

28.02.07

## Personvern etter 11. september

*Lee A. Bygrave*

### Betydningen av «9/11»

Det er lett å være pessimistisk på personvernets vegne.<sup>1</sup> Dette gjelder særlig etter terroristhandlingene i USA den 11. september 2001. Et viktig element i den statlige «krigen mot terror» som ble innledet i kjølvannet av «9/11» er en vesentlig økning i overvåknings- og andre kontrolltiltak.<sup>2</sup> Planlegging og innføring av slike tiltak har hittil vært langt mer markant i USA enn i mange europeiske land (deriblant Norge). Etter bombeangrepene i Madrid den 11. mars 2004 og London den 7. juli 2005 er det likevel økt vilje blant europeiske regjeringer til å iverksette lignende tiltak.<sup>3</sup>

Selv om siktemålet formelt sett er å avsløre terrorister (eller andre kriminelle), har tiltak mot terror i praksis en tendens til å rette seg mot allmennheten. Kontrolltiltakene tar mange former, bl.a.

- skjerpede rutiner for grensekontroll (f.eks. innføring av pass med biometriske data),
- omfattende tapping av kommunikasjon på Internett (f.eks. bruk av den såkalte «Carnivore»-teknologien av US Federal Bureau of Investigation),<sup>4</sup>
- forbedrede rutiner for tverrnasjonal utveksling av informasjon mellom politienheter (f.eks. bruk av «The Europol Computer System» (TECS)),

---

<sup>1</sup> Personvernbegrepet brukes her som overordnet betegnelse på beskyttelse av personlig integritet. Denne begrepsforståelsen synes å ha festnet seg i allmenn diskurs, men ofte uten at det like diffuse integritetsbegrepet er forsøkt definert. I denne artikkelen betegner «personlig integritet» en tilstand av harmonisk tilværelse som er et resultat av andre personers respekt for enkeltmennesket. En viktig dimensjon ved en slik tilværelse er at den enkelte i utgangspunktet kan bestemme hva andre skal få vite om ens egne forhold, og hvordan andre skal kunne tre inn i ens egen privatsfære. I det følgende brukes også begrepet «personopplysningsvern», en underkategori av personvern som omhandler normer for behandling av personopplysninger med sikte på å beskytte personlig integritet (herunder autonomi og privatlivets fred). Se nærmere om disse og beslektede begrep i D.W. Schartum og L.A. Bygrave, *Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger* (Bergen: Fagbokforlaget, 2004) kapittel 1–2.

<sup>2</sup> Nyttige oversikter over slike tiltak finnes i Electronic Privacy Information Center (EPIC) og Privacy International (PI), *Privacy and Human Rights 2005. An International Survey of Privacy Laws and Developments* (Washington, DC: EPIC/PI, 2005).

<sup>3</sup> Jf. eksempelvis Det europeiske rådets «Declaration on Combating Terrorism», Brussel, 25. mars 2004.

<sup>4</sup> Se nærmere om «Carnivore» (eller «DCS1000» som det offisielt heter) i T. Nabbali og M. Perry, «Going for the throat: Carnivore in an Echelon World», *Computer Law & Security Report*, 2003, bind 19, nr. 6, s. 456–467.

- statlige bevisstjøringskampanjer for å varsle befolkningen om å være på vakt mot mistenkelige personer i nabolaget (f.eks. brosjyren «Preparing for Emergencies: What You Need to Know» som ble delt ut av UK Home Office juli 2004 til alle husholdninger i Storbritannia),<sup>5</sup>
- utvidede plikter for næringsdrivende mv. til å rapportere til politiet ved mistanke om kriminell virksomhet (f.eks. rapporteringsplikten etter Norges hvitvaskingslov),<sup>6</sup>
- utvidede plikter for å oppbevare logger over elektronisk kommunikasjon (se f.eks. EUs datalagringsdirektiv);<sup>7</sup>
- reduserte muligheter for anonym kommunikasjon (eksemplifisert i Norge ved en nylig innført plikt for tilbydere av offentlige telefontjenester til å registrere identifikasjonsopplysninger om sluttbrukere bl.a. ved utstedelse av kontantkort for mobiltelefoni).<sup>8</sup>

Både omfanget og gjennomslagskraften av noen av disse kontrolltiltakene er imidlertid usikre. Dette gjelder eksempelvis EUs datalagringsdirektiv. Direktivet skal etter planen implementeres innen 15. september 2007. Irland mener imidlertid at direktivet mangler et tilstrekkelig EU-rettslig grunnlag og har anlagt sak for å få direktivet kjent ugyldig. Flere andre EU-medlemsstater har valgt å utsette implementering av enkelte av direktivets bestemmelser fordi bestemmelsene er for vage og tvetydige. Enkelte juridiske eksperter på feltet har dessuten hevdet – med betydelig styrke – at direktivet er i strid med Den europeiske menneskerettskonvensjon (EMK) artikkel 8.

Vi må uansett ikke legge all skyld på «9/11» og den påfølgende opptrappingen av overvåkning for at personvernets stilling er skjør. Mange av de kontrolltiltakene som er referert til ovenfor, fantes eller var under oppseiling lenge før «9/11». Personvernets stilling har dessuten lenge vært svært utsatt på grunn av grunnleggende trekk ved samfunnsutviklingen som i det store og hele har lite med «9/11» å gjøre. Et vesentlig element ved dagens samfunn er en stadig mer intensiv utnyttelse av personopplysninger. Dette innebærer

- økt samordning av måter organisasjoner samler inn, registrerer og lagrer informasjon på,
- tiltakende flyt og tilgjengelighet av opplysninger på tvers av organisasjonsgrenser,
- oftere anvendelse av én informasjonstype til flere ulike formål.

---

<sup>5</sup> Se særlig avsnittet «Helping to prevent a terrorist attack» på s. 16–17 av brosjyren, også tilgjengelig ved <<http://www.preparingforemergencies.gov.uk/you/booklet/pdfs.shtm>> (sist besøkt 28. februar 2007).

<sup>6</sup> Jf. lov om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. av 20. juni 2003 nr. 41.

<sup>7</sup> Jf. Direktiv 2006/24/EF av 15. mars 2006 om lagring av data generert eller behandlet i forbindelse med tilbivelse av offentlig tilgjengelige elektroniske kommunikasjonstjenester eller elektroniske kommunikasjonsnett og om endring av direktiv 2002/58/EF – heretter «datalagringsdirektivet». Direktivet pålegger tilbydere av visse kommunikasjonstjenester en plikt til å lagre trafikkdata i en periode på ikke mindre enn 6 måneder og ikke mer enn to år. Hensikten med en slik lagring er å bekjempe terror og alvorlig kriminalitet ellers. Data som må lagres inkluderer bl.a. slik data som er nødvendig for å identifisere avsenderen, mottakeren samt tid og sted for kommunikasjonen, men ikke kommunikasjonens innhold.

<sup>8</sup> Jf. forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste av 16. februar 2004 nr. 401 § 6-2.

Disse tendensene gir mening til begrepet «informasjonssamfunn». De er kun delvis drevet frem av behovet for å bekjempe terrorisme eller annen kriminalitet. Også andre interesser er viktige drivkrefter – så som ønsket om bedre service (f.eks. gjennom raskere saksbehandling) og ønsket om bedre ressursutnyttelse (f.eks. kostnadsreduksjoner gjennom økt gjenbruk av innsamlede opplysninger). Vi ser dette dokumentert i bl.a. nyere statlig informasjons- og forvaltningspolitikk i Norge.<sup>9</sup>

I tillegg finnes det sikkerhetskulturer som lever i beste velgående nokså uavhengig av bekymringer for terrorisme eller annen alvorlig kriminalitet, og som gir grobunn for stadig flere overvåkings- og kontrolltiltak. Utslag av en slik kultur kommer godt til syne i f.eks. myndighetenes satsing på trafikksikkerhet. Satsingen her innebærer i økende grad bruk av «smarte» kontrollmekanismer som digitale fotobokser for registrering av fartsovertredelse og (i nær fremtid) automatiske ferdskrivere i biler.

Til grunn for mange av disse tendensene ligger selvsagt en voldsom utvikling på det teknologiske planet – en utvikling med røtter delvis i menneskers iboende dragning mot «the technically sweet». Teknologiske nyvinninger er i og for seg sjelden direkte skadelige for personvernet. Enkelte teknologier (så som krypteringsmekanismer) kan til og med være personvern fremmende. Likevel bidrar en god del andre teknologiske nyvinninger til å utradere fysiske/tekniske begrensninger som har hatt en (ofte utilsiktet) personvernbevarende virkning. De åpner samtidig for nye handlingsrom som setter personvern under press. Et godt eksempel på dette er de nye sporingsmulighetene som RFID-brikker (radiofrekvensidentifikasjon) gir.<sup>10</sup>

Videre skjer det en spredning av enkelte nye teknologier blant befolkningen som øker mulighetene for at enkeltmennesker og ikke bare store organisasjoner kan overvåke folks dagligliv. Allmennhetens tilgang til Internett, mobiltelefoni med kamera mv. gjør det lettere for privatpersoner å opptre som «lillebror». Hensikten kan ofte være forholdsvis uskyldig (underholdning, nysgjerrighet), men kan fort få preg av en «vigilante»-virksomhet som er hemmende for fri livsutfoldelse i nabolaget, på arbeidsplassen, på skoler og i privatsfæren.

Terrorangrepene den 11. september 2001, 11. mars 2004 og 7. juli 2005 har bidratt til å forsterke de nevnte generelle tendensene først og fremst ved å gi overvåkning og kontroll større moralsk legitimitet. Angrepene har bidratt til å flytte en god del av begrunnelsene for økende innsamling og (gjen-)bruk av informasjon fra kategorien «nice to know» til «need to know». Angrepene har samtidig gitt mer næring til uro – især den grunnleggende engstelsen for risiko som allerede preger vår bevissthet.<sup>11</sup> Alt dette skaper

---

<sup>9</sup> Se f.eks. *Arkitektur for elektronisk samhandling i offentlig sektor*, Arbeids- og Administrasjonsdepartementet, 24. juni 2004.

<sup>10</sup> Det er rapportert om at Mexicos justisminister, samt flere av hans medarbeidere, har fått implantert slike brikker i armene sine. Tiltaket skal kunne lette både personlokalisering (i tilfellet kidnapping) og adgangskontroll. Jf. «Mexico vil bekjempe kriminalitet med mikrobrikke», *Aftenposten* (morgenutgave) 19. juli 2004 s. 5.

<sup>11</sup> Se generelt U. Beck, *Risikogesellschaft. Auf den Weg in eine andere Moderne* (Frankfurt aM: Suhrkamp, 1986).

en unntaksstemning som gjør det lettere å få allmenn aksept for vidtgående begrensninger i vår personlige autonomi.

### **Personvern – en kuriositet uten fremtid?**

Når kontrollen øker i omfang og intensitet, er det viktig å stille spørsmål om dette vil vare. Vil nye kontrolltiltak utvikle seg fra å representere unntak som vi godtar på grunn av en spesiell situasjon, til å bli det normale? Vil de nye begrensningene i vår personlige autonomi bli fjernet dersom terrortrusselen avtar? Svaret avhenger delvis av hvor hardt vi vil kjempe for å gjenvinne herredømmet over vårt privatliv og vår selvbestemmelse.

En vil kunne håpe at viljen til å kjempe for personvern er til stede. Ivaretagelse av personlig integritet er ikke bare av vesentlig betydning for oss som enkeltindivider, men også for samfunnslivet generelt, særlig for graden av pluralisme og demokrati. Uten et sterkt personvern får vi ikke et levende demokratisk felleskap. Eller som Georg Apenes sier, «den som for villig og for ofte veksler inn sin frihet for trygghet, risikerer å miste begge deler». <sup>12</sup> Dette er et visdomsord som ikke kan gjentas for ofte, særlig i kjølvannet av «9/11». Jeg er dessverre ikke helt sikker på om vi som felleskap har tilstrekkelig motstandsvilje på personvernets vegne.

Noen har hevdet at personvern alt har mistet sin samfunnsrelevans. Da Scott McNealy, sjefen for Sun Microsystems, ble spurt på en pressekonferanse i januar 1999 om hvilke personvern fremmende tiltak selskapet hans skulle integrere i en nylansert programvare, svarte han: «You already have zero privacy. Get over it». <sup>13</sup> Denne lakoniske uttalelsen antyder at personvern ikke bare er en kuriositet som hører fortiden til, men også noe som *bør* høre fortiden til. At uttalelsen kom fra en av verdens mektigste aktører innen databransjen – og dermed en innflytelsesrik premissleverandør for (morgen)dagens informasjonssamfunn – er urovekkende, i hvert fall for den som er opptatt av at personvernet forblir liv laga.

McNealy tar feil. Personvern er ikke så lett å avfeie som han vil ha det til. Heldigvis vil nok mange andre viktige premissleverandører for informasjonssamfunnet være uenige i hans synspunkt. En betydelig del av dem vil likevel oppleve at personvern som diskusjonstema har en tendens til å dukke opp i deres virksomhet på et ubeleilig tidspunkt, dvs. rett før slutføring av en antatt samfunnsnyttig prosess – om den gjelder vedtagelse av en lov, lansering av et forretningsprodukt, effektivisering av en forvaltningstjeneste mv. Da er det ofte kun personvern temaet som må forseres før «saken er i boks». I en slik sammenheng blir personvern – praktisk sett – lett et irritasjonsmoment.

---

<sup>12</sup> Jf. bl.a. Datatilsynet, *Personvernrapporten* (Oslo, april 2004) s. 11.

<sup>13</sup> Jf. bl.a. «Sun on Privacy: Get over It», *Wired News*, 26. januar 1999, <<http://www.wired.com/news/politics/0,1283,17538,00.html>> (sist besøkt 26. juli 2004).

Flere andre forhold vil kunne forsterke irritasjonen. Blant disse er det diffuse innholdet av personvernbegrepet, samt det faktum at rettsregler som skal ivareta personvern, er kompliserte og til dels uoversiktlige. Personvernjuss i Norge består langt på vei av vanskelig tilgjengelig forvaltningspraksis (hovedsakelig i form av enkeltvedtak av Datatilsynet) basert på ad hoc-interesseavveininger. Det er lite klargjørende rettspraksis på området for juriststanden og andre her i landet å forholde seg til. Alt dette bidrar til at personvern (og personvernjussen) ofte blir forbigått.

Samtidig har personvern ingen naturlig trofast venn blant etablerte politiske partier. Dette skyldes delvis at personvern er et knippe med interesser som gjør seg gjeldende på tvers av tradisjonelle partipolitiske grenser – i hvert fall innen rammene for et liberaldemokratisk politisk system som i Norge. Det blir dermed svært vanskelig for et bestemt parti å «eie» personvern som fanesak. Gitt at respekt for privatliv og personlig integritet utgjør liberalismens kjerne, ville vi kunne forvente at partier som tradisjonelt har forfektet en liberalkonservativ ideologi – så som Høyre – i utgangspunktet ville være personvernets nærmeste allierte, men vi ser mange tilfeller der disse i praksis er villige til å nedprioritere personvern til fordel for andre interesser, særlig kriminalitetsbekjempelse. Den partipolitiske debatten rundt Politimetodeutvalgets innstilling<sup>14</sup> er et eksempel på dette.

Internasjonalt ser vi en tendens til at datatilsynsmyndigheter sliter med å få nødvendige ressurser fra politikere til å kunne fullføre sine oppgaver på formålstjenlig vis.<sup>15</sup> Det skal likevel bemerkes at i Norge har Stortinget på dette punktet vært relativt raus (ikke minst sammenlignet med Justisdepartementet). En bør dessuten ikke glemme at Stortinget generelt har støttet opp under Datatilsynets politikk. Tilsynet har likevel slitt med vedvarende ressursmangel.

## Folks holdninger til personvern

Personvern har ingen tallrik, sterk og trofast «heiagjeng» blant befolkningen. Folk flest ser ut til å prise personvern høyt på det abstrakte plan, men denne verdsetningen gjenspeiles kun i liten grad i måten folk oppfører seg. Dette kommer bl.a. frem i en omfattende undersøkelse fra 1997 av den norske befolkningens personvernholdninger.<sup>16</sup> Til tross for at mange syntes at personvern er både viktig og under sterkt press, viste de fleste seg som forholdsvis lite aktive når det gjelder å unngå registrering. For eksempel sa under 10 prosent av respondentene i undersøkelsen at de hadde latt være å bruke bonuskort på grunn av transaksjonsregistrering. De øvrige respondentene oppgav at de ikke opplevet registreringen knyttet til bruken av bonuskort som problematisk. Det er også interessant å merke seg at antallet respondenter som syntes at elektroniske spor er nyttige, var større enn antallet som anså slike spor som en ulempe. Folk flest hadde

<sup>14</sup> Jf. *Mellom effektivitet og personvern*, NOU 2004: 6.

<sup>15</sup> Jf. Europa-kommisjonen, *First report on the implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265 final, Brussel, 15. mai 2003.

<sup>16</sup> Jf. Statistisk sentralbyrå (E. Gulløy), *Undersøkelse om personvern: Holdninger og erfaringer 1997*, Notat 97/48 (Oslo: SSB, 1997).

dessuten vært lite aktive i å ta i bruk sine rettigheter etter personvernlovgivningen. I den forbindelse er det verdt å vise til Glenn English, tidligere medlem av Kongressen i USA, som har bemerket at «privacy is an issue in which public concern runs a mile wide and an inch deep».<sup>17</sup>

Hvorfor ser det ut til at mange har et noe overfladisk syn på personvern? Trolig skyldes dette flere overlappende faktorer. Én faktor er at interessene bak personvern langt på vei er ideelle. Interessenes verdi(er) er dermed lite håndgripelige. De blir lett tilsidesatt av (legitime) behov som er begrunnet i mer konkrete og målbare verdier. Svekkelse av interessene blir også vanskelige å fornemme, særlig når svekkelsen skjer gradvis – noe som ofte er tilfellet. Det blir likedan vanskelig for enkeltindividet å fornemme de langsiktige konsekvensene av denne svekkelsen. Beslektet med denne nærsyntheten er det jeg kaller for *det faustiske syndromet*. Med dette mener jeg en tendens til at folk ser bort fra sine ideelle interesser i bytte mot fordeler med mer umiddelbar materiell/fysisk virkning.

Personvernets gjennomslagskraft svekkes også av at det finnes få skrekkbilder eller kriser som kan danne motvekt mot skrekkbildene fra eksempelvis «9/11». Vi har som personvernmessige tankevekkere enkelte dystopier skildret i skjønnlitteratur samt dystre minner fra Det tredje riket, Stalins diktatur og lignende. Det finnes imidlertid lite ellers fra vår *nåtidige* virkelighet. I de fleste vestlige samfunn finnes ingen fryktinngytende «Storebror» i Orwells forstand, kun mange småbrødre med stort sett gode hensikter. Det nærmeste en kommer et personvernmessig «Tsjernobyl» i Norge er Lund-kommisjonens avsløringer om misbruk av statlige systemer for sikkerhetskontroll.<sup>18</sup> Kommisjonens rapport ble imidlertid utgitt for over 10 år siden og gjelder i stor grad hendelser fra enda lenger tilbake i tid. Mye av rapportens innhold har gått i glemmeboken for de fleste.

Folk flest i Norge synes å ha stor tillit til at opplysninger om dem blir behandlet på lovlig og forsvarlig vis. Offentlige virksomheter – og særlig politiet – synes å nyte størst tillit i den forbindelse. Dette kommer frem av en omfattende undersøkelse som Transportøkonomisk institutt (TØI) gjennomførte i 2005 for Justisdepartementet og Moderniseringsdepartementet (nå Fornyings- og administrasjonsdepartementet).<sup>19</sup> Undersøkelsen viser samtidig at tillitsforholdet også er preget av stor grad av uvitenhet og noen grad av passivitet. For eksempel hadde 44 prosent av respondentene ikke kjennskap til Datatilsynet, mens 41 prosent ikke kjente til plikten i personopplysningsloven<sup>20</sup> til å gi informasjon til registrerte personer. De aller fleste respondentene oppga videre at de ikke hadde benyttet seg av sine innsynsrettigheter. Om dette skal tolkes som passivitet eller likegyldighet er imidlertid ikke lett å si. Vi må huske at i svært mange tilfeller med behandling av personopplysninger er opplysningene av

---

<sup>17</sup> Sitert i W.H. Dutton og R.G. Meadow, «A tolerance for surveillance: American public opinion concerning privacy and civil liberties», i K.B. Levitan (red.), *Government Infrastructures* (New York: Greenwood Press, 1987) s. 148.

<sup>18</sup> Jf. Dokument nr. 15 (1995–96), *Rapport til Stortinget fra kommisjonen som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere* (Lund-rapporten).

<sup>19</sup> Jf. TØI-rapport 789/2005.

<sup>20</sup> Jf. lov om behandling av personopplysninger av 14. april 2000 nr. 31.

forholdsvis triviell karakter eller så er potensialet for personvernskade beskjedent. I slike situasjoner er det derfor lite behov for å ta i bruk innsynsrettigheter.

Undersøkelsen antyder aldersforskjeller vedrørende tillit. Tilliten til at personvern er godt ivaretatt synes å være størst blant de yngste. Dette samsvarer med resultatene til en mindre spørreundersøkelse som Teknologirådet gjennomførte i 2004 om lekfolks holdninger til personvern i tilknytning til IKT. Tenåringene som deltok i undersøkelsen var mindre bekymret for personvernkonsekvenser ved bruk av IKT enn de eldre deltakerne. De voksne var mer bevisste og mer reflekterte vedrørende hvorledes IKT-bruken kan påvirke personvernet.

Mangel på kunnskap om personvernregelverk er ikke et særnorsk fenomen. En omfattende undersøkelse om personvernholdninger til folk i EU-landene som ble gjennomført i 2003 i regi av Europakommisjonen viste at ca. to tredjedeler av de spurte ikke kjente til at det finnes regelverk som gir dem rett til innsyn i, og retting/sletting av, registrerte opplysninger om dem.<sup>21</sup> En tilnærmet like stor andel kjente heller ikke til at det finnes nasjonale datatilsynsmyndigheter. Uvitenhet på begge punkter var særlig høy blant respondenter fra Norden. Samtidig viste nettopp disse respondentene forholdsvis stor tillit til at organisasjoner behandler opplysninger om dem på ansvarlig vis.

Det som gjør kunnskapsnivået og godtroenhet hos nordmenn særlig urovekkende, er resultatene av en annen personvernundersøkelse som TØI gjennomførte i 2005 og som var rettet mot virksomheter i offentlig og privat sektor.<sup>22</sup> Undersøkelsen viser på den ene siden at de fleste virksomheter virker positive til personvern og personopplysningsloven. På den annen side avdekker undersøkelsen at de aller fleste virksomheter har svært begrensede kunnskaper om personopplysningsloven og synes å etterleve lovens krav i til dels skremmende liten grad. På spørsmål om kjennskap til loven, svarte hele 82 prosent av virksomhetene enten «lite kjennskap» eller «verken eller». Kun 4 prosent av respondentene opplyste at de oppfylte fem sentrale krav som følger av loven. Undersøkelsen gir dessverre liten innsikt i om hvorfor etterlevelsen synes å være så slett. Vi kan imidlertid ikke konkludere med stor sikkerhet at personverninteresser ikke er ivaretatt av de fleste norske virksomheter. Det at de rettslige normene har dårlig gjennomslag utelukker ikke at andre normsett innen bransjer og profesjoner m.v. kan ha virkninger som er positive for personvernet. Det er likevel meget som tyder på at mange virksomheter ikke er befolkningens tillit verdig.

### **Selvbestemmelse til besvær**

Enkeltpersoner i Norge har etter personopplysningsloven fått større mulighet enn de hadde etter den gamle personregisterloven<sup>23</sup> til selv å bestemme hvorvidt og hvordan

---

<sup>21</sup> Jf. <[http://europa.eu.int/comm/public\\_opinion/archives/ebs/ebs\\_196\\_data\\_protection.pdf](http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_data_protection.pdf)> (sist besøkt 20. juli 2004).

<sup>22</sup> Jf. TØI-rapport 800/2005.

<sup>23</sup> Jf. lov om personregistre mm av 9. juni 1978 nr. 48 (opphevet).

opplysninger om dem selv skal kunne behandles av andre. Økningen i selvbestemmelsesrett har skjedd delvis som følge av at plikten til å søke om tillatelse fra Datatilsynet for å igangsette behandling av personopplysninger (konsesjonsplikten) er blitt betydelig begrenset i forhold til omfanget etter personregisterloven. Ideologisk sett er det gode grunner til å hilse velkommen de økte muligheter for selvbestemmelse som personopplysningsloven tilbyr. Ideen om at enkeltpersoner skal kunne bestemme – iallfall langt på vei – hvorvidt og hvordan opplysninger om dem selv brukes av andre, har alltid stått sentralt i personvernteori og i de mer generelle doktriner om menneskerettigheter som personvern hviler på. En slik selvbestemmelsesrett er del av et mer generelt krav på autonomi som bunner i respekt for mennesket og dets egenverdi.

Dersom folks holdninger til personvern i stor grad er preget av uvitenhet og passivitet, har økt mulighet for selvbestemmelse imidlertid en klar bakside. Det foreligger en betydelig risiko for at mange vil benytte denne muligheten til å velge et personvernnivå som er lavere enn det nivået som Datatilsynet ville ha fremmet innenfor et konsesjonssystem. Folk flest vil trolig være mindre innstilt på å innta en føre var-holdning enn Datatilsynet.

Vi må heller ikke glemme at situasjonen kan forverre seg på grunn av det jeg kaller for *samtykketretthet* – en tilstand der kravet til å avgi samtykke dukker opp så ofte at folk rett og slett blir trette av kontinuerlig å måtte ta stilling. Denne trettheten kan bli forsterket av den økende kompleksiteten i utnyttelse av personopplysninger. I verste fall kan trettheten føre til apati overfor personvernet. Dette gjelder spesielt for ressursvake mennesker.

Vi er her ved kjernen av et nokså klassisk dilemma som ofte oppstår når et regulatorisk system med paternalistiske trekk (i dette tilfellet konsesjonssystemet) bygges ned for å gi bedre plass til den enkeltes selvbestemmelsesrett: En risikerer at vektlegging av borgernes umiddelbare autonomi øker muligheten for en gradvis uthuling av deres frihet på lengre sikt.

## **Lyspunkter**

Ikke alt er svart i personvernets horisont. Flere nyere utviklingstrekk – særlig på det rettslige planet – er med på å styrke personvernet. Disse må vi ikke glemme, ikke minst ut fra rettspolitiske hensyn.

Blant de viktigste utviklingstrekk er at personopplysningsvern («data protection») i økende grad er anerkjent som grunnleggende rettighet i seg selv – det vil si i tillegg til den tradisjonelle retten til respekt for privatliv som er nedfelt bl.a. i Den europeiske menneskerettskonvensjon (EMK) artikkel 8. Dette ser vi i nyere EU-instrumenter som

inkluderer en særskilt rett til «protection of personal data» som del av de grunnleggende menneskerettighetene i EU.<sup>24</sup>

Denne utviklingen gir viktige signaleffekter for hvorledes nasjonal lovgivning om personopplysningsvern bør utformes. Den gir dessuten grunnlag for en oppjustering av denne lovgivningens normativ rang. Den gjør det enda mer berettiget å spørre hvorfor vi i Norge fremdeles ikke har gitt bedre plass til personvern i grunnloven – et spørsmål som jeg tar opp i slutten av artikkelen.

I takt med den formelle utbyggingen av personvernrettigheter i EU-instrumenter, har toneangivende domstoler i senere tid fattet flere avgjørelser som forsterker personvernet på forskjellige vis. En prinsipielt viktig avgjørelse i så måte er dommen av juni 2004 fra Den europeiske menneskerettighetsdomstolen (EMD) i en sak som gjaldt tysk tabloidpresses trykking av fotografier av Prinsesse Caroline von Hannover i forskjellige daglige situasjoner utenom offisielle oppdrag.<sup>25</sup> Domstolen slo fast at selv om EMK artikkel 8 først og fremst beskytter enkeltindivider i forhold til statlige myndigheter, medfører bestemmelsen begrensninger på private aktørers behandling av personopplysninger – selv når opplysningene omhandler offentlig kjente personer. Kjendiser har med andre ord en rett til privatliv og skal dermed ikke være «fritt vilt» for massemedier. Domstolen uttalte videre at pressens offentliggjøring av personopplysninger i hovedsak kun er berettiget (i henhold til EMK) når informasjonen bidrar til en debatt av generell samfunnsmessig interesse (i motsetning til formidling som kun er ment å tilfredsstille nysgjerrighet).

Av stor prinsipiell betydning er også EMDs avgjørelse fra april 2002 i en sak som omhandlet franske tilsynsmyndigheters ransaking av forretningskontorer til tre selskaper.<sup>26</sup> Domstolen slo her fast at selskaper og andre juridiske personer (og ikke bare fysiske personer) har en egen rett til respekt for sine «hjem» i henhold til artikkel 8. Både denne avgjørelsen og Caroline-dommen viser at artikkel 8, og EMDs praktisering av denne, har betydelig dynamisk kraft.

Strasbourg-domstolens linje danner nå et viktig utgangspunkt for EU-retten, inklusive EUs personverndirektiv.<sup>27</sup> I 2003 erkjente EF-domstolen at personverndirektivet har en sterk menneskerettslig forankring (og ikke kun markedsmessige formål), og at direktivet i stor grad må tolkes i lys av EMDs praksis.<sup>28</sup> Avgjørelsen er særlig interessant for Norge fordi den omhandler offentliggjøring av inntektsopplysninger for navngitte arbeidstakere i visse offentlige organer, som ledd i revisjonsvirksomhet til den østerrikske Riksrevisjon.

---

<sup>24</sup> Jf. traktaten om innføring av en europeisk grunnlov (*Treaty establishing a Constitution for Europe*, ennå ikke i kraft) artikkel I-50. Jf. også EUs charter om grunnleggende rettigheter (*Charter of Fundamental Rights*, vedtatt 7. desember 2000) artikkel 8 (sml. artikkel 7 om beskyttelse av privatliv).

<sup>25</sup> Dom av 24. juni 2004 i saken *Von Hannover mot Germany*.

<sup>26</sup> Dom av 16. april 2002 i saken *Sociétés Colas Est and others mot France*.

<sup>27</sup> Direktiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

<sup>28</sup> Jf. dom av 20. mai 2003 i sak 465/00, *Rechnungshof mot Österreichischer Rundfunk m.fl.* og forente saker 138/01 og 139/01, *Neukomm og Lauer mann mot Österreichischer Rundfunk*.

EF-domstolen fant at lovligheten av denne offentliggjøringspraksisen i det vesentlige beror på en vurdering av hvorvidt offentliggjøringen utgjør et *forholdsmessig* («proportionate») inngrep i rettighetene etter EMK artikkel 8 – en vurdering som først og fremst tilfaller den nasjonale domstol. Den østerrikske forfatningsdomstol konkluderte deretter at virkningen av Riksrevisjonens offentliggjøringspraksis ikke sto i forhold til formålet med det en ønsket å oppnå, og dermed måtte opphøre.<sup>29</sup> Litt overraskende synes denne dommen å ha gått nesten upåaktet hen her i Norge. Selv om den ikke er bindende for norske myndigheter, setter den nok et spørsmålstejn ved lovligheten av ligningskontorenes utlegging av skattelistene til alminnelig ettersyn.

Av andre personvern fremmende trekk på europeisk nivå kan det nevnes at EU nylig har etablert en særskilt tilsynsordning for personopplysningsvern i forbindelse med EF-institusjoners behandling av personopplysninger.<sup>30</sup> Desember 2003 ble Peter Hustinx (tidligere leder for det nederlandske datatilsynet) utpekt som første tilsynsmann under denne ordningen. I tillegg er det allerede etablert en arbeidsgruppe om personopplysningsvern i henhold til personverndirektivet artikkel 29 (Working Party on the Protection of Individuals with regard to the Processing of Personal Data). Arbeidsgruppen består av representanter fra nasjonale datatilsynsmyndigheter innenfor EØS-området og skal i hovedsak gi råd til Europa-kommisjonen.<sup>31</sup> Selv om arbeidsgruppen kun har rådgivende myndighet, har den vært svært virksom og utstedt en lang rekke beslutninger, rekommandasjoner og veiledninger.<sup>32</sup>

Det finnes dessuten mye positivt ved utviklingen av personvernregelverket i Norge. Personopplysningsloven (med tilhørende forskrifter) er på mange måter et bedre regelverk enn den gamle personregisterloven. Mens sistnevnte i stor grad var en diffust formulert rammelov som skulle utfylles med regler gitt av Datatilsynet (først og fremst gjennom konsesjonsvilkår), inneholder personopplysningsloven i langt større grad detaljerte bestemmelser som nedfeller forholdsvis klare rettigheter og plikter. Grunnleggende prinsipper for personopplysningsvern er bedre utviklet og synliggjort. Det nye regelverket legger også opp til en mer effektiv utnyttelse av Datatilsynet. Ved at konsesjonsplikt nå oppstår mer som et unntak enn hovedregelen, har tilsynet bl.a. fått større mulighet til å drive systematisk etterkontroll ved databehandlingsansvarliges implementering av regelverket. Ved opprettelsen av Personvernemnda har vi dessuten fått en ordning for behandling av klager på tilsynets vedtak som er langt ryddigere enn den forrige ordningen der Justisdepartementet var første klageinstans.<sup>33</sup>

Det er videre grunn til å minne om at flere personvern fremmende grunnpilarer ved den norske stats IKT-politikk ikke er blitt borte etter «9/11». Statens kryptopolitikk er et

---

<sup>29</sup> Jf. dom av 28. november 2003, tilgjengelig ved <<http://www.ris.bka.gv.at/vfgh/>> (sist besøkt 24. juli 2004).

<sup>30</sup> Jf. forordning (EF) nr. 45/2001 kapittel V (jf. artikkel 47).

<sup>31</sup> Datatilsynsmyndighetene fra Norge og de andre EFTA-landene deltar i arbeidsgruppen som observatører uten stemmerett.

<sup>32</sup> Tilgjengelige ved <[http://europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/)>.

<sup>33</sup> Videre om den gamle klageordningen, se L.A. Bygrave, *Personvern i praksis: Justisdepartementets behandling av klager på Datatilsynets enkeltvedtak 1980–1996* (Oslo: Cappelen Akademisk Forlag, 1997).

eksempel på dette. I «Norsk kryptopolitikk», vedtatt av regjeringen Stoltenberg i august 2001,<sup>34</sup> omtales kryptografi i svært positive ordelag. Holdningen til allmennhetens tilgang til sterk kryptering er også positiv. En kan naturligvis spørre om regjeringen ville ha inntatt samme standpunkt dersom den hadde vedtatt sin kryptopolitikk et par uker senere, dvs. rett etter terroristhandlingene 11. september 2001. I kjølvannet av «9/11» oppsto det en del diskusjon – særlig i USA – om hensiktsmessigheten ved en liberal kryptopolitikk. Enkelte personer tok til orde for kraftige begrensninger på allmennhetens tilgang til sterke kryptoprodukter.<sup>35</sup> Likeledes ble det reist forslag om å innføre omfattende systemer for obligatorisk nøkkeldeponering.<sup>36</sup> Men i Norge og de fleste andre vestlige land (inklusive USA) er slike meninger foreløpig ikke fulgt opp ved statlige vedtak. Antagelig er en grunn til dette mangel på bevis på at kryptografi i noe særlig grad ble brukt av Al-Quaida i forberedelsene til «9/11» angrepene.<sup>37</sup> Like viktig er at allmenn bruk av kryptering er blitt en forutsetning for effektiv gjennomføring av en rekke samfunnsnyttige prosesser, ikke minst i forbindelse med elektronisk handel.<sup>38</sup>

### **Fremtidige personvern fremmende tiltak**

Hva bør gjøres for å sikre at personvernet forblir liv laga, særlig i en tid der bekymringer for *personikkerhet* får særdeles gode vekstvilkår? Gitt at allmennheten i stor grad synes å være lite opplyst og aktive på personvernets vegne, er det fristende å foreslå at vi vender tilbake til et reguleringssystem som i stor grad styres av Datatilsynet gjennom utstrakt konsesjonsplikt. Et slikt forslag er imidlertid lite realistisk. Den nødvendige støtten for den slags reguleringssystem mangler i dagens klima. Et slikt system er dessuten nokså problematisk gitt dets utpregede grad av paternalisme. Et annet og mer praktisk problem er at konsesjonsordningen – iallfall når den har stort omfang – lett kan medføre uønsket arbeidsbelastning for Datatilsynet. Ordningen i henhold til personregisterloven påførte tilsynet (og mange konsesjonssøkere) mye rutinearbeid av liten umiddelbar betydning for personvern. Dette arbeidet skjedde på bekostning av andre oppgaver som tilsynet skulle utføre – særlig oppfølgingskontroll med etterlevelse av lovregler og konsesjonsvilkår.

Jeg tror at det mest effektive personvern fremmende tiltak på sikt vil være systematiske kampanjer for å opplyse folk om viktigheten av personvernet både for deres velvære som

---

<sup>34</sup> Dokumentet foreligger som brosjyre utgitt av Nærings- og handelsdepartementet, og er også tilgjengelig ved <<http://odin.dep.no/nhd/norsk/enorge/p10001878/024101-990058/index-dok000-b-n-a.html>> (sist besøkt 28. juli 2004).

<sup>35</sup> Jf. bl.a. «US citizens back encryption controls», *CNET News*, 18. september 2001, <<http://news.com.com/2100-1023-273129.html>>; «Former FBI chief takes on encryption», *CNET News*, 14. oktober 2002, <<http://news.com.com/2102-1023-961969.html>> (sist besøkt 25. juli 2004).

<sup>36</sup> Jf. bl.a. «Proposed crypto limits draw broad criticism», *CNET News*, 26. september 2001, <<http://news.com.com/2100-1023-273566.html>> (sist besøkt 25. juli 2004). Litt forenklet er obligatorisk nøkkeldeponering (engelsk: «key escrow») et tiltak der nøkkelen som skal benyttes til å dekryptere krypterte informasjon også må oppbevares av en tredjepart. Sistnevnte vil typisk kunne utlevere nøkkelen etter en rettslig kjennelse slik at klartekst av den krypterte informasjonen kan fremskaffes.

<sup>37</sup> Jf. D. Campbell, «How the plotters slipped US net», *The Guardian*, 27. september 2001.

<sup>38</sup> Se videre L.A. Bygrave, «Kryptopolitikk i en brytningstid», i H. Godø (red.), *IKT etter dotcom-boblen* (Oslo: Gyldendal Akademisk, 2003) s. 252–278.

enkeltindivider og for samfunnslivet generelt. I lys av undersøkelsene om allmennhetens personvernholdninger som er referert til ovenfor, er det svært mye som kan forbedres når det gjelder bevisstgjøring. Hvis vi skal satse riktig langsiktig, bør hovedstøtet settes inn i de vanlige skolene, inklusive grunnskolen. Hittil har mesteparten av offentlig diskusjon om IKT og skolevesenet vært altfor fokusert på fremskaffelse av IKT utstyr; forholdsvis liten vekt har vært lagt på undervisning i de etiske sidene ved *bruken* av IKT. Heretter bør større ressurser settes inn på å utvikle skolekurs i informasjonsetikk. Datatilsynet kan og bør spille en sentral rolle i denne prosessen og bør følgelig få økte ressurser til å drive mer utstrakt opplysningsarbeid.

Da han var Justisminister hevdet Odd Einar Dørum at personvernet «må bringes nærmere dem som skal vernes».<sup>39</sup> Dette er jeg enig i. Som en forlengelse av denne tankegangen er det gode grunner til å «desentralisere» noen av Datatilsynets oppgaver. En opplagt strategi i den forbindelse er å oppfordre organisasjoner til å etablere egne personvernombud. De fleste organisasjoner i Norge har hittil ikke benyttet seg av en slik ordning, til tross for positive tilbakemeldinger fra de få som har.<sup>40</sup> En bør vurdere om ikke organisasjoner over en viss størrelse skal pålegges å opprette egne personvernombud – slik situasjonen f.eks. er i Tyskland.<sup>41</sup> Jeg har derimot langt mindre sans for Dørums forslag om å overføre tilsyn og kontroll med videoovervåking til kommunene. Jeg er redd for at kommunenes sikring av personvernet på det planet vil være like vilkårlig som enkelte kommuners sikring av allmennhetens adgang til fri ferdsel i strandsonen.

Enda et tiltak som bør igangsettes er å gi mer direkte lovmessig støtte til bruken av personvernøkende teknologier og til integrering av personvernkrav i systemutvikling. Reglene i personopplysningsloven – samt EUs personverndirektiv – er i for liten grad formulert med den slags tilnærming.<sup>42</sup>

Når det gjelder lovreform er kanskje det viktigste på sikt at vi får en nasjonal oppjustering av personvernrettighetenes normativ rang. Personvern (inklusive personopplysningsvern og vern av privatliv) – sammen med andre grunnleggende menneskerettigheter – bør få bedre plass i grunnloven. Spørsmålet om grunnlovsfesting av personvernet får større aktualitet når en tenker på den formelle anerkjennelsen og utbyggingen av personvernrettigheter i folkeretten. Spørsmålet får også større aktualitet når en tenker på hvor mye tid og energi som i Norge har gått med til å forberede (antatte) forbedringer av grunnlovsbeskyttelsen for ytringsfriheten de siste år.

---

<sup>39</sup> Jf. *Personvernrapporten 2004* (Oslo: Datatilsynet, april 2004) s. 19.

<sup>40</sup> Jf. bl.a. «Ullevål først med personvernombud», *Aftenposten* (morgenutgave) 19. august 2004 s. 9; «Første eksterne jurist som personvernombud: Advokater med kontroll over personvernet», *Juristkontakt*, 2004, nr. 6 s. 22–25.

<sup>41</sup> Jf. den tyske *Bundesdatenschutzgesetz* (føderale lov om personopplysningsvern) av 1990 § 4f – 4g.

<sup>42</sup> Se videre L.A. Bygrave, «Privacy-enhancing technologies – caught between a rock and a hard place», *Privacy Law & Policy Reporter*, 2002, bind 9, s. 135–137, også tilgjengelig ved <[http://europa.eu.int/comm/internal\\_market/privacy/docs/lawreport/bygrave\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/bygrave_en.pdf)> (sist besøkt 27. juli 2004).

Ytringsfrihetskommisjonen foreslo riktignok grunnlovsfesting av privatlivets fred,<sup>43</sup> men forslaget fikk lite støtte hos regjeringen Bondevik.<sup>44</sup> Enkelte i den nåværende regjeringen ser imidlertid ut til å være mer positive til forslaget.

Nedprioriteringen av personvern i forhold til ytringsfrihet er noe underlig fordi det ikke finnes solide holdepunkter i rettspraksis fra EMD for å hevde at ytringsfrihet skal ha høyere normativ status enn personvern. Begge sett rettigheter er tvert imot likestilt og – både på det personlige og samfunnsmessige plan – uløselig knyttet sammen. Som John Rawls så treffende påpeker, « ... the basic liberties constitute a family, and ... it is this family that has priority and not any single liberty by itself».<sup>45</sup>

[Oppdatert versjon av en artikkel som opprinnelig ble publisert i D. Ekelberg og M. Ludvigsson (red.), *Frihet – samtalen fortsetter* (Oslo: Civita, 2004), s. 142–159]

### **Om forfatteren:**

Dr. juris Lee Andrew Bygrave er førsteamanuensis ved Institutt for privatrett ved Universitetet i Oslo. Han er internasjonalt anerkjent som en ledende ekspert på personvern. Han er rådgiver for Europakommisjonen vedrørende rettslig regulering av overføring av personopplysninger til land utenfor EU. Han er videre medlem i Advisory Board i Data Protection Research and Policy Group ved British Institute for International and Comparative Law. Han har tidligere også vært gjesteprofessor ved Universitetet i Wien og Universitetet i Tilburg.

Hans forfatterskap omfatter bl.a. bøkene *Personvern i praksis* (1997), et internasjonalt standardverk: *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002) og *Personvern i informasjonssamfunnet* (2004 – skrevet sammen med Dag Wiese Schartum)

---

<sup>43</sup> Jf. «*Ytringsfrihed bør finde Sted*», NOU 1997: 27 s. 88, 113, 252.

<sup>44</sup> Jf. St.meld. nr. 26 (2003–2004) s. 48. Kontroll- og konstitusjonskomiteen har imidlertid fremmet forslag om at «Stortinget ber Regjeringen utrede vernet av privatlivets fred, herunder spørsmålet om mulige utforminger av en eventuell grunnlovsfesting». Jf. Inst. S. nr. 270 (2003–2004) s. 14, 71.

<sup>45</sup> Jf. J. Rawls, *Political Liberalism* (New York: Columbia University Press, 1993) s. 356.