Sitering av artikkelen i APA (6th):
Sunde, I. M. (2013). Økosystemeffekten: Om personvernet i sosiale medier. *Lov og rett, 52*(1), 85-102.

Økosystemeffekten – Om personvernet i sosiale medier

Av førsteamanuensis ph.d. Inger Marie Sunde

«Økosystemeffekten» betegner at sosiale medier som Facebook og YouTube inngår i en større sammenheng med gjensidig forsterkende effekter. Bruken av mediene har konsekvenser for personvernet fordi opplysninger kan utnyttes i en annen kontekst enn de ble publisert for, og få uheldige følger for den de gjelder. Krenkelser kan dessuten bli varige som følge av vidtrekkende spredning og lagring av data og effektive tjenester som søker opp den krenkende informasjonen. Artikkelen tar utgangspunkt i at innholdet i personvernet må reformuleres og presiseres i takt med samfunnsutviklingen, og at det gjelder en rett til å ha et effektivt personvern også på internett. Det antas at filtrering bør innføres for å få brakt vedvarende krenkelser til opphør. Videre drøftes «retten til å bli glemt», og om lovgiver burde innføre et fotoforbud. Bakteppet er ytringer som er rettsstridige, og i tillegg, ytringer som er lovlige, men som blir et problem over tid. Temaet er aktuelt i lys av EU-domstolens dommer om filtrering av 24. november 2011 og 13. februar 2012, og filosofen Mayer-Schonberges bok *Delete* (2011) om retten til å bli glemt.

Inger Marie Sunde er født i 1962. Cand.jur. UiO 1987. Ll.M. Harvard Law School 1992. Førstestatsadvokat Økokrim 1993–2005. Ph.d. UiO 2010. Førsteamanuensis Politihøgskolen i Oslo fra 2010.

1 Problemstilling

Artikkelen behandler noen personvernspørsmål som aktualiseres av sosiale medier. Sosiale medier er viktige daglige informasjonskilder for en stor del av befolkningen. I en nyhetssending på TV2 30. januar i år om Facebooks nye «timeline»-funksjon, ble det opplyst at nordmenn har 3 millioner Facebook-profiler og at 70 % bruker Facebook daglig. I tillegg brukes andre sosiale medier som for eksempel LinkedIn, Twitter, Blogspot og YouTube.

Ytringer i sosiale medier kan ha stor påvirkningskraft og ramme personvernet. Effektene kan oppstå nokså uavhengig av den omtalte persons nettbruk fordi ytringene påvirker *alle andre* som leser dem, og det kan enkeltindividet vanskelig forhindre. Men også ytringer man selv har lagt ut, kan ha uforutsette følger, kanskje i form av problemer på arbeidsmarkedet. Det gir grunn til å spørre om for eksempel festbilder fra studietiden bør være relevant bakgrunnsinformasjon for en potensiell arbeidsgiver? Og gjelder det et vern mot at private opplysninger brukes for et annet formål enn de ble publisert for?

På nettet lever ytringene sitt eget liv. Årsakene ligger i digitalisering, kontinuerlig tilgjengelige «skytjenester» («cloud computing») med effektive søketjenester, ubegrenset publiseringsflate og tilnærmet gratis lagringsplass. Innhold kan derfor få vid og varig spredning langt utenfor den opprinnelige konteksten.

Dypest sett er personvernet forankret i ulovfestede normer. Det betyr at å gi en presis og uttømmende beskrivelse neppe er mulig, snarere kreves en stadig reformulering og presisering av vernet i lys av samfunnsutviklingen. Dette reflekteres i EMDs vanlige utgangspunkt i saker om retten til privat liv, jf. EMK artikkel 8, hvor det konstateres at «private life is a broad term not susceptible to exhaustive definition».[1] Uttalelsen er vel dekkende også for personvernet etter norsk rett.

Samfunnsutviklingen kan gi grobunn for *nye tanker* om personvernets rekkevidde (for eksempel rett til innsyn i egen sykejournal (Rt. 1977 s. 1035)) og kan *skape nye trusler* som aktualiserer presiseringer av vernets innhold. Høyesterett har flere ganger hatt foranledning til

[1] *P.G. og J.H. mot Storbritannia* dom 25. september 2001 (avsnitt 56).

å uttale seg om personvernets innhold i lys av teknologiske nyvinninger, og underbygger argumentasjonen med en henvisning til alminnelige rettsgrunnsetninger.[2]

Sosiale mediers endringskraft på sosiale omgangsformer og teknisk funksjonalitet som i seg selv innebærer personvernutfordringer, gir grunn til å drøfte tre spørsmål, nemlig (i) om det gjelder en rett til å få brakt en vedvarende krenkelse til opphør, (ii) om det gjelder en rett til å bli glemt, og (iii) om det er behov for et fotoforbud. Med hensyn til det første spørsmålet tar analysen et *de lege lata* perspektiv. Gitt personvernets dynamiske karakter, er utgangspunktet at det kan være sider av det materielle vern som hittil ikke har vært tilstrekkelig kartlagt, simpelthen fordi man ikke har hatt foranledning til det før nettverksteknologien og web 2.0-tjenester satte disse sidene under press. Retten til å bli glemt og fotoforbudet drøftes under en *de lege ferenda* synsvinkel, som dog ikke utelukker at holdepunkter for (deler av) et slikt vern finnes i gjeldende rett.

Innen dette artikkelformatet kommer det ikke på tale å være rettskildemessig uttømmende. Formålet er å skape bevissthet omavgrensede problemstillinger som har stor betydning for personvernet.

2 Avgrensning og presisering

Artikkelen behandler krenkelser borgerne imellom, dvs. personvern i et horisontalt perspektiv. Det er typisk tale om publisering av ytringer som krenker privatlivets fred, trusler, spredning av overgrepsbilder av barn og av personfoto uten samtykke mv.

Individet er avhengig av statens hjelp til å få stanset vedvarende krenkelser på nettet. Dette aktualiserer doktrinen om statens positive forpliktelse til å effektivisere personvernet for sine borgere, jf. EMK artikkel 8, jf. artikkel 1. Spørsmålet er om staten forsømmer sin plikt til å sikre retten til privat liv ved å unnlate å innføre tiltak som stanser slike krenkelser. Det er også mulig at den positive forpliktelsen gjør seg gjeldende i forhold til et fotoforbud, mens den er mindre aktuell i forhold til retten til å bli glemt, ikke minst fordi innholdet i dette vernet er uavklart. Formålet med å nevne «retten til å bli glemt» er å belyse at personvernet er i utvikling, noe som illustreres av den pågående internasjonale diskusjonen om denne rettigheten.

Jeg avgrenser også mot spørsmål vedrørende kommersielle foretak, hvor problemstillingen gjelder utnyttelse av personopplysninger generert ved bruk av sosiale medier. Opplysningene kan si noe om personlige interesser, forbrukerpreferanser, bopel, alder, kjønn, sivil status osv. Det er som kjent «no such thing as a free lunch», så forklaringen på hvorfor en rekke populære tjenester er «gratis», for eksempel Facebook (sosialt medium) og Google (søketjeneste), er at dataene har stor kommersiell verdi. Avgivelse av personopplysninger kan anses som «betaling». I tillegg brukes personlig tilpasset reklame, noe som reiser markedsførings- og forbrukervernspørsmål.

Beskyttelsesnivået for personopplysninger i tredjeland er en kontinuerlig problemstilling på grunn av nettets globale rekkevidde, fordi mange dominerende foretak er lokalisert utenfor rekkevidden til europeisk personopplysningsregulering, og fordi man ikke

[2] Tekniske muligheter ga Høyesterett foranledning til å uttale seg om personvernet blant annet i Rt. 1952 s. 1217 (To mistenkelige personer) som gjaldt spredning av personopplysninger om en eksisterende person, til et bredt publikum via en spillefilm på kino. I Rt. 1991 s. 616 (Videobevis) ble bevismateriale anskaffet ved hemmelig kameraovervåking på arbeidsplassen avskåret som bevis, og i Rt. 1996 s. 1114 (polygraf) foretok Hlyesterett en bred drøftelse om bruk av avansert løgndetektorteknologi i bevistilbudet i en straffesak. Løgndetektorbeviset ble avskåret som bevis, selv etter domfeltes anmodning om å føre beviset, gitt de inngripende personvernkonsekvenser en slik adgang kunne få.

vet hvor data i «nettskyen» faktisk lagres. I «Lindquist-saken» sa imidlertid EU-domstolen at en sluttbrukers publisering av personopplysninger på en allment tilgjengelig web-side, ikke var å anse som overføring av opplysningene til tredjeland, jf. personopplysningsdirektivet (95/46) artikkel 25. Begrunnelsen var at publisering på web ellers ville være generelt umulig.[3] I det følgende fokuserer jeg imidlertid på krenkelser borgerne imellom og rekkevidden av statens effektiviseringsplikt med hensyn til personvernet.

3 Rettspolitiske utgangspunkter

3.1 Informasjonsspredning i sosiale medier: Økosystemeffekten

Sosiale medier er utformet for sosialisering og dialog, de er interaktive og «lever» i kraft av at brukerne tilfører innholdet (innholdet er «brukergenerert»). Tjenestene anses som «halvoffentlige», dvs. at innholdet legges ut i en privat kontekst, men kan likevel få svært vid spredning. (Mediene kan også utnyttes for å nå ut til allmennheten, noe statsministerens «Twitter-blogg» er et eksempel på.)

Tjenestene er umedierte, de har ikke redaktør og faller utenfor tradisjonell medielovgivning. Publiseringsflaten er ubegrenset og integrerer tekst, foto, tegninger, lyd og video.[4] De kalles derfor «rike medier».

Med «økosystemeffekten» mener jeg den effekten på personvernet som skapes av at sosiale medier fungerer i samspill med andre internettjenester og inngår i en større virkelighet utenfor nettet. Søketjenester, lagringstjenester og digitalisering av informasjon i kombinasjon med webbasert lenketeknologi og spredningstjenester som fildeling og RSS-feed («pushing» av informasjon til sluttbruker), medfører reproduksjon og spredning av innhold som blir varig tilgjengelig. «Reproduksjon» betyr digital kopiering, dvs. fremstilling av «dubletter» som er identiske instanser av én fil.[5] Dublettene medfører at krenkelser av personvernet kan bli svært massive målt i varighet og utbredelse.

Tilfellet «hemmelig.com» fra desember 2011 er illustrerende. Abcnyheter.no meddelte at hemmelig.com hadde blitt «hacket» og at deltakerlisten og chatloggene hadde blitt kopiert. Hemmelig.com – en lovlig tjeneste – tilbød møteplass for folk som ønsket sexpartner og hadde 26 000 norske brukere. Deltakerlisten ble publisert på sosiale medier, blant annet Facebook. Riksmedia meddelte at det var tale om «politikere, offiserer i Forsvaret, folk i sikkerhetsbransjen, flykapteiner, leger, advokater, kjendiser og næringslivsledere».[6] Personverntjenesten slettmeg.no opplyste at man hadde liten mulighet for å hjelpe deltakerne med å unngå å bli identifisert, fordi

> «du kan vanskelig slette deg fra brukerdatabasen for hemmelig.com som er spredt på nett. … Årsaken til dette er at delingen av dette dokumentet foregår i hovedsak via torrrents. Dette betyr at selve dokumentet er lagret på enkeltpersoners private maskiner, og derfra får du den ikke bort.»[7]

---

[3] Sak C-101/01, *Sverige mot Bodil Lindquist,* Sml. 2003 s. I-12992 (avsnitt 52–71, se avsnitt 69).

[4] Gisle Hannemyr, «Personvern i deltakerskapte rike medier» i Heidi Grande Røys (red.), *Delte meninger,* Oslo 2009 s. 161–175.

[5] Inger Marie Sunde, *Automatisert inndragning,* Oslo 2011 kapittel 3.

[6] http://www.dagbladet.no/2011/12/22/nyheter/hemmeligcom/sex/hacking/innenriks/19518250/.

[7] http://www.slettmeg.no/39334-Sletting-av-hemmelig-com.

«Torrents» er effektiv fildelingsteknologi hvor brukernes datamaskiner utveksler filer direkte, noe som resulterer i masseproduksjon av dubletter. Deltakerlisten ble altså lastet ned av Facebookbrukerne og redistribuert på fildeling.

Et annet eksempel er «the dog poop girl». En hund gjorde fra seg på en T-bane i Korea. Til tross for anmodning om det, plukket ikke eieren, en ung kvinnelig student, opp etter hunden sin. Opptrinnet ble fotografert av en medpassasjer som postet det på en koreansk blogg. På kort tid hadde videoklippet spredt seg over hele verden, og en amerikansk bloggtjeneste rapporterte nesten 10 millioner nedlastinger per måned.[8] Spredningen kan forklares ved at veldig mange brukere har postet kopi av videoklippet, kombinert med spredningsfunksjoner i nettet. Studenten ble utsatt for sterk fordømmelse og utvist fra universitetet.

Eksemplene viser at innhold på sosiale tjenester kan få kraftig spredning. Fildeling og søketjenester effektiviserer spredningen. Eksemplene viser også at innhold som først er lagt ut spres uhindret. Lagring lokalt i tillegg til i «nettskyen» medfører at innholdet resirkuleres fra stadig nye kilder. «Brukergenerert» betyr ikke mer enn at brukerne har lagt ut innholdet selv. Det betyr ikke nødvendigvis at brukeren har skapt informasjonen eller det kreative uttrykket. I tilfellet «the dog poop girl» var det for eksempel bare fotografen på T-banen som skapte innholdet.

På samme vis som dublettene representerer et stort problem for underholdningsindustrien i form av piratvirksomhet på fildeling, og et globalt sikkerhetsproblem i form av «malware», er dublettene en vesentlig årsak til vedvarende integritetskrenkelser på nettet.[9] Innføring av redaktøransvar i sosiale medier er neppe et hensiktsmessig tiltak, fordi problemet i hovedsak skyldes ukontrollert viderespredning utenfor mediet.[10] Derfor er det behov for andre tiltak.

3.2 Nettet som en del av virkeligheten

Forskeren Petter Bae Brantzæg skriver at «[s]killene mellom Internett og det virkelige liv er i ferd med å opphøre».[11] Nettet er med andre ord en del av vår virkelighet. Saken «hamarungdom.no» gir en tydelig illustrasjon av sammenhengen mellom integritetskrenkelser på og utenfor nettet.[12]

Nettstedet hamarungdom.no var en sosial møteplass for ungdom på Hamar. Nettstedet var blitt benyttet til å poste sjikanerende meldinger om en navngitt pike i 16-års-alderen, noe som ble ansett som «hensynløs atferd som krenker en annens fred», jf. straffeloven 1902 § 390a. Ved skyldvurderingen la retten vekt på at fornærmede «i større grad enn vanlig, var blitt plaget av andre elever på barne- og ungdomsskolen … og har vært plaget i alle år». Bruken av nettstedet forsterket den personlige integritetskrenkelsen i de fysiske omgivelsene.

Også et leserinnlegg fra en deltaker på hemmelig.com er talende: Vedkommende hadde brukt tjenesten

---

[8] Tilfellet er omtalt av Daniel D. Solove, *The Future of Reputation – Gossip, Rumor, and Privacy on the Internet*, USA 2007 s. 1 flg.

[9] Se nærmere omtale av dubletter og integritetskrenkelser i Sunde, *Automatisert inndragning*, kapittel 3.3.4 s. 47 flg.

[10] Medieansvarsutvalget har drøftet innføring av redaktøransvar i sosiale medier og gitt en dissenterende anbefaling. NOU 2011: 12 Ytringsfrihet og ansvar i en ny mediehverdag.

[11] Petter Bae Brantzæg, «Privat 2.0» i Heidi Grande Røys (red.), *Delte meninger*, Oslo 2009 s. 194–213 (s. 212).

[12] THEDM-2004-3964.

> «for å finne likesinnede når det gjelder litt mer kinky greier som faktisk er helt lovlig. Nå truer monstrene som har lastet ned lista med å offentliggjøre alt sammen. … Jeg kjenner nå at jeg blir helt kvalm og kald … selvmord vil ikke umulig følge i kjølvannet … Redsel for å bli banket opp kan ikke sammenlignes med den enorme og ødeleggende skammen som offentlig uthenging i denne saken innebærer … Skjønner folk hva det innebærer, å bli satt i gapestokk for resten av livet? Vi har bare et eneste liv som vi forsøker å gjøre det beste ut av.»[13]

Sosiale medier er først og fremst et instrument for samkvem mellom mennesker som også omgås i den fysiske del av verden. Dermed kan nettbaserte krenkelser sjelden forklares eller bedømmes isolert fra handlinger utenfor nettet. Dagens internettinnbyggere kan heller ikke «slå av» nettet siden en stor del av sosialt liv skjer over nett. Endringen fra den voksne generasjons omgangsformer er så radikal at den antakelig knapt kan fattes.

Dermed er personvernet ikke bare et individuelt, men også et samfunnsanliggende. Samfunnet tjener på å ha et robust personvern. Samfunnet har behov for utvikling av modne, trygge borgere som senere vil ha mot til å bidra på den offentlige arena. Det å være trygg, i den forstand at man kan bruke nettet uten frykt for å bli konfrontert med sjikanerende meldinger eller av bilder som ble tatt i uheldige situasjoner for flere år siden osv., er viktig for personlig utvikling. Derfor bør det skapes bevissthet om det materielle innholdet av personvernets digitale side og mulige statlige effektiviseringsplikter identifiseres.

Personvernet forutsetter en balansering av interesser, så også motstående hensyn kan gjøre seg gjeldende. I digital sammenheng gjør særlig hensynene til ytringsfriheten og til ekomtilbydernes næringsinteresser seg gjeldende. Dessuten kan personvernfremmende tiltak ha sidevirkninger som går ut over personvernet til tredjeparter, noe som også må tas inn i vurderingene. På den annen side er det mulig at eiendomsretten til egne data kan støtte opp under personvernet.

3.3 Oppsummering

Siden så mange mekanismer gjør seg gjeldende i presset mot personvernet, kan man knapt påberope seg å kunne gi en enegyldig fremstilling av problemet. Men jeg synes den britiske kriminologen David S. Wall er inne på noe vesentlig når han hevder at problemet består i «the globalized aggregate volume».[14] Han skriver at krenkelser

> «may not be individually as serious as many of the statistics claim, but their seriousness lies in their globalized aggregate volume.»[15]

Oxfordfilosof Viktor Mayer-Schonberger peker på noe av det samme når han skriver at internett er en «gigantic collective external memory».[16] Digitalisering, spredning, søkbarhet og lagring gjør at informasjon stadig reproduseres. Dette skaper en gigantisk felles «hukommelse» som til forskjell fra vår biologiske hukommelse, aldri lar et informasjonsfragment «gå i glemmeboken».

---

[13] http://debatt.sol.no/content/liste-fra-hemmelig-com.

[14] David S. Wall, *Cybercrime – The Transformation of Crime in the Information Age*, UK 2007 s. 19.

[15] Ibid.

[16] Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age*, UK 2011.

4 Integritetskrenkelser på grunn av ytringer

4.1 Innledning

I det følgende skal jeg behandle retten til å få en vedvarende krenkelse brakt til opphør, retten til å bli glemt og fotoforbud. Bakteppet er ytringer som er rettsstridige (vedvarende krenkelse) og ytringer som er lovlige, men som blir et problem over tid (retten til å bli glemt). Behovet for et fotoforbud kan begrunnes i begge type ytringer.

Jeg avgrenser mot en drøftelse av ytringers rettsstrid i sosiale medier. Alminnelige lovregler gjelder også på nettet, så en ytring som er ulovlig i den fysiske del av verden er også ulovlig på nettet. Motsatt må man tåle på nettet det man må tåle i den fysiske del av verden. Uansett må det tas hensyn til kontekst. Blogginnlegg som lyder: «Du skal døøøøø, døøøøøøø, døøøøøøøøøø…!!!» er muligens vanlige, ufarlige og derfor ikke krenkende; i hvert fall kan det være slik ifølge den norske bloggeren Vampus.[17] I en annen kontekst, for eksempel familievold, ville man derimot konkludert med at det var en straffbar trussel. Men siden rettsstriden må vurderes i lys av konkrete omstendigheter, går jeg ikke nærmere inn på dette.

4.2 Retten til å få en vedvarende krenkelse brakt til opphør

4.2.1 Problemet

Utgangspunktet er at rettsstridige integritetskrenkende ytringer er publisert på nettet. Hvis identiteten til personen som står bak er kjent, kan vedkommende etter omstendighetene straffes og holdes erstatningsansvarlig. Men individuell reaksjon er av flere grunner utilstrekkelig. For det første kan muligheten for reaksjon være avskåret fordi gjerningspersonen er anonym (ikke sporbar) på grunn av tekniske forhold. Også streng konfidensialitetsplikt kan skape anonymitet, noe saken *K.U. mot Finland* (2008) illustrerer.[18] Finsk taushetslovgivning avskar adgang for internettilbyder til å utlevere opplysning om identiteten til en internettbruker som hadde lagt ut en falsk meddelelse i navnet til en 12 år gammel gutt, om at gutten var interessert i kontakt med pedofile menn. Ifølge finsk rett var ikke handlingen, selv om den var straffbar, tilstrekkelig alvorlig til å begrunne unntak fra taushetsplikten. Finland ble domfelt fordi konfidensialitetsplikten var for absolutt og ikke sikret guttens krav på respekt for privat liv, jf. EMK artikkel 8.1.

Et annet problem er at en kjent gjerningsperson kan oppholde seg i et land som ikke forfølger handlingen. Men selve *problemets kjerne* består i at selv om reaksjon idømmes og erstatning betales, er det krenkende innholdet *fremdeles tilgjengelig på nettet*, og fortsetter å representere en krenkelse.

Problemet er veldokumentert for overgrepsbilder av barn og private intimbilder av voksne. Publiseringen er straffbar etter straffeloven 1902 § 204 a, § 390 og § 390 a, og etter bestemmelsen om retten til eget bilde i åndsverkloven § 45 c, jf. § 54.

Årsakene til at bildene havner på nettet er forskjellige. Overgrepsbilder tas for å bli spredt. Bildene er «hard valuta». De gir tilgang til pedofile miljøer, kan byttes mot andre bilder og selges til betalende kriminelle kunder. For private intimbilder er det vel gjerne slik at partene er enige om fotograferingen, under forutsetning av at bildene behandles fortrolig. Men forhold kan ta slutt og bildene kan havne på nettet som en hevnakt fra ekskjæresten. Bilder kan også komme på avveie etter datainnbrudd slik som i «Photobucket»-saken (Oslo tingretts dom 5. april 2011). Domfelte – en IT-ingeniør i 20-årene – hadde «hacket» den

[17] Vampus (Heidi Nordby Lunde) i nyhetsinnslag på NRK etter statsministerens nyttårstale hvor han oppfordret det norske folk til å bli «digitale nabokjerringer». Vampus advarte mot nidkjærhet og overreagering. http://vampus.blogspot.com/.

[18] *K.U mot Finland* dom 2. desember 2008.

amerikanske fototjenesten Photobucket.com som hadde 66 millioner brukere, hvorav 120 000 norske. Han kopierte brukerdatabasen og skaffet seg brukerdata, epostadresser og passord som han benyttet til å oppnå tilgang til tjenesten BBW.no (Big Beatiful Women Norge). Herfra lastet han ned private intimbilder fra 187 norske brukere. Det at bildene har kommet på avveie har medført personlige problemer for flere av de fornærmede.[19]

Personvernkrenkelser kan også skje ved manipulasjon av bilder. Ifølge en reportasje i A-magasinet, opplevde en lokalpolitiker og småbarnsmor bosatt i Våler at noen hadde kopiert Facebook-bildet hennes inn i erotiske nakenbilder. Disse var lagt ut på prostitusjonstjenester med hennes navn, som var unikt i Norge.[20] Hun ble følgelig kontaktet av menn som var ute etter sextreff. Kvinnen erfarte at det var umulig å få slettet navn og bilder som blant annet lå på svensk, polsk og ukrainsk nettsted. Prostitusjonsannonsene kom opp ved å «google» navnet hennes. Opplevelsen var svært belastende og hun orket ikke lenger å fronte i lokalpolitikken. Gjerningspersonen er ukjent.

En tilbyder av en nettjeneste ønsker ikke nødvendigvis å slette innhold som genererer lukrativ interesse når risikoen fremstår som liten. I tillegg må man regne med at bildene deles på fildeling, så sletting fra tilbyders side har begrenset virkning. Enkeltindividet kan derfor vanskelig få stanset krenkelsen. Og barn krenkes nettopp av voksne personer som burde ha beskyttet dem, så de er uansett ute av stand til å ivareta sine interesser.

For overgrepsbilder av barn har Høyesterett karakterisert spredningen som «en livsvarig krenkelse» (Rt. 2002 s. 1187).

> «I tillegg til den enorme spredning som oppnås ved å legge bilder ut på Internett er det i praksis ikke mulig å få slettet dem. Barn som er blitt misbrukt gjennom produksjon av pornografi, vil således oppleve å kunne bli gjenkjent i årevis. Det dreier seg i slike tilfeller om en livsvarig krenkelse … Man må regne med at risikoen for at andre kommer over bildene vil være en betydelig tilleggsbelastning senere i livet for den det gjelder.» (s. 1192).

Når individet mangler midler til å få stanset krenkelsen, som man utvilsomt hadde hatt rettskrav på dersom kravet kunne vært gjort gjeldende direkte mot gjerningspersonen, er det nærliggende å vurdere bruk av filtrering for å blokkere tilgangen til bildene, slik at de i praktisk forstand «forsvinner». Forskjellige teknikker kan brukes, og et hovedskille går mellom filtrering av adresser til nettsteder og datamaskiner (web og IP-filtrering) på den ene siden, og filtrering av data på den andre siden. Jeg vurderer kun den sistnevnte metoden som innebærer filtrering på linje med den som brukes mot skadelig dataprogram («malware»). Filteret blokkerer bare innholdselementer som på forhånd er klassifisert som rettsstridige, dvs. de rettsstridige dublettene.

Filtrering utløser tre spørsmål, nemlig (i) om filtrering er forenlig med det europeiske forbudet mot å pålegge tilbyderne en generell overvåkingsforpliktelse, jf. ehandelsdirektivet artikkel 15; (ii) dersom svaret er bekreftende, hvorvidt staten har en positiv forpliktelse til å innføre filtrering; og (iii) om det finnes hjemmel for filtrering etter gjeldende rett.

Rent praktisk må filteret settes på nettverket til tilbyderen av internettilgang (ISP) eller på serveren til en vertstjeneste. Blokkeringen gjøres på grunnlag av «match» mot en database som inneholder de rettsstridige filene. Blokkeringen baserer seg således på at filene i nettet er dubletter (identiske), eller så like filene i databasen at kravet til rettsstrid ikke byr på tvil. Likhet kan blant annet konstateres ved bruk av bildegjenkjenningsteknologi.

---

[19] Dommen s. 18.

[20] Aftenpostens A-magasin 4. november 2011 s. 8 flg.

4.2.2 Forbudet mot å pålegge en generell overvåkingsforpliktelse

Første spørsmål er om filtrering er forenlig med det europeiske forbudet mot å pålegge ekomtilbyder en generell overvåkingsforpliktelse, som er implementert i ehandelsloven (lov 35/2003) § 19:

> «Bestemmelsene i §§ 16–18 [om ansvarsfrihet for tilbyderne] medfører ikke at tjenesteyteren har en generell plikt til å kontrollere eller overvåke den informasjonen som lagres eller overføres på oppfordring fra en tjenestemottaker, eller en generell plikt til å undersøke forhold som antyder ulovlig virksomhet.»

EU-domstolen har uttalt seg om fortolkningen av overvåkingsforbudet i to saker om filtrering av musikkfiler som ble distribuert på nettet uten samtykke fra belgiske rettighetshavere (SABAM). Den første saken gjaldt filtrering pålagt en ISP (Scarlet), mens den andre gjaldt filtrering pålagt tilbyderen av en sosial tjeneste kalt Netlog, som hadde flere titalls millioner brukere hver dag.[21] SABAM disponerte en database med all musikk som de hadde rettigheter til og som ble brukt som «match» for filtrering av dubletter i nettet. Filtrene skulle blokkere musikkfiler som ble piratdistribuert på fildeling som skjedde over Scarlets nett og på Netlog.

Scarlet-dommen er viktigst siden «Netlog» i det vesentlige viser tilbake til denne, både med hensyn til resonnement og konklusjon. Retten mente at spørsmålet om hvorvidt filtreringen sto seg i forhold til overvåkingsforbudet, måtte avgjøres etter en interesseavveining (avsnitt 37 flg.). Vern av opphavsrettigheter (SABAM) sto mot ekombransjens næringsinteresser (Scarlet). Retten presiserte at opphavsrettigheter er viktige, men ikke enerådende, ordningen var ensidig bebyrdende, og dermed urettferdig for Scarlet som måtte bære hele omkostningen ved filtreringen (avsnitt 48). Ordningen hadde også den svakhet at alle brukernes IP-adresser ble kjent. IP-adresser som kan kobles til sluttbrukernes identitet regnes som personopplysninger. Ytterligere var det risiko for filtrering av lovlig innhold, fordi lovverket varierte medlemsstatene imellom med hensyn til rekkevidden av den opphavsrettslige eneretten for de verk som lå i SABAMs database. Ordningen skapte følgelig risiko både for personvern og ytringsfrihet (avsnitt 38―40 og 51). På denne bakgrunn ble filtreringen ansett for å være i strid med det generelle overvåkingsforbudet.

I forhold til filtrering av integritetskrenkende innhold, synes avgjørelsene å gi noen viktige føringer. For det første utelukkes ikke bruk av filtrering, det hele beror på en interesseavveining. Videre synes forholdene å ligge vesentlig annerledes an for integritetskrenkelser enn for opphavsrettskrenkelser. Den siste gruppen rettighetshavere kan kompenseres økonomisk, for eksempel ved avgiftsordninger og over statsbudsjettet, mens erstatning ikke løser problemet for straffbare integritetskrenkelser. For barn er dette uttrykkelig presisert av EMD i «K.U.»-dommen (avsnitt 46). EMD konstaterte først at kriminalisering alene ikke er tilstrekkelig. I tillegg er effektiv etterforsking og strafforfølgning nødvendig for at straffetrusselen skal få en preventiv effekt. Økonomisk kompensasjon til offeret fra en tredjepart har ikke slik effekt, og er derfor utilstrekkelig som tiltak for å sikre retten til privat liv.

«K.U.» må anses å være relevant for interesseavveiningen i overvåkingsspørsmålet, selv om den ikke direkte gjelder filtrering. Det vesentlige er at EMD uttrykker sterk støtte til effektive tiltak for å sikre barns rett til respekt for privat liv, såfremt det skjer på rettsstatens premisser og med tilbørlig hensyn til andre grunnleggende rettigheter. Siden det neppe finnes noe annet tiltak enn filtrering som kan stanse den vedvarende krenkelsen, synes meget

[21] Sal C-70/10, dom 24. november 2011 *Scarlet Extended SA mot Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*. Sak C-360/10, dom 13. februar 2012 SABAM mot Netlog NV.

tungtveiende innvendinger å måtte påvises for at filtrering skulle komme i konflikt med overvåkingsforbudet.[22]

I «Scarlet» var det uheldig at økonomiske og driftsmessige ulemper ensidig var lagt på tilbyderen. Men siden integritetskrenkelsene er klart straffbare forhold av alvorlig karakter, synes det lite naturlig å sende hele regningen til ekombransjen. Finansieringen bør i slike tilfelle være en offentlig oppgave, og i så fall rammes ikke ekombransjens næringsinteresser. (Man kan se bort fra et privat kommersielt marked for filtre, fordi verken de som vil ha, eller de som ikke vil ha bildene, vil betale for filter.)

Avgjørelsene synes å kreve at man unnlater å samle på sluttbrukernes IP-adresser. Dette er naturlig i lys av prinsippet om formålsbestemthet: Filteret skal blokkere, ikke brukes til oppsporing. Myndighetenes oppdrag til teknologene må være å designe et filter som er slik at akkumulering av IP-adresser avskjæres. I tillegg må det føres kontroll med at designkravet overholdes. I så fall synes ikke forbudet mot overvåking å være til hinder for datafiltrering.

4.2.3 En positiv forpliktelse til å filtrere

Forutsatt at det er adgang til filtrering, burde ikke myndighetene gjøre dette? Etter mitt syn kommer statens positive forpliktelse til å sikre borgernes respekt for privat liv, jf. EMK artikkel 8 og artikkel 1, inn her med full tyngde. Ifølge doktrinen har staten ikke bare en plikt til å avstå fra selv å gjøre inngrep i konvensjonsrettighetene, staten plikter også å opptre aktivt for å sikre rettighetene for sine borgere. EMD understreker hyppig at EMK skal «guarantee not rights that are theoretical or illusory but rights that are practical and effective».[23] Det innebærer også vern mot krenkelse fra andre borgere. Doktrinen gjelder generelt, men i forhold til barn står den særlig sterkt, se blant annet den nevnte K.*U. mot Finland*, *M.C. mot Bulgaria* dom 4. desember 2003 og *X og Y mot Nederland* dom 26. mars 1985. Forpliktelsen er derfor særlig aktuell for overgrepsbilder.

EMD har understreket at de tekniske utviklingstrekk som ligger til grunn for økosystemeffekten gjør personvernet særlig sårbart. I «von Hannover-dommen» uttalte EMD at

> «increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data.»[24]

Domstolen hadde uttrykt dette synet mange ganger før, men da i saker som gjaldt statens inngrep i personvernet ved bruk av overvåking.[25] I «von Hannover» gjaldt spørsmålet individets rett til personvern kontra private mediehus' rett til å publisere artikler med omtale av personens privatliv. Hensynet til de tekniske utviklingstrekk bidro til at ytringsfriheten i denne saken måtte vike for personvernet. Nettopp det at private opplysninger lagres, reproduseres og gjøres søkbare («to store and reproduce personal data») medfører varig krenkelse og tilsier iverksettelse av positive tiltak fra statens side for å sikre personvernet.

Ifølge EMDs praksis må visse vilkår være oppfylt for å utløse handlingsplikten. De kommer i tillegg til en konstatering av at retten til privat liv ellers krenkes. For det første må

---

[22] EMDs avgjørelser er relevant i forhold til ekomdirektivet, jf. EUs Charter og TEU som integrerer EMK i EU-retten. Både «Scarlet» og «Netlog» viser til EMK.

[23] Her er det sitert fra *Artico mot Italia*, dom 13. mai 1980 (avsnitt 33).

[24] *Von Hannover mot Tyskland*, dom 24. juni 2004 (avsnitt 70).

[25] *Amann mot Sveits* dom 16. februar 2000 (avsnitt 65-67); *Rotaru mot Romania* dom 4. mai 2000 (avsnitt 43–44); *P.G. og J.H. mot Storbritannia* dom 25. september 2001 (avsnitt 57–60) mfl.

krenkelsen være forutsigbar slik at det er mulig å treffe mottiltak, og tiltaket må ikke være urimelig byrdefullt for staten. Tiltaket må heller ikke ramme rettssikkerheten eller andre borgeres grunnleggende rettigheter.

I det foreliggende tilfellet synes ingen av disse vilkårene å gjøre seg gjeldende; problemet er velkjent, standardisert og kan håndteres ved bruk av kjent teknologi. Alternative virkemidler står ikke til rådighet.

At problemet er velkjent, behøver ikke nærmere begrunnelse. Problemet er standardisert fordi krenkelsen skjer ved spredning av dubletter. Har man identifisert én, kan man blokkere alle. Og teknologien er kjent fordi den er den samme som datasikkerhetsbransjen har brukt i alle år for å filtrere «malware». Filtreringen er presis og rammer ikke lovlige ytringer.

Filtrering har begrensninger, det er ikke et «vidundermiddel» som løser problemet i sin helhet. Men dette er heller ikke et vilkår for plikten til å ta tiltaket i bruk. Det er tilstrekkelig at tiltaket er rimelig effektivt. Som man forstår, kan bare kjente bilder blokkeres, fordi bilder som ikke ligger i databasen ikke fanges opp. Det er også tenkelig at filteret kan omgås av kriminelle. Men nær sagt ethvert tiltak er sårbart for omgåelse, så innvendingen kan ikke legitimere at man helt unnlater å sette inn tiltak som er rimelig effektive. Blokkering hever terskelen for spredning og anskaffelse, og er det mest presise tiltaket som kan settes inn. Det er også det eneste tiltaket som virker på fildeling hvor størstedelen av distribusjonen skjer. Rettsikkerhetsgarantier overholdes (se nedenfor) og personvernet til andre internettbrukere respekteres (jf. ovenfor), og samlet sett gir dette god støtte for å konkludere med en positiv plikt til å filtrere.

4.2.4 Hjemmel for filtrering

Siste spørsmål er om filtrering utløser behov for nye lovregler? Etter mitt syn er svaret negativt fordi hjemmel finnes i gjeldende bestemmelser om inndragning av «ting», jf. straffeloven 1902 § 35.[26] Med rettsapparatets hjelp kan påtalemyndigheten inndra integritetskrenkende datafiler og fullbyrde inndragningen ved filtrering av dublettene i nettet. Rettsapparatet kan bygge opp en fullbyrdelsesdatabase med inndratte filer som brukes som «match» mot dublettene i nettet. SOMB-databasen ved Kripos er et godt utgangspunkt for en fullbyrdelsesdatabase. På denne måten implementeres gjeldende rett i en digital kontekst hvor rettshåndhevelse er nødvendig slik som på andre samfunnsarenaer.[27] Samtidig ivaretas rettssikkerhetsgarantier i form av domstolskontroll og kontradiksjon.

4.3 En rett til å bli glemt

Nettverksteknologien har gitt foranledning til nye tanker om personvernets innhold, nemlig den såkalte «retten til å bli glemt». I boken *Delete: The Virtue of Forgetting in the Digital Age* (2011) gir Viktor Mayer-Schonberger et filosofisk forsvar for retten til å bli glemt.

Hans fundamentale argument er at den tekniske og økonomiske utvikling bryter mot biologiske og dypt forankrede sosiokulturelle mekanismer. I motsetning til tidligere, er det blitt lønnsomt å lagre *alle* data, og stadig mer lagres fordi stadig mer informasjon digitaliseres og tilgjengeliggjøres. Dermed er Internett blitt en gigantisk «kollektiv hukommelse». Dette

---

[26] Se Rt. 2011 s. 296 (avsnitt 24) om beslag i data («ting») og straffeloven 2005 § 69 annet ledd som presiserer at «som ting regnes også elektronisk lagret informasjon». Dette er gjeldende rett, jf. Ot.prp. nr. 90 (2003–2004) s. 347. Mer generelt oppfyller data alminnelige kriterier for ting; de kan individualiseres, spesifiseres, konkretiseres og kontrolleres, se Sunde, *Automatisert Inndragning,* kapittel 6–10.

[27] Den nærmere fremgangsmåte er belyst i Sunde, *Automatisert Inndragning*. Se også Inger Marie Sunde, «Automatisert rettshåndhevelse på nettet», *Nordisk Tidsskrift for Kriminalvidenskab* 3/11 s. 245–264.

strider mot menneskets natur som er innrettet på at hukommelsen svekkes over tid, noe som har mange fordeler. Ved at minnet svekkes, eller i det minste overskygges av nye minner, kan strid lettere bilegges og man kan komme over sorg og tap («tiden leger alle sår»). Sosialt er det heller ikke vel ansett «å rippe opp i» gamle skandaler, og individet får nye muligheter når «et glemselens slør» legges over eldre eskapader. Også samfunnet er tjent med dette.

Retten til å bli glemt er tematisert i EUs forslag til revidert personopplysningsregulering.[28] Artikkel 17 gjelder «Right to be forgotten and to erasure», og effektiviserer datasubjektets krav på sletting av personopplysninger ved bruk av digitale tjenester.

Mer generelt er retten til å bli glemt aktualisert av et problem som kalles «dekontekstualisering», nemlig at private opplysninger brukes utenfor sin opprinnelige sammenheng. Mayer-Schonberger viser til et tilfelle hvor en kvinne på 25 år ble nektet stilling som lærer fordi hun ble ansett som en dårlig «rollemodell» for elevene. Begrunnelsen var at et privat bilde på MySpace som den potensielle arbeidsgiver hadde søkt opp, viste henne med partyhatt og en festlig drink i hånden.

Et annet eksempel er lokalpolitikeren som la ut sin private mening om vinneren av den norske MGP-finalen på Facebook:

> «Gi meg samer, isbjørner og moskuser. Jeg synes det er det vi skal selge, og ikke at vi har åpne asylmottak!»

Problemet var at MGP-vinneren hadde afrikansk bakgrunn, og ytringen ble raskt kritisert i riksmedia som rasistisk. Lokalpolitikeren ble ikke hørt med at ytringen var en spøk som verken var alvorlig ment eller beregnet på offentligheten, og hun ble kastet ut av politikken.[29] Innholdet lever videre på nettet fordi det stadig er søkbart, og spørsmålet er om man behøver å finne seg i at opplysninger blir varig tilgjengelige for enhver?

Nærmere ettersyn viser at «retten til å bli glemt» er et komplekst tema. Et spørsmål er om det bare gjelder dekontekstualisering, eller er det koblet til tid, slik at personvernet på et tidspunkt trumfer ytringsfriheten?

Foreldelsesreglene kan ses som utslag av et slikt temporært betinget vern under synsvinkelen at integritetsvernet ikke bare gjelder den man *er*, men også det man *har gjort,* for eksempel å stifte gjeld eller begå lovbrudd. Begge deler kan foreldes. Nettopp slike forhold ble tatt i betraktning i Rt. 1952 s. 1217 (To mistenkelig personer), hvor Høyesterett ga personvernet forrang fremfor ytringsfrihet og næringsinteresser. Filmen som ble stanset, gjaldt et gammelt drap. Den ene drapsmannen levde fortsatt, hadde sonet sin straff og startet et nytt liv med kone og barn. Visning av filmen ville lede til stor belastning fordi hans fortid ville bli kjent. Høyesterett nevnte nettopp «det glemselens slør» som man kan innrette seg etter når forhold er oppgjort. Dommen kan altså leses som et uttrykk for retten til å bli glemt, som under gitte omstendigheter trumfer en ellers lovlig ytring. Også personvernrettslige regler om formålsbestemthet og sletting av data kan ses som utslag av en slik rett.

En annen mulig tilnærming er at vernet gjelder et saklighetskrav, for eksempel som en skranke mot at private opplysninger fra nettet anses som gyldig beslutningsgrunnlag ved ansettelser.

Før man går for dypt inn i overveielser av om det gjelder en rett til å bli glemt, bør man stille spørsmål om hvordan en slik rett skulle kunne effektiviseres, gitt at man fant egnede

---

[28] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 25.1.2012. Com (2012) 11 final.

[29] http://politisk.tv2.no/nyheter/vraket-h%C3%B8yre-varaordf%C3%B8rer-etter-habahaba-utsagn/(besøkt 3.1.12).

kriterier. Den foreslåtte EU-regulering er utilstrekkelig i og med at den retter seg mot den behandlingsansvarlige og i mindre grad forholder seg til økosystemeffekten. Men to andre tiltak har vært foreslått:

Det ene er å innføre restriksjoner på søketjenester, slik at de ikke lenger skal kunne indeksere og gjøre privatpersoners navn søkbare.[30] Informasjonen fjernes ikke fra nettet, men muligheten til å finne frem til den uten å ha en personlig relasjon til vedkommende som har lagt den ut, reduseres vesentlig. Dekontekstualiseringsproblemet blir mindre fordi informasjonen i større grad blir forbeholdt individer som også har annen oppdatert kunnskap om personen.

Et annet forslag er å innføre utløpsdato på data, for eksempel i form av en dialogboks som gir brukeren valgmuligheter i spennet fra ikke å lagre til å lagre i 10 år. Utløpsdatoen er metainformasjon som medfører at dataene sletter seg selv på angitt tidspunkt. Dette skjer for alle instanser av dataene, dvs. både for originalfilen og dublettene.[31]

Man kan si at en slik råderett over data er en naturlig del av eierbeføyelsene over data. En eier har rett til å ødelegge sin eiendel, noe som for data kan innebære en rett til å slette dem. På den annen side synes konsekvensene av å innføre utløpsdato å være nokså uoverskuelige og forslaget innbyr til debatt. Jeg nøyer meg derfor bare med å nevne muligheten her.

4.4 Fotoforbud

I norsk rett har man nokså ensidig konsentrert seg om den avbildetes kontroll med *publisering* av personfoto, dvs. at samtykke må innhentes før publisering, jf. åvl. § 45 c. Men gitt at kamerafunksjon er integrert i mobiltelefonen med umiddelbar overføringsfunksjonalitet til sosiale medier, synes det lovfestede vernets innslagspunkt å være for sent til å være effektivt. Kontrollmuligheten er tapt når bildet er tatt. Til forskjell fra enkelte andre kulturer, har man i Norge ikke tradisjon for å spørre om tillatelse til å ta et personfoto. I Norge har man da også uhemmet fotografering (og filming) i nær sagt enhver sammenheng, og det uten at gamle begrensninger som maksimalt bildeantall og fremkallingskostnader gjør seg gjeldende.

Et fotoforbud ville markere at det å ta et personfoto griper inn i den personlige integritet. Det er inngripende fordi man «fryser» en situasjon med en identifiserbar person og overtar den reelle kontrollen med om og hvordan hendelsen formidles. Fotografen har et overtak på den avbildete som det ikke er rimelig å få uten samtykke.

Praksis viser at overtaket blir misbrukt. Et meget grovt eksempel er menns misbruk av sosiale medier til å manipulere ungjenter til å sende nakenbilder via webcam eller mms. Når vedkommende først har bildene, brukes de som pressmiddel for å få piken til å utføre seksuelle handlinger med seg selv. Trusselen går ut på at nakenbildene ellers vil bli spredt på Facebook. På den måten kan hele ungdomstiden legges i grus og offeret påføres psykiske skader. Se et eksempel i Rt. 2009 s. 140, som riktignok ikke innebar trusler, men manipulasjon, av en mann i 30 årene som utga seg for å være «Stian» på 15 år og skaffet seg slike bilder fra jenter helt ned i 12-årsalderen. Med tanke på at sosiale medier er en viktig del av ungdommens virkelighet, sier det seg selv at offerets verdensbilde kollapser når hun finner ut at den kjekke kjæresten var en (for henne) gammel mann som kynisk utnyttet henne. Og at han delte bilder og webcam-opplevelser med pedofile venner. Saken viser, blant mye annet, behovet for å innskjerpe respekten for personlig integritet, noe et fotoforbud kan bidra til. Forbudet bør selvsagt ikke bare gjelde den som tar bildet, men også den som bevirker at offeret tar bildet. Med dagens toveisteknologi kan det komme ut på ett. Ytterligere bør man vurdere å skjerpe strafferammen for straffeloven 1902 § 200 som rammer forledelse av noen

[30] Gisle Hannemyr i A-magasinets oppslag «Fritt vilt» i nr. 44, 4. november 2011.
[31] Mayer-Schonberger lanserer dette forslaget i *Delete*.

til å foreta seksualiserte handlinger med seg selv, slik at den blir på linje med voldtektsbestemmelsens.

Mange flere grunner kan anføres for et fotoforbud, for eksempel å få bukt med «happy slapping», som er voldelige overfall utført for å filme det og legge opptaket ut på YouTube. Dessuten ville det ramme tilfeller hvor menn doper kvinner og fotograferer dem i avkledt bevisstløs tilstand, slik som i Rt. 2000 s. 40. Et spørsmål her gjaldt inndragning av bilder hvor ofrene var ukjent. Bildene var av en slik karakter at ofrene utvilsomt ikke hadde samtykket til publisering dersom de hadde vært konfrontert med dem. Situasjonen tilsier at fotograferingen var et overgrep og at bildene automatisk burde blitt inndratt og destruert. I stedet måtte Høyesterett foreta en vurdering av om inndragning var nødvendig, jf. lovens krav om «fare for at [bildene] ville bli benyttet til en straffbar handling» (spredning), se straffeloven 1902 § 37 b. En slik rettstilstand er lite tilfredsstillende.

Personvernkommisjonen konkluderte med at det ikke er behov for et fotoforbud.[32] Et blikk over kjølen gir imidlertid grunn til refleksjon, for der har man nemlig innført fotoforbud, og det etter en mye bredere og grundigere utredning enn i Norge. Forbudet står i brottsbalken 4 kap., 4 b §, jf. 6 a § andra meningen, og setter straff for den som fotograferer på «et sätt som är påträngande» uansett hvor fotograferingen foregår og om det skjer skjult eller åpent. Behovet begrunnes blant annet i statens positive forpliktelse til å effektivisere personvernet, jf. EMK artikkel 8.[33] Et fotoforbud må selvsagt ta hensyn til mange kryssende interesser, ikke minst journalistiske. Men i lys av behovet og den svenske løsningen synes norske myndigheter å ha grunn til å se nærmere på spørsmålet.

5 Avslutning

Økosystemeffekten skaper utfordringer som krever en reformulering av personvernets innhold. Videre må man undersøke hvordan personvernet kan håndheves i digital kontekst slik at den blir mer enn en rettighet på papiret. Et stykke på vei er virkningene for personvernet en konsekvens av individets egen nettbruk og det kan nok diskuteres hvor langt rettsordenen bør gå for å verne individer mot seg selv. Men i artikkelen har jeg søkt å drøfte problemstillinger som er en forutsigbar følge av dagens nettbruk. Denne bruken bør kunne skje i trygge digitale omgivelser, noe som krever bevissthet om personvernets rekkevidde og rettsordenens støtte.

[32] NOU 2009: 1 s. 121–122.
[33] Ds 2011: 1 Olovlig fotografering s. 17.