l'impatto diretto delle strategie proposte è limitato e che le azioni specifiche intraprese successivamente nel quadro di una di queste strategie saranno valutate separatamente in quella fase. La presente valutazione ha quindi carattere preliminare.

4.2. Scelta dell'opzione politica

Dall'analisi emerge chiaramente che l'opzione migliore è la n. 4, che per giunta risponde anche meglio agli obiettivi generali indicati al punto 2.4.

L'opzione di non intraprendere nessuna azione non sembra percorribile. Un approccio passivo porterebbe, con buone probabilità, al mantenimento di numerosi progetti di cooperazione bilaterale di lotta contro la cibercriminalità, senza che sia possibile trarre profitto da uno scambio orizzontale di migliori pratiche o da effetti sinergici. Una legislazione generale diretta a istituire nuovi organi a livello dell'UE, ad armonizzare le definizioni di reato e a chiarire le responsabilità e gli obblighi di tutte le parti interessate potrebbe essere interessante, ma da un'analisi della situazione politica emerge chiaramente che le proposte di legislazione generale e orizzontale avrebbero pochissime probabilità di essere adottate. Per ben poche delle parti consultate non è questa la priorità del momento. L'opzione di una legislazione generale potrà invece rivelarsi opportuna nel lungo periodo. Analogamente, può essere una

buona idea nel lungo periodo anche la creazione di nuove strutture informali per l'attività di contrasto a livello dell'UE o la cooperazione pubblico/privato; tutte le parti interessate, però, sembrano convenire che le strutture esistenti sono sufficienti ma richiedono un intervento urgente che ne migliori l'efficacia. A seguito dell'analisi è stata preferita l'opzione n. 4, "una strategia coerente". Va osservato che questa non esclude la creazione di una struttura formale (opzione n. 3) o l'adozione successiva di una legislazione generale (opzione n. 2). L'opzione prescelta, in realtà, lascia la porta resta aperta a nuove azioni.

Dall'analisi preparatoria e dai dibattiti organizzati emerge senza dubbio che la "strategia coerente" è l'opzione che, meglio delle altre, può raggiungere gli obiettivi strategici della politica. Tale strategia dovrebbe avere importanti ripercussioni positive sulla lotta contro la cibercriminalità transnazionale, in quanto ne risulteranno chiariti e rafforzati le competenze e i ruoli di tutti i partecipanti alla lotta. Inoltre, contribuirà a migliorare il dialogo e la comprensione reciproca tra i settori pubblico e privato, il che, a sua volta, potrebbe avere molte ricadute. Da un punto di vista economico, l'opzione prescelta può avere effetti sinergici importanti e ridurre i danni causati dalle attività criminali e i costi dei singoli programmi di sicurezza.

È tuttavia probabile che occorrano anni per vedere i risultati dell'opzione prescelta. È quindi difficile, allo stadio attuale, valutare tutte le potenziali ripercussioni, tanto più che i dettagli concreti della politica devono ancora essere decisi. Le ripercussioni specifiche degli elementi concreti della politica andranno pertanto valutate in una fase successiva.