# Regeringskansliet
# Faktapromemoria 2006/07:FPM101

# En allmän strategi för kampen mot IT-brottslighet

Justitiedepartementet

2007-07-08

## Dokumentbeteckning

KOM (2007) 267
Meddelande från Kommissionen till Europaparlamentet, Rådet och Regionkommittén - Mot en allmän strategi för kampen mot IT-brottsligheten

SEK (2007) 641

SEK (2007) 642

SEK (2007) 641

SEK (2007) 642

## Sammanfattning

All ny teknik kan ge upphov till nya former av kriminalitet och Internet är inget undantag. Inget land undgår den växande brottsligheten på Internet och därför lägger kommissionen nu fram en strategi mot denna typ av kriminalitet för att stärka kampen mot IT-brottslighet på nationell, europeisk och internationell nivå. Åtgärderna inriktas mot traditionella brottsformer i datasammanhang (ex. bedrägeri och förfalskning), mot publicering av illegalt innehåll (ex. barnpornografi eller anstiftan till hatbrott) och mot brott unika för elektroniska nätverk (ex. dataintrång och angrepp mot informationssystem). Den svenska ståndpunkten är i huvudsak positiv till strategin som ligger i linje med svenska åtgärder på området.

# 1 Förslaget

## 1.1 Innehåll

I meddelandet avser IT-brottslighet kriminella handlingar begångna genom användandet av elektroniska kommunikationsnätverk och informationssystem eller mot sådana system och nätverk. Begreppet appliceras på tre kategorier av kriminella aktiviteter: i) traditionella brottsformer i datasammanhang (ex. bedrägeri och förfalskning), ii) publicering av illegalt innehåll (ex. barnpornografi eller anstiftan till hatbrott samt iii) brott unika för elektroniska nätverk (ex. dataintrång och angrepp mot informationssystem). Gemensamt för samtliga kategorier är att aktiviteterna kan begås i stor skala och med stort geografiskt avstånd mellan den kriminella handlingen och dess effekter. Dessa gemensamma drag utgör fokus i kommissionens meddelande.

Senaste utvecklingen inom IT-brottslighet

Generellt sett ökar antalet IT-brott och de kriminella aktiviteterna blir alltmer sofistikerade och internationaliserade. Det finns även tydliga indikationer på en ökad inblandning av organiserade, kriminella grupper inom IT-brottsligheten. Antalet europeiska åtal på basis av samarbete mellan brottsbekämpande myndigheter över landsgränserna ökar emellertid inte.

Målsättning

Med anledning av IT-brottslighetens ombytliga natur anser kommissionen att det finns ett brådskande behov av att vidta åtgärder mot alla dess former. IT-brottslighet utgör ett tilltagande hot mot viktig infrastruktur, samhälle, affärsliv och medborgare. Kommissionens lansering av initiativ till en allmän strategi för förbättrad samordning av kampen mot IT-brottslighet ska ses som ett försök att komma till rätta med problemet. Syftet är således att stärka kampen mot IT-brottslighet på nationell, europeisk och internationell nivå.

Genom att mobilisera brottskämpande organ, den privata sektorn och genom att komplettera nationella och internationella insatser är målen för den nya EU-strategin att:

* förbättra operativa gränsöverskridande brottsbekämpningsåtgärder avseende IT-relaterad brottslighet i allmänhet och allvarliga former av sådan brottslighet i synnerhet, och att förbättra utbytet av information, underrättelser och bästa metoder mellan brottsbekämpande myndigheter i medlemsstaterna och i länder utanför EU;

* formulera en sammanhållen EU-politik mot IT-brottslighet i samarbete med medlemsstaterna, berörda EU- och internationella organisationer och aktörer, samt övriga experter inom EU;

* öka den allmänna medvetenheten om hotet från IT-relaterad brottslighet, särskilt bland konsumenter och andra sårbara grupper av potentiella brottsoffer.

Befintliga, rättsliga instrument på EU-nivå

Meddelandet utgår bland annat från 2001 års meddelande om skapandet av ett säkrare informationssamhälle, vilket följdes av flera åtgärder. En av dessa ledde till rambeslut 2005/222/RIF om angrepp mot informationssystem. Även annan mer generell lagstiftning rörande kampen mot IT-brottslighet har antagits.

I meddelandet menas att det specifika fokus kommissionen lagt vid att skydda barn exemplifieras väl av rambeslut 2004/68/RIF rörande sexuell exploatering av barn och särskilt väl i kampen mot publicering av material dokumenterande alla former av sexuella övergrepp mot barn med hjälp av informationssystem. Kommissionens prioritet att skydda barn kommer att bestå även i framtiden.

För att handskas med de säkerhetsutmaningar som informationssamhället ställs inför har kommissionen skapat ett trefaldigt angreppssätt för nätverks- och informationssäkerhet: i) specifika åtgärder rörande nätverks- och informationssäkerhet, ii) reglerande rambeslut rörande elektronisk kommunikation och iii) kampen mot IT-brottslighet. Ett flertal åtgärder på samtliga punkter har vidtagits i form av antagna direktiv, stadgar och inrättandet 2004 av ENISA (European Network and Information Security Agency).

Befintliga, rättsliga bekämpningsinstrument på internationell nivå

På grund av informationsnätverkens globala omfattning har kommissionen deltagit i internationella diskussioner och samarbetsformer. Det dominerande internationella bekämpningsinstrumentet är Europarådets konvention om IT-brottslighet från 2001. Konventionen som antogs och trädde i kraft 2004 innehåller gemensamma definitioner av IT-brottslighet och lägger grunden för ett fungerande rättsligt samarbete mellan kontrakterade stater. Många länder både inom och utom EU har undertecknat konventionen men ett antal länder har fortfarande inte ratificerat den. Kommissionen vill därför uppmuntra övriga medlemsstater och berörda tredje länder att ratificera konventionen.

Ytterligare utveckling av specifika instrument

De traditionella, gränsöverskridande samarbetsstrukturerna har visat sig vara långsamma och ineffektiva beträffande IT-brottslighet och kommissionen anser att nya strukturer ännu inte har utvecklats tillfredsställande. Ett nytt

koordinerat, europeiskt angreppssätt måste vara både operationellt och strategiskt samt täcka informationsutbyte och bästa praxis. Den teknologiska utvecklingen skapar ett behov av utbildning och träning i IT-brottslighet för brottsbekämpande myndigheter och rättsliga myndigheter, vilket kommissionen vill lägga tonvikt vid. Kommissionen vill även samordna möten för medlemsstaternas experter vid brottsbekämpande myndigheter och andra kompetenta organ såsom Europol, CEPOL (European Police College) och EJNT (European Judicial Training Network). Den första av flera träffar ska äga rum under 2007.

Utvecklingen av modern informationsteknologi och elektroniska kommunikationssystem är framför allt kontrollerad av privata aktörer. Industrin har dock visat en positiv inställning till att bistå offentliga myndigheter i kampen mot IT-brottslighet, särskilt gällande barnpornografi och andra typer av illegalt innehåll. Kommissionen anser att en effektiv, generell strategi i kampen mot IT-brottslighet också måste innehålla en strategi för samarbete mellan den offentliga sektorn och aktörer inom den privata sektorn. För att främja samarbetet mellan privat och offentligt kommer kommissionen att anordna en konferens för experter vid brottsbekämpande myndigheter och representanter för den privata sektorn under 2007.

Kommissionen anser att det för närvarande inte är lämpligt med en generell harmonisering av brottsdefinitioner och nationell straffrättslig lagstiftning inom området IT-brottslighet på grund av variationen av brottstyper som begreppet innefattar. Däremot är en harmonisering av medlemsstaternas lagstiftning istället ett långsiktigt mål. Ett område där kommissionen överväger lagstiftning är situationer där IT-brott begås i samband med identitetsstöld. Generellt tolkas identitetsstöld som användandet av personlig identitetsinformation (på Internet vanligen kreditkortsnummer). Identitetsstöld som sådant är inte kriminaliserat i någon medlemsstat och oftast åtalas brottslingen för bedrägeriet utfört med hjälp av identitetsstölden istället för själva identitetsstölden. Kommissionen anser att EU:s brottsbekämpande myndigheter skulle vara betjänta av om identitetsstöld kriminaliserades i samtliga medlemsstater då identitetsstöld oftare är lättare att bevisa än bedrägeri.

Information rörande utbredningen av brott är i sitt befintliga tillstånd inte tillräcklig och särskilt mycket återstår att göra för att kunna jämföra data medlemsstaterna emellan.

Vägen framåt

Kommissionen önskar föra den generella strategin gällande kampen mot IT-brottslighet framåt. Denna strategi kan dock endast utgöra ett komplement till medlemsstaternas och andra organs åtgärder då kommissionens kompetens på det kriminalpolitiska området är begränsat. De viktigaste

åtgärderna kommer att finansieras genom det finansiella programmet för förebyggning av och kampen mot brottslighet.

Bekämpningen av *IT-brottsligheten generellt* kommer att bestå av följande punkter:

* Etablera ett stärkt, operationellt samarbete mellan medlemsstaternas brottsbekämpande- och rättsliga myndigheter, vilket inleds med ett expertmöte under 2007 och som kan komma att inkludera inrättandet av en central kontaktpunkt för IT-brottslighet;

* Öka det finansiella stödet till förbättrad utbildning av brottsbekämpande- och rättsliga myndigheter beträffande hantering av IT-brott och koordinera multinationell utbildning genom inrättandet av en europeisk utbildningsplattform;

* Främja ett starkare engagemang från medlemsstaterna och offentliga myndigheter för att genomföra åtgärder mot IT-brottslighet och anslå tillräckliga medel för att bekämpa sådan brottslighet;

* Stödja forskning om IT-brottslighet;

* Organisera minst en större konferens under 2007 för brottsbekämpande myndigheter och privata aktörer;

* Ta initiativet till och medverka i privat-offentliga satsningar för att höja medvetenheten (särskilt bland konsumenter) om kostnaden för och riskerna med IT-brottslighet, utan att enbart fokusera på den negativa inverkan på säkerheten;

* Aktivt deltaga i och främja globalt samarbete i kampen mot IT-brottslighet;

* Initiera, stödja och delta i internationella projekt som är i linje med kommissionens strategi inom detta område;

* Vidta konkreta åtgärder för att uppmuntra samtliga medlemsstater och relevanta tredje länder att ratificera Europarådets konvention om IT-brottslighet och dess tilläggsprotokoll, liksom överväga deltagande från EU:s sida i egenskap av egen part;

* Tillsammans med medlemsstaterna, undersöka fenomenet storskaliga angrepp på medlemsstaternas infrastruktur med avsikt att förhindra och bekämpa dessa.

Bekämpningen av *traditionella brott inom elektroniska nätverk* kommer att bestå av följande punkter:

*Initiera en analys med syfte att förbereda ett lagförslag gällande identitetsstöld;

* Främja utvecklingen av tekniska metoder och procedurer för att bekämpa bedrägeri och illegal handel på Internet;

* Utveckla arbetet inom specifika områden, såsom expertgruppen för bedrägeriförebyggning, i bekämpningen mot Internetbedrägeri rörande icke-kontanta betalningsmedel

Bekämpningen *av illegalt innehåll* kommer att bestå av följande punkter:

* Fortsatt utveckling av insatser mot specifikt illegalt innehåll, särskilt barnpornografi och anstiftan till terroristbrott, genom implementeringsuppföljning av rambeslutet rörande sexuell exploatering av barn;

* Inbjuda medlemsstaterna till att anslå adekvata, finansiella medel för att stärka brottsbekämpande myndigheters arbete med särskild betoning på identifiering av offer utsatta för sexualbrott dokumenterade och distribuerade på Internet;

* Initiera och stödja åtgärder mot illegalt innehåll som kan sporra minderåriga till våldsamt eller på annat sätt olagligt beteende av grövre art (ex. vissa typer av extremt våldsamma dataspel on-line);

* Initiera och främja dialog mellan medlemsstater och tredje länder rörande tekniska metoder för att bekämpa såväl illegalt innehåll som procedurer för nedläggning av illegala webbsidor, med syfte att eventuellt möjliggöra formella överenskommelser länder emellan;

* Utveckla överenskommelser och konventioner på frivillig basis mellan offentliga myndigheter och privata aktörer, särskilt Internetleverantörer, gällande procedurer för att blockera och lägga ned illegala Internetsidor.

# 2 Övrigt

## 2.1 Fortsatt behandling av ärendet

Som nästa steg uttrycker kommissionen en önskan att driva de föreslagna åtgärderna vidare, utvärdera aktiviteternas implementering och rapportera till rådet och europaparlamentet. Mer specifikt hur detta ska ske är oklart varpå fortsatt behandling av ärendet idag är ovisst.

## 2.2 Gällande svenska regler och förslagets effekt på dessa

Allmänt kan konstateras att kommissionens föreslagna strategi kan komma att få effekt på gällande svenska regler.

## 2.3 Budgetära konsekvenser

Strategins budgetära konsekvenser går ej att förutsäga på detta stadium.

# 3 Ståndpunkter

## 3.1 Svensk ståndpunkt

Regeringen tycker det är positivt att kommissionen presenterar detta meddelande som innehåller både en bra översikt över vad som gjorts och förslag till förbättringar. Regeringen är medveten om IT-brottslighetens ombytliga och globala natur, och att detta skapar ett behov av samarbete. Den svenska ståndpunkten är i huvudsak positiv till strategin som ligger i linje med svenska åtgärder på området. Strategin innebär större samarbete och gemensamma ansträngningar för att bekämpa IT-brottslighet, vilket regeringen ser som värdefullt. Att samarbetet inte enbart ska ske länder emellan utan även mellan myndigheter är mycket positivt, liksom samarbetet mellan privat och offentligt, vilket bekräftar det horisontella synsätt (dvs att de brottsbekämpande myndigheterna skall samverka i största möjliga mån) som Sverige har.

Den svenska regeringen kommer kontinuerligt att följa kommissionens arbete på området i syfte att beakta svenska intressen.

## 3.2 Medlemsstaternas ståndpunkter

Inga ståndpunkter redovisade.

## 3.3 Institutionernas ståndpunkter

Inga ståndpunkter redovisade.

## 3.4 Remissinstansernas ståndpunkter

Inga ståndpunkter redovisade.

# 4 Övrigt

## 4.1 Fortsatt behandling av ärendet

## 4.3 Fackuttryck/termer

IT-brottslighet : (här) kriminella handlingar begångna genom användandet av elektroniska kommunikationsnätverk och informationssystem eller mot sådana system och nätverk