

## Økonomi- og indenrigsminister Margrethe Vestagers talepapir

*Det talte ord gælder*

**Anledning: Samråd O og P**

**Tid og sted: Torsdag d. 4. april 2013**

### **Spørgsmål O**

”Med henvisning til de seneste aktuelle sager om brist i sikkerheden omkring CPR-numre, f.eks. som vist i indslag på TV2-Fyn den 6. februar 2013, bedes ministeren redegøre for omfanget af sikkerhedsbrist omkring CPR-numre og give et skøn over misbrug af CPR-numre og give et skøn over identitetstyveri, herunder tyveri og misbrug af CPR-numre, samt redegøre for hvilke initiativer regeringen vil tage for at styrke sikkerheden omkring CPR-numrene.

### **Spørgsmål P**

”Vil ministeren i forlængelse af samrådet om CPR-sikkerhed redegøre for, hvilke analyser og overvejelser regeringen har vedr. muligheden for, at man i særlige tilfælde kan tildele nyt CPR-nummer”.

### **Talens struktur og væsentligste budskaber**

- Personoplysninger - herunder personnumre - skal beskyttes.



- Der gennemføres løbende kontrol med, at det ikke via private virksomheders hjemmesider med integration til CPR er muligt at gætte sig frem til en andens personnummer.
- Vi kender ikke omfanget af identitetstyveri og misbrug af personnumre – men der er stigende fokus på området.
- Identitetstyveri skal først og fremmest forhindres ved, at der foretages den nødvendige identitetskontrol – det vil regeringen påpege over for erhvervslivet.
- Regeringen ser samtidig på, om det giver mening at tildele nyt personnummer i særlige tilfælde.

## **Indledning**

Det er meget brede spørgsmål, som rejses under disse samråd, og som samtidig breder sig over flere ministres områder. Jeg skal forsøge at runde de mange emner, så godt som det nu kan lade sig gøre.

### **1. Persondataloven**

Kravene til offentlige myndigheder og private virksomheders beskyttelse af personoplysninger, er reguleret i persondataloven, som administreres af Datatilsynet.

Det var derfor også Datatilsynet, som af egen drift den 4. februar 2013 efter medieomtale af sagen fra Region Syddanmark, bad regionen om en redegørelse om offentliggørelsen af en række personers personnumre.

Sagen er fortsat under behandling i Datatilsynet, og jeg vil derfor ikke komme nærmere ind på den konkrete sag.



Til brug for samrådet har Datatilsynet mere generelt oplyst, at persondataloven stiller krav om, at offentlige myndigheder og private virksomheder m.fl. beskytter alle de personoplysninger, som de håndterer, med tilstrækkelige sikkerhedsforanstaltninger. Persondataloven indeholder altså en forpligtelse for den dataansvarlige til at beskytte såvel følsomme oplysninger som fortrolige og almindelige ikke-følsomme oplysninger.

Den dataansvarlige skal derfor sikre sig, at it-systemer, organisation og arbejdsgange indrettes sådan, at kravene om datasikkerhed efterleves. At sikre at personoplysninger, herunder personnumre, ikke uberettiget offentliggøres på en hjemmeside, er utvivlsomt omfattet af den dataansvarliges forpligtelse efter persondataloven.

I situationer, hvor der er en potentiel risiko for offentliggørelse af fortrolige personoplysninger – som personnumre jo er – peger Datatilsynet på, at der skal udvises særlig påpasselighed.

Det er naturligvis ikke muligt helt og holdent at undgå, at personoplysninger ved en fejl offentliggøres.

Datatilsynet oplyser, at hvis det sker, medfører kravet om god databehandlingskik, at den dataansvarlige skal vurdere, om - og i givet fald hvordan - de berørte personer skal underrettes.

God databehandlingskik betyder også, at den dataansvarlige skal rydde op efter fejlen eller sikkerhedsbristen og forsøge at begrænse skadevirkningerne. Ved uberettiget offentliggørelse på internettet skal oplysningerne derfor fjernes fra hjemmesiden i en fart, og den ansvarlige må prøve også at få dem fjernet fra Google og andre søgemaskiner.



Hvad angår omfanget af sager, hvor der er tale om brist i sikkerheden omkring personnumre, har Datatilsynet oplyst, at tilsynet løbende håndterer sager om sikkerhedsbrister herunder sager, hvor personnumre er blevet offentliggjort. Alene inden for de seneste måneder er der rejst flere sager ud over den aktuelle sag fra Region Syddanmark. Datatilsynets fokus er først og fremmest på, at få den dataansvarlige til at tage affære og gøre det nødvendige for at begrænse skadevirkningerne. Der kan også blive tale om kritik og forslag til fremadrettede foranstaltninger.

## **2. Videregivelse af data fra CPR**

Inden for mit eget område har det i medierne været fremme, at man ved misbrug af visse selvbetjeningsløsninger på hjemmesider med integration til CPR har kunnet gætte en anden persons personnummer ved at foretage gentagne indtastninger af navn og vilkårligt personnummer.

CPR-kontoret har flere gange indskærpet over for virksomheder med adgang til CPR, at virksomheden skal sikre, at et sådant misbrug ikke kan finde sted.

Derudover har CPR-kontoret i 2012 gennemført en kontrol af 115 private virksomheders anvendelse af CPR.

Kontrollen har vist, at stort set alle virksomheder hver især har etableret foranstaltninger, som forhindrer førnævnte mulighed for misbrug. Det synes jeg er meget positivt.



### 3. Omfanget af identitetstyveri

Der spørges også til omfanget af identitetstyveri og misbrug af personnumre.

Jeg har derfor via Justitsministeriet af Rigspolitiet fået oplyst, at identitetstyveri eller anden form for identitetsmisbrug som altovervejende udgangspunkt sker for at begå anden kriminalitet, for eksempel forskellige former for berigelseskriminalitet, hacking, databedrageri og chikane og trusler.

Det er ikke muligt umiddelbart ud fra politiets systemer at opgøre antallet af sager om identitetstyveri og anden form for identitetsmisbrug, der typisk vil være registreret som f.eks. en sag om bedrageri. En opgørelse vil således forudsætte en manuel gennemgang i politikredsene af et meget stort antal potentielt relevante sager.

Rigspolitiet kan derfor ikke udtale sig med sikkerhed om, hvorvidt der er tale om en stigning i antallet af identitetstyverier, herunder tilfælde hvor der sker misbrug af den forurettedes personnummer.

Rigspolitiet har dog oplyst, at der i den seneste tid været et øget fokus på identitetstyverier, der fra flere sider opleves som et stigende problem.

Derfor har Rigspolitiet, Det Kriminalpræventive Råd og Digitaliseringsstyrelsen i samarbejde udarbejdet 10 gode råd til at undgå identitetstyveri. Rådene kan findes på Det Kriminalpræventive Råds, politiets og Digitaliseringsstyrelsens hjemmesider.



#### 4. Identitetstyveri, herunder misbrug af personnummeret

Utsigtet offentliggørelse af personnummeret kan ske på forskellig vis. Det kan f.eks. ske ved, at en person lægger sit C.V. indeholdende personnummeret ud på internettet. En person kan også få stjålet sin pung med sundhedskort og kørekort, hvoraf personnummeret fremgår. Der kan også være tale om, at en virksomhed eller en myndighed ved en fejl offentliggør personnumre på sin hjemmeside, som vi har set det i den omtalte sag fra Region Syddanmark.

Personnummeret alene er aldrig tilstrækkeligt til at identificere en person og må derfor ikke i sig selv kunne medføre, at der f.eks. kan udleveres oplysninger, handles via nettet osv.

Noget tyder på, at langt de fleste tilfælde af identitetstyveri sker ved misbrug af personoplysninger, når der handles på internettet.

Det har vist sig, at der findes webbutikker, som tilsyneladende alene baserer deres identitetskontrol på et oplyst navn, adresse og personnummer. Det åbner for misbrug, hvor kriminelle kan handle i andres navn.

Kriminalitet af den her karakter giver tab for erhvervslivet, men kan frem for alt have store konsekvenser for de sagesløse personer, det går ud over, ligegyldigt hvordan vedkommendes identitet er kommet til den kriminelles kendskab.

Der er i dag ikke hjemmel til at tildele nyt personnummer til ofre for identitetstyveri. Det er der en god grund til. Der er nemlig ikke grundlag for at antage, at det i almindelighed vil hjælpe at tildele nyt personnummer. Det skyldes først og fremmest, at når en erhvervsdrivende ikke foretager den nødvendige identitetskontrol,



kan den kriminelle blot fortsætte misbruget ved brug af det gamle personnummer, uanset hvor mange nye personnumre offeret tildeles.

Regeringen vil derfor tage initiativ til, at problemstillingen rejses over for de relevante virksomheder og brancheorganisationer med fokus på vigtigheden af, at man ved indgåelse af handler er meget omhyggelig med at sikre sig, at det er den rigtige person, man indgår aftalen med.

Mange virksomheder anvender allerede CPR i deres webbutikker bl.a. for at opnå stor sandsynlighed for korrekt identitet. Nogle virksomheder går videre og kombinerer CPR-adgangen med krav om anvendelse af betalingskort eller NemID for at opnå større sikkerhed for, at de har handlet med den rigtige person. Det er efter min opfattelse den helt rigtige vej at gå.

## **5. Regeringens overvejelser om nyt personnummer i særlige tilfælde**

Der spørges også til regeringens overvejelser omkring muligheden for i særlige tilfælde at tildele nyt personnummer.

Når vi taler om muligheden for at forebygge identitetstyveri, er det som nævnt min helt klare opfattelse, at det der virkelig vil hjælpe er, at erhvervslivet foretager den nødvendige identitetskontrol. Uden den nødvendige identitetskontrol vil kriminelle fortsat kunne købe smartphones og Ipads ved brug af offerets gamle personnummer. Det er derfor regeringen nu griber fat i de relevante virksomheder og brancheorganisationer og påpeger vigtigheden af, at der foretages en ordentlig identitetskontrol.



Regeringen ser samtidig på, om det giver mening at tildele nyt personnummer til ofre for identitetsmisbrug i visse, helt særlige tilfælde. Kan der identificeres tilfælde, hvor det faktisk kan hjælpe den person, hvis identitet bliver misbrugt, vil regeringen søge at tilvejebringe lovhjemmel til at tildele nyt personnummer.