JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Dato: 3. februar 2017
Kontor: Politikontoret
Sagsbeh: Pernille Østergaard
Sagsnr.: 2017-0035-0398
Dok.: 2187358

UDKAST TIL TALE

til brug for besvarelsen af samrådsspørgsmål AJ, AI og AH fra Folketingets Retsudvalg den 7. februar 2017

Samrådsspørgsmål AJ:

"Ministeren bedes redegøre for, hvilke initiativer regeringen vil iværksætte for at bekæmpe bedrageri på internettet, herunder politiets indsats i forhold til at opdage, efterforske og retsforfølge personer eller virksomheder, behovet for strafskærpelse samt muligheden for forebyggelse?"

Samrådsspørgsmål AI:

"Ministeren bedes oplyse, hvor borgere kan hente hjælp, hvis de er udsat for svindel på internettet, herunder regeringens holdning til, hvordan ofre kan hjælpes bedre end det sker i dag?"

Samrådsspørgsmål AH:

"Ministeren bedes redegøre for omfanget af sager omhandlende bedrageri på internettet, herunder de forskellige typer af bedra-

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

geri på internettet og udviklingen i antal og indhold af sagerne?"

Spørgsmålene er stillet efter ønske fra Trine Bramsen (S).

[Indledning]

1. Tak for invitationen til at komme her i udvalget i dag.

Dagens tema er bedrageri via internettet.

[Afgrænsning]

2. Bedrageri via internettet er en form for økonomisk it-kriminalitet. Det er altså en såkaldt berigelsesforbrydelse, hvor gerningsmanden har økonomisk gevinst for øje, og som sker ved anvendelse af it.

Ifølge Rigspolitiet vedrører sagerne om økonomisk it-kriminalitet typisk misbrug af betalingskort på nettet og bedrageri i forbindelse med køb på nettet.

Derudover kan der f.eks. være tale om såkaldte *phishing*-angreb, hvor kriminelle via e-mails forsøger at formå borgere eller virksomheder til at udlevere eksempelvis kontooplysninger.

Som et eksempel på *phishing* kan nævnes den situation, hvor man modtager en e-mail eller SMS, som ser ud til at være fra en myndighed eller en bank. Man bliver i den forbindelse bedt om

at indtaste fortrolige informationer, f.eks. dankortooplysninger eller cpr-nummer, på en hjemmeside, der ligner myndighedens eller bankens. Afsenderen vil herefter bruge oplysningerne til f.eks. at overføre penge fra ens bankkonto.

Der kan også være tale om virksomhedsrettede angreb, såsom det såkaldte *CEO-fraud*, hvor kriminelle udgiver sig for at være en medarbejder eller en handelspartner og derigennem forsøger at få virksomheder til at udlevere pengebeløb eller forretningshemmeligheder.

Og de kriminelle bliver stadig mere kreative. Rigspolitiet har således konstateret en stor vækst i og udvikling af den måde, de kriminelle arbejder på i forbindelse med samhandel på internettet, misbrug af elektroniske betalingsmidler og virksomhedsrettede angreb.

Denne udvikling stiller store krav til politiets efterforskning. Både når det kommer til de ressourcer og til de redskaber, der kræves for at opklare sagerne. Og sagernes kompleksitet, størrelse og ofte internationale og organiserede karakter gør, at det kan tage lang tid at opklare dem.

[Omfang]

3. Ifølge Rigspolitiets oplysninger er det samlede antal af anmeldelser vedrørende såkaldt databedrageri steget med ca. 240 pct. i perioden fra 2009 til 2015. Samtidig er antallet af anmel-

delser vedrørende almindeligt bedrageri steget med ca. 300 pct. i samme periode.

Selvom disse opgørelser vedrører bedrageri og databedrageri generelt, og således ikke kun internetrelaterede forbrydelser, er det Rigspolitiets opfattelse, at der er sket en kraftig stigning i særligt økonomisk it-kriminalitet de seneste år.

F.eks. er misbrug af dankort ved fjernsalg steget fra ca. 20 mio. kr. i 2014 til ca. 30 mio. kr. i 2015.

Det er Rigspolitiets vurdering, at stigningen i omfanget af bedrageri, der foregår via internettet, bl.a. skyldes, at handel i stadig stigende grad sker via internettet.

Den digitale udvikling gør det desuden muligt at begå et stort antal strafbare forhold inden for kort tid. Som eksempel herpå har Rigspolitiet oplyst om et konkret tilfælde, hvor den samme gerningsmand havde gentaget det strafbare forhold 1.500 gange.

[Indsats på området]

4. Den kraftige stigning i antallet af anmeldelser vedrørende økonomisk it-kriminalitet kalder selvsagt på handling.

I flerårsaftalen for politiets og anklagemyndighedens økonomi i 2016-2019 har vi derfor udpeget cyberkriminalitet og økonomisk kriminalitet som højt prioriterede områder, hvor politiets indsats skal styrkes i aftaleperioden.

[**Politiets indsats**]

5. I Rigspolitiet er området vedrørende forebyggelse og bekæmpelse af it-kriminalitet forankret i det såkaldte Nationale Cyber Crime Center (NC3). Centeret råder over ca. 100 medarbejdere, og opgaverne varetages af en bredt forankret personalegruppe, herunder polititjenestemænd, it-ingeniører og it-specialister.

Politiets indsats på området afhænger bl.a. af mulighederne for at kunne identificere de enkelte kriminalitetstyper i forhold til hinanden, således at indsatsen målrettes de enkelte kriminalitetstyper. Rigspolitiet har derfor fokus på et løbende udviklingsarbejde med at sikre anvendelsen af korrekte gerningskoder og søgenøgler.

Da bekæmpelse af økonomisk it-kriminalitet, herunder bedrageri på internettet, er et prioriteret indsatsområde for dansk politi, har Rigspolitiet desuden iværksat en række yderligere initiativer.

Rigspolitiet er således ved at udarbejde en operativ strategi for bekæmpelse af økonomisk it-kriminalitet, som gennem strategisk analyse skal sætte rammerne for dansk politis indsats på området i 2017-2020.

Strategien skal bl.a. fastlægge en række fokusområder for politiets indsats på området, ligesom strategien vil fokusere på politiets muligheder for at iværksætte forebyggende og skadesbegrænsende initiativer.

Rigspolitiet vil forbindelse med udmøntningen af den operative strategi også styrke bl.a. politiets sagsbehandling.

Rigspolitiet har desuden fokus på at sikre, at politiets it-kompetencer i de afdelinger, der behandler sager om økonomisk it-kriminalitet, er tilstrækkelige. Og der er også fokus på, at borgerne bliver vejledt på en god og professionel måde, hvis de har været udsat økonomisk it-kriminalitet.

Rigspolitiet har i den forbindelse udrullet den såkaldte cybercrime I-uddannelse, som har til formål at klæde politiets servicecentre på til at modtage anmeldelser om it-kriminalitet.

I 2017 vil politiet desuden udrulle den såkaldte cybercrime II-uddannelse, som har til formål at sikre, at efterforskere og anklagere har det fornødne it-kendskab til at håndtere anmeldelser og straffesager vedrørende økonomisk it-kriminalitet.

Derudover vil Rigspolitiet styrke det nationale overblik på området, bl.a. ved hjælp af en forbedret datakvalitet. Rigspolitiet vil også undersøge mulighederne for at samle sagstyper på tværs af politikredsene med henblik på en mere specialiseret og effektiv sagsbehandling.

[**Fokus hos anklagemyndigheden**]

6. Hos anklagemyndigheden er der også stort fokus på sager om økonomisk it-kriminalitet, herunder sager om bedrageri på internettet.

Rigsadvokaten har oplyst, at der gennem de seneste år er taget en række initiativer for at styrke politiets og anklagemyndighedens behandling af straffesager om it-kriminalitet.

Rigsadvokaten har bl.a. udarbejdet en videnspakke til anklagemyndigheden om it-kriminalitet. Videnspakken indeholder bl.a. retningslinjer for efterforskning af sager, hvor der indgår digitale spor og beviser. Det kan f.eks. være muligheden for at beslaglægge et internetdomæne, der bliver anvendt af en falsk webbutik. Jeg kan i den forbindelse oplyse, at SØIK i 2016 beslaglagde ca. 670 hjemmesider.

Videnspakken indeholder også vejledning om de relevante bestemmelser i straffeloven, herunder bestemmelserne om bedrageri og bestemmelserne om dansk straffemyndighed.

Rigsadvokaten udbyder desuden et e-læringskurs om it-relateret kriminalitet, som er obligatorisk for alle anklagere. Kurset omhandler emner som grundlæggende it-forståelse, straffeproces og strafferet.

Rigsadvokaten udbyder også et tredages kursus, som er målrettet anklagemyndighedens specialkompetencer inden for it-kriminalitet.

[**Politiets samarbejde med andre aktører**]

7. Dansk politi samarbejder og skaber fælles indsatser (såkaldt *co-creation*) med private og offentlige aktører, herunder bl.a. Rådet for Digital Sikkerhed, Kommunernes Landsforening, Det Kriminalpræventive Råd, Forbrugerombudsmanden, Dansk Erhverv, Den Blå Avis, Digitaliseringsstyrelsen og Forbrugerrådet TÆNK.

Samarbejdet sker med henblik på at forebygge, at borgere udsættes for økonomisk it-kriminalitet og med henblik på at begrænse skaderne, når der er begået denne slags kriminalitet.

Derudover har *co-creation*-projekterne til formål at styrke borgernes viden og kompetencer om sikker internetadfærd. Der arbejdes bl.a. på løsninger til udvikling af redskaber, der kan hjælpe borgerne med at navigere uden om svindelsider på internettet, og løsninger, der gør det lettere for borgere og virksomheder at indgive anmeldelse, når de har været udsat for bedrageri på internettet.

8. Politiet arbejder også løbende med at advare borgere og virksomheder – bl.a. via de sociale medier – om igangværende it-angreb, herunder f.eks. *phishing*-angreb. Formålet er bl.a. at begrænse kriminalitetens omfang.

Dertil kommer, at politiet i forbindelse med konkrete efterforskninger om økonomisk it-kriminalitet via telefon og e-mails kon-

takter borgere, der er i risiko for at blive udsat for økonomisk it-kriminalitet.

[**Information til borgere**]

9. Borgerne har også selv mulighed for at søge nærmere information om emnet, herunder hvordan man skal forholde sig, hvis man har været udsat for it-kriminalitet.

Jeg har fra Digitaliseringsstyrelsen [som hører under ministeren for offentlig innovations ressort] fået oplyst, at borgere, der f.eks. har været udsat for bedrageri på internettet, bl.a. kan hente hjælp og vejledning på borger.dk, hvor der findes en række råd og artikler om emnet.

F.eks. kan man på borger.dk under emnet "internet og sikkerhed" læse mere om, hvordan man skal forholde sig, og hvor man kan henvende sig, hvis man har været udsat for f.eks. misbrug af kortoplysninger.

Derudover kan man under emnet "*phishing* – falske mails" finde eksempler på, hvordan en sådan e-mail kan se ud, ligesom man kan finde information om, hvordan man kan undgå at blive udsat for *phishing*.

Digitaliseringsstyrelsen har endvidere oplyst, at materialet på borger.dk udbygges løbende, så informationen hele tiden er i trit med trusselsbilledet.

[**Internationalt samarbejde**]

10. Men det er ikke bare nationalt, at der er fokus på at bekæmpe it-kriminalitet.

Bekæmpelse af forskellige former for it-kriminalitet har i en længere årrække været et prioriteret indsats- og monitoreringsområde for Europol, og medlemslandene anvender i stigende grad Europol-samarbejdet til at indsamle og udveksle oplysninger om it-kriminalitet.

Europol-samarbejdet har særdeles stor operativ betydning for dansk politis arbejde. Det vil således have store operative konsekvenser for politiet, hvis Danmark mister adgang til de oplysninger og analyser bl.a. om it-kriminalitet, som deles inden for rammerne af Europol.

Regeringen gør derfor også en betydelig indsats i forhold til EU-institutionerne for at sikre en samarbejdsaftale mellem Danmark og Europol, så dansk politi også efter den 1. maj 2017 kan deltage i Europol om forebyggelse og bekæmpelse af grænseoverskridende it-kriminalitet.

[Straffelovens bestemmelser]

11. Jeg vil nu vende mig mod straffelovens bestemmelser om bedrageri og databedrageri.

Bedrageri og databedrageri kan i dag straffes med fængsel i op til 8 år, hvis det er af særlig grov beskaffenhed.

Det er en meget høj strafferamme, som jeg ikke aktuelt har planer om at hæve.

Det skal også ses i lyset af, at regeringen jo har besluttet, at der skal nedsættes en straffelovskommission. En sådan kommission skal bl.a. se på de generelle principper for strafudmåling, strafferabat og forholdet mellem strafferammer og strafniveauer i sager om forskellige kriminalitetstyper.

Kommissionen skal også foreslå en modernisering af straffeloven, som tager højde for et nutidigt kriminalitetsmønster, og som beskytter borgeren i nutidens digitale verden.

I forbindelse med en modernisering af straffeloven er det et oplagt spørgsmål, om straffeloven passer på de former for kriminalitet, vi ser i dag i en stadig mere digitaliseret verden, herunder økonomisk it-kriminalitet.

Det er et større arbejde, som skal sættes i gang. Og det giver efter min opfattelse ikke mening at overveje at forhøje en strafferamme, som i dag er på 8 år, før kommissionen er færdig med sit arbejde.

[Afslutning]

12. Jeg vil slutte med at gentage, at økonomisk it-kriminalitet er et højt prioriteret område, som både politiet og anklagemyndigheden har stor fokus på.

Derudover gør regeringen alt, hvad den kan for at sikre, at Danmark også efter den 1. maj 2017 kan være en del af Europolsamarbejdet med at forebygge og bekæmpe grænseoverskridende it-kriminalitet.

Tak for ordet!