Dok.: JJA40461

Udkast til tale til brug for besvarelse af samrådsspørgsmål AZ (Alm. del) fra Folketingets Retsudvalg

Samrådsspørgsmål AZ:

"Ministeren bedes redegøre for de eksisterende muligheder for at efterforske sager om identitetstyveri, om han mener, at de er tilstrækkelige, og om ministeren vil tage initiativ til at styrke politiets muligheder for at efterforske sager om identitetstyveri og i givet fald hvilke initiativer, samt om ministeren vil tage initiativ til at forbedre mulighederne for at hjælpe ofrene for identitetstyveri."

[Indledning]

1. Jeg vil gerne starte med at takke spørgeren for med samrådet at sætte fokus på tyveri og misbrug af andres identitet. Det er efter min opfattelse et meget relevant og alvorligt kriminalitetsområde, som vi – som samfund – bør give stor bevågenhed.

Jeg har allerede ved flere lejligheder besvaret skriftlige spørgsmål om dette emne, herunder bl.a. fra spørgeren. Jeg vil derfor indledningsvis tillade mig at henvise til disse besvarelser, som mit svar her i dag naturligt vil tage udgangspunkt i.

[Krænkende for ofrene]

2. Jeg tror, at vi alle sammen har stor forståelse for, at personer, som oplever at deres identitet bliver stjålent og misbrugt, kan føle sig dybt krænket og magtesløse.

Det gælder f.eks. i de tilfælde, hvor offeret ikke har den fjerneste idé om, hvem gerningsmanden er – eller hvordan den pågældende er kommet i besiddelse af offerets identitetsoplysninger – men hvor det i hvert fald kan konstateres, at der løbende dumper regninger og rykkere ind af offerets brevsprække. De kan f.eks. vedrøre låneaftaler og telefonabonnementer, som den pågældende ikke har noget kendskab til.

Derfor vil jeg også gerne understrege, at identitetstyveri og identitetsmisbrug er kriminalitetsformer, jeg som justitsminister ser på med stor alvor.

[De forskellige former for identitetstyveri]

3. Det er i den forbindelse vigtigt at være opmærksom på, at identitetstyveri og identitetsmisbrug spænder meget vidt, idet de enkelte tilfælde varierer fra mindre forhold, der ligger uden for det strafferetlige område, til meget grove sager om bl.a. bedrageri.

Jeg kan eksempelvis nævne, at det som udgangspunkt ikke i sig selv anses for strafbart, hvis en person opretter en falsk profil på internettet, hvor den pågældende alene udgiver sig for at være en anden eksisterende person.

Dermed ikke sagt at anvendelsen af en falsk profil i en andens navn slet ikke vil kunne være strafbar. For hvis man f.eks. også videregiver oplysninger om den pågældende person, vil det efter omstændighederne kunne udgøre en overtrædelse af straffelovens § 264 d om uberettiget videregivelse af bl.a. meddelelser vedrørende en andens private forhold.

Der vil også kunne være tale om en strafbar ærekrænkelse efter straffelovens § 267, hvis man opretter en profil i en andens navn og eksempelvis bruger profilen til at fremstille den pågældende i et dårligt lys ved at give udtryk for ekstreme synspunkter, som den pågældende ikke kan tillægges.

4. Rigspolitiet har oplyst, at identitetstyveri i praksis ofte sker som led i forskellige former for formueforbrydelser.

Det kan eksempelvis foregå ved, at gerningsmanden får kendskab til en anden persons bank- eller kreditkortoplysninger og herefter over internettet bestiller varer i den pågældendes navn, men med levering til sin egen adresse. Der kan også tænkes tilfælde, hvor gerningsmanden i en anden persons navn bestiller kreditkort eller indgår låneaftaler.

Jeg kan også nævne, at politikredsene i de senere år har efterforsket en række sager, hvor e-mail-konti er blevet overtaget via hacking med henblik på at samle informationer om ejeren af den enkelte e-mail-konto, ligesom der har været efterforsket sager, hvor en persons spillekonto hos en spiludbyder på internettet er blevet hacket og tømt for betalingsmidler.

[Den politimæssige indsats]

5. Jeg vil herefter vende mig mod den del af samrådsspørgsmålet, der vedrører den politimæssige indsats på området.

Rigspolitiet har mere generelt oplyst, at sager om identitetstyveri og identitetsmisbrug bliver efterforsket i den politikreds, hvor det strafbare forhold er begået.

Rigspolitiet kan dog yde bistand til den pågældende politikreds i forbindelse med efterforskningen af sådanne sager. Det kan eksempelvis ske ved, at Kriminalteknisk Center i Rigspolitiet bistår med undersøgelser af fysiske dokumenter, der kan bære spor af en gerningsmand.

6. Der kan også være tale om, at Rigspolitiets nationale it-efterforskningscenter – NITEC – bistår med tekniske undersøgelser af it-udstyr samt gennemgang og sikring af data mv., der kan indeholde elektroniske spor.

Bistanden med de tekniske undersøgelser af it-udstyr vil typisk bestå i at indhente oplysninger i form af såkaldte logfiler hos bl.a. internetudbyderne. Disse oplysninger, herunder IP-adresser, er ofte afgørende for opklaringen af det enkelte strafbare forhold.

I 2010 har NITEC bl.a. ydet politikredsene bistand med en it-teknisk gennemgang af data i sager, hvor der efterfølgende er rejst sigtelse for at have anvendt andres identitet til bl.a. falske kørekort og pas.

NITEC deltager endvidere internationalt i bekæmpelsen af identitetstyveri og identitetsmisbrug. Det sker både gennem samarbej-

de med de øvrige EU-lande inden for rammerne af Europol og gennem en række internationale arbejdsgrupper, hvor der løbende sker erfaringsudveksling og vidensdeling.

Rigspolitiet har således forskellige muligheder for at bistå politikredsene i efterforskningen af sager om identitetstyveri og identitetsmisbrug, og det er Rigspolitiets vurdering, at etableringen af NITEC i 2005 i relevant og nødvendigt omfang har fremmet politikredsenes indsats med at forebygge og efterforske it-kriminalitet, herunder sager om identitetstyveri og identitetsmisbrug via internettet.

[Forebyggelse – generelt]

7. Selv om Rigspolitiet har mulighed for at yde konkret it-bistand mv. til politikredsene i sager om identitetstyveri og identitetsmisbrug, er der tale om et kriminalitetsområde, hvor det kan være meget vanskeligt at afdække identiteten på den enkelte gerningsmand. Det skyldes, at de pågældende i vid udstrækning slører eller sletter de elektroniske spor, der måtte kunne danne grundlag for en effektiv efterforskning.

Derfor er det helt centralt at understrege, at hvis vi på effektiv vis skal komme identitetstyverierne til livs, vil det kræve en bredspektret indsats, der supplerer den politimæssige indsats på området.

Der er bl.a. behov for veludviklede sikkerhedsprocedurer hos myndigheder og virksomheder, der håndterer personhenførbare oplysninger, ligesom der er behov for skærpede legitimationskrav på områder, hvor identitetsmisbrug typisk forekommer.

Dernæst vil det kræve, at man fortsat fra myndighedernes side har fokus på at højne det tekniske niveau for en sikker identifikation af personer, der indgår aftaler eller anvender offentlige selvbetjeningssystemer på internettet.

Herudover er der behov for øget bevågenhed hos den enkelte borger.

[Forebyggelse – borgernes ansvar]

8. Og netop det sidstnævnte er meget centralt:

Hvis identitetstyveri på effektiv vis skal kunne forebygges, må vi alle sammen i vores dagligdag være meget opmærksomme på, at vi ikke uforvarende udleverer personoplysninger til uvedkommende. Herudover må vi sørge for at træffe de nødvendige foranstaltninger for at sikre vores private it-udstyr – f.eks. ved at knytte en adgangskode til den trådløse internetadgang derhjemme.

Jeg kan i den sammenhæng nævne, at Videnskabsministeriet i sin tilbagevendende kampagne *"netsikker nu!"* netop har sat fokus på en sikker adfærd blandt borgere på internettet og beskyttelse af personfølsomme oplysninger.

[Forebyggelse – myndigheders og virksomheders ansvar]

9. Men som sagt er det ikke kun borgernes ansvar.

Virksomheder og myndigheder, der betjener borgere i situationer, hvor der kan være særlig anledning til identitetsmisbrug, må naturligvis være opmærksomme på at stille skærpede legitimations-

krav, inden eksempelvis en aftale indgås eller en anmodning gennemføres.

Det gælder f.eks. for pengeinstitutter i forbindelse med indgåelse af låneaftaler og oprettelse af bankkonti og for kommunerne i forbindelse med anmeldelse af flytning.

[Forebyggelse – nye tekniske løsninger]

10. Når det gælder spørgsmålet om at højne det tekniske niveau for sikker identifikation har Videnskabsministeriet oplyst, at indførelsen af NemID i 2010 generelt har tilført øget sikkerhed til den tidligere digitale signatur. NemID indebærer bl.a., at der ved adgang til en række offentlige selvbetjeningssystemer skal angives to adgangskoder og et bruger-id, hvoraf den ene adgangskode er knyttet til et personligt fysisk nøglekort med engangskoder.

Der stilles desuden meget strenge krav til valideringen af den enkelte borgers identitet i forbindelse med udstedelse af NemID. Disse krav indebærer, at den enkelte borger enten skal møde fysisk op i f.eks. den lokale borgerservice og legitimere sig med de fornødne dokumenter eller bestille sit NemID online med angivelse af både cpr-nummer og kørekort- eller pasnummer, som derefter valideres hos henholdsvis Rigspolitiet og Det Centrale Personregister.

11. Ved mistanke om misbrug af en persons NemID kan der foretages spærring af det enkelte NemID, ligesom der inden for retsplejelovens rammer kan indhentes oplysninger om bl.a. tidspunkter for anvendelsen af det konkrete NemID og IP-adressen på den computer, som i den forbindelse er benyttet.

[Nye efterforskningsredskaber til politiet]

12. I samrådsspørgsmålet spørges også til, om der er behov for nye initiativer til styrkelse af politiets efterforskningsmuligheder.

Rigspolitiet har i den forbindelse oplyst, at politiet allerede i dag har en række relevante værktøjer til efterforskning af sager om identitetstyveri og identitetsmisbrug.

Rigspolitiet har samtidig oplyst, at man følger udviklingen på området tæt bl.a. med henblik at vurdere, om der i lyset af den teknologiske udvikling kan være behov for yderligere tiltag.

13. Rigspolitiet har i den forbindelse peget på, at det vil rumme betydelige efterforskningsmæssige fordele for politiet, hvis der indføres en generel forpligtelse for alle udbydere til at foretage registrering og opbevaring – såkaldt logning – af oplysninger om internetrelateret teletrafik.

Som logningsreglerne er i dag, er det således alene de kommercielle udbydere, som er forpligtede til at logge oplysninger om den teletrafik, der behandles i deres systemer. Det betyder, at en række offentlige myndigheder og institutioner, der på ikke-kommercielt grundlag stiller internet til rådighed – f.eks. biblioteker og kommunale borgerservicecentre – ikke er forpligtet til at foretage logning.

Jeg kan i den forbindelse oplyse, at en arbejdsgruppe med repræsentanter fra Justitsministeriet og Videnskabsministeriet samt Rigspolitiet, Politiets Efterretningstjeneste og IT- og Telestyrelsen for tiden er ved at overveje, hvordan oplysninger om brugere

af internetcaféer, gratis hotspots og internetadgang på biblioteker mv. kan registreres, så det sikres, at politiet har mulighed for at sammenholde oplysninger om brugeren med oplysninger om det enkelte kommunikationsapparat.

Arbejdsgruppen forventes at afslutte sit arbejde omkring 1. juli, og jeg ser meget frem til at modtage arbejdsgruppens anbefalinger og forslag til konkrete initiativer på området.

[Ofre for identitetstyveri]

14. Spørgeren ønsker også oplyst, hvad man kan gøre for at hjælpe ofrene for identitetstyveri.

Jeg vil i den forbindelse gerne understrege, at regeringen helt generelt lægger stor vægt på, at de, der bliver ofre for forbrydelser, behandles med alvor og respekt, og at de får den hjælp og støtte, der er relevant og effektiv i situationen.

Regeringen har meget stor fokus på indsatsen over for ofre og har løbende taget en række initiativer på dette område. Politi og anklagemyndighed har også stor fokus på at yde den nødvendige støtte og bistand til ofre for en forbrydelse.

Jeg kan i den forbindelse nævne, at der i 2007 blev gennemført nye regler for at styrke og udbygge politiets og anklagemyndighedens information og vejledning til forurettede. Der kan desuden udpeges en kontaktperson hos politiet eller anklagemyndigheden, som yder hjælp og bistand til den forurettede, og som den pågældende altid kan henvende sig til.

15. Herudover nedsatte Justitsministeriet i 2009 en bredt sammensat arbejdsgruppe, som bl.a. skulle overveje, hvordan indsatsen over for ofrene yderligere kunne styrkes.

Arbejdsgruppen konkluderede bl.a., at ordningerne for ofre for forbrydelser generelt er velfungerende. Arbejdsgruppen pegede dog på enkelte områder, hvor der kunne være behov for at give ofrene endnu bedre forhold. Og på den baggrund fremsatte jeg i begyndelsen af 2011 et lovforslag med en række forbedringer på offerområdet i overensstemmelse med arbejdsgruppens anbefalinger. Forslaget blev vedtaget af et bredt flertal i Folketinget og træder i kraft den 1. juli 2011.

[Afslutning]

16. Afslutningsvist vil jeg gerne understrege, at identitetstyveri og identitetsmisbrug er grove former for kriminalitet, som jeg ser meget alvorligt på.

Rigspolitiet har – som jeg har været inden på – forskellige muligheder for at bistå politikredsene i efterforskningen af disse sager. Og navnlig med etableringen af NITEC er der skabt mulighed for fra Rigspolitiets side at yde kvalificeret teknisk bistand til politikredsene i forbindelse med efterforskningen af konkrete sager om f.eks. misbrug af personoplysninger via internettet.

Rigspolitiet følger udviklingen på området tæt, og jeg vil naturligvis være parat til at overveje de yderligere tiltag, som Rigspolitiet eller andre måtte vurdere, at der kan være behov for.

Samtidig må det dog erkendes, at den politimæssige indsats på området ikke kan stå alene.

Der er derfor bl.a. vigtigt, at man både hos myndigheder og virksomheder er opmærksom på at håndhæve strenge sikkerhedsprocedurer ved håndtering af personhenførbare oplysninger samt at sikre skærpede legitimationskrav på områder, hvor identitetsmisbrug typisk forekommer.

Men der er herudover også anledning til at fremhæve, at forebyggelse af sager om identitetstyveri og identitetsmisbrug i høj grad forudsætter, at borgerne er bevidste om, hvordan man anvender it-udstyr på sikker vis, og at vi som samfund må hjælpe med at skærpe borgernes opmærksomhed på dette område.

TAK.