Datatilsynet

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres referanse	Vår referanse	Dato
15/8216	15/01605-2/SDK	15.03.2016

Høringsuttalelse - Digital sårbarhet - NOU 2015:13

Datatilsynet takker for en interessant og grundig utredning.

Mange av temaene som tas opp har personvernproblematikk. Vårt overordnede inntrykk er at rapporten beskriver utfordringer og dilemmaer på dette området på en god måte.

Vårt høringssvar er delt i tre:

- Personvern og sikkerhet: Vi ønsker innledningsvis å knytte noen overordnede kommentarer til forholdet mellom personvern og digital sårbarhet/sikkerhet. Dette gir et bakteppe for de påfølgende kommentarene til rapportens konkrete deler.
- Kommentarer til rapporten – fire viktigste temaer: Vi vil her fremheve de temaene vi mener det er viktigst å formidle vårt syn på. Disse handler i stor grad om utvalgets hovedanbefalinger og tilknyttede underpunkter til disse.
- Øvrige kommentarer til rapporten: Vi vil her formidle våre øvrige kommentarer til rapporten, opplistet etter tilhørighet til ulike kapitler eller anbefalinger i rapporten.

Personvern og sikkerhet

I den offentlige debatt er det en utbredt forståelse at personvern og sikkerhet er motstridende interesser. Det er i beste fall villedende. Hensynet til sikkerhet og hensynet til personvern følger ofte hverandre. Personopplysningsloven har egne krav til informasjonssikkerhet, og sikring av personopplysninger er ikke vesensforskjellig fra sikring av annen beskyttelsesverdig informasjon. Et godt IKT-sikkerhetsarbeid vil normalt også favne om sikringen av personopplysninger, eller i det minste få positive ringvirkninger for dette arbeidet. Vi kan vanskelig se for oss et godt personvern uten gode sikkerhetsmekanismer i dagens digitale hverdag.

Etter vårt syn er oppmerksomhet om samfunnets digitale sårbarhet svært viktig i dag. Å redusere vår digitale sårbarhet er i hovedtrekk også i personvernets interesse. Interessekonflikt mellom personvern og IKT-sikkerhet finnes først og fremst i forbindelse med tiltak som samler inn personopplysninger for å avdekke trusler mot sikkerheten, eller omfattende innsamling av opplysninger for å kunne rekonstruere hvem som har gjort hva til bruk i

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

eventuelle undersøkelser i etterkant av hendelser. Det finnes grenser for hvor inngripende et forsvarlig tiltak kan være, og under alle omstendigheter bør tiltak som griper inn i personvernet være så skånsomme som mulig. Det finnes et betydelig potensiale i dag for å gjøre tiltak mindre inngripende ved å ta i bruk prinsippene om innebygd personvern (privacy by design)[1].

Kommentarer til rapporten – fire viktigste temaer

1. Behov for utredning og debatt ved vurdering av inngripende tiltak

Datatilsynet er tilfreds med at rapporten identifiserer og poengterer behovet for utredning og debatt i forbindelse med vurdering av inngripende tiltak, satt frem som et av utvalgets viktigste anbefalinger: «Sikre balansen mellom personvern og et sikrere samfunn gjennom utredninger og offentlig debatt.» (side 16)

Utvalget merker seg at inngripende metoder foreslås uten særlig utredning av konsekvenser. Dette er også vår erfaring. Svak eller manglende utredning av personvernkonsekvenser utgjør et betydelig problem etter vårt syn.

Risikoen er stor å implementere løsninger eller lovbestemmelser som ikke er proporsjonale, dersom det ikke i forkant utredes og debatteres konsekvensene for personvern og andre viktige individuelle rettigheter. I verste fall kan tiltak som bryter menneskerettigheter bli< iverksatt. Manglende konsekvensutredninger er ikke kun et problem i forhold til hvert tiltak for seg, men også summen av tiltakene, og hvilken inngripen de samlet representerer.

Datatilsynet stiller seg altså bak utvalgets generelle anbefaling. Her viser vi også til vårt forslag om en personvernkommisjon på justissektoren, som er omtalt i punkt 2.
I sammenheng med behov for utredninger, vil vi kommentere konkrete anbefalinger fra to steder i rapporten:

<u>Rapportens 11.7.5 Etablere tiltak for å regulere utlevering av trafikkdata til politiet</u>
Her sier rapporten at «Utvalget mener at formålsutglidning av bruk av opplysninger som omtalt over (særlig signaleringsdata) bør utredes. I denne sammenheng bør også dommernes tekniske kompetanse som grunnlag for å ta stilling til innsynsbegjæringer vurderes.

Utvalget mener det er behov for å avklare hjemmelsgrunnlaget for regulering av tilgang til signaleringsdata. Utvalget er videre av den oppfatning at bruk av signaleringsdata er blitt så utbredt som etterforskningsverktøy at det bør vurderes å lovregulere dette som et særskilt tvangsmiddel.»

Datatilsynet er enig i både forslag og begrunnelse. En slik lovregulering bør blant annet ha bestemmelser for politiet eller teleselskapet om informasjonsplikter overfor involverte. Det må også etableres nærmere bestemmelser om sletteplikt for data som ikke blir brukt som bevis.

[1] https://www.datatilsynet.no/Teknologi/Innebygd-personvern/

Rapportens 21.11.8 – Sikre balansen mellom personvern og et sikrere samfunn

Utvalget peker her ut to områder hvor det må foretas viktige avveininger, og hvor eventuelle endringer i særlig grad krever forutgående debatt og et godt beslutningsgrunnlag:

- Utrede innføring av digitalt grenseovervåking
- Utrede politiet og PSTs skjulte metodebruk på Internett

I sammenheng med digitalt grenseovervåking, mener utvalget at debatten bør forberedes gjennom en Norsk offentlig utredning (NOU) eller et tilsvarende utredningsdokument. Det digitale sårbarhetsutvalget mener at utvalget som skal gjøre denne utredningen «må ha en erfaringsbase som gjør at hensyn til etterretningsbehov, teknologisk kompetanse og personvernhensyn ivaretas, og at man sikres en grundig redegjørelse for de teknologiske, rettslige og samfunnsmessige spørsmålene saken reiser». I tillegg foreslår digitalt sårbarhetsutvalg punkter til et mandat. Punktene handler blant annet om formålsavklaring, tiltak for å motvirke formålsutglidning, gevinster ved tiltaket, alternative løsninger og konsekvenser for individer, næringsliv og nasjonal sikkerhet.

For utredning av politiets og PSTs skjulte metodebruk på internett, sier rapporten at mange av de samme hensyn vil gjøre seg gjeldende.

Datatilsynet er her helt enig. På disse to områdene må det ikke gis nye fullmakter eller metoder uten grundig utredning og debatt. Datatilsynet er også enig i de kvalitetskrav utvalget skisserer for utredningene. Dette er gode prinsipper også ut over de to nevnte områdene.

En analyse av gevinster er svært viktig. Hva kan vi ha tillit til at nye eller utvidede fullmakter vil oppnå? Spørsmålet kan ikke ses løsrevet fra hvilke hjemler som allerede finnes. Om nye fullmakter *egentlig* er nødvendige må også ses i sammenheng med om eksisterende fullmakter utnyttes på en god måte.

Bør digital grenseovervåking og skjult metodebruk på internett utredes uansett?

Selv om Datatilsynet er for grundige utredninger, mener vi ikke at nye og inngripende metoder bør utredes uansett. Vi mener tvert imot at det er gode grunner for tilbakeholdenhet med å legge ut nye og inngripende tiltak til vurdering. Vi ser at personvernet settes under press allerede når man beslutter å utrede nye og inngripende tiltak. Det kan på denne måten skapes en forventning om at noe skal innføres i nær fremtid. Dette er noe vi erfarer at kan skape politisk handlingspress på å imøtekomme krav og ønsker fra sikkerhetsmyndigheter.

Vi merker oss at utredning av digital grenseovervåking allerede er besluttet og annonsert 24. februar av forsvarsministeren. For politiet og PSTs skjulte metodebruk på Internett er vi ikke kjent med noen beslutning. Rapporten sier at «Dersom PST igjen reiser forslag om å registrere ytringer på sosiale medier og analysere informasjon fra åpne kanaler, mener utvalget at det er et særskilt behov for en full offentlig utredning.»

Datatilsynet mener at ønsker om nye midler fra PST selv, ikke alene bør være nok. Behov for utredninger forutsetter en politisk vilje til i det hele tatt å vurdere en slik innføring. I august 2014 foreslo sjef for PST, Benedicte Bjørnland, at PST burde kunne lagre informasjon om nettbruk og at PST burde kunne ta i bruk stordataanalyse, noe som vil føre til innsamling av

informasjon om personer som ikke ellers er av interesse for PST. NRK meldte at «etter at PSTs ønske ble kjent, har norske toppolitikere stått i kø for å ta avstand fra slike virkemidler»[2].

Datatilsynets holdning til masseinnsamling og faren for konflikt med grunnleggende rettigheter
Datatilsynet er svært kritisk til tiltak som bærer preg av masseovervåking og masseinnsamling av personopplysninger om alminnelige borgere. Det må være full trygghet for at aktuelle tiltak – det være seg digitalt grenseovervåking, PSTs mulighet til å lagre informasjon om nettbruk og bruk av stordataanalyse, eller andre omfattende og inngripende tiltak – lar seg løse uten å komme i konflikt med menneskerettighetsforpliktelser og grunnloven. Her bør det særlig trekkes lærdom av skjebnen til Datalagringsdirektivet (DLD), som ble kjent ugyldig av EU-domstolen i 2014 (også nevnt i utvalgets rapport).

I oktober 2015 leverte Hans Petter Graver og Henning Harborg sin utredning, bestilt av Samferdselsdepartementet og Justisdepartementet[3]. Temaet her var om den norske implementeringen av DLD helt eller delvis lot seg redde uten å komme i konflikt med grunnleggende rettigheter. Graver og Harborg tegner et dystert bilde av framtidsutsiktene for den norske løsningen for datalagring, selv i modifisert form. I rapporten står det:

«Det kan etter vår oppfatning ikke utelukkes at de personvernmessige betenkelighetene ved overvåkningselementet er så fremtredende og tungtveiende at man simpelthen ikke kan anse datalagring nødvendig i et demokratisk samfunn.» (side 67)

Vi vil også presisere at det ved fremtidige vurderinger forventes et godt datagrunnlag om behov for tiltaket, noe utvalget også trekker frem: *«De hensynene som underbygger behovet for nye etterretnings- og etterforskningsmetoder, må baseres på et solid empirisk grunnlag. Dette er vesentlig for å kunne vurdere om tiltakene er nødvendige og proporsjonale i et demokratisk samfunn»* (side 286). Store svakheter på dette feltet var også et sentralt poeng i utredningen fra Graver og Harborg i forbindelse med DLD.

2. Rapporten underbygger behovet for en personvernkommisjon på justissektoren

I forlengelsen av temaet over, gjentar vi at det er behov for en *helhetlig oversikt*:

Datatilsynet mener det bør nedsettes en personvernkommisjon for justissektoren (i bred forstand).

En personvernkommisjon for justissektoren kan gi en status for personvernets kår i sektoren, gi en beskrivelse av hvilket inngrep totaliteten av tiltakene representerer, vurdere hvordan personvernet kan avveies mot andre interesser, og utvikle en obligatorisk analysemodell for hvordan gode personvernvurderinger i justissektoren skal foretas.

[2] http://www.nrk.no/norge/sv_-_-gar-kaldt-nedover-ryggen-1.11892589
[3] DATALAGRING OG MENNESKERETTIGHETENE
https://www.regjeringen.no/no/aktuelt/ekspertutredning-om-datalagring-og-menneskerettighetene/id2455164/

Datatilsynet har tatt til orde for en slik personvernkommisjon i brev til, og i møte med justisministeren. En personvernkommisjon på justissektoren er også foreslått i Politidirektoratets datakrimstrategi,[4] noe vi er svært godt fornøyd med.

3. Forbud mot eller regulering av kryptering er et blindspor

Datatilsynet merker seg med glede utvalgets konklusjon om at bruk av kryptografi ikke bør reguleres. Vi mener dette både er en riktig konklusjon og en svært viktig konklusjon. Datatilsynet er også enig i at norske myndigheter bør arbeide aktivt mot regulering eller forbud internasjonalt. I dag er dette viktig for både virksomheter og enkeltmennesker, som i stort omfang tar i bruk forskjellige elektroniske tjenester levert av utenlandske aktører, hvor kryptering er i bruk eller burde bli tatt i bruk.

Kryptering, og muligheten for å kunne stole på krypteringen, er av stor betydning for personvernet i dag. Dette har ikke minst Snowden-saken illustrert. Avsløringene har også fungert som en katalysator for en mer omfattende bruk av kryptering i forskjellige tjenester. Datatilsynet støtter altså utvalgets konklusjon og begrunnelse, og håper at diskusjonen om bakdører og innebygde svakheter som «løsninger» på sikkerhetsutfordringer kan stilne hen. Det er ikke et fruktbart spor.

4. Behov for styrket kompetanse i IKT-sikkerhet

Ett av utvalgets hovedforslag handler om nasjonal kompetansestrategi innen IKT-sikkerhet. I rapportens 19.8.1 sies det: «Justis- og beredskapsdepartementet bør sammen med Kunnskapsdepartementet utarbeide en overordnet nasjonal strategi for å sikre en langsiktig oppbygging av kompetanse innen IKT-sikkerhet i det norske samfunnet. En slik strategi må dekke tiltak for å bygge opp kapasitet innen både forskning og utdanning.»

Datatilsynet støtter utvalgets mål om økt kompetanse i IKT-sikkerhet, og vi er enige i at en nasjonal kompetansestrategi er ønskelig. For å sikre at personvernrelevante problemstillinger knyttet til IKT-sikkerhet blir tydelig i dette arbeidet anbefaler vi at også Kommunal- og moderniseringsdepartementet (KMD) tas med som aktør. KMD er ansvarlige for personopplysningsforskriften og har kompetanse på personvern på departementsnivå. Om ønskelig stiller også Datatilsynet seg til disposisjon.

Sikringen av personopplysninger og den øvrige IKT-sikkerheten er ofte tett sammenvevd. Våre erfaringer fra tilsyn, veiledningsarbeid og bransjekontakt tilsier at mangel på kunnskap er blant de viktigste grunnene til det at sikkerheten ofte ikke er god nok. Samfunnet bør sørge for at kompetanse i IKT-sikkerhet ikke er et knapphetsgode. Behovet for kompetanse vil øke i takt med digitaliseringen.

Ny personvernforordning, som etter all sannsynlighet vil tre i kraft våren 2018, vil fordre et mer profesjonalisert personvernarbeid i virksomhetene. Her er IKT-sikkerhet av stor betydning. Videre setter forordningen krav til at alle offentlige virksomheter skal ha et personvernombud (Data Protection Officer). Det samme vil gjelde for private virksomheter som oppfyller visse krav.

[4] https://www.regjeringen.no/contentassets/4d2ba37bf2ae4cc9ac39afdf20a2f41b/datakrimstrategi_2015.pdf

Etter vårt syn er det svært viktig at kompetansetiltak ment for å møte virksomhetsbehov også inkluderer informasjonssikkerhetskrav ved behandling av personopplysninger. Dette vil gjøre det lettere å ha nødvendig kunnskap til å ivareta flere hensyn og krav samtidig. Vi ser også behov for tiltak som handler om vurdering av konsekvenser for personvernet før man skal ta i bruk eller utvikle IKT-løsninger. Dette er krav som tydeliggjøres i den kommende personvernforordningen. Innebygd personvern («privacy by design» og «privacy by default») og vurdering av personvernkonsekvenser («privacy impact assessment») må etter vår vurdering være elementer i et undervisningsopplegg.

I rapportens 23.6.1 vises det til cyberstrategier i andre land. Her står det at «den nederlandske cyberstrategien går langt i å vise til viktigheten av næringsaspektet ved sikkerhetsløsninger. I strategien fremheves det at innovasjon, sikkerhet og personvern i designfasen av produkter og systemer er initiativer myndighetene og næringslivet skal fokusere på og belønne». Datatilsynet mener at dette bør gjøres også i Norge. Dette kan understøttes ved å innføre emner som innebygd personvern og innebygd informasjonssikkerhet[5] i undervisningen for alle IKT-bachelorgrader innen IKT.

Datatilsynet støtter også utvalgets mål om tiltak rettet mot de yngste aldersgruppene.

Øvrige kommentarer til rapporten

Nedenfor gir vi øvrige kommentarer til innholdet i rapporten, sortert etter aktuelt kapittel.

Forslaget om å redusere kritikaliteten av Telenors kjerneinfrastruktur

Behovet for å redusere kritikaliteten i Telenors kjerneinfrastruktur står først nevnt blant utvalgets viktigste forslag (utdypet i kapittel 10). Rapporten beskriver at et utfall i Telenors kjerneinfrastruktur får «alvorlige og samtidige konsekvenser på de aller fleste samfunnsområder, og for alle de kritiske samfunnsfunksjonene som er omtalt i denne rapporten» (side 16). Dette vedrører også et viktig aspekt ved informasjonssikkerhet for personopplysninger, nemlig tilgjengelighet.

I dagens situasjon er mange virksomheter avhengige av tilgang til personopplysninger som ikke er lagret lokalt. Et utfall vil altså ikke bare kunne hindre det å sende eller motta personopplysninger, men også muligheten til å kunne aksessere fjernlagrede personopplysninger.

Datatilsynet støtter utvalgets forslag om å arbeide for en situasjon hvor minst én annen aktør har et landsdekkende kjernenett som er på samme nivå som Telenors.

---

5 https://www.regjeringen.no/contentassets/b7d0918e555b418abda2993a71969cdc/handlingsplan_informasjonssikkerhet_staten.pdf

Kapittel 3 om rettsstatsprinsipper og grunnleggende samfunnshensyn

Rapporten beskriver grunnleggende samfunnshensyn, menneskerettigheter og rettsstatsprinsipper allerede i kapittel 3. Datatilsynet mener dette er viktig innhold og en god plassering. Beskrivelsen gir den videre lesningen et nødvendig perspektiv.

En viktig verdi med kapittelet er presiseringen av at tiltak ikke kun er et spørsmål om formålstjenlighet og politisk vilje – handlingsrommet er begrenset av ytre rammer i form av menneskerettigheter og grunnloven, hvor retten til personvern, blant flere fundamentale rettigheter, er nedfelt.

Kapittel 13 om energiforsyning

Behovet for å beskytte personopplysninger økes kraftig ved innføring av automatisk strømmåling (AMS). Å koblet den enkelte strømmåler mot internett fører med seg et nytt sikkerhetsbehov. Hyppig avlesning av målerstand gir også kundedata med et langt større beskyttelsesbehov enn tidligere. Detaljerte data om strømforbruk kan si mye om beboeren/ beboernes dagsrytme, tilstedeværelse og bruk av eget hjem, noe rapporten også rekker frem.

Slik vi ser det, er det behov for at tiltak for styring av IKT-sikkerheten i sektoren også har betydelig oppmerksomhet om sikring av personopplysninger.

Kapittel 17 om helse og omsorg

Datatilsynet er enig i utvalgets vurderinger og forslag (sidene 199-200). Helsesektoren er preget av tung personvernproblematikk. Etter vårt syn peker helsesektoren seg ut som et område hvor det er et særlig behov for utredninger av bredt sammensatte eksterne utvalg. Dette vil i større grad kunne sikre at sektorens behov blir godt drøftet mot personvernkonsekvenser.

Øvrige kommentarer til kapittel 21 om å avdekke og håndtere digitale trusler og utvalgets forslag om styrke politiets evne til å bekjempe IKT-kriminalitet

Datatilsynet er enig i målet for å styrke politiets evne til å bekjempe IKT-kriminalitet (ett av utvalgets hovedanbefalinger). Vi ønsker også å gi klar støtte til målet om å sikre sterke fagmiljøer for IKT-kriminalitet i politidistriktene, som omtalt i 21.11.6.

I forbindelse med CERT-er, VDI, sektorvise responsmiljøer og mulig samlokalisering gir utvalgets rapport lite informasjon for å kunne vurdere personvernkonsekvenser. I rapportens 21.11.1 om vurderinger og tiltak foreslår utvalget bedre koordinering og deling av informasjon, herunder også mellom myndigheter og private aktører.

Dette vil sannsynligvis også kunne innbefatte personopplysninger. Uten gode analyser av personvernkonsekvenser er det vanskelig for oss å ha klare meninger om dette feltet. Vi vil imidlertid påpeke et par viktige poenger:

Mål om deling og bedre informasjonsflyt på tvers av virksomhetsgrenser krever stor bevissthet og klare føringer for hva som er tillatt å dele mellom aktørene. Behovet for

bevissthet og klare føringer blir også betydelig hvis det blir slik utvalget foreslår at det skal være samhandling og informasjonsdeling mellom de offentlige aktørene og private aktører. Det krever også stor bevissthet om hva som er å forstå som personopplysninger, jf personopplysningslovens § 2 nr 1. I denne sammenheng er det neppe alltid intuitivt. Vi presiserer at hvorvidt det er *hensikten* å behandle personopplysninger ikke er det avgjørende, men om det faktisk skjer.

Klarhet, tydelige rutiner og kontroll med at praksis er i tråd med personvernregelverket blir enda viktigere ved en eventuell samlokalisering for å lette informasjonsflyten, som utvalget foreslår i 21.11.2.

Høringsuttalelse til forslaget om endringer i sikkerhetsloven
I forbindelse med VDI og CERT-er viser vi også til vår høringsuttalelse fra august 2015 om forslag til endringer i sikkerhetsloven (2013/00552/FD). Vi er i hovedsak fornøyd med at VDI- og NorCERT-ordningene er foreslått lovregulert, men Datatilsynet mente at høringen manglet en adekvat beskrivelse av både de tiltakene som lovhjemmelen ga rom for å gjennomføre, og hvilke konsekvenser tiltakene kunne føre med seg.

Kapittel 22 om felleskomponenter

Datatilsynet er enige i utvalgets vurderinger og forslag på dette området (sidene 285-287). Vi er særlig tilfreds med at utvalget peker på viktigheten av regulering av elektronisk identitet, samt at det pekes på utfordringene ved bruk av private eID-er til jobbrelaterte forhold.

Datatilsynet ser også utfordringene ved å vente på det nasjonale ID-kortet, men vi er usikre på om det er fornuftig å videreutvikle MinID. Slik vi ser det vil en videreutvikling av MinID kun være hensiktsmessig dersom man beslutter at en framtidig kvalifisert MinID skal være den eID som skal finnes i tilknytning til Nasjonalt ID-kort. Uten en slik beslutning ser vi det ikke som hensiktsmessig å videreutvikle MinID, når man i ID-porten allerede har markedsbaserte løsninger som fungerer tilfredsstillende.

Kapittel 23 om tverrsektorielle sårbarhetsreduserende tiltak og anbefaling om å styrke IKT-sikkerhetskompetansen i flere sektortilsyn

Datatilsynet er enig i at det er behov for styrket kompetanse innen IKT-sikkerhet i sektortilsyn (et av utvalgets viktigste anbefalinger), og vi tror det er hensiktsmessig å etablere fellesarenaer for erfaringsutveksling og dialog mellom sektortilsyn og tverrsektorielle tilsyn.

I punkt 23.4.2 anbefaler utvalget «at Justis- og beredskapsdepartementet tar initiativ til å etablere en fellesarena for tilsynssamarbeid på IKT-sikkerhetsområdet.» Datatilsynet mener at vi naturlig vil høre hjemme på en slik fellesarena.

Datatilsynet er enig i at redegjørelse for IKT-sikkerheten bør inngå i årsmeldinger, slik utvalget foreslår i rapportens 23.5.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Stian Kringlebotn
seniorrådgiver

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0032 OSLO