POLITIJURISTENE

Samferdselsdepartementet
Postboks 8010
0030 Oslo

Sendes også på e-post til;
postmottak@sd.dep.no

Deres referanse	*Vår referanse*	*Dato*	
09/585 – HK	jof	Mandag 12. april 2010	Kopi; Riksadvokaten, Politidirektoratet

Datalagringsdirektivet og politiets behov

Innledning

Politijuristene er grunnleggende positive til innføring av de regler som er foreskrevet i datalagringsdirektivet (dld).

Innledningsvis vil vi bemerke at prosessen fra direktiv til lovforslag, skiller seg fra den vanlige prosessen i Norge, med et utvalg som skriver en omfattende NOU, som deretter danner utgangspunkt for en høring. Hvis dette hadde vært gjort, ville muligens behovene for politi og påtalemyndighet vært bedre kjent, på et tidligere tidspunkt, og med en enda bedre beskrivelse av virkeligheten. Den offentlige debatten om direktivet har vært preget av et stort og sunt engasjement, herunder følelser og tilhørende steile fronter. Et gjentatt argument har vært nettopp mangelen på faktabeskrivelse fra de kriminalitetsbekjempende miljøene. Ett gjentatt synspunkt er at "alle settes under overvåkning". For vår del er et viktig perspektiv at det ikke er "mistenkte" som er i fokus, men mulige spor i straffesaker. Spor kan komme fra mange impliserte, også fornærmede eller fra tredjeparter. Straffeprosessloven har alltid åpnet for tredjemannsransakning, og det er ingen ny tanke at krenkelser, med det formål å avdekke bevis, gjøres hos andre enn den direkte berørte.

Politiet har i flere år brukt ulike typer data fra telefoni og internettrafikk, i etterforskning av straffesaker, samt ved redningsaksjoner, saker om savnede personer og lignende. Begrepet ”datalagring” er en litt misvisende beskrivelse av hva saken handler om: tidsbegrenset utsatt sletting av spesifiserte typer data fra telefoni og internettbruk, slik at opplysningene kan være tilgjengelige som bevis i straffesaker. Videre, det skal ikke lagres data som ikke allerede finnes i systemene til teletilbyderne. En slik utsatt sletting skiller seg derfor fra begrepet ”overvåkning”, som forutsetter en form for aktiv innhenting av informasjon som ikke allerede var i systemene. Prinsippet er ikke nytt. Allerede i dag lagres opplysninger om økonomiske transaksjoner i flere år etter særskilte regler i valutaregisterloven, regnskapsloven, skatte- og avgiftslovgivningen m.v. De opplysningene som skal lagres, er kun tilgjengelige ut fra lovregulerte retningslinjer. Direktivet har også regler om sletting og om datasikkerhet, derunder dokumentasjon og statistikker av informasjon som hentes ut.

Dagens regelverk er ikke teknologinøytralt og er derfor ikke forberedt på overgang til nye tekniske løsninger. Dette påpekes også i høringsnotatets pkt. 4.8 side 43. Vi deler den bekymringen. Uten en

form for utsatt sletting, vil politiet miste viktige spor som av type har vært tilgjengelige i flere år, og som har vært brukt til å oppklare alvorlige straffesaker. I dag er det kommersielle behov som kan begrunne lagring. Med fastprisløsninger er behovet for å lagre ikke lenger det samme for teletilbyderen. I dag er fastpris den vanlige løsningen for internettabonnenter, og blir stadig vanligere også for mobiltelefoni og andre typer kommunikasjon. Dette vil få betydning for hvilke typer data som kan finnes igjen.

I. Ulike elektroniske spor

Det er viktig å skille mellom de ulike typer elektroniske spor som skal reguleres, både fordi personvernutfordringene er ulike, og fordi politiets tilgangsmuligheter vil være ulike. Politiets faktiske behov er også ulike. En tilleggsdimensjon er at politiets behov er ulike når det gjelder planlagt eller ikke-planlagt kriminalitet. Narkotikanettverk er typetilfellet av planlagt kriminalitet, mens for eksempel drapssaker ofte er affekthandlinger uten forutgående planlegging. Disse ulikhetene vil påvirke bl.a. hvorvidt gjerningsmannen har gjort forberedende handlinger for å skjule sine spor eller ikke.

1. Abonnentopplysninger, altså opplysninger som gjør det mulig å knytte en bestemt abonnent til et bestemt telefonnummer eller til en IP-adresse. Rettslig grunnlag for utlevering er ekomloven § 2-9 tredje ledd, men for telefoni er abonnentopplysninger stort sett åpent tilgjengelig også via tjenester som telefonkatalogen.no. Høyesterett har allerede likestilte abonnementsopplysninger for internettbruk, med opplysninger om et upublisert telefonnummer, Rettstidende(Rt) 1999 side 1944. Når det gjelder muligheten for å knytte en IP-adresse til en navngitt abonnent, uttalte Høyesterett i 1999 at dette tilsvarte å få opplyst abonnenten til et telefonnummer som ikke står i katalogen. Politiet har et behov i mange saker, og personvernutfordringene er ikke annerledes for IP-adresser enn for telefonnumre. I mange tilfeller, for eksempel saker om overgrepsbilder mot barn, er det nettopp denne type opplysninger politiet trenger. Innspillet forutsetter at Ekomloven § 2-9 tredje ledd videreføres.

   For å kunne knytte en abonnent til en IP-adresse, er det nødvendig at teletilbyderen lagrer en tidsbegrenset logg, som viser hvilke abonnenter som har benyttet hvilke IP-adresser på hvilket tidspunkt. Tilbyderne lagrer slike opplysninger i dag, for telefoni og internett, ut fra behov for fakturering eller drift. Etter pålegg fra Datatilsynet lagres IP-logger nå i inntil 21 dager, mot tidligere 3-5 måneder. Etter direktivet skal slike data lagres i 6-24 måneder. Vi mener at personvernutfordringene er mindre for rene abonnementsopplysninger enn for trafikkloger og posisjonsdata m.v.

2. Trafikklogger. Her forutsetter høringsbrevet en regel om tre års strafferamme, evt særskilte lovbud. Dette er data med noe større personvernutfordringer, men likevel data som har stor betydning for politiet i flere sakstyper, alt fra narkotikanettverk til drapssaker. Dette er opplysninger som viser hvilke andre telefonnummer eller IP-adresser en bruker har vært i kontakt med. I dag lagres også disse opplysningene ut fra behov for fakturering eller drift, eksempelvis 3-5 måneder for mobiltelefoni. Etter direktivet skal slike data lagres i 6-24 måneder. For vår del, gitt eksisterende teknologi, er det viktig at slike bevis fortsatt kan benyttes. Det er ofte slik informasjon som gjør det mulig både å begrense en krets av mistenkte personer, eller utelukke noen fra mistanke.

3. Basestasjonsopplysninger. Samme som for trafikklogger. Dette er også data av stor betydning for politiet i mange alvorlige saker, alt fra savnede personer til NOKAS-ranet er relevante eksempler. Et praktisk eksempel er hvilke basestasjoner en mobiltelefon har vært i kontakt med. Teleoperatørene har svært begrenset adgang til å lagre slike opplysninger, og også en anonymiseringsplikt, men i praksis lagres posisjonsdata av hensyn til utvidet faktura, slik at kundene lettere kan kontrollere sin egen faktura. Nedenfor har vi forsøkt å illustrere hvordan slike opplysninger får anvendelse.

4. Innholdsdata, dvs innhold i e-post, tekstmeldinger etc. Skal ikke lagres. Flere andre typer elektroniske spor faller også utenfor direktivet:
   - surfelogg for den enkeltes bruk av internett, lagres ikke
   - bedriftsinterne nettverk, eksempelvis Uninett, faller utenfor
   - innholdstjenester, eksempelvis Nettby.no, faller utenfor
   - kommunikasjonstjenester som defineres som innholdstjenester (MSN chat, Skype, webmail), faller utenfor
   - virksomheter som er utenfor nasjonal jurisdiksjon. I tillegg til at det anses som en innholdstjeneste, er Facebook i utgangspunktet underlagt amerikansk lovgivning, og faller derfor utenfor datalagringsreglene.
   - ikke krav om bruker-identifikasjon for internett-kafeer eller forbud mot usikrede trådløse nettverk

   For vår del, hadde vi gjerne sett at også enkelte av de sporene som er nevnt ovenfor, men som faller utenfor direktivet, var omfattet. For eksempel er det mange straffbare forhold som utelukkende legger igjen spor på ulike nettsamfunn, men det er forholdsvis enkelt å se de innvendinger som ligger bak vurderingene.

II. Sakseksempler

a) Én straffesak som belyser klart betydningen av basestasjonsopplysninger, er dommen LB-2008-61703, vedrørende grovt ran og drap, i Drammen den 28.1.2007. Dommen er av spesiell interesse fordi lagmannsretten her begrunnet sine bevisvurderinger. Bakgrunnen var at lagretten først hadde svart nei på skyldspørsmålet, men frifinnelsen ble satt til side og saken ble behandlet på ny med stor meddomsrett. NN ble funnet død på bopel den 31.1.2007. Mistenkte A ble pågrepet en måned seinere, den 28.2.2007. Fra dommen:

"Rettsmedisinernes konklusjoner samsvarer med observasjoner fra personell som kom til åstedet og de støttes av utskrifter fra [avdøde] Bs telefon- og bankkortbruk. Vitneobservasjoner av B etter dette tidspunkt er ikke tillagt vekt og må skyldes erindringsfeil" (…) "Det er i tiden mellom disse kjøreturene at påtalemyndigheten mener at ranet og voldsutøvelsen mot B har funnet sted. På bakgrunn av telefonutskrifter over hvilke basestasjoner [domfelte] As mobiltelefon har slått inn på, kan tidsrommet fastslås til mellom kl. 20:06 og 20:49. Lagmannsretten mener det er overveiende sannsynlig at voldsutøvelsen har funnet sted i dette tidsrom. De bevegelser som lagmannsretten nå har redegjort, understøttes av mobiltrafikkdata som viser de involvertes mobilbruk og hvilke basestasjoner som har slått inn til enhver tid."

Saken belyser også et annet viktig poeng: ved etterforskning av drapssaker er det vanlig å undersøke trafikkloggen til avdøde. Det er altså ikke bare hos mulige mistenkte det er behov for å innhente viktige opplysninger. Manglende datalagring vil få konsekvenser for denne fremgangsmåten.

b) Et annet eksempel er søk etter domfelte som rømmer fra fengsel. Dersom David Toska eller Kjell Alrich Schumann skulle rømme fra soning, ville det være i samsvar straffeprosessloven å innhente eventuelle trafikkdata for mobiltelefoner? Dersom høringsnotatets forslag om strafferammer innføres, ville det neppe være adgang til å undersøke noen elektroniske spor knyttet til lovbrytere som har rømt fra soning.

Når det gjelder problemstillinger om innsatte som rømmer fra soning, er det en annen dimensjon som kan påvirke løsningen. Dersom etterforskningen også omfatter soningsgjennomføring, vil metodene som var åpne før dom ble avsagt, også være det i forhold til gjennomføring av soning. Det kan derfor være misvisende å trekke frem rømte soningsfanger som et eksempel. For vår del vil løsningen uansett kreve en uttrykkelig avklaring, og vi ber derfor om at departementene tar det med i det videre arbeidet.

c) Et tredje eksempel gjelder grove gruppevoldtekter av to kvinner ved forskjellige anledninger. I sakens behandling ved Oslo tingrett (rettskraftig avgjort først ved lagmannsrettens behandling), var mobiltelefonutskriftene sentrale, fordi de viste at en eller flere av overgriperne var i Oslo sentrum, i den relevante tidsperioden. *"Videre legger retten vekt på mobiltelefonutskriften der ringemønsteret for den aktuelle perioden viser at det var han selv som brukte telefonen og at han med basestasjon --- ringte en femminutters utgående samtale den 18. desember kl. 0219. Retten har nøye vurdert om A kunne ha vært personen som forlot stedet i gråtysningen, men utelukker dette. Hadde det vært A som forlot stedet, tilsier hans aktive mobiltelefonbruk at han ville tatt med seg telefonen og brukt den med annen basestasjon i tidsrommet fra han gikk og frem til kl. 1704 da telefonen igjen er i bruk med basestasjon ---".* Eksempelet er illustrerende for den betydning som slike beviskilder kan innebære.

III. Mistankekravet

Et problem med forslaget er at det foreslår å innskjerpe mistankekravet, slik at noen bestemt person må kunne identifiseres før trafikkdata kan utleveres. I eksempelet Nokas-saken ville et slikt mistankekrav bety at politiet måtte identifisere med navn alle ranerne for å kunne få ut aktuelle trafikkdata for de involverte. Det tok ett år fra Nokas-ranet fant sted, til noen ble pågrepet. Siden politiets formål med trafikkdata typisk er å identifisere ukjente gjerningsmenn, framstår denne innskjerpingen som lite gjennomtenkt. Vi kan heller ikke se at forslaget er spesielt godt egnet til å styrke tilliten til prosessen eller er egnet til å styrke rettsikkerheten. Vi ber om at innskjerpingen fjernes.

Ved overgang til ny teknologi, som vi tror vil bli mer og mer merkbar, får politiet tilgang til stadig færre spor fra tradisjonell telefoni. Kommunikasjonskontroll og trafikkdata-ananlyse henger ofte sammen. Det er nødvendig å kunne identifisere brukeren bak en IP-adresse, men loggen som kan knytte en abonnent til en IP-adresse på et bestemt tidspunkt, slettes kontinuerlig, etter null til 21 dager. Politiet risikerer derfor å sitte igjen med kalde spor og løse tråder, samtidig som internett og telefoni i praksis blir totalanonymt. Enkelte har tatt til ordet for at dette problemet avhjelpes ved bruk av kommunikasjonskontroll. En utvidelse av adgangen til kommunikasjonskontroll vil ikke hjelpe, hvis en ikke har mulighet til å identifisere hvem kommunikasjonskontrollen skal rette seg mot.

En sak for seg er at diskusjonen om politiets behov for trafikkdata, bare i liten grad har berørt politiets behov for trafikkdata ved redningsaksjoner og søk etter savnede personer. Det er tilfeller hvor Post- og teletilsynet (PT) har nektet politiet tilgang til mobilopplysninger knyttet til savnede

personer. Dersom en sak er definert som en leteaksjon, har ikke Post- og teletilsynet hjemmel til å gi politiet tillatelse til å spore mobiltelefoner.

IV. Internasjonale signaler

Både norsk rettstradisjon og Den europeiske menneskerettsdomstolen (jf. EMD-dommen K.U. vs Finland) har lagt til grunn at personvern for den enkelte må vurderes opp mot både hensynet til samfunnssikkerhet og bekjempelse av kriminalitet, og også mot personvern for andre, ettersom personvern ikke bare kan krenkes av store systemeiere, men også av tilfeldige enkeltpersoner. Avveiingen er ikke ny. Etter en debatt over flere år, besluttet Post- og Teletilsynet i 2004 at teletilbyderne ikke lenger kunne tilby anonyme kontantkort. Begrunnelsen for denne registreringen av sluttbrukere, var hensyn til blant annet politiets behov og samfunnssikkerheten. Til sammenligning uttalte Datatilsynet i 2000 at teletilbyderne burde legge til rette for anonym tilgang til telefoni. (Problemene med anonyme kontantkort ble også belyst i NOKAS – saken. "Etter ranet i Stavanger fant politiet et SIM-kort i en utbrent bil som var forlatt. Ved hjelp av dette klarte de å spore opp seks uregistrerte telefoner som ble brukt under forberedelsene og gjennomføringen av ranet i 2004." Det viste seg senere at de nevnte SIM-kort var registrert feilaktig i navnet til flere kjente fotballspillere)

Nylig slo også den tyske forfatningsdomstolen fast at den foreslåtte implementeringen i tysk rett var grunnlovstridig. I den sammenheng er det verdt å merke seg at direktivet ikke var grunnlovsstridig og at det utelukkende var den foreslått innføringen som ikke var forenelig med den tyske grunnloven.

V. Planlag eller ikke-planlagt kriminalitet

Er det bare de "dumme" forbryterne vi vil ramme med en innføring av direktivet. En bekymring som enkelte har påpekt, er at de "flinke" forbryterne vil benytte muligheten til å benytte teknologi som ikke er utsatt for utsatt lagring, jf pkt 1, nr 4. Innspillet er ikke uten mening, men også bruk av teknologi som "skype" og ulike nettsamfunn forutsetter en åpenhet i forhold til kontaktlister, brukerprofil etc. Slik informasjon er åpent tilgjengelig også i kriminalitetsbekjempelsen, og vil derfor fortsatt ha verdi. Den kriminaliteten som ikke forberedes vil stå i en annen stilling, og verktøyet vil derfor uansett ha høy verdi. Mye av den kriminalitet som rammer planløst og uten åpenbare motiv, er ofte begått i affekt. Det er særlig i de innledende faser av slike saker, at behovet for lagret informasjon vil være størst.

VI. Lagringstid- og sted

I forslaget er det diskutert både om en skal pålegge tilbyder av ekomtjenester å lagre opplysningene, eller om en skal opprette et sentralt "lager" for opplysningene. Vi deler de vurderinger departementene har gjort med tanke på å la den enkelte tilbyder, til en viss grad, velge dette selv. Vi vil like vel peke på at den fornuftige løsningen, dersom man velger å tilby en sentral lagerplass, vil være kryptering av informasjonen. En slik løsning kan også være egnet til å avdempe noe av den bekymringen mange har i forhold til misbruk av informasjonen. Dersom det ble laget en krypteringsløsning, vil det også være forholdsvis enkelt å føre tilsyn med at lovens vilkår er til stedet

de gangene informasjonen blir etterspurt. En annen side ved en slik løsning, er at det vil være mindre fare for at miljøer som ikke har noe rettmessig behov for informasjonen, får tak i den. Eksempelvis vil ikke utro tjenere, i noe ledd av kjeden, ha mulighet til på egen hånd å få tilgang til informasjon.

I denne sammenheng har vi også en bekymring knyttet til eventuelle kostnader ved utlevering av informasjon. Dersom den enkelte tilbyder selv kan diktere sine egne betingelser, vil det i realiteten bli redusert til et kostnadsspørsmål om politi og påtalemyndighet innhenter informasjon. (Etter det vi er kjent med er det blant annet i ferd med å bli et problem i Sverige). Et alternativ vil etter vår vurdering være å pålegge den konsesjonsberettigede å dekke slike utgifter selv.

Når det gjelder lagringstid, deler vi de argumenter som underbygger behovet for lagringstid noe lenger enn 6 – måneder. Like fullt fremstår det for oss, som mindre realistisk å nå frem med vårt primære syn – utsatt sletting i hele 24 måneders perioden. Det er klart nok gode motforestillinger mot en såpass lang utsatt sletteplikt. Det er også riktig som departementene selv skriver, at det i dag i beste fall er utsatt sletting i fem måneder. Når det likevel blir etterspurt et syn på tidsintervallet, så er det vår vurdering at behovet er vedvarende og sterkt i 8 – 12 måneder. Deretter avtar det noe. Begrunnelsen for det er særlig tiden det tar fra et forhold blir oppdaget, til det når innsiden av norske domstoler. Dersom det er tråder som blir hengende løse under etterforskningen, eller først blir avdekket under førsteinstans behandlingen i retten, kan en utsatt sletting i 12 måneder være avgjørende. Et trekk ved den mer "moderne" kriminalitet og etterforsking, er at sakene verserer kontinuerlig underveis. Det innebærer også at undersøkelser gjøres fortløpende i en annen grad enn tidligere, slik for eksempel tilfellet var i NOKAS – saken og ved den s.k. ENEA – etterforskingen, som er nevnt i høringsnotatet. Vi foreslår derfor at slettingen utsettes i 12 måneder – uavhengig av type.

VII. Tilsynsorgan

En sak som fortjener en særskilt kommentar er Datatilsynets rolle som tilsynsorgan. Problemstillingen er ikke nevnt i høringsnotatet, men vi finner likevel grunn til å kommentere det.

For det tilfellet at datalagring innføres, vil lagringen kontrolleres av både Datatilsynet og Post og teletilsynet. Dette framgår av høringsnotatets pkt. 4.10, særlig pkt. 4.10.2. Dette er en konsekvens av at Datatilsynet er kontrollorgan etter personopplysningsloven, mens PT er det etter lov om elektronisk kommunikasjon. Datatilsynet har etter personopplysningsloven § 42 en rolle som uavhengig forvaltningsorgan med to ulike funksjoner: dels et tilsynsorgan og dels et fristilt organ som skal delta i samfunnsdebatten. Datatilsynet er motstander av direktivet. I tilsynets bemerkninger beskrives datalagring som "totalitært svermeri". Dette uttrykket har tilsynet brukt gjentatte ganger i flere år for å beskrive datalagring.

Dette skaper spørsmål som kan nærme seg inhabilitet. Skal Datatilsynet føre tilsyn med et tiltak som tilsynet ikke ønsker innført? Datatilsynet er ikke en stor virksomhet, med knapt 40 ansatte på ett felles arbeidssted. Dette gjør det vanskelig å ha "kinesiske vegger", som skiller personer som gjør ulike oppgaver. Tilsynet har heller ikke noe styre eller andre som fører tilsyn med den daglige driften. En kan kanskje også si at det ikke er fair overfor Datatilsynet at de - som en konsekvens av lovens system - i tilfelle må føre tilsyn med en virksomhet som tilsynet offentlig har tatt avstand fra.

I Personvernkommisjonens rapport NOU 2009:1 foreslo et mindretall at Datatilsynet burde skilles i to virksomheter: et tilsyn og et ombud, hvor ombudet viderefører funksjonen Datatilsynet i dag har

som samfunnsdebattant etc. Et slikt skille ville kunne løse noe av de problemene som beskrevet over.

VIII. Kildevern

Spørsmålet om pressens kildevern er også et tema som har kommet i forbindelse med det offentlige ordskifte om direktivet. Heller ikke dette er spesielt behandlet i det notat som er sendt på høring. Et spørsmål som heller ikke berøres, er om også bloggere kan påberope seg regler om kildevern, og hvordan det vil stille seg til en eventuell beskyttelse av pressens kilder. Politijuristene kan ikke se at datalagring vil utgjøre noen praktisk forskjell for arbeidsrommet til norske journalister, og at spørsmålet om pressens kildevern i tilfelle bør utredes separat. At myndighetene kan fange opp kommunikasjon mellom journalister og deres anonyme kilder er ikke noe nytt. Virkeligheten er at dette kan gjøres allerede i dag, dersom det foreligger en pågående kommunikasjonskontroll rettet mot den person som viser seg å være en kilde til pressen. Etter det vi er kjent med har ikke dette vist seg å være et praktisk problem i dag. Er kildene beskyttet, vil politiet ikke kunne bruke eventuelle data som bevis, og vil også risikere avskjæring allerede på beslagstidspunktet. Vi konstaterer også at de mange negative spådommene om datalagring som er framsatt, ikke synes å ha inntrådt i eksempelvis Danmark og Nederland, som begge var tidlige med å innføre datalagring. Dette gjelder alt fra kostnadsnivået for teletilbyderne til mulige inngrep i pressefriheten.

IX. Konklusjon

Samtidig som politiet i flere henseende har fått økte tilgang til elektroniske spor, har to andre utviklingstrekk gått i motsatt retning. For det første har muligheten for å kommunisere fullt ut, eller i praksis, anonymt med andre økt pga. ny teknologi og nye bruksmønstre. For det andre har Datatilsynet introdusert strengere sletteplikt for trafikkdata. Flere tilbydere sletter tidligere, og noen lagrer ingen sporbare data.

Enkelte viser til datalagring kommer som et krav fra EU, og ble tatt opp for å bekjempe terrorisme, dels etter 9/11 (2001), men særskilt etter bombeaksjonene i Madrid (2004) og London (2005). Men det var en debatt om datalagring i Norge også før dette. Sårbarhetsutvalget (NOU 2000:27) anbefalte enstemmig at tjenestetilbyderne bør pålegges å føre logger for en begrenset tidsperiode. I avisdebatten knyttet til høringsuttalelsen fra Økokrim av 18.12.2000, foreslo Økokrim å lagre trafikkdata i ett år.

I en senere utredning, politimetodeutvalget (NOU 2004:6) framgår i pkt. 10.7.12.3.1:
”Flertallet vil etter dette foreslå at det innføres plikt for teleselskapene til å oppbevare trafikk- og posisjonsdata i 1 år slik at politiet får tilgang på viktig informasjon i kriminalitetsbekjempelsen.” (…)
”Mindretallet mener det er god grunn til å overlate spørsmålet til Datakrimutvalget.”

I disse dager innfører Datatilsynet tjenesten Slettmeg.no. Fra nettsiden:

”Formålet med tjenesten er å gi råd og veiledning til deg som føler deg krenket på nett, eller som av andre grunner ønsker å få slettet eller rettet personopplysninger publisert på internett. (…) Vi har

ikke mulighet til å pålegge noen å slette krenkende opplysninger fra Internett. Utøvelse av eventuelle sanksjoner overlates til tilsynsmyndigheter, politi, domstoler og andre."

I dette ligger paradokset. Mange, også Datatilsynet, ser et behov for å bistå enkeltpersoner som får sitt personvern krenket av andre, henviser til politiet for eventuelle sanksjoner, men vil ta fra politiet muligheten til å identifisere den som står bak krenkelsene. Problemstillingen er ikke abstrakt. Politiet er kjent med at overgrepsbilder av identifiserte, norske barn fra tidligere pådømte, norske straffesaker, fortsatt er tilgjengelige på internett.

I siste instans er det politikerne som bestemmer hvilken verktøykasse politiet skal ha til rådighet for å forebygge og oppklare kriminalitet. Datatilsynet, og andre kritikere av datalagringsdirektivet, hevder at utsatt sletting av trafikkdata er prinsipielt galt. Imidlertid kan ingen prinsipper vurderes uten å ta hensyn til konsekvensene. Konsekvensene av manglende innføring av datalagringsdirektivet vil bli negative, merkbare og vil øke over tid. For vår del er dette perspektivet avgjørende, og vi støtter derfor den foreslåtte innføringen.

For Politijuristene,

Jan Olav Frantsvold