POLITIET

Notat

Fra	Politiets data- og materielltjeneste	*Dato*	13.12.2012
		Vår referanse	201200429-2
Til	Politidirektoratet/Juridisk avdeling/Utredningsseksjonen	*Saksbehandler*	Kathinka Bull-Engelstad og Bente Bergh
		Telefon	
		Telefaks	
Kopi til			

Høringsinnspill digital kommunikasjon som hovedregel
Politiets data- og materielltjeneste har sett på høringsbrevet vedrørende digital kommunikasjon som hovedregel, og har enkelte innspill.

Juridisk har følgende bemerkninger:
PDMT støtter POD sitt forslag om at digital kommunikasjon som hovedregel kun reguleres i fvl. § 15a da dette etter vår mening vil fremstå mer oversiktlig. For de to alternativene til endring av fvl. § 15a støtter PDMT forslaget til POD om digitalt førstevalg for digitalt aktive (alternativ 2). På denne måten sikrer man en effektiv innføring av digital kommunikasjon som hovedregel samtidig som man ivaretar de som ikke har tilgang til eller kunnskap om bruk av elektronisk kommunikasjon. Videre tror PDMT dette alternativet best vil sikre valgfrihet for den enkelte bruker.

Dersom departementet velger å gå for løsningen hvor digital kommunikasjon som hovedregel også skal reguleres i fvl. §§ 16 og 27 anbefaler PDMT at man velger alternativ 3 digitalt førstevalg for de digitalt aktive. Begrunnelsen for valget av dette alternativet følger av foregående avsnitt.

Videre har PDMT noen bemerkninger til de varslede endringene i eForvaltningsforskriften. PDMT synes det er positivt at tilgang til kontaktinformasjonsregisteret blir begrenset til den registrerte og forvaltningsorganet som skal sende digital post til vedkommende, jfr. punkt 6.2.3 bokstav c i utredningen. Det bemerkes at det ikke ser ut til å være lagt opp til en tilsvarende tilgangsstyring for reservasjonsregisteret og PDMT synes dette er uheldig av hensyn til den enkeltes personvern. Videre bemerkes det at selv om det legges opp til en begrenset tilgang til kontaktinformasjonsregisteret så sies det ikke noe om hvorvidt det skal tilgangsbegrenses innad i forvaltningen. Det fremstår som uklart om samtlige saksbehandlere i et forvaltningsorgan som sender digital post skal ha full tilgang til registeret, eller om det kun skal gis registertilgang til utvalgte personer. PDMT ønsker å

peke på viktigheten av tilgangsstyring til registre samt tilstrekkelige sikkerhetsløsninger for å sikre personvernet og forvanske mulighetene for ID-tyveri.

IKT har følgende bemerkninger:
Politiets data og materielltjeneste har gått igjennom høringsdokumentene og i tillegg til fokusområder i høringen ønsker vi å rette oppmerksomheten mot følgende områder:

- Har man et helhetsperspektiv når man oppretter konkurrerende register?
- Har e-id forvaltningen tilstrekkelig fokus på identitets tyveri, falske og dublerte identiteter?

Lovverkets konservering av måter å kommunisere på, vil kreve hyppige endringer i lover og forskrifter. Generell regulering av kommunikasjon mellom det offentlige og borgere/næringsliv burde være å foretrekke. Form burde styres av tilbud og etterspørsel og vil gi stor grad av valgfrihet. Det er kun alternativ 2, digitalt førstevalg for de digitalt aktive, som vil sikre at det er borgeren selv som tar initiativ og bestemmer kommunikasjonsform.

Departementet vil utarbeide egen forskrift for kontaktregisteret, men vi vil allerede nå peke på noen utfordringer knyttet til et slikt kontaktregister og spesielt e-id tildeling og forvaltning.

Opprettelse av kontaktregisteret vil bli en kopi av og konkurrent til folkeregisteret, spesielt sett i lys av folkeregisterets fornyelsesprosess. Spørsmålet er om kontaktregisteret er i stand til å ta opp i seg de utfordringene som folkeregisteret har identifisert og står overfor i fornyelsesprosessen. Dette kan være alt fra ny personidentifikator, personer med kode 6 og 7, verge og umyndige, gradering av hvor sikker identitet er, misbruk av fødselsnummer som pin kode, samhandling der falske identiteter er konstatert etc.

Datatilsynet definerer identitetstyveri på følgende måte: «Identitetstyveri oppstår når noen anskaffer, overfører, besitter eller fremstår som rette innehaver av personlige opplysninger tilhørende en privatperson eller selskap på en uautorisert måte, med den hensikt å begå bedrageri eller annen kriminalitet.»[1]

Utfordringen for politiet og andre offentlige organer (SKD, NAV med flere), med et kontaktregister, er at dette kan bli et nytt "brohode" for identitetstyveri og falske identiteter. "Brohodet" etableres gjennom å tilegne seg e-id gjennom inngåtte avtaler.

Å fastslå at en person er den samme som identitetsdokumentet tilsier, kan kun gjøres av personelle som er trent til dette. Slik trening har ikke ansatte i post og butikk. Selv et trent øye sliter innefor dette området da produksjon av falske identifikasjonsdokumenter er svært profesjonell.

Problemstillinger knyttet til identitetstyveri, falsk identitet og "id hvitevasking" er belyst i en rekke rapporter, eksempelvis "Politiets omverdensanalyse (POD 2012)" og "Identitetstyverier i tillitsfulle systemer (SIFO 2010). Det er derfor viktig at man i det norske samfunn ikke legger til rette for økt misbruk.

---

[1] http://www.datatilsynet.no/Sikkerhet-internkontroll/ID-tyveri/

Oslo Politidistrikt har sett en eksplosiv økning de siste årene hva gjelder bruk av forfalskede identitetsdokumenter og aliasidentiteter. Under er en oversikt over antall straffesaker for bruk av forfalskede identitetsdokumenter per år registrert ved Oslo Politidistrikt:

År	**Antall saker**	**År**	**Antall saker**	**År**	**Antall saker**	**År**	**Antall saker**
2010	363	**2007**	39	**2004**	51	**2001**	15
2009	121	**2006**	34	**2003**	47	**2000**	3
2008	208	**2005**	50	**2002**	44	**1990**	0

De fleste eksempler på slik kriminalitet går på å oppmå rettigheter i det norsk samfunn samt økonomisk vinning.

Her følger noen eksempler:

- Over 100 falske greske, italienske og belgiske identiteter ble bekreftet aktive i 2010 ved at de hadde betalt skatt i 2009 og mottok skattekort for 2010. Identitetene ble benyttet av flere personer og sågar har en forsøkt å søke statsborgerskap.
- Kvinner føder under falsk identitet og barnet blir automatisk statsborger.
- Tre forskjellige personer fått utstedt norske pass på samme identitet.
- Personer tatt med flere utenlandske pass på forskjellige identiteter

Å være offer for identitetstyveri kan være en traumatisk opplevelse og konsekvensene for den det gjelder er stor. Det er vanskelig å rydde opp i og ikke minst krevende å etterforske. Omfanget av denne type kriminalitet antas å være økende. Det er derfor i politiets interesse at tildeling av e-id har et best mulig sikkerhetsregime.

En sikker identitet kan kun fastslås gjennom biometri, men det offentlige er engstelige for at biometri skal resultere i et overvåkingssamfunn. På en annen side åpner biometri for at det blir langt mindre bruk for det vi i dag omtaler som personinformasjon. Biometri til erstatning for personinformasjon reduserer "Se og Hør faktoren" samt problemstillinger som personopplysningsloven forsøker å regulere.

I Aftenposten mandag 10.12.2012, skriver Christian Gjøsteen om hvor lett det er å utnytte en annen persons bank-id, logge seg inn på "Mine resepter" og spre dette i sosiale medier.

Biometri gjør det mulig å være sikker på hvem en har en dialog med. Et fremtidsscenario kan være automatisk grensekontroll ved hjelp av biometri. En person som er utvist ved dom fra Norge kommer til en automatisk grensekontroll. Her henvises vedkommende gjennom en "rød dør", hvor han får vite at han ikke har adgang til riket. Dersom vedkommende ønsker å vite hvorfor han ikke har anledning til å komme inn i landet, kan han gå til en egen terminal og, ved hjelp av biometri, få se grunnlaget for nektet innreise.

Alt dette kan foregå uten at tjenestemann trenger å kjenne til personinformasjon som navn, bosted etc. Biometri vil på denne måten kunne erstatte reisedokumenter som pass og identifikasjonsdokumenter. Dette gjør det enkelt for de med lovlig adgang å kunne ferdes mellom ulike land, og det blir tilsvarende vanskeligere for kriminelle å kunne gjøre det samme.

Tilgang til offentlig forvaltning med tanke på rettigheter og plikter bør foregå på en sikrest mulig måte og det bør legges hindringer i veien for identitetstyveri. Vi mener at tildeling av e-id hvor ansatte i bank, post og butikk er ansvarlig for autentisering av personer, er en alt

for svak og usikker metode. E-id tildeling bør være basert på biometri primært, sekundært bør tildeling gjennomføres av myndighet som er trent for å vurdere identifikasjonsdokumenter.

Med hilsen

Jan Westbye
Avdelingsdirektør JAS