JUSTITSMINISTERIET
Retsforbehold

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 8. oktober 2015
Kontor: Retsforbehold
Sagsbeh: Tina Chris Mogensen
Sagsnr.: 2015-0030-3828
Dok.: 1736300

Hermed sendes besvarelse af spørgsmål nr. 195 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 18. september 2015. Spørgsmålet er stillet efter ønske af Trine Bramsen (S).

Søren Pind

/

Lene Steen

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 195 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren i kort form redegøre for de senere års EU-initiativer på området vedr. cyberkriminalitet, herunder eksempler på EUROPOL-aktiviteter på området?”

Svar:

1. Europa-Parlamentets og Rådet vedtog den 12. august 2013 direktiv 2013/40/EU om angreb på informationssystemer.

Cybercrimedirektivet erstatter Rådets rammeafgørelse 2005/222/RIA af 24. februar 2005 om angreb på informationssystemer. Rammeafgørelsen blev sammen med Europarådets konvention om IT-kriminalitet fra 2001 gennemført i dansk ret ved lov nr. 352 af 19. maj 2004 om ændring af straffeloven mv.

Direktivet har til formål at sikre, at der sker en yderligere tilnærmelse af medlemsstaternes lovgivning i forhold til rammeafgørelsen, idet det er af afgørende betydning for borgere, virksomheder og samfundet i øvrigt, at der er tillid til informationssystemers funktionsdygtighed og sikkerhed. Direktivet indeholder minimumsregler om afgrænsningen af de handlinger vedrørende cybercrime, der skal være strafbare. Det drejer sig bl.a. om ulovlig adgang til informationssystemer, ulovlige indgreb i informationssystemer, ulovlige indgreb i data og ulovlig opfangning, herunder medvirken hertil og forsøg herpå. Direktivet fastsætter endvidere regler om sanktioner for strafbare handlinger omfattet af direktivet i relation til både fysiske og juridiske personer, regler om straffemyndighed og regler om udveksling af oplysninger mellem medlemsstaterne. Derudover viderefører direktivet allerede eksisterende informationsudveksling og indsamling af statistik i det bestående netværk af kontaktpunkter, der er etableret i regi af Europarådet, og som Danmark allerede deltager i. Efter direktivet skal hasteanmodninger mellem EU-medlemsstater håndteres inden for 8 timer.

Cybercrimedirektivet er vedtaget med hjemmel i Traktatens artikel 83, stk. 1. Danmark deltager på grund af retsforbeholdet derfor ikke i direktivet.

Venstre, Det Konservative Folkeparti, Socialdemokraterne, Det Radikale Venstre og Socialistisk Folkeparti blev den 17. marts 2015 enige om i tilfælde af et ja ved folkeafstemningen den 3. december 2015 at tilvælge 22 eksisterende retsakter på området for retlige og indre anliggender, herunder cybercrimedirektivet.

2. Rådet (retlige og indre anliggender) vedtog den 8. november 2010 konklusioner om fastlæggelse og gennemførelse af en flerårig EU-politikcyklus for grov international og organiseret kriminalitet med henblik på at tackle de vigtigste kriminalitetstrusler, som påvirker EU, på en sammenhængende og metodisk måde gennem det bedst mulige samarbejde mellem de relevante tjenester i medlemsstaterne, EU-institutionerne og EU-agenturerne samt relevante tredjelande og organisationer. Den gældende politikcyklus, der løber i perioden fra 2014 til 2017, fokuserer på en række kriminalitetsprioriteter, som er fastsat på baggrund af EU's trusselsvurdering fra 2013 af grov og international kriminalitet (EU SOCTA 2013) og vedtaget af Rådet (retlige og indre anliggender) den 6.-7. juni 2013. En af disse kriminalitetsprioriteter er organiseret IT-kriminalitet, herunder betalingskortsvindel og seksuelt misbrug af børn online.

3. Justitsministeriet har til brug for besvarelsen af spørgsmålet endvidere indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

> "Bekæmpelse af forskellige former for cyberkriminalitet har i en længere årrække været et prioriteret indsats- og monitoreringsområde for Europol, ligesom medlemslandene i stigende grad har anvendt Europol-samarbejdet til at indsamle og udveksle oplysninger om cyberkriminalitet.
>
> Med henblik på at understøtte medlemslandenes indsats mod cyberkriminalitet oprettede Europol i 2013 European Cyber crime Centre (EC3). EC3 bistår medlemslandene i forbindelse med forebyggelse og bekæmpelse af kriminalitet via internettet, herunder f.eks. online seksuelt misbrug af børn og en række former for berigelseskriminalitet. Herudover bistår EC3 medlemslandene med forebyggelse og bekæmpelse af angreb mod IT strukturer og informationssystemer – såkaldte cyberattacks – og hacking.
>
> Arbejdet i EC3 understøttes af flere projekter, herunder bl.a. projektet Focal Point Terminal, projektet Focal Point Cyborg og Projektet Focal Point Twins.
>
> I forhold til projektet Focal Point Terminal kan Rigspolitiet oplyse, at projektet systematisk indsamler og analyserer oplysninger vedrørende kriminelle netværk, der er involveret i bedrageri med kreditkort til brug for generelle situationsrapporter om kriminalitetens omfang, modus mv. samt konkrete efterforskninger i medlemslandene.
>
> I 2012 registrerede projektet 93 sammenfald mellem de oplysninger, som medlemslandene har indberettet, f.eks. oplysninger

om gerningspersoner, anvendt udstyr og modus. Tilsvarende registrerede projektet i 2013 og 2014 henholdsvis 222 og 172 sammenfald.

Samtidig har projektet i 2014 understøttet 31 operationer i medlemslandene, herunder en spansk og bulgarsk operation mod organiserede kriminelle netværk, der var involveret i kreditkortbedrageri og tyveri fra hæveautomater. Europol bistod med bl.a. "on the spot" tilstedeværelse ved operationerne med direkte adgang til oplysninger i Focal Point Terminal. Operationen medførte bl.a. afdækning af otte laboratorier indeholdende kortlæsere samt data fra kopierede kreditkort.

Projektet Focal Point Cyborg indsamler og analyserer systematisk oplysninger vedrørende kriminelle netværk, der er involveret i organiseret kriminalitet i relation til internet og informations- og kommunikationsteknologi med økonomisk vinding for øje, herunder hacking og computerrelateret bedrageri.

I 2012 har projektet registreret 14 sammenfald mellem de oplysninger, som medlemslandene har indberettet, f.eks. oplysninger om gerningspersoner, anvendt udstyr og modus. Tilsvarende har projektet i 2013 og 2014 registreret henholdsvis 43 og 47 sammenfald. Samtidig understøttede projektet i 2014 48 operationer i medlemslandene.

Herudover bistod Europol og FBI i november 2014 en række medlemslande i en Joint Action Day mod det såkaldte TOR netværk. Operationen medførte bl.a. beslaglæggelse af bitcoins til en værdi af ca. 1 million US dollar og ca. 180.000 Euro.

I forhold til medlemslandenes brug af Europols Informationssystem (EIS) i forbindelse med cyberkriminalitet kan Rigspolitiet oplyse, at der ved udgangen af 2012 var indsamlet oplysninger om 2.182 personer og genstande relateret til "computer crime", mens antallet ved udgangen af 2014 udgjorde 5.170 personer og genstande.

Det bemærkes, at cyberkriminalitet kan være begået i forbindelse med andre typer af kriminalitet end de nævnte.

Rigspolitiet kan afslutningsvis oplyse, at Rigspolitiet deltager i både det strategiske og det operative samarbejde i Europol vedrørende cyberkriminalitet."

For en mere generel beskrivelse af Europols virksomhed henvises til Justitsministeriets tidligere besvarelse af 1. september 2014 af spørgsmål nr. 1336 (Alm. del) fra Folketingets Retsudvalg.

Der kan endvidere henvises til den samtidig besvarelse af spørgsmål nr. 191 og 194 (Alm. del) fra Folketingets Retsudvalg for så vidt angår det samlede antal søgninger i Europols Informationssystem (EIS) og online seksuelt misbrug af børn.