JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 4. februar 2016
Kontor: Politikontoret
Sagsbeh: Rasmus Hjalte Niess Bak
Sagsnr.: 2016-0030-4073
Dok.: 1841122

Hermed sendes besvarelse af spørgsmål nr. 170 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 8. januar 2016. Spørgsmålet er stillet efter ønske fra Peter Skaarup (DF).

Søren Pind

/

Esben Haugland

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 170 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren forklare, hvorfor myndighederne ikke griber mere konsekvent ind, når de bliver bekendt med, at der sker bedrageri på bestemte hjemmesider, og hvorfor myndighederne ikke foretager en efterforskning af ejerne af de pågældende hjemmesider, jf. artikel ”Danske myndigheder giver netsvindlere let spil”, TV2/Nyheder Online, 14. december 2015?”

Svar:

1. Det fremgår bl.a. af artiklen, som der henvises til i spørgsmålet, at danske myndigheder kunne sætte en stopper for flere hundrede danske hjemmesider med kinesiske ejere, der efter alt at dømme forsøger at fuppe og bedrage forbrugerne. Det fremgår også af artiklen, at i en sag, hvor Statsadvokaten for Særlig Økonomisk og International Kriminalitet ved kendelse fra Københavns Byret fik overdraget fem hjemmesider, der var under mistanke for bedrageri samt overtrædelse af varemærkeloven, foretog statsadvokaten efterfølgende ikke yderligere efterforskning.

2. Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet udtalelser fra Rigsadvokaten og Rigspolitiet.

Rigsadvokaten har oplyst følgende:

> ”Jeg har til brug for besvarelsen af spørgsmålene indhentet en udtalelse fra Statsadvokaten for Særlig Økonomisk og International Kriminalitet (SØIK), som har oplyst følgende:
>
> > ”**1.** Om den konkrete sag, der omtales i artiklen, kan det oplyses, at sagen blev indledt, da SØIK modtog en liste fra organisationen e-mærket med cirka 870 hjemmesider, som var mistænkt for at være såkaldte falske webbutikker. Hovedparten af hjemmesiderne var registreret under udenlandske topdomæner som f.eks. ”.com”, ”.eu” og ”.org”, og SØIK videresendte derfor oplysningerne til Europol, således at disse kunne indgå i fælleseuropæiske aktioner mod kriminelle hjemmesider. Der redegøres nærmere for disse aktioner under pkt. 2.
> >
> > Af de 870 hjemmesider var der 24 ”.dk” hjemmesider, som var registreret hos DK Hostmaster A/S. SØIK indledte derfor en efterforskning, der skulle afklare, hvem der havde registreret hjemmesiderne hos DK Hostmaster A/S, og hvorvidt de pågældende hjemmesider fortsat var aktive.

I forbindelse med denne efterforskning blev det konstateret, at 10 af hjemmesiderne enten var registrerede som inaktive hos DK Hostmaster A/S eller fremstod med en blank side ved opslag på internettet. Der blev ikke foretaget yderligere i relation til disse hjemmesider, eftersom de ikke udgjorde en trussel for danske forbrugere.

SØIK, som tidligere havde fået overdraget tre af hjemmesiderne, fik ved kendelser af 18. juni 2015 beslaglagt og overdraget de resterende 11 aktive hjemmesider, der alle var registrerede til personer bosiddende i udlandet, herunder primært Kina.

SØIK foretog ikke yderligere efterforskningsskridt i sagerne, da udlevering af hjemmesiderne effektivt skærmede danske forbrugere mod de falske webbutikker, og da der ud fra de konkrete oplysninger i sagen ikke var udsigt til, at en efterforskning ville lede til strafforfølgning af selskaber eller personer.

Der foretages altid en konkret vurdering af efterforskningsmulighederne i forhold til hver enkelt hjemmeside. DK Hostmaster A/S validerer imidlertid ikke identiteten på de personer, som er registranter af danske hjemmesider, og det er statsadvokaturens erfaring, at det kan være vanskeligt at efterforske yderligere, når det drejer sig om udenlandske registranter, der oftest er hjemmehørende i tredjelande. Der henvises i øvrigt til Rigspolitiets udtalelse om erfaringerne med efterforskning og strafforfølgning af falske webbutikker til brug for besvarelse af spørgsmålet.

I artiklen oplyses det endvidere, at en navngiven person bosiddende i Kina var registreret med 23 hjemmesider med falske webbutikker, og at SØIK alene beslaglagde og fik overdraget 5 af disse hjemmesider.

Herom kan det oplyses, at SØIK den 18. juni 2015 har fået beslaglagt og overdraget 5 hjemmesider, hvor den pågældende var registrant hos DK Hostmaster A/S. SØIK havde på kendelsestidspunktet ikke oplysninger om, at den pågældende var registrant på andre hjemmesider, og SØIK har ikke efterfølgende modtaget oplysninger herom. SØIK vil på grundlag af artiklens oplysninger anmode TV2 om at oplyse navnene på de hjemmesider, som den pågældende nu er registrant på.

SØIK har endvidere i december 2015 modtaget nye anmeldelser om hjemmesider med falske webbutikker, hvor den pågældende person på ny optræder som registrant af hjemmesider. SØIK har på baggrund af disse anmeldelser indledt nye efterforskninger. Anmeldelserne beskrives nærmere under pkt. 2.

2. Danmark har siden 2010 deltaget i den fælleseuropæiske aktion "In Our Sites" (IOS), som har til formål at koordinere fælles aktioner mod falske hjemmesider. Aktionen koordineres af Europol.

I forbindelse med IOS samarbejder SØIK bl.a. med e-mærket, der scanner internettet for hjemmesider, som er oprettet for at snyde danske forbrugere enten til at købe falske varer eller til at bestille varer, som aldrig leveres. E-mærket overdrager herefter oversigt over mistænkelige hjemmesider til SØIK. Hjemmesiderne er erfaringsmæssigt registreret med en lang række forskellige domæner, herunder ".dk", ".com", ".eu". For så vidt angår hjemmesider, som er registreret med et ".dk"-domæne, efterforskes sagerne af SØIK. De øvrige hjemmesider overdrages til Europol med henblik på at indgå i de fælles aktioner.

Hvis der er mistanke om, at en hjemmeside registreret med et ".dk"-domæne sælger falske varer, eller der foregår "phishing" af betalingsoplysninger, anmoder SØIK retten om at afsige kendelse om, at DK Hostmaster A/S skal udlevere domænenavnet til SØIK. Hjemmesiden vil herefter fremstå med et banner fra SØIK, som oplyser, at hjemmesiden er udleveret eller beslaglagt og henviser til rettens kendelse.

SØIK modtager endvidere anmeldelser fra danske forbrugere, der har købt varer på internettet, som viser sig at være falske. Omhandler anmeldelserne andre domæner end ".dk"-domæner, overdrages navnet på hjemmesiden til Europol for at indgå i IOS operationer. Omhandler anmeldelserne ".dk"-hjemmesider, foretager SØIK en nærmere undersøgelse af, hvorvidt hjemmesiden er en falsk webbutik. Denne undersøgelse omfatter bl.a. hjemmesidens sprog, prisangivelser, kontaktmuligheder samt eventuelle oplysninger om hjemmesidens registrant. Er der mistanke om, at hjemmesiden er falsk, eller der foregår "phishing" på hjem-

mesiden, anmoder statsadvokaturen retten om at afsige en kendelse om beslaglæggelse og overdragelse af hjemmesiden til SØIK.

I nogle tilfælde er en hjemmeside, hvor der er mistanke om salg af falske varer eller "phishing", registreret til en person bosiddende i Danmark. I disse sager har statsadvokaturens efterforskning vist, at den pågældende ikke har haft kendskab til at stå som registrant på en hjemmeside. I disse tilfælde har SØIK foranlediget, at den pågældende ved en erklæring har overdraget domænet til SØIK, hvorefter statsadvokaturens banner indsættes.

SØIK modtager også anmeldelser fra eksempelvis Lægemiddelstyrelsen om hjemmesider, der har ".dk"-domænenavne, hvor der sælges falske eller ulovlige lægemidler.

Har disse hjemmesider udenlandske registranter, herunder ofte fra Kina eller Indien, indhentes der kendelser på udlevering eller beslaglæggelse af domænenavnet. SØIK foretager derudover en konkret efterforskningsvurdering i forhold til muligheden for at afdække registrantens identitet, men dette leder erfaringsmæssigt ikke til strafforfølgning af selskaberne eller enkeltpersoner bag selskaberne, jf. herved redegørelsen under pkt. 1.

Har hjemmesiden derimod en dansk registrant, iværksættes efterforskning i form af ransagning, indhentelse af bankoplysninger eller f.eks. teleoplysninger med henblik på en nærmere afdækning af omfanget af de mulige begåede strafbare forhold og retsforfølgning af personerne bag hjemmesiden. Dette gælder såvel i sager om salg af ulovlige eller falske lægemidler som i andre sager, hvor der er mistanke om falske webbutikker eller "phishing".

Det kan endeligt oplyses, at SØIK i december 2015 har modtaget en anmeldelse om mere end 200 falske hjemmesider fra indehaveren af hjemmesiden www.esvindel.dk og en anmeldelse fra e-mærket vedrørende ca. 500 falske hjemmesider. Alle hjemmesider har ".dk"-domænenavne. Disse sager er under efterforskning i SØIK, og statsadvokaturen vil snarest indhente kendelser om beslaglæggelse af de hjemmesider, hvor der er mistanke om bedrageri efter straffelovens § 279 eller overtrædelse af varemærkeloven.

3. Rigspolitiet har oplyst, at Rigspolitiet har gode erfaringer med blokering af internetsider med ulovligt indhold. Rigspolitiet driver således i samarbejde med Red Barnet et såkaldt netfilter, hvis formål er på frivillig basis at blokere for adgang til materiale med seksuelt misbrug af børn på internettet. Det er Rigspolitiets vurdering, at en sådan blokeringsordning også vil kunne anvendes i forhold til falske webbutikker.

Det kan i den forbindelse oplyses, at Rigspolitiet og SØIK i den kommende tid vil afdække mulighederne for en frivillig blokeringsordning med IT-udbyderne på området for falske hjemmesider. Dette kan i givet fald danne baggrund for en kontakt til teleudbyderne med henblik på en nærmere drøftelse.

Det kan i den forbindelse nævnes, at engelske teleudbydere netop på denne måde – og således på frivillig basis – blokerer ".uk"-hjemmesider, hvor politimyndighederne oplyser, at der er mistanke om salg af falske varer eller bedrageri i form af "phishing"."

Som det fremgår, har SØIK i første række fokus på at få beslaglagt og overdraget hjemmesider med falske webbutikker mv., så hjemmesiderne bliver lukket, og den kriminelle aktivitet bliver stoppet. Herudover vurderer SØIK naturligvis efterforskningsmulighederne i hver enkelt sag, men det kan dog erfaringsmæssigt være sager, som giver efterforskningsmæssige vanskeligheder, herunder ikke mindst når det gælder mulighederne for at identificere og efterforske mod gerningsmændene bag udenlandske hjemmesider. SØIK deltager i den forbindelse bl.a. i en fælleseuropæisk aktion koordineret af Europol, som har til formål at koordinere fælles aktioner mod falske hjemmesider.

Jeg kan i øvrigt tilføje, at politiet og anklagemyndigheden i de senere år har iværksat en lang række initiativer med henblik på at styrke behandlingen af straffesager om økonomisk kriminalitet og sager om it-relateret kriminalitet. Det gælder f.eks. kompetenceudvikling af anklagemyndigheden i forhold til it-relateret kriminalitet og udarbejdelse af vejledninger mv. om håndtering af sådanne sager. Det er områder, som der også i de kommende år vil være et stærkt fokus på, så der sikres en kompetent, målrettet og effektiv behandling af sagerne, herunder når økonomisk kriminalitet foregår via internettet."

Rigspolitiet har oplyst følgende:

> ”I forhold til efterforskning af de i artiklen fra den 14. december 2015 omtalte sager om bedrageri og overtrædelse af varemærkeloven mv. begået via hjemmesider på internettet henvises til bidraget til besvarelsen af spørgsmålet fra Rigsadvokaten.
>
> Rigspolitiet kan mere generelt oplyse, at der er sket en kraftig stigning i antallet af anmeldelser om økonomisk it-kriminalitet, herunder er der siden 2009 sket en tredobling i antallet af anmeldelser om bedrageri, der kan relateres til online køb, salg og bytte. En del af denne vækst kan tilskrives, at handel i stigende omfang foregår på internettet. På baggrund af dette kriminalitetsbillede arbejder Rigspolitiet på at udarbejde en operativ strategi, som skal fastlægge rammerne for de operative indsatser på området for økonomisk drevet kriminalitet på internettet.
>
> For så vidt angår mere konkrete initiativer kan det oplyses, at Københavns Politi i samarbejde med Rigspolitiet har iværksat et ”co-creation”-initiativ til bekæmpelse af økonomisk it-kriminalitet. Formålet med initiativet er – i tæt samarbejde med relevante myndigheder og virksomheder – at udarbejde en række nye og langsigtede tiltag, der på forskellig vis kan bidrage til at nedbringe økonomisk motiveret kriminalitet via internettet.
>
> Rigspolitiet har endvidere for nylig indledt en dialog med ”e-mærket” stiftet af Forbrugerrådet Tænk, Dansk Erhverv, Dansk Industri, Foreningen for Dansk Internethandel (FDIH), Finansrådet, Dansk IT og HK med henblik på at styrke politiets håndtering af svindel på nettet, herunder falske webbutikker.
>
> Endvidere er Rigspolitiet i øjeblikket i dialog med interesseorganisationen ”Rettighedsalliancen” vedrørende mulighederne for, at Rigspolitiet, Nationalt Cyber Crime Center (NC3), kan bistå Rettighedsalliancen i deres kommunikationsarbejde på internettet, således at borgere, der handler på internettet, bliver gjort opmærksomme herpå, når de er i færd med at bevæge sig ind på en hjemmeside, der sælger piratkopier. Formålet med denne indsats er at forsøge at motivere en eventuel køber til at fravælge piratvarer og i stedet købe lovlige varer.
>
> Rigspolitiet kan endelig oplyse, at Rigspolitiet via Facebook og Twitter yder en forebyggende indsats bl.a. ved at komme med advarsler om nye kriminelle trends eller kriminalitetsformer, der er særligt fremherskende i forhold til for eksempel julehandlen. Rigspolitiet advarede således f.eks. i begyndelsen af december 2015 via Facebook om falske webbutikker i forbindelse med julehandlen.

I forhold til eventuelle yderligere tiltag, der kunne medvirke til at imødegå problemet med svindel via webbutikker, kan Rigspolitiet oplyse, at Rigspolitiet har god erfaring med blokering af internetsider med ulovligt indhold. Rigspolitiet driver således i samarbejde med Red Barnet og størstedelen af de danske internetudbydere det såkaldte netfilter, hvis formål er på frivillig basis at blokere adgang til materiale med seksuelt misbrug af børn på internettet. I den forbindelse stiller Rigspolitiet løbende oplysninger til rådighed for internetudbyderne om internetadresser, som Rigspolitiet finder indeholder materiale, som er omfattet af straffelovens bestemmelser om børnepornografi. Det er herefter internetudbyderne, der blokerer for siderne i henhold til internetudbydernes forretningsbetingelser. Dette samarbejde har vist sig nyttigt og effektivt i en lang række sager vedrørende online seksuelt misbrug af børn, herunder særligt i sager med servere placeret i udlandet.

Det er Rigspolitiets vurdering, at en sådan blokeringsordning også vil kunne anvendes i forhold til de i artiklen nævnte webbutikker, herunder være særligt hensigtsmæssig i forhold til hjemmesider hostet uden for Danmark. Dette forudsætter dog, at udbyderne vil være indstillet på at udvide samarbejdet til også at omfatte denne form for kriminalitet. Der henvises i den forbindelse til bidraget til besvarelsen af spørgsmålet fra SØIK, som er enig i, at det vil være hensigtsmæssigt at søge at etablere en tilsvarende frivillig ordning for disse webbutikker, hvor der er mistanke om f.eks. salg af falske varer eller anden form for svindel."