



# Notat

---

## Samrådstale

Besvarelse af Social- og Indenrigsudvalgsspørgsmål L af 6. januar 2021 stillet efter ønske fra Preben Bang Henriksen (V)

### Samrådsspørgsmål

*Vil ministeren forholde sig til den problemstilling, der er blevet omtalt i TV-Avisen på DR søndag den 6. december 2020 og mandag den 7. december 2020 vedrørende afluring af personlige data via installationer på bibliotekernes computere, og vil ministeren endvidere oplyse, hvilke tiltag ministeren vil igangsætte med henblik på at undgå denne form for svindel med bl.a. NEMID?*

### Det talte ord gælder

#### [Indledning]

- Tak for ordet og for samrådsspørgsmålet stillet af Preben Bang Henriksen fra Venstre.
- Jeg vil til en start forsikre jer om, at jeg tager sikkerheden i vores offentlige digitale løsninger *meget* alvorligt.
- Det er helt afgørende, at alle danskere trygt kan gøre brug af vores offentlige digitale løsninger.
- Derfor er sikkerheden i løsninger som NemID og NemKonto et vigtigt fokus for regeringen.
- Og lad mig med det samme slå fast, at både NemID og NemKonto helt generelt er præget af en meget høj sikkerhed. Og vi holder løbende øje med, om der er brug for at justere løsningerne for at beskytte danskerne endnu bedre.
- Det ændrer ikke på, at det selvfølgelig er dybt beklageligt og ulykkeligt, når der så *alligevel* sker svindel og kriminalitet.
- Identitetstyveri, som vi har set i de sager, som TV-Avisen tog op, er en alvorlig forbrydelse, som påvirker de mennesker, som det rammer, dybt.
- Det skal vi selvfølgelig gøre alt, hvad vi kan for at beskytte danskerne imod.

- Men samtidig vil jeg – desværre - også minde om, at det er vanskeligt – for ikke at sige umuligt – at gardere sig 100 pct. mod kriminelle handlinger. Det gælder både i den fysiske og den digitale verden.

### **[Beskrivelse af sagen - identitetstyveri]**

- Jeg er blevet bedt om at forholde mig til kriminelles afluring af data på offentligt tilgængelige computere og fortælle om, hvilke tiltag regeringen igangsætter for at undgå svindel med blandt andet NemID.
- I den forbindelse finder jeg det også naturligt at adressere den historie om sikkerheden i NemKonto og NemID, som DR bragte for nyligt.
- De sager, som DR beskriver, handler om identitetstyveri, hvor it-kriminelle gennem avancerede metoder ulovligt får adgang til en borgers NemID.
- Identitetstyveri er, når personlige oplysninger bliver stjålet og misbrugt.
- Personlige oplysninger kan fx være CPR-nummer, adgangskoder, sundhedsoplysninger eller NemID-oplysninger.
- De oplysninger, som den kriminelle får fat i, kan misbruges til for eksempel at optage lån i borgerens navn eller tømme borgerens bankkonto.
- Der findes forskellige former for identitetstyveri, og ofte skal den kriminelle stjæle mere end én oplysning fra borgeren.
- Identitetstyveri og svindel med NemID blev drøftet på et samråd i Social - og Indenrigsudvalget den 27. august 2020, hvor jeg forklarede, hvordan kriminelle har gjort brug af såkaldte keyloggere til at foretage identitetstyveri og franske borgere deres NemID.
- En keylogger kan være installeret i tastaturet, i computeren eller være en usb-nøgle, som er tilsluttet computeren, og den bruges til at registrere alt, hvad der taster på et tastatur.
- Hvis en borger bruger en computer, hvor der er installeret keyloggere, kan it-kriminelle begå identitetstyveri ved at opsnappe de oplysninger, som borgeren taster. Fx bruger-id, adgangskoder, kontonumre og lignende følsomme oplysninger.
- De it-kriminelle kan derefter bruge disse oplysninger til fx at teste, om oplysningerne giver dem adgang til at logge ind med NemID.

- For at svindle med NemID er det dog ikke tilstrækkeligt at aflure borgernes bruger-id og adgangskode. De it-kriminelle skal også skaffe sig adgang til borgerens NemID-nøglekort.
- Når en kriminel har begået identitetstyveri og franarret en borger sit NemID, kan den kriminelle ulovligt gøre en række forskellige ting. Den kriminelle kan fx få adgang til borgerens netbank, bestille kreditkort i borgerens navn eller optage kviklån.
- Den kriminelle kan *også* få adgang til at ændre, hvilken bankkonto der er registreret som borgerens NemKonto, så det er den kriminelle, der fx modtager borgerens udbetalinger fra det offentlige.
- Derfor er det særligt vigtigt at sætte ind over for identitetstyveri og minimere risikoen for, at kriminelle svindler med andre borgeres NemID.

### **[Respons på DR's kritikpunkter]**

- Inden jeg går nærmere ned i de konkrete tiltag, vi har igangsat, vil jeg gerne sige et par ord om DR's dækning af sagen.
- DR har fremført forskellige kritikpunkter af Digitaliseringsstyrelsens håndtering af forskellige henvendelser vedrørende sikkerheden i NemID og NemKonto.
- Som det fremgår af de svar til udvalget, jeg har oversendt her til formiddag, redegøres her for, hvorfor artiklerne ifølge Digitaliseringsstyrelsen ikke giver et fyldestgørende billede af, hvordan Digitaliseringsstyrelsen har forholdt sig til henvendelserne.
- Men jeg vil selvfølgelig sørge for, at der tilgår Folketinget en redegørelse herom, så alle kan være betrygget.

### **[Tiltag foranledige af konkrete svindelsager]**

- Lad mig igen understrege, at NemID og NemKonto er gode og sikre løsninger. Siden 2016 er der årligt foretaget omkring 90 mio. udbetalinger via NemKonto. Der er over 5,2 mio. unikke brugere af NemID-identiteter, og der har været 6 mia. NemID-transaktioner, siden løsningen blev lanceret i 2010. Løsninger bliver brugt meget, og er til stor gavn for borgerne.
- Men it-kriminelle udvikler – desværre – hele tiden deres metoder.
- Det er én af grundene til, at vores digitale løsninger bliver løbende vedligeholdt, opdateret og nogle gange udskiftet.

- Digitaliseringsstyrelsen har løbende fokus på, hvordan sikkerheden i og omkring de digitale løsninger som NemID styrkes.
- Det gælder både den tekniske opbygning af løsningerne, og – lige så vigtigt – hvordan vi kan informere og hjælpe danskerne med en sikker brug af løsningerne, så de kan beskytte sig mod svindel.
- Sikkerheden i og omkring NemID afhænger nemlig både af de tekniske foranstaltninger i selve løsningen, af sikkerheden på offentlige tilgængelige computere, fx på biblioteker, og af borgernes fornuftige adfærd.
- På samrådet i august beskrev jeg omfanget af misbrug og konkrete tiltag for at begrænse misbrug med NemID.
- Her beskrev jeg, at Digitaliseringsstyrelsen allerede tilbage i 2017 implementerede en teknisk ændring i NemID.
- Ændringen afværger det scenarium, hvor kriminelle ved brug af borgerens NemID-bruger-id og –adgangskode kunne melde et nøglekort mistet. Når den kriminelle gjorde det, blev et nyt nøglekort automatisk sendt til borgerens adresse, hvor den kriminelle så kunne stjæle nøglekortet fra borgerens postkasse.
- Ændringen betyder, at der ikke længere automatisk fremsendes et nyt nøglekort, når et nøglekort bliver spærret. Nu skal borgerens aktivt bestille et nyt nøglekort og i den forbindelse validere sig med sit danske pas eller kørekort.
- Efterfølgende udviklede de kriminelle imidlertid en ny tilgang, hvor de systematisk overvågede borgerens brug af nøgler fra NemID-nøglekortet. De kriminelle udnyttede visningen af antal resterende nøgler til at gætte, hvornår et nyt nøglekort ville blive sendt til borgeren. Herefter stjal de kriminelle borgerens nye nøglekort fra postkassen.
- Som beskrevet på samrådet i august 2020 blev visningen af, hvor mange nøgler der er tilbage på nøglekortet, fjernet for at mindske risikoen for denne type svindel.
- I begge disse scenarier er der tale om ganske avanceret kriminalitet, hvor der er sket en række alvorlige kriminelle handlinger, der både omfatter digital afluring af borgernes oplysninger **og** fysisk tyveri fra borgernes postkasser. Digitaliseringsstyrelsen har i begge tilfælde sat hurtigt og effektivt ind for at forhindre svindlen.
- Det er derfor også - i alle tilfælde, hvor en borger er udsat for kriminelle handlinger, vigtigt, at politiet inddrages, så sagen kan efterforskes med henblik på

retsfølgelse af de skyldige. I sidste uge så vi et eksempel på, hvordan to mænd er idømt fængselsstraffe for svindel med NemID.

### **[Øvrige tiltag for at styrke sikkerheden]**

- Derudover er der også på flere andre tidspunkter gennemført ændringer i NemID, som har højnet sikkerheden.
- I 2018 blev NemID-nøgleappen introduceret. Den gør det nemmere for borgeren at se, hvilken transaktion vedkommende er i gang med at foretage – fx at logge ind på sundhed.dk eller at gennemføre en konkret betaling.
- Med nøgleappen kan man heller ikke blive lokket eller presset til at udlevere sine NemID-oplysninger til svindlere på samme måde som med nøglekortet, da der ikke er ”nøgler”, altså talkoder, som man kan komme til at oplyse.
- Som jeg beskrev på samrådet i sommer, vurderer Digitaliseringsstyrelsen løbende, hvilke nye tiltag der skal iværksættes for at beskytte danskerne mod digital kriminalitet. Denne vurdering sker blandt andet på baggrund af afrapporterede risici fra fx leverandøren af it-løsningerne.
- På baggrund af de oplysninger, som Digitaliseringsstyrelsen indsamler, bliver det vurderet, om der er behov for justering af NemID-løsningen eller for kampanjer, der skal oplyse om sikker brug af NemID.
- Sikker og fornuftig adfærd er en central del af al it-sikkerhed. Hvis borgerne fx bruger de samme adgangskoder på tværs af de digitale løsninger, er der større risiko for, at it-kriminelle kan opsnappe deres adgangskoder.
- Derfor gennemfører Digitaliseringsstyrelsen løbende forskellige indsatser i form af fx kampanjer og vejledning til borgere.
- Målet med disse er at skabe en større bevidsthed om sikker digital adfærd. Digitaliseringsstyrelsen vejleder bl.a. borgerne i, hvor vigtigt det er at have et unikt bruger-id og en stærk adgangskode til NemID.
- Digitaliseringsstyrelsen har sammen med KL og Danske Regioner flere gange iværksat landsdækkende kampanjer om it-sikkerhed. De to sidste år under overskriften ”*Et klik kan ændre alt*”, og der vil også i år blive gennemført en lignende kampagne med fokus på identitetstyveri.
- På hjemmesiden sikkerdigital.dk kan borgere, virksomheder og myndigheder også få råd og vejledning om, hvad man skal være opmærksom på, når man har mistanke om identitetstyveri. Og ikke mindst vejledning i at spotte de digitale fælder, så man bedre kan undgå at blive udsat for svindel.

- Siden samrådet i sommer har Digitaliseringsstyrelsen opdateret en række sider på NemID.nu og Borger.dk, så det er tydeligere, hvordan man som borger kan bruge sit NemID sikkert og have de nye svindelmetoder for øje.

### **[Tiltag på kommunernes område]**

- Derudover har Digitaliseringsstyrelsen en tæt dialog med KL om tiltag, som kan styrke sikkerheden på offentligt tilgængelige computere.
- Digitaliseringsstyrelsen har senest den 16. februar 2021 afholdt møde med KL, hvor sikkerheden blev drøftet.
- Allerede i 2017 satte KL og kommunerne ind med tiltag for at højne sikkerheden på de offentlige computere.
- KL har også i sommeren 2020 fulgt op på kommunernes sikring af offentligt tilgængelige computere.
- Jeg beskrev på samrådet den 27. august, at sikkerheden på offentlige tilgængelige computere skulle skærpes.
- Som udvalget blev orienteret om efter samrådet, har KL fulgt op på konkrete anbefalinger fra Rigspolitiet og har sat ind med en række målrettede initiativer. Det drejer sig om blandt andet konkrete tekniske anbefalinger og medarbejdervendte vejledninger.
- Som daværende fungerende finansminister Morten Bødskov også beskrev i svaret på Social- og Indenrigsudvalgets spørgsmål nr. 177 af 22. december 2020 ser KL blandt andet på, hvilke digitale løsninger der kan benyttes for at sikre offentlige computere mod it-kriminalitet.
- Det er dog ingen garanti for, at de it-kriminelle ikke finder på nye og mere avancerede metoder.
- Derfor skal vi fortsætte med at følge udviklingen inden for identitetstyveri og digital svindel tæt – og vi skal løbende vurdere, hvordan løsninger som NemID fortsat kan være sikre at benytte for borgerne.

### **[Afrunding]**

- Til sidst vil jeg igen understrege, at regeringen tager borgeres digitale sikkerhed meget alvorligt. Vi ser løbende på, hvordan man bedst kan sikre de offentlige it-løsninger, så kriminelle ikke kan misbruge dem.

- Derfor er der også sat flere tiltag i gang, som vil bidrage til at styrke sikkerheden i de offentlige løsninger.
- Senere i år lancerer vi det nye MitID, der skal afløse NemID, og her er der indført en række nye tiltag, der skal beskytte danskerne mod svindel. Det vil gøre MitID til en endnu mere sikker løsning.
- Med finansloven for 2021 har vi desuden afsat en bevilling til udviklingen af et nyt NemKonto-system. Det arbejde sættes i gang i år.
- Vi skal blandt andet se på, hvordan vi – i højere grad end i dag – kan bruge data, så det bliver nemmere at reagere på svindelmønstre. Med bedre datadatatudnyttelse kan vi gennemføre datadrevne analyser, så vi kan identificere svindelmønstre og sætte ind over for dem.
- Sidst, men ikke mindst arbejder regeringen også på en ny national strategi for cyber- og informationssikkerhed. Med den nye strategi vil regeringen bl.a. sætte fokus på, hvordan man kan hjælpe borgere og virksomheder og vejlede dem ved mistanke om it-sikkerhedshændelser som fx identitetstyveri.
- Som jeg sagde indledningsvis, så har vi gjort meget og der er også en høj grad af sikkerhed i vores it-løsninger.
- Men jeg syntes ikke, at vi i Danmark er gode nok til at hjælpe borgere, der kommer i klemme, hvis man på trods af alle sikkerhedsindsatser alligevel er så uheldig at blive ramt af svindel.
- Og derfor syntes jeg også, at det er vigtigt, at vi tager yderligere skridt.
- Helt konkret betyder det blandt andet, at regeringen vil oprette en ”hotline”, der 365 dage om året skal hjælpe og vejlede borgere og virksomheder vedr. digitale trusler og sikker digital adfærd.
- Eller sagt på en anden måde – hvis man som borger bliver udsat for identitetstyveri, er det et utroligt stort indgreb i sit liv – de fleste ved ikke, hvordan man præcist skal agere i sådan en situation og har brug for hurtigt hjælp og vejledning.
- Jeg opfatter det her som en dagsorden, vi i fællesskab har et ansvar for at prøve at løfte.
- Med patientvejledere inden for sundhedsvæsenet kan man, hvis man er udsat for en alvorlig sygdom, få hjælp til at finde rundt i systemerne i et tidspunkt, hvor man har nok at se til og tænke på.

- Vi skal gøre noget lignende, hvis man bliver udsat for it-kriminalitet, hvor ens identitet bliver stjålet.
- Der skal være én indgang, hvor man kan henvende sig, og få vejledning til henvendelse hos andre myndigheder.
- På den måde skal borgere ikke stå alene med problemet.
- Det er også vigtigt, at denne ordning kører 365 dage om året. Ofte ses det, at fredag eftermiddag er et populært tidspunkt at lave den slags handlinger over for borgere. Og borgere skal ikke vente med at få hjælp til efter weekenden.
- Borgere skal hurtigt og effektivt kunne få hjælp, hvis de kommer i klemme
- Og så er det regeringens klare holdning, at borgere ikke skal hæfte ved andres misbrug af fx deres NemID, hvis borgeren ikke har handlet uagtsomt.
- Eller sagt på en anden måde – vi er optaget af, at der skal gælde det samme udgangspunkt, hvis man får stjålet sine oplysninger eller kort, mens man handler i brugsen, som hvis det sker digitalt.
- Udgangspunktet i dag er allerede, at man får dækket sine tab, men vi vil i samarbejde med andre ministerier se på, om der er nogle huller, vi skal have håndteret, så man som borger, uden at have handlet uagtsomt, bliver udsat for svindel, kan få bedre hjælp og støtte end i dag og også være sikker på, at man ikke kommer til at hænge på regningen.
- Det håber jeg, at der vil være opbakning til i folketinget på tværs af partier.
- Det vil vi tage initiativ til, og jeg vil også gerne have en tæt dialog med folketingets partier og jeg håber vi i fællesskab kan finde nogle gode løsninger til gavn for borgerne.
- Tak for ordet.