JUSTITSMINISTERIET
Civil- og Politiafdelingen

Dato: 21. oktober 2010
Kontor: Det Internationale Kontor
Sagsnr.: 2010-305-1033
Dok.: AHS40296

GRUND– OG NÆRHEDSNOTAT

vedrørende forslag til Europa-Parlamentets og Rådets direktiv om angreb på informationssystemer og om ophævelse af Rådets rammeafgørelse 2005/222/RIA

KOM(2010) 0517

Resumé

Forslaget til direktiv om angreb på informationssystemer har til formål at sikre en yderligere tilnærmelse af medlemsstaternes lovgivning i forhold til den gældende rammeafgørelse om angreb på informationssystemer (2005/222/RIA). Forslaget indeholder en række forpligtelser for medlemsstaterne særligt med hensyn til kriminalisering af forskellige former for IT-kriminalitet og fastsætter bl.a. minimumsregler for straffene herfor. Forslaget indeholder desuden bestemmelser, der har til formål at forbedre samarbejdet mellem de retlige og andre kompetente myndighed-er, herunder politiet og andre retshåndhævende myndigheder i medlemsstaterne. Forslaget vurderes ikke at være i strid med nærhedsprincippet. Forslaget er omfattet af Danmarks forbehold vedrørende retlige og indre anliggender, og det har derfor hverken lovgivningsmæssige eller statsfinansielle konsekvenser. Der ses ikke at foreligge offentlige tilkendegivelser om de øvrige medlemsstaters holdninger til forslaget. Fra dansk side finder man på nuværende tidspunkt – hvor der endnu ikke foreligger høringssvar – ikke at burde tage endelig stilling til forslaget. Danmark er dog umiddelbart positiv over for forslaget.

1. Baggrund

Den 30. september 2010 fremsatte Kommissionen et forslag til rammeafgørelse om angreb på informationssystemer. Formålet med forslaget er at sikre en yderligere tilnærmelse af medlemsstaternes lovgivning i forhold til den gældende rammeafgørelse om angreb på informationssystemer (2005/222/RIA). Forslaget bygger på denne rammeafgørelse og Europarådets konvention om IT-kriminalitet af 23. november 2001. Kommissionen har derudover medtaget enkelte nye elementer.

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Direktivforslaget behandles efter den almindelige beslutningsprocedure, hvilket indebærer, at Europa-Parlamentet og Rådet skal vedtage forslaget.

Det danske retsforbehold

Forslaget er fremsat med hjemmel i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF), 3. del, afsnit V. Forslaget er derfor omfattet af Danmarks forbehold vedrørende retlige og indre anliggender. Protokollen om Danmarks stilling, der er knyttet til Lissabon-traktaten, finder således anvendelse.

Ifølge protokollens artikel 1 deltager Danmark ikke i Rådets vedtagelse af foranstaltninger, der foreslås i henhold til TEUF, 3. del, afsnit V, og ifølge artikel 2 er ingen af de foranstaltninger, der er vedtaget i henhold til TEUF, 3. del, afsnit V, bindende for eller finder anvendelse i Danmark ("retsforbeholdet").

En eventuel gennemførelse af forslaget er derfor ikke bindende for eller finder anvendelse i Danmark.

2. Indhold

2.1. Generelt

Forslaget til direktiv er fremsat efter artikel 83 i TEUF, hvorefter Europa-Parlamentet og Rådet bl.a. på området for grænseoverskridende edb-kriminalitet af særlig grov karakter ved direktiv kan fastsætte minimumsregler for, hvad der skal anses for strafbare handlinger, og for straffene herfor.

Direktivforslaget har til formål at tilnærme medlemsstaternes strafferetlige regler til hinanden med hensyn til angreb på informationssystemer og at forbedre samarbejdet mellem de retlige og andre kompetente myndigheder, herunder politiet og andre retshåndhævende myndigheder i medlemsstaterne.

Det foreslås, at den eksisterende rammeafgørelse om angreb på informationssystemer (2005/222/RIA) formelt ophæves.

Direktivet fastsætter nærmere bestemmelser om de strafbare handlinger i forbindelse med angreb på informationssystemer og fastsætter minimumsregler for straffene herfor. Der lægges endvidere op til en styrkelse af den eksisterende struktur med døgnbemandede kontaktpunkter.

Direktivforslaget lægger i vidt omfang op til at videreføre den gældende rammeafgørelse, men forslaget indeholder også at en række nye elementer, som har til formål at sikre en yderligere tilnærmelse af medlemsstaternes lovgivning på området, tilføjes. Det drejer sig om:

1) Kriminalisering af "værktøj", der anvendes til at begå lovovertrædelserne,

2) nye skærpende omstændigheder,

3) kriminalisering af "ulovlig opfangning" ikke-offentlige overførsler af edb-data,

4) styrkelse af den eksisterende struktur med døgnbemandede kontaktpunkter, og

5) nye regler vedrørende indsamling af statistiske oplysninger om it-forbrydelser.

Forslaget indeholder på den baggrund bestemmelser om, hvilke strafbare handlinger der som minimum skal kriminaliseres, sanktioner, straffemyndighed, informationsudveksling, overvågning og statistik.

De nye bestemmelser i direktivforslaget vedrørende ”ulovlig opfangning” og ”værktøjer” bygger på tilsvarende bestemmelser i Europarådets konvention om IT-kriminalitet.

2.2. Nærmere om hovedelementerne i forslaget

2.2.1. Strafbare handlinger

Forslagets indledende bestemmelser om ulovlig adgang til informationssystemer, ulovligt indgreb i informationssystemer og ulovligt indgreb i data svarer til den gældende rammeafgørelse.

Efter forslaget skal medlemsstaterne i grovere tilfælde kriminalisere forsætlig uretmæssig adgang til et informationssystem (”hacking”) eller en del heraf.

Medlemsstaterne skal endvidere kriminalisere forsætligt og uretmæssigt forårsagelse af en alvorlig hindring eller afbrydelse af et informationssystems drift ved at indlæse eller overføre edb-data eller ved at beskadige, slette, forvanske, ændre, tilbageholde eller hindre adgang til dets edb-data, i det mindste i grovere tilfælde.

Medlemsstaterne forpligtes endvidere til i grovere tilfælde at kriminalisere forsætlig uretmæssig sletning, beskadigelse, forvanskning, ændring,

tilbageholdelse eller hindring af adgang til edb-data i et informationssystem.

Direktivforslaget indeholder en ny bestemmelse om "ulovlig opfangning". Ifølge bestemmelsen skal medlemsstaterne kriminalisere forsætligt og uretmæssigt opfangning af ikke-offentlige overførsler af edb-data til, fra eller inden for et informationssystem, herunder elektromagnetisk stråling fra et informationssystem (der indeholder sådanne edb-data) ved hjælp af tekniske hjælpemidler. Bestemmelsen omfatter bl.a. aflytning af ikke offentligt tilgængelige elektroniske data, som transmitteres fra et edb-system til et andet, eller som er lagret i et edb-system, herunder elektromagnetisk stråling fra et edb-system, der bærer sådanne elektroniske data.

Direktivforslaget indeholder også en bestemmelse om udbredelse og besiddelse af "værktøjer", dvs. de anordninger og adgangsmidler til edb-systemer, som kan anvendes til at begå en af de strafbare handlinger. Ifølge forslaget skal medlemsstaterne kriminalisere forsætlig og uretmæssig fremstilling, salg, erhvervelse (med henblik på brug), import, besiddelse, distribution eller i øvrigt at stille sådanne anordninger og adgangsmidler til rådighed med henblik på at begå en af de strafbare handlinger omfattet af direktivet.

Som "værktøjer" i direktivets forstand nævnes anordninger, herunder edb-programmer, der hovedsagelig er beregnet eller tilpasset til at begå en af de strafbare handlinger nævnt i direktivet, og edb-password, adgangskoder eller tilsvarende data, hvorved der kan opnås adgang til et helt informationssystem eller dele heraf.

Ifølge forslaget skal medlemsstaterne kriminalisere medvirken til og forsøg på de nævnte strafbare handlinger.

2.2.2. Sanktioner

Direktivforslaget pålægger medlemsstaterne at sikre, at de foreslåede strafbare handlinger kan straffes med strafferetlige sanktioner med en maksimal fængselsstraf på mindst to år.

Ifølge forslaget skal medlemsstaterne sikre, at de nævnte strafbare handlinger kan straffes med strafferetlige sanktioner med en maksimal fængselsstraf på mindst fem år, når de begås inden for rammerne af en kriminel organisation.

Forslaget indeholder i forhold til den gældende rammeafgørelse en række tilføjelser om, hvornår der foreligger skærpende omstændigheder. Medlemsstaterne skal således sikre, at de strafbare handlinger kan straffes med strafferetlige sanktioner med en maksimal fængselsstraf på mindst fem år, når de begås ved hjælp af et værktøj, som er beregnet til at foretage angreb, der berører et betydeligt antal informationssystemer, eller angreb, der volder betydelig skade som f.eks. afbrydelse af systemtjenester, økonomiske omkostninger eller tab af personlige data. Medlemsstaterne skal endvidere sørge for, at de strafbare handlinger kan straffes med strafferetlige sanktioner med en maksimal fængselsstraf på mindst fem år, når de begås ved at skjule gerningsmandens rigtige identitet og skade den, som identiteten egentlig tilhører.

Juridiske personer, der ifalder strafansvar i forbindelse med angreb på informationssystemer, skal kunne straffes med sanktioner, der er effektive, står i et rimeligt forhold til lovovertrædelsens grovhed og har en afskrækkende virkning. Sådanne sanktioner skal omfatte bødestraffe, men kan også omfatte en række andre sanktioner som f.eks. udelukkelse fra at modtage offentlige ydelser eller forbud mod at udøve erhvervsvirksomhed.

2.2.3. Straffemyndighed

Direktivforslaget forpligter medlemsstaterne til at etablere straffemyndighed (jurisdiktion), når lovovertrædelsen er begået helt eller delvist på medlemsstatens område. Medlemsstaten skal i sådanne tilfælde sørge for straffemyndighed, hvor gerningsmanden begår lovovertrædelsen, mens den pågældende fysisk befinder sig på landets område. Det gælder uanset, om lovovertrædelsen er rettet mod et informationssystem på det pågældende lands territorium eller et andet lands territorium. Herudover forpligtes medlemsstaterne til at etablere straffemyndighed i det tilfælde, hvor lovovertrædelsen begås mod et informationssystem på landets område, uanset om gerningsmanden på gerningstidspunktet fysisk befandt sig på det pågældende lands område.

Medlemsstaterne forpligtes endvidere til at etablere straffemyndighed, når lovovertrædelsen er begået af en af dens statsborgere eller en person, som har bopæl på den pågældende medlemsstats område eller for at skaffe en juridisk person, som har hjemsted på medlemsstatens område, vinding.

2.2.4. Informationsudveksling

Direktivforslaget indeholder en forpligtelse for medlemsstaterne til inden en vis tidsfrist at efterkomme anmodninger om bistand fra de operationelle kontaktpunkter. Medlemsstaterne skal endvidere sørge for at etablere procedurer, som gør det muligt at besvare hasteanmodninger inden 8 timer. Formålet hermed er at sikre, at kontaktpunkterne inden en nærmere fastsat frist oplyser, om de kan finde en løsning på anmodningen, og hvornår det kontaktpunkt, der fremsætter anmodningen, kan forvente, at dette sker.

2.2.5. Overvågning og statistik

Direktivforslaget pålægger medlemsstaterne at sikre, at der i medlemsstaten findes et passende system til registrering, fremstilling og fremlæggelse af statistiske oplysninger om de lovovertrædelser, der er omfattet af forslaget.

3. Gældende dansk ret

3.1. Strafbare handlinger og sanktioner

Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet (Brydensholt-udvalget) afgav i september 2002 betænkning nr. 1417/2002 om IT-kriminalitet. I betænkningen behandledes navnlig spørgsmålet om, i hvilket omfang udviklingen på IT-området nødvendiggør nye straffebestemmelser eller ændring af gældende bestemmelser. På grundlaget af betænkningen og for at Danmark kunne ratificere Europarådets konvention om IT-kriminalitet samt med henblik på Danmarks deltagelse i rammeafgørelsen om angreb på informationssystemer gennemførtes i 2004 en række straffelovsændringer, herunder straffelovens §§ 193 og 263 (lov nr. 352 af 19. maj 2004).

Efter straffelovens § 193 straffes den, der på retsstridig måde fremkalder omfattende forstyrrelse i driften af almindelige samfærdselsmidler, offentlig postbesørgelse, telegraf- eller telefonanlæg, radio- eller fjernsynsanlæg, informationssystemer eller anlæg, der tjener til almindelig forsyning med vand, gas, elektrisk strøm eller varme, straffes med bøde eller fængsel indtil 6 år. Begås forbrydelsen groft uagtsomt, er straffen bøde eller fængsel indtil 6 måneder.

Ved lovændringen i 2004 ændredes det tidligere anvendte begreb ”databehandlingsanlæg” i straffelovens § 193, stk. 1, til ”informationssystemer”, der er neutralt i forhold til mulige teknologiske løsninger. Ved et informationssystem forstås en computer eller andet databehandlingsan-

læg. Omfattet heraf er navnlig personlige computere, herunder både stationære og bærbare computere. Også andet elektronisk udstyr vil imidlertid kunne være omfattet, hvis udstyret har funktioner svarende til dem, der findes i computere. Det gælder således elektronisk udstyr, der kan anvendes til at oprette og/eller behandle dokumenter, billeder og lyde, udføre regnskabsfunktioner og lignende, herunder også hvis sådanne funktioner senere forekommer i kombination med andet elektronisk udstyr, f.eks. fjernsyn.

Efter straffelovens § 263, stk. 2, om krænkelse af datahemmeligheden (hacking), straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem med bøde eller fængsel indtil 1 år og 6 måneder. Begås forholdet med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særligt skærpende omstændigheder, kan straffen stige til fængsel indtil 6 år. Dette gælder endvidere, når der er tale om overtrædelser af mere systematisk eller organiseret karakter. Det vil afhænge af en konkret vurdering, om overtrædelsen skønnes at være af mere systematisk eller organiseret karakter.

For databedrageri straffes efter straffelovens § 279 a den, som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt forsøger at påvirke resultatet af sådan databehandling. Efter straffelovens § 285 straffes databedrageri med fængsel indtil 1 år og 6 måneder. Det følger af straffelovens § 286, stk. 2, at straffen for databedrageri kan stige til fængsel indtil 8 år, når forbrydelsen er af særlig grov beskaffenhed, eller fordi forbrydelsen er udført af flere i forening, eller som følge af omfanget af den opnåede eller tilsigtede vinding, eller når der er begået et større antal forbrydelser.

Efter straffelovens § 291 straffes den, der ødelægger, beskadiger eller bortskaffer ting, der tilhører en anden, med bøde eller fængsel indtil 1 år og 6 måneder. Øves der hærværk af betydeligt omfang, af mere systematisk eller organiseret karakter, eller er gerningsmanden tidligere fundet skyldig efter hærværksbestemmelsen eller en række nærmere angivne bestemmelser, (herunder den nævnte bestemmelse i straffelovens § 193), kan straffen stige til fængsel i 6 år.

Efter § 293, stk. 2, straffes den, der uberettiget hindrer en anden i helt eller delvis at råde over ting, med bøde eller fængsel indtil 1 år. Straffen

kan stige til fængsel i 2 år, hvor der er tale om overtrædelser af mere systematisk eller organiseret karakter, eller der i øvrigt foreligger særligt skærpende omstændigheder. Bestemmelsen blev ændret i 2004, hvorved det blev præciseret, at bestemmelsen også omfatter elektroniske rådighedshindringer. Elektronisk rådighedshindring kan eksempelvis forekomme ved e-mail bomber (f.eks. såkaldte Denial-of-Service angreb), der består i at hindre almindelig brug af systemet ved at forårsage overbelastning eller nedbrud.

3.2. Forsøg og medvirken

Forsøg på og medvirken til overtrædelse af de nævnte straffelovsbestemmelser er strafbart i medfør af straffelovens § 21 og § 23.

3.3. Bestemmelser om straffastsættelse

Efter straffelovens § 80 skal der ved straffens udmåling tages hensyn til lovovertrædelsens grovhed og til oplysninger om gerningsmandens person. Efter straffelovens § 81 vil bl.a. det forhold, at gerningen er begået af flere i forening, og/eller at gerningen er særligt planlangt eller led i omfattende kriminalitet som udgangspunkt være at anse som en skærpende omstændighed.

3.4. Juridiske personer

Efter straffelovens § 306 kan der pålægges selskaber mv. (juridiske personer) strafansvar for overtrædelse af straffelovens bestemmelser. En juridisk person kan efter straffelovens § 25 straffes med bøde.

3.5. Straffemyndighed

Straffelovens §§ 6-12 indeholder de almindelige bestemmelser om, hvornår en strafbar handling hører under dansk straffemyndighed. Disse bestemmelser afgrænser således, hvilke straffesager der kan pådømmes ved danske domstole.

Hovedreglen om dansk straffemyndighed er det såkaldte territorialprincip, jf. straffelovens § 6, hvorefter handlinger, som er begået i Danmark, hører under dansk straffemyndighed. Herudover følger det af straffelovens §§ 7-8 b, at handlinger, som er begået uden for Danmark, i en række nærmere bestemte tilfælde hører under dansk straffemyndighed. Det gælder f.eks. efter omstændighederne, når en lovovertrædelse er begået i udlandet af en dansk statsborger eller mod en dansk statsborger (jf. hen-

holdsvis straffelovens § 7 om det aktive personalprincip og § 7 a om det passive personalprincip).

Efter straffelovens § 8, nr. 5, om det såkaldte universalprincip omfatter dansk straffemyndighed handlinger, som foretages uden for den danske stat, uden hensyn til hvor gerningsmanden hører hjemme, når handlingen er omfattet af en international bestemmelse, ifølge hvilken Danmark er forpligtet til at have straffemyndighed. Ved "internationale bestemmelser" forstås bl.a. bestemmelser i EU-direktiver.

3.6. Informationsudveksling

Danmark er tilsluttet G8-landenes 24-timers/7 dages informationsnet til bekæmpelse af højteknologikriminalitet. Rigspolitiets Kommunikationscenter er i den forbindelse udpeget som kontaktpunkt, og centeret har døgnet rundt en specialist i højteknologikriminalitet fra Nationalt Efterforskningsstøttecenter (NEC) tilknyttet. Denne specialist kan til enhver tid formidle kontakt til den relevante politikreds, der vil kunne træffe operative foranstaltninger.

4. Lovgivningsmæssige og statsfinansielle konsekvenser

4.1. Lovgivningsmæssige konsekvenser

Forslaget er som nævnt fremsat efter TEUF, 3. del, afsnit V, og er derfor omfattet af Danmarks forbehold vedrørende retlige og indre anliggender. Danmark deltager således ikke i vedtagelsen af direktivet, som ikke vil være bindende for eller finde anvendelse i Danmark.

I 2004 gennemførtes som nævnt de ændringer i straffeloven, der var nødvendige for, at Danmark kunne ratificere Europarådets konvention om IT-kriminalitet, og for at Danmark kunne gennemføre deltage i vedtagelsen af rammeafgørelsen om angreb på informationssystemer. De nye bestemmelser i direktivforslaget vedrørende "ulovlig opfangning" og "værktøjer" bygger som nævnt på tilsvarende bestemmelser i Europarådets konvention.

Hvis forslaget til direktiv fandt anvendelse i Danmark, vurderes det, at dansk lovgivning allerede i vidt omfang opfylder de forpligtelser, der er indeholdt i direktivforslaget. En gennemførelse i dansk ret ville imidlertid nødvendiggøre enkelte lovændringer, bl.a. at strafferammen i hvert fald i en bestemmelse skal forhøjes til 2 år. Det kan endvidere ikke ude-

lukkes, at forslagets bestemmelse om skærpende omstændigheder kunne nødvendiggøre visse lovændringer.

4.2. Statsfinansielle konsekvenser

Da forslaget som nævnt ikke vil være bindende for Danmark, har forslaget ikke statsfinansielle konsekvenser.

Hvis forslaget til direktiv fandt anvendelse i Danmark, skønnes det at ville have statsfinansielle konsekvenser af mindre betydning.

5. Høring

Forslaget er sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Procesbevillingsnævnet, Domstolsstyrelsen, Rigspolitiet, Politiets Efterretningstjeneste, Rigsadvokaten, Den Danske Dommerforening, Dommerfuldmægtigforeningen, Datatilsynet, Direktoratet for Kriminalforsorgen, Foreningen af offentlige anklagere, Politiforbundet, Advokatrådet, Landsforeningen af beskikkede advokater, Danske Advokater, Amnesty International, Institut for Menneskerettigheder, Retspolitisk Forening og Retssikkerhedsfonden.

Justitsministeriet har fastsat høringsfristen til den 30. november 2010.

6. Nærhedsprincippet

Kommissionen har om nærhedsprincippet bl.a. anført, at it-kriminalitet og navnlig angreb på informationssystemer har en væsentlig grænseoverskridende dimension, som er mest iøjnefaldende i forbindelse med omfattende angreb, hvor de forskellige elementer af angrebet ofte befinder sig på forskellige steder og i forskellige lande. Forslaget vil medføre en yderligere indbyrdes tilnærmelse af medlemsstaternes materielle strafferet og retsplejeregler på området.

Regeringens foreløbige vurdering er, at forslaget ikke er i strid med nærhedsprincippet. Regeringen kan i den forbindelse tilslutte sig Kommissionens betragtninger.

7. Andre landes kendte holdninger

Der ses ikke at foreligge offentlige tilkendegivelser om de øvrige medlemsstaters holdning til forslaget.

8. Foreløbig generel dansk holdning

Fra dansk side finder man på nuværende tidspunkt – hvor den igangsatte høring ikke er afsluttet – ikke at burde tage endelig stilling til forslaget. Man er dog umiddelbart positiv over for forslaget.

9. Orientering af andre af Folketingets udvalg

Grundnotatet sendes – ud over til Folketingets Europaudvalg – til Folketingets Retsudvalg.