Feil nummerbruk
av Gisle Hannemyr

Er det bruk av fødselsnummer som er problemet når systemene lekker informasjon?
I sommer havnet personopplysninger om 60 tusen nordmenn på avveie. Datatilsynet svarer med å vurdere forbud mot bruk av fødselsnummer. Problemet er imidlertid ikke bruk av fødselsnummer, men *feil* bruk av fødselsnummer.

Det ble en smule oppstyr i sommer, da Aftenposten (*Nordmenn lett bytte i storskala ID-tyveri*, 2007-07-19) omtalte en rapport *(http://www.nowires.org/IDtheft/)* der forskerne Klingsheim og Hole påviste hvordan en rekke norske nettjenester – teleselskaper, banker, helsevesenet, Posten og den statlige tjenesten Altinn – kunne tappes for opplysninger eller misbrukes på grunn av grove designfeil i de berørte systemene.

Med utgangspunkt i rapporten var det enkelt å lage et program for å hente ut opplysninger fra de berørte systemene. Jeg laget et slikt program, og hentet ut fødselsnummer, navn, adresse og kredittverdighet for et vilkårlig antall personer fra flere mobiloperatører. Andre gjorde tydeligvis det samme, for opplysninger om anslagsvis 60 tusen personer ble hentet fra Tele2 i tidsrommet 28.-30. juli 2007.

Det er siden kommet fram at feilen i Tele2s datasystem var kjent av selskapet lenge før tappingen skjedde. Den ble påtalt av Datatilsynet i et brev datert 26. november 2006, uten å bli rettet. Da mediene i juli 2007 omtalte feilen, ble den heller ikke rettet. Først etter at misbruket ble kjent i august 2007 ble feilen rettet. Ifølge personopplysningsloven plikter behandlingsansvarlige å «sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet» (Personopplysningsloven § 13 første ledd). Har Tele2 oppfylt lovens krav til forsvarlig forvaltning?

I kjølvannet av denne saken håpet jeg at forskernes gode rapport om designfeilene i de berørte systemene skulle gi fokus på viktigheten av design for å ivareta personvernet. Så langt har det ikke skjedd. I stedet har vi fått fokus på bruk av *fødselsnummer*. Brønnøysundregistrene vil slutte med å bruke fødselsnummer som identifikator, og Datatilsynet vurderer å forby det (jf.: *Personnummer vekk som ID*, Forbruker.no, 2007-08-30)

Dette er en avsporing. Poenget i rapporten er ikke bruk av fødselsnummer, men at feil bruk av fødselsnummeret er et personvernproblem. Det er for eksempel feil bruk at et system *gir fra seg informasjon eller tjenester* bare det blir presentert for et fødselsnummer, eller at nummeret brukes til noe det aldri har vært meningen å benytte det til, som *autentisering*.

Fødselsnummeret er ikke uproblematisk: I fødselsnummeret er det innbakt unødige personopplysninger som alder og kjønn; og kanskje gjør fødselsnummeret det *for* enkelt å koble opplysninger fra ulike registre. Men dette er ikke begrunnelsen for at Datatilsynet vurderer forbud, så det er en annen debatt.

Fødselsnummer ble i sin tid innført fordi det var behov for en slik unik identifikator. Det behovet eksisterer fortsatt. Med mindre man tenker seg veldig godt om, kan det hende at det som ev. erstatter fødselsnummeret i disse systemene, blir minst like problematisk fra et personvern- og sikkerhetsperspektiv.

Benyttet på forsvarlig vis mener jeg at fødselsnummer er en god løsning for identifikasjon. Den mest åpenbare fordelen med fødselsnummeret er at de fleste av oss kjenner vårt eget fødselsnummer. I en verden der vi må identifisere oss i stadig flere ulike sammenhenger vil det å måtte forholde seg til de mange *ulike* personidentifikatorer som vil måtte komme i stedet for fødselsnummer utvilsomt komplisere hverdagen for den enkelte. Og kompleksitet er en risiko. Folk kan bli avskåret fra tjenester de har krav fordi de roter med sine ulike digitale identifikatorer, eller at folk hjelper på hukommelsen ved å skrive ned sine digitale identiteter, noe som åpner opp for identitetstyveri ved at utenforstående får tilgang til disse notatene.

Vi bør altså vende tilbake til forskernes rapport for å se hva som er galt med de berørte systemene. Her er en kort oppsummering:

1. Systemene forteller om et fødselsnummer er i bruk, typisk ved å gi feilmelding dersom det tastes inn et ubrukt fødselsnummer, og ved å gå videre i prosessen dersom fødselsnummeret finnes. Det trenger de ikke gjøre. Ved å sørge for at systemet responderer på samme vis enten fødselsnummeret er i bruk eller ikke vil det ikke

lenger være mulig å misbruke systemet til å hente ut fødselsnummer som er i bruk.
2. Systemene bruker fødselsnummer til *autentisering*, ikke til *identifisering*. Forskjellen på de to er at når fødselsnummeret brukes til autentisering, så gir nummeret tilgang til informasjon eller tjenester som skal være forbeholdt den autentiske person som identifikasjonen er knyttet til. Tele2, Posten og flere nettbanker hadde denne feilen i sine systemer. Hadde disse systemene i stedet vært konstruert slik at verken informasjon eller tjenester hadde vært tilgjengelig før *etter* at personen, i tillegg til å *identifisere* seg ved å oppgi fødselsnummer, også må *autentisere* seg på en uavhengig og sikker måte (f.eks. gjennom å oppgi en engangskode fra en kodekalkulator) hadde bruken av fødselsnummer til identifikasjon etter min mening ikke vært en personvernrisiko.

Jeg frykter at i denne saken, der det forståelig nok kreves handling etter at personopplysninger om 60 tusen nordmenn er kommet på avveie, kan det bli tatt grep som sannsynligvis ikke bidrar til å sikre forsvarlig forvaltning av personopplysninger i norske virksomheter.

Det finnes allerede lover som pålegger de behandlingsansvarlige å sikre at disse ikke kan misbrukes på grunn av feildesign. Det Datatilsynet burde gjøre, er å sørge for å bruke de fullmakter de har til håndheve de lover som allerede er i kraft, i stedet for å vurdere å innføre nye paragrafer eller forskrifter, som mildt sagt virker lite gjennomtenkte.

Artikkelen ble først publisert i: *Klassekampen,* 12. september 2007, og gjengis med tillatelse av forfatteren.

Gisle Hannemyr er lektor og forsker ved Institutt for Informatikk, Universitetet i Oslo.

Overskuddsinformasjon ved kommunikasjonskontroll

Høyesteretts kjennelse av 11.10.2007 (HR-2007-01742-A), dommerne Indreberg, Tønder, Flock, Øie og Gussgard). Den offentlige påtalemyndighet (statsadvokat Tormod Haugnes) mot [E] (advokat Erik Keiserud), [D] (advokat Geir Jøsendal), [C], [B] (advokat Odd Rune Torstrup) og [A] (advokat John Christian Elden).

Straffeprosess. Adgang til bruk av overskuddsinformasjon fra kommunikasjonskontroll når retten vil dømme for et mindre alvorlig forhold enn det tiltalen gjelder og som i seg selv ikke kunne ha begrunnet kommunikasjonskontroll.

Saken gjelder flere siktede, og retten fører et lengre resonnement. Her er det bare tatt inn referat av det sentrale spørsmålet – dommen er ellers tilgjengelig gjennom Lovdatas system.

Saken dreier seg om ulovlig innførsel i august 2003 av 56.000 liter øl, og omsetning av betydelige mengder av ølet. Bevisene i saken består i all hovedsak av opplysninger som er kommet fram ved avlytting av telefonen til [F] på grunnlag av mistanke om innførsel av narkotika – det vil si at det er tale om overskuddsinformasjon fra en annen sak. Saken gjelder rettens adgang til å ta i betraktning som bevis fremlagt overskuddsinformasjon fra kommunikasjonskontroll når retten vil dømme for et *mindre* alvorlig forhold enn tiltalen gjelder, slik at strafferammekravet i straffeprosessloven § 216i første ledd litra b jf. §216a første ledd litra a ikke lenger er oppfylt. Av Høyesteretts bemerkninger siteres:

«(26) Begge sider har under forhandlingene pekt på at dersom retten tillates å ta i betraktning de førte bevisene selv om den ikke finner at forholdet er så alvorlig at det kunne begrunnet kommunikasjonskontroll, kan det oppstå en fare for at påtalemyndigheten vil ta ut tiltale for et mer alvorlig forhold enn det er grunnlag for - at forholdet vil bli 'oppsubsumert' – for å kunne fremlegge kommunikasjonskontrollmateriale som bevis.

(27) Jeg er enig i at i den grad det er en slik fare, vil den være større der materialet stammer fra en annen sak, fordi ingen domstol i et slikt tilfelle har vurdert om det er skjellig grunn til å mistenke de tiltalte for et så alvorlig forhold at det gir adgang til telefonkontroll. Jeg finner det imidlertid vanskelig å tillegge faren for oppsubsumering avgjørende vekt. Blant annet kontroll fra overordnet påtalemyndighet bør forhindre det. Når det gjelder straffeloven § 60a, antar jeg forøvrig at avgrensningen etter hvert vil bli klarere. Aktor har også fremholdt at dersom retten ser at det er direkte uskjønnsomt av påtalemyndigheten å henføre et forhold under et straffebud som gjør at kommunikasjonskontrollmateriale kan brukes som bevis, må den kunne se bort fra materialet. Forsvarerne har innvendt at dette gir en skjønnsmessig regel som ikke harmonerer med kravet til klar lovhjemmel i EMK artikkel 8 nr. 2. Jeg kan ikke se at en slik sikkerhetsventil ville stride mot EMK. Dette må eventuelt være en mulighet ved klart misbruk – ikke en vurdering som retten må foreta rutinemessig.

(28) Forsvarer har pekt på at dersom retten tillates å legge vekt på fremlagt kommunikasjonskontrollmateriale selv om den ikke kommer til at saken er så alvorlig at den kunne begrunnet kommunikasjonskontroll, vil tiltalte ved å anke over bevisvurderingen under skyldspørsmålet likevel måtte frifinnes i neste instans: Hvis tingretten i vår sak hadde kommet til at straffeloven § 60a ikke kom til anvendelse, men domfelt de tiltalte på grunnlag av kommunikasjonskontrollmaterialet, og de tiltalte hadde anket over bevisvurderingen under skyldspørsmålet, ville påtalemyndigheten etter forsvarers mening vært avskåret fra å legge opplysningene fra kommunikasjonskontrollen fram for lagmannsretten. De tiltalte måtte da frifinnes. Jeg ser ikke dette som et opplagt spørsmål, men det bør eventuelt vurderes nærmere av lovgiver.

(29) Jeg har funnet saken vanskelig. Jeg er imidlertid kommet til at retten må kunne legge til grunn det bevismaterialet som lovlig er fremlagt for den, for hele saken, selv om den ikke finner bevis for det forholdet som medførte at materialet kunne framlegges. Jeg kan ikke se at det er grunnlag for å komme til et annet resultat for noen av de tiltalte, slik en av forsvarerne har anført.»

På dette grunnlag opphevet en enstemmig Høyesterett delvis lagmannsrettens dom.

Kjennelsen er ennå ikke trykt, men finnes i Lovdatas base over Høyesteretts avgjørelser som HR-2007-01742-A.