Overvåkning og personvern – om innsynsrett i teori og praksis

av Stine Bergersen

Den omfangsrike praksisen med innsamling, lagring, behandling og deling av personopplysninger, skjer ikke alltid på en slik måte at den personen opplysningene omhandler legger merke til det, eller ved at vedkommende gir sitt aktive og kompetente samtykke. Ved å ta utgangspunkt i et bredt overvåkningsbegrep, som inkluderer alle former for systematisk innhenting og behandling av personopplysninger, viser denne artikkelen hvordan en aktiv hevdelse av retten til innsyn i disse opplysningene kan fungere som en motreaksjon mot overvåkningen. Tross lovmessig innsynsrett, tyder imidlertid funnene fra en norsk casestudie på at praktiseringen av denne retten byr på en rekke utfordringer, noe som bidrar til å svekke effekten av en sentral rettighet for beskyttelse av personvernet.

Vi deler våre personlige opplysninger med andre hver dag. Dette skjer aktivt og bevisst ved at vi frivillig deler informasjon om oss selv gjennom for eksempel sosiale medier, men også passivt og ubevisst, for eksempel ved at opplysninger knyttet til vår finansielle profil anvendes på måter vi ikke er klar over, eller at vi skriver under på noe med uklare retningslinjer. I sum genererer denne informasjonsdelingen store mengder data som i ulik grad kan knyttes direkte til oss som individer. Denne rikholdige datamengden er i beste fall uklar, fremstår i verste fall som usynlig for individet, og ens bidrag til de ulike databasene skjer uten at en nødvendigvis er klar over det. For flere aktører er denne størrelsen, eller deler av den, av uvurderlig betydning. Dette gjelder for eksempel for kommersielle aktører, som på ulike måter kan tjene på selektiv markedsføring, på at våre bevegelser følges av overvåkningskameraer eller at vår oppførsel online overvåkes, lagres, indekseres og analyseres.

Det er flere betenkelige og problematiske sider ved denne utviklingen

knyttet til personvernets stilling, en stilling som utfordres av digitalisering og bruk av ny teknologi. Noen eksempler er muligheten for uheldige (fremtidige) krysskoblinger mellom ulike databaser, den til dels innebygde forkjøpslogikken knyttet til overvåkningens ønskede effekt, og økt og ny sårbarhet for både individ og samfunn. I tillegg er det risiko for at lovverket i fremtiden endres slik at kravene for tilgang til databasene senkes eller at antall tillatte metoder for datainnsamling øker.[1] Nok et eksempel kan være at det er vanskelig for individet, både som passiv og aktiv bidragsyter til databasene, å få oversikt over denne datainnsamlingen. For eksempel hvordan ens personlige opplysninger brukes, hvem de deles med, og hvordan en kan få slettet eller endret opplysninger som er uriktige eller irrelevante. Dette problemet ble nylig aktualisert da en avgjørelse i EU-domstolen slo fast at en søkemotor er ansvarlig for behandlingen av personopplysninger som fremstår på websider publisert av tredjeparter, i den såkalte «The right to be forgotten»-saken (Court of Justice of the European Union 2014). Siden mai 2014 har Google mottatt over 160 000 forespørsler om sletting av irrelevante, utdaterte, overflødige eller uriktige personopplysninger, noe som indikerer at kontroll over ens digitale spor er en aktuell utfordring (Google 2014).

Ivaretakelse av personvernet

Personvern er en menneskerett definert i Artikkel 8 i den europeiske menneskerettskonvensjonen (inkorporert i norsk lov gjennom menneskerettsloven av 21. mai 1999), implementert i lovgivning på europeisk nivå gjennom EUs personverndirektiv (Direktiv 95/46EC) og regulert nasjonalt av personopplysningloven og personopplysningsforskriften. Den individuelle retten til innsyn i de av dine personopplysninger som ulike organisasjoner og institusjoner lagrer og behandler, reguleres i Norge først og fremst av personopplysningsloven § 18.[2] Denne loven har i grunnleggende forstand som mål å beskytte oss mot å få personvernet krenket. Samtidig kan noen rettigheter knyttet til denne loven bidra til å skape bevissthet rundt overvåkningspraksiser, og kanskje kan praktiseringen av disse fungere som en slags motreaksjon mot overvåkningen. Innsynsrett er et eksempel på en slik rettighet, men forsøk på å benytte retten til innsyn avdekker imidlertid vanskeligheter med muligheten for å etterleve denne i praksis. Utfordringene innebærer blant annet problemer med å sørge for at en innsynsbegjæring havner hos den behandlingsansvarlige,[3] og den mangelfulle responsen som ofte etterfølger en slik forespørsel.[4]

Artikkelens empiriske grunnlag er i stor grad hentet fra det EU-finansierte

forskningsprosjektet *Increasing Resilience in Surveillance Societies* (IRISS). Casestudier ble gjennomført i ti europeiske land og totalt ble 184 innsynsbegjæringer sendt til behandlingsansvarlige i ulike organisasjoner og institusjoner, både offentlige og private.[5] I Norge ble 15 innsynsbegjæringer sendt. Prosessen med å sende disse, samt responsen vi fikk eller ikke fikk, dannet det empiriske utgangspunktet for rapporten *Exercising democratic rights under surveillance regimes. Norway country reports* (Bellanova mfl. 2014).[6] Selv om størrelsen på det norske utvalget er begrenset, kan det likevel, og særlig fordi resultatene i rimelig stor grad samsvarer med de andre europeiske casestudiene, fungere som en indikator på hva slags typer vanskeligheter en kan støte på i forsøket på å benytte seg av retten til innsyn og hvordan disse kan forklares.

Et bredt overvåkningsbegrep

Begrepet overvåkning assosieres kanskje mest intuitivt med videoovervåkning, men denne artikkelen, samt det empiriske utgangspunktet for den, tar utgangspunkt i en bredere tilnærming til begrepet, der *alle* former for systematisk innhenting og behandling av personopplysninger, være seg videoovervåkningsopptak eller informasjon om et kundeforhold, faller inn. David Lyons (2001) definisjon av overvåkning rommer for eksempel all innsamling og behandling av personopplysninger (uavhengig av om opplysningene gjør deg identifiserbar eller ikke) som har til formål å påvirke eller administrere de individer dataene er innsamlet fra.[7] En slik definisjon vil dermed også romme praksiser som kanskje ikke tradisjonelt assosieres med overvåkning, for eksempel kredittopplysningspraksis.[8] Dette eksempelet kan samtidig illustrere en motreaksjon mot overvåkningen, eller en strategi for å unnslippe denne.

Kredittopplysningsvirksomhet som overvåkningspraksis

Praksisen med kredittopplysning kan defineres som en type sosial sortering tilrettelagt av teknologi som sorterer statistiske mengder og appliserer en algoritme, for å avgjøre hvem som skal og ikke skal innvilges bestemte muligheter (Lyon 2002). Følger vi Lyons definisjon av overvåkning kan kredittopplysning beskrives som en tilsynelatende triviell og ukontroversiell, men likevel omfattende form for overvåkning. Det er en kjent mekanikk for de fleste nordmenn som må forholde seg til de aspekter som økonomiske interaksjoner med et kredittelement innebærer på flere tidspunkt gjennom livet. For at et kredittvurderingsbyrå skal kunne vurdere kredittverdighet eller betalingsevne hos et individ

forutsettes et saklig behov.[9] Her henger personvern og kredittopplysning sammen, blant annet fordi Datatilsynet både fungerer som tilsynsorgan, klageinstans, og utsteder av konsesjonen som kreves for å kunne bedrive kredittopplysningspraksis.[10]

Å velge vekk overvåkningen

For å unngå overvåkning fra kredittopplysningsbyråer er en strategi å be samtlige av disse byråene sette opp en såkalt kredittsperre på den det gjelder.[11] Implikasjonene ved å sette opp en slik sperre frivillig, eller ved ikke å bli funnet kredittverdig, vil komplisere deltakelse på en rekke finansielle arenaer (i prinsippet alle handlinger som innebærer etterskuddsvis betaling), og i ytterste konsekvens ekskludere individet fra disse (Ball mfl. 2014). Å sette opp en kredittsperre kan også medføre sosiale kostnader, særlig hvis vi tar i betraktning det Gandy (2009) kaller «kumulative ulemper», noe som innebærer at ett ugunstig utfall av en sosial sortering, slik som en dårlig kredittscore, ikke nødvendigvis betyr så mye, men at det kan ta tid å bli kvitt konsekvensene fordi man kanskje må ty til andre løsninger på ens økonomiske utfordringer.[12] Frivillige kredittsperrer bunner sjelden i en kunnskap om, eller i en holdning til overvåkningen (og kan således ikke anses som en bevisst motreaksjon), men fungerer heller som en selvdisiplineringsstrategi for individer i vanskelige økonomiske situasjoner. Verdt å merke seg er likevel at konsekvensene av å velge vekk overvåkningen, uavhengig av motivasjonen som ligger bak, i praksis innskrenker friheten for individet ved at den kompliserer eller reduserer mulighetene for nokså hverdagslige handlinger.

Overvåkning begrunnes ofte med et sikkerhetsargument, men eksempelet med kredittopplysning viser at dette ikke er en nødvendig begrunnelse. Det store omfanget av, og mulighetene for, elektroniske offentlige registre, som i høy grad baseres på personopplysninger fra størsteparten av befolkningen, gjør at spørsmål om personvern bør høre til under denne diskursen. I noen tilfeller er det mulig å strekke seg langt for å unngå overvåkningen dersom en ønsker det, men dette er ikke alltid mulig eller særlig praktisk. En slags alternativ motreaksjon, som kan øke følelsen av kontroll over egne personopplysninger, er å benytte innsynsretten.

Innsynsrett i teorien

Europeisk og nasjonal lovgivning gir individet rett til å vite hvordan ens personlige data behandles av private og offentlige organisasjoner. I Norge reguleres denne innsynsretten i hovedsak av personopplysningloven § 18, og

innsyn skal gis vederlagsfritt innen 30 dager fra henvendelsen er mottatt av behandlingsansvarlig (personopplysningsloven § 16). Innsynsretten gjelder både «enhver som ber om det» og «den registrerte» i en konkret sammenheng. For «enhver som ber om det» (uavhengig av om vedkommende er registrert selv) innebærer denne rettigheten, på generelt grunnlag, for eksempel innsyn i hvor lenge personopplysninger lagres, hva som er formålet med behandlingen, hvor opplysningene hentes fra og om de vil bli utlevert til eventuelle tredjeparter. For «den registrerte» har en i tillegg til dette rett til å be om en beskrivelse av hvilke typer personopplysninger som behandles og i noen tilfeller sikkerhetstiltak knyttet til behandlingen.

I personopplysningsloven §§ 19-22 defineres behandlingsansvarliges informasjonsplikt overfor den registrerte. Denne informasjonsplikten omfatter for eksempel spesifikasjon av hvilke tredjeparter informasjonen eventuelt deles med, om det benyttes såkalte automatiserte avgjørelser i behandlingen,[13] og om avgjørelser tas på bakgrunn av personprofiler basert på analyser av adferd, preferanser, evner eller behov (noe som er særlig relevant i markedsføringssammenheng). Når det gjelder videoovervåkning, krever for eksempel loven at all overvåkning skal merkes tydelig slik at alle som blir berørt får informasjon om denne, i henhold til § 40.[14] Denne plikten grunner både i den ønskelige preventive effekten overvåkningen skal ha, men også i at informasjon om at en overvåkes lettere skal nå frem til alle som beveger seg foran kameraet. Merkingen skal inneholde kontaktinformasjon til behandlingsansvarlig for overvåkningen, for eksempel et telefonnummer henvendelser kan rettes til. For andre behandlingsansvarlige som samler inn eller behandler personopplysninger skal tilsvarende informasjon gis i en personvernerklæring på nettsider eller lignende. De ovenfor nevnte rettigheter i personopplysningsloven, som i teorien skal bidra til åpenhet rundt informasjonsbehandling, indikerer en relativt bred tilgang til ens personlige data. Den praktiske tilgangen ser likevel ut til å være heftet med noen utfordringer og problemer.

Innsynsrett i praksis

Til tross for lovmessig innsynsrett i teorien, tyder imidlertid både den norske casestudien (Bellanova mfl. 2014) og den komparative europeiske analysen (Norris og L'Hoiry 2014) i IRISS på at det som skulle vært en relativ enkel og ukomplisert prosess, i praksis viser seg å være en såpass kompleks, forvirrende og frustrerende fremgangsmåte at den ikke kan sies å være særlig vellykket. Den europeiske studien, som undersøkte

327 individuelle tilfeller av innsamling av data fra både offentlige og private organisasjoner i ti europeiske land, viser en gjennomgående lite tilfredsstillende praksis når det kommer til å gi innsyn i hva disse organisasjonene og institusjonene faktisk vet om deg. De ulike organisasjonene ble valgt fordi de representerer ulike tilfeller der alminnelige borgere møtes av overvåkningsmekanismer på daglig basis. Dette var blant annet organisasjoner og institusjoner som har å gjøre med helse, transport, arbeidsliv, utdanning, finans, kommunikasjon, sikkerhet og rettsvesen. Personopplysningene vi ba om innsyn i ble samlet inn ved hjelp av ulike overvåkningsmekanismer og fantes både i form av videoovervåkningsopptak, digitale arkiver og informasjon på papir. Noen eksempler er informasjon om et kundeforhold (herunder opplysninger knyttet til medlemskap i en kundeklubb som innebar bruk av et lojalitetskort), personopplysninger fra offentlige registre, videoovervåkningsopptak fra både offentlige og private rom, og personopplysninger innsamlet og behandlet av multinasjonale selskaper som Facebook, Microsoft og Google.

Første steg på veien mot å få innsyn i ens egne personopplysninger er å lokalisere den aktuelle behandlingsansvarlige som innsynsbegjæringen skal rettes til. Våre undersøkelser viser at en allerede her risikerer å møte på store problemer, for eksempel ettersom skiltingen som skal opplyse om at videoovervåkning foregår, og om hvem som er ansvarlig for denne, ofte er fraværende eller mangelfull. I totalt 27 % av tilfellene i Norge var kontaktinfo til behandlingsansvarlig ikke mulig å finne på første forsøk (Bellanova mfl. 2014). For den europeiske komparative analysen gjaldt dette i 20 % av tilfellene (Norris og L'Hoiry 2014). Dersom man likevel lykkes i å lokalisere behandlingsansvarlige, tyder våre erfaringer på at man kan forvente å møte et vidt spenn av større eller mindre utfordringer med å få innsyn. I noen tilfeller møtte vi full fornektelse fra mottaker av innsynsbegjæringen om at en slik rett til innsyn eksisterer. I andre tilfeller endte den registrerte opp med å gi fra seg *mer* personlig informasjon (slik som en kopi av en faktura sendt til din bostedsadresse og kopi av pass eller førerkort) for å etterleve krav om å bekrefte sin identitet før informasjonen kunne gjøres tilgjengelig. Hva angår beskyttelse av personvernet kan slike verifiseringskrav i teorien styrke personvernets stilling ved at det bidrar til å unngå falske positiver og uautorisert innsyn, men slik vi erfarte risikerer man i praksis å ende opp i en verre situasjon enn det en i utgangspunktet var i, all den tid en slik verifisering ikke etterfølges av innsyn. I ett tilfelle hørte vi aldri

mer fra behandlingsansvarlig etter at en slik verifisering hadde skjedd, og vi fikk ikke vite hva som skjedde med vår innsendte kopi av pass og strømregning, eller hvordan *disse* personlige opplysningene ble behandlet.

Andre faktorer som hindret oss innsyn var påstander om at kun politiet har tilgang til den innsamlede informasjonen, og at denne kun ville bli utlevert ved en kriminell hendelse. I de fleste tilfeller ble vår henvendelse møtt med en rekke spørsmål tilbake, for eksempel om vi kom fra politiet, om det hadde skjedd noe kriminelt, hva vi skulle med opplysningene, eller hva som lå til grunn for vår nysgjerrighet. Dette gjaldt særlig i tilfeller da vi så oss nødt til å møte opp i levende live for å for eksempel få greie på hvilke overvåkningskameraer som tilhørte hvilke aktører, og hvem som var ansvarlige for dem. Når det gjelder dette siste, spørsmålet om bakenforliggende motivasjon, krever ikke loven at dette redegjøres for. Retten til innsyn gjelder, som tidligere nevnt, «enhver som ber om det» (personopplysningsloven § 18), og i vår sammenheng hadde vi i tillegg rettighetene til «den registrerte» (personopplysningsloven § 18, andre ledd), noe som innebar noe mer enn innsyn i de generelle rutiner for behandling av personopplysninger. I de tilfeller der vi ble møtt med en slik forespørsel tilbake, informerte vi om at motivasjonen simpelthen grunnet i et ønske om å ta i bruk den lovregulerte retten til beskyttelse av våre egne personopplysninger. Dette var i minst ett tilfelle ikke nok til at vi fikk innvilget innsyn. I de tilfellene vi rettet skriftlige henvendelser til behandlingsansvarlige, var et gjentakende problem at ansvarsfordelingen opplevdes som uavklart, og at administrasjonen og beredskapen for å ta i mot en slik henvendelse ikke var til stede. Noen skjønte ikke spørsmålet, andre sa rett ut at det ikke fantes noen i deres organisasjon som jobbet med denne typen spørsmål, og ved telefonisk kontakt ble røret i ett tilfelle lagt på med beskjed om at de hadde «viktigere ting å gjøre».[15]

Slike administrative problemer kan tolkes som en indikasjon på at denne typen spørsmål verken er spesielt vanlige eller har blitt gitt særlig prioritet. Resultatet var både forvirring og forsinkelser, og ofte var informasjonen vi fikk tilgang til mangelfull og lite spesifikk, eller den viste seg å ikke være annet enn utklipp fra personvernerklæringene som allerede lå tilgjengelige på nettsidene eller lignende. Dette gjaldt særlig henvendelser til multinasjonale selskaper som ofte tilbød ferdige maler for innsynsbegjæringer, noe som kan være en god administrativ strategi, men som i praksis ikke nødvendigvis legger til rette for verken

omfanget eller detaljrikdommen i informasjonen behandlingsansvarlige trenger for å kunne innfri innsyn.[16] Dette gjelder særlig ved videoovervåkning, der nøyaktig informasjon er viktig for at behandlingsansvarlige skal kunne finne frem til riktige bilder.

Andre utfordringer vi møtte på var at behandlingsansvarlige unnlot å svare på spesifikke forespørsler om personopplysningene deles med tredjeparter, og i tilfelle eksakt hvilke, samt om automatiserte avgjørelser benyttes. Ønsket om innsyn i eventuell tredjepartsdeling og bruk av automatiserte avgjørelser ble fremsatt i samtlige innsynsbegjæringer vi sendte, men i all hovedsak var responsen vi fikk på disse spørsmålene ikke tilstrekkelig spesifikk. I minst ett tilfelle tok det et tosifret antall utvekslinger, ved hjelp av både e-post, faks og utfylling av elektroniske skjema, uten at vi endte opp med tilfredsstillende svar på disse to punktene. Å investere slike mengder tid og arbeid i en innsynsbegjæring synes nok urimelig for de fleste, og vil neppe friste til gjentakelse. Rutiner for hvordan en innsynsbegjæring skal behandles burde eksistere i alle organisasjoner og institusjoner som behandler personopplysninger og burde samtidig inkludere det å legge til rette for oppfølgingsspørsmål siden dette kan være en kompleks prosess.

En annen problematisk faktor hadde å gjøre med den språklige og formmessige tilgjengeligheten i informasjonen. I de tilfeller der informasjon faktisk ble utlevert eller gjort tilgjengelig for oss, særlig fra internasjonale sosiale medier og tjenester der betydelige mengder metadata var inkludert,[17] førte manglende krav til hvilket format og grad av forståelighet denne skal ha til at informasjonen oppleves som til dels svært vanskelig å tolke for en som ikke har spesifikk IT-kompetanse. Et påfølgende problem blir da at det er umulig å vurdere om de utleverte opplysningene er å anse som komplette eller ikke. Dette gjelder både terminologi og selve formatet på informasjonen, men også språket. Til tross for at alle innsynsbegjæringene ble skrevet og sendt på norsk, fikk vi i minst fem tilfeller svar på engelsk (i et tilfelle undertegnet av en medarbeider med et norskklingende navn fra en norsk adresse). Engelsk respons på norske henvendelser er kanskje ikke i utgangspunktet et stort problem, men bruk av tekniske termer, nødvendigheten av å være presis og konkret, og en mulig forhøyning av terskelen for oppfølgingsspørsmål gjør at muligheten for misforståelser må kunne sies å øke, og at språk dermed kan være en forkludrende faktor.

Det finnes noen unntak fra innsynsretten, for eksempel dersom hemmelighold er nødvendig for ikke

å skade en pågående etterforskning (personopplysningsloven § 23), men i all alminnelighet skal denne tilgangen innfris innen 30 dager, og skje vederlagsfritt (personopplysningsloven § 16-17). Til tross for dette viste den europeiske komparative studien i IRISS, at data ikke ble gjort tilgjengelig, eller at det ble forklart hvorfor den ikke ble gjort tilgjengelig, i 43 % av tilfellene der en innsynsbegjæring ble sendt. I 31 % av de tilfeller der data ble gjort tilgjengelig eller utlevert, var informasjonen ufullstendig og krevde videre oppfølging, for eksempel fordi behandlingsansvarlige svarte «ja» på spørsmålet om våre personopplysninger deles med andre, men unnlot å spesifisere til hvem og hvordan (Norris og L'Hoiry 2014).

Når det gjelder videoovervåkning er en mulig forklaring på mangelfull eller manglende tilgjengeliggjøring av informasjon at de relevante data allerede var slettet. Dette ble trukket frem av noen av de norske behandlingsansvarlige og refererer til personopplysningsforskriften § 8-4 der det presiseres at videoopptak i all hovedsak skal slettes innen syv dager. I ett tilfelle i den norske casestudien fikk vi forklart at selv om opptakene ikke allerede hadde blitt slettet ville vi likevel ikke fått tilgang til disse fordi tredjeparter var synlige i bildet, noe som refererer til personopplysningsloven § 39. Dette kan være en akseptabel forklaring som tar hensyn til personvernet, men en løsning som kunne vært tilfredsstillende for begge parter er en enkel form for sensurering av eventuelle tredjeparter, slik det ble gjort i noen tilfeller i andre europeiske land som deltok i studien. Oppsummert ble resultatet av våre undersøkelser at under halvparten av de norske behandlingsansvarlige helt eller delvis ga oss tilgang til personopplysningene våre, og i den komparative europeiske studien ble hele 15 % av innsynsbegjæringene møtt med ingen respons overhodet.

Ingenting å skjule, ingenting å tape?

Innsynsretten kan i teorien bidra til å justere det ujevne maktforholdet mellom overvåker og overvåket. Det er flere grunner til at dette kan være viktig. Thon og Tennøe (2014a) peker på at vi står ved et veiskille for personvernet. På den ene siden har omfanget av, og ikke minst mulighetene for å bedrive overvåkning, aldri vært større. På den andre siden oppgir åtte av ti respondenter i Personvernundersøkelsen 2014 at godt personvern er en forutsetning for et fritt og demokratisk samfunn (Thon og Tennøe 2014b, s. 24), noe som impliserer at begrepet har en mening for de fleste, og at personvern er en verdi som må tas vare på. Personvernets aktualitet synliggjøres

også av engasjementet og oppmerksomheten rundt Edward Snowdens lekkasjer av mengdevis av dokumenter som viste omfanget av det amerikanske overvåknings- og etterretningsprogrammet PRISM, samt den nasjonale og internasjonale debatten rundt datalagringsdirektivet.

Personvernundersøkelsen, gjennomført av Datatilsynet og Teknologirådet (Thon og Tennøe 2014b,) peker imidlertid også på tendenser til det som kalles en generell nedkjølingseffekt i Norge etter Snowden- avsløringene, hvilket innebærer at vanlige borgere endrer sin «digitale oppførsel» på bakgrunn av frykt for hvordan opplysningene knyttet til den bestemte handlingen kan bli brukt senere. Dette betyr for eksempel at man unnlater å skrive under på et opprop, foreta et bestemt søk på nettet, eller at man tar en muntlig samtale i stedet for å kommunisere elektronisk (Thon og Tennøe 2014a). Til tross for at fravær av handling er betydelig vanskeligere å måle enn handling i seg selv, kan slike tendenser til nedkjølingseffekt tolkes i retning av å være en reaksjon på overvåkningen.

Den norske åpenheten trekkes frem i mange og ulike sammenhenger, og er i personvernsammenhenger tilstede i folks bevissthet under retorikk som «jeg har ingenting å skjule, overvåking er greit for meg». Til dels kan kanskje en tradisjon for nokså høy grad av tillitt til myndighetene forklare en slik passiv holdning til overvåkning, men når hele 45 % av respondentene i samme undersøkelse oppgir at selv om *all elektronisk kommunikasjon og aktivitet* overvåkes av myndighetene,[18] ville de fortsette som før (Thon og Tennøe 2014b, s. 31), kan det gi grunn til bekymringer. For eksempel fordi en så omfattende overvåkning av Internett som kanal og arena for meningsutveksling kunne hatt negative konsekvenser både for et levende og aktivt demokrati, men også for den digitale økonomien som ville kunnet lide under viten om at hver transaksjon lagres og indekseres av ulike myndigheter (ibid). I tillegg kan vi trekke inn mer klassiske rettssikkerhetskonsekvenser, som at den politiske målsettingen om samfunnsvern går på bekostning av ideen om den liberale, demokratiske rettsstat (Wessel-Aas 2011), undergravingen av rettsprinsippet om skjellig grunn til mistanke (Lomell 2011) og andre utfordringer ved forkjøpstanken som sikkerhetslogikk (Bye og Sjue 2008).

Personvernsundersøkelsen viser samtidig at 53 % av respondentene ser på seg selv som den som har størst innflytelse på hvordan personvernet blir ivaretatt (Thon og Tennøe 2014b). Hvordan kan så denne innflytelsen skje? Hvordan kan en som individ få større makt over egen situasjon? Prinsippet bak innsynretten kan være

en nøkkel for å gi individet tilbake en følelse av kontroll, og bidra til å korrigere for det skjeve forholdet mellom overvåker og overvåket. I tillegg kan innsynsretten, dersom den benyttes, fremtvinge noen nødvendige forbedringer når det gjelder administreringen av denne rettigheten i praksis.

Demokratiske verdier og personvern

De sentrale demokratiske verdiene sikkerhet og frihet omtales av og til som om de står i et slags avveiningsforhold til hverandre, der mer av det ene betyr mindre av det andre. Her er det lett å overse de kvalitative nyansene som ligger i de to begrepene. En akseptabel definisjon av begrepene må derfor romme den subjektive opplevelsen av sikkerhet og frihet, og den påvirkningen som leder til at begrepene med sin iboende forståelse formes, enten individuelt eller kollektivt. Uten denne nyanseringen kommer denne avveiningen til kort når den brukes som metode for å vurdere det ene begrepet opp mot det andre.

Likevel kan det være nyttig å anvende begrepene for å si noe om en tredje sentral verdi, personvern. Personvernet, friheten til å disponere ens egne personlige opplysninger, er for mange en viktig del av frihetsutøvelsen. Erkjennelsen av at det eksisterer en avveining mellom frihet og personvern fra myndighetenes side, har i den senere tid blitt aktualisert av for eksempel de tidligere nevnte Snowden-avsløringene i juni 2013. Ambisjonene om å beskytte vår frihet gjennom økte kontroll- og sikkerhetstiltak, slik retorikken særlig fremstår i den såkalte krigen mot terror, setter personvernet under press.

Et paradoksalt aspekt i dette er at både kontrollen og personvernet har beskyttelse av individet som mål, og at de verdier vi søker å beskytte mot uønskede handlinger, i virkeligheten står i fare for å svekkes eller undergraves av selve naturen ved de relevante beskyttelsesmekanismene. Det er kanskje her den egentlige avveiningen ligger: mellom personvernet og de kontrollmekanismene som truer det.

Prosess og innhold

Ved å rette oppmerksomheten mot en bred overvåkingsdefinisjon, og be om innsyn i personopplysninger som finnes i noen databaser som omfattes av denne definisjonen, er noe av det mest oppsiktsvekkende med denne studien at den avdekker hvor mye data om oss som faktisk finnes. I tillegg ble det tydelig for oss at opplysningene våre ikke er lett tilgjengelige, til tross for aktiv innsats for å få tak i den. Sett i sammenheng med at den norske lovgivningen gir rett til relativt stor grad av innsyn, og at Datatilsynet i europeisk sammenheng har en nokså viktig

rolle (Ball mfl. 2014), er den overordnede konklusjonen at den individuelle retten til innsyn (herunder også behandlingsansvarliges informasjonsplikt) ikke fungerer tilstrekkelig godt.

Både innsynsretten og informasjonsplikten bør gjennomgås, og spesielt viktig er det å gjøre en vurdering som både tar hensyn til det kvalitative innhold i de opplysninger som utleveres, og også de administrative rutinene for utlevering av opplysninger. Vår undersøkelse synliggjør et behov for å skille mellom systematiske utfordringer rundt selve prosessen med å be om innsyn og det kvalitative innholdet på den tilgjengeliggjorte informasjonen. Vi opplevde for eksempel tilfeller der de prosessuelle rutinene for innsyn i personopplysninger opplevdes som gode, men der kvaliteten på den informasjonen som utleveres ikke er god nok eller forståelig nok. God og komplett informasjon må med andre ord innebære at den er mulig å forstå for den registrerte. På den andre siden fant vi, til tross for til dels store vanskeligheter med å lokalisere behandlingsansvarlige og sørge for at innsynsbegjæringen havnet i de rette hender, at informasjonen som ble utlevert når de praktiske problemer først var løst, oppfylte alle krav. Prosess og innhold er med andre to aspekter som med fordel kan vurderes hver for seg, selv om de i praksis henger nøye sammen.

Potensiale

Et velfungerende juridisk og praktisk system, som på en uproblematisk, klar og effektiv måte tillater individer å få innsyn i sine personopplysninger, kan fungere som en slags beskyttelsesmekanisme eller motreaksjon mot overvåkning. Denne lovfestede rettigheten er særlig relevant all den tid det å unngå overvåkningen i stor grad er komplisert, upraktisk eller umulig. Å benytte seg av innsynsretten kan avdekke omfanget av ulike overvåkningspraksiser, bidra til bevisstgjøring rundt disse, og åpne for muligheten for å avdekke overtramp eller urettmessige sider ved overvåkningen. Prinsippet om retten til innsyn gir noe av makten tilbake til individet, og kan være med på å jevne ut det skjeve forholdet mellom overvåker og overvåket. Så lenge denne ordningen ikke fungerer, eller ikke fungerer spesielt tilfredsstillende, verken i norsk eller europeisk sammenheng, er den kanskje mer til skade enn til gagn, ved at den ytterligere kompliserer, frustrerer og til dels også tildekker en tilsynelatende irreversibel utvikling i overvåkingssamfunnet.

Artikkelen er fagfellevurdert.

Stine Bergersen er utdannet kriminolog fra Universitetet i Oslo, og jobber som forskningsassistent ved PRIO (Peace Research Institute Oslo).

NOTER

1 Et eksempel er telefonavlytting. De viktigste trekk ved telefonavlyttingens historie i Norge beskrives i NOU 2009:15: *Skjult informasjon - åpen kontroll*. Se for eksempel sidene 106-108. Tilgjengelig på: http://www.regjeringen.no/pages/2210108/PDFS/NOU200920090015000DDDPDFS.pdf

2 I følge Datatilsynets ordliste (tilgjengelig på: http://www.datatilsynet.no/verktoy-skjema/Ordbok-A-til-A/) er en personopplysning en opplysning eller en vurdering som kan knyttes til en enkeltperson. Dette kan være navn, adresse, bilder, telefonnummer eller fødselsdato.

3 I følge Datatilsynets ordliste (tilgjengelig på: http://www.datatilsynet.no/verktoy-skjema/Ordbok-A-til-A/) er en behandlingsansvarlig den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes. Dette er vanligvis en bedrift.

4 Innsynsbegjæringene vi sendte inneholdt all informasjon som behandlingsansvarlig trenger for å finne frem til den informasjonen vi etterspurte. For videoovervåkning kunne dette for eksempel være detaljerte beskrivelser av bevegelsesmønster og fysiske kjennetegn ved den registrerte. I tillegg inneholdt brevet helt konkrete spørsmål som en i følge personopplysningsloven har rett til å få informasjon om.

5 Norge, Storbritannia, Italia, Spania, Romania, Ungarn, Tyskland, Østerrike, Belgia og Slovakia.

6 Rapporten fra den norske casestudien utført av PRIO kan i sin helhet leses her: http://irissproject.eu/wp-content/uploads/2014/06/Norway-Composite-Reports-Final.pdf. Et sammendrag av den komparative europeiske rapporten er tilgjengelig her: http://irissproject.eu/wp-content/uploads/2014/06/IRISS-WP5-Executive-Summary-for-Press-Release.pdf

7 Min oversettelse. Lyon (2002, s. 2) definerer dette slik på originalspråket: «any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered».

8 En norsk casestudie som omhandlet kredittopplysningspraksis var også en del av IRISS- prosjektet. I likhet med casestudien om innsynsrett, ble norsk kredittopplysningspraksis undersøkt og analysert, og deretter sammenstilt i en europeisk komparativ rapport, der kredittopplysning, automatisk gjenkjennelse av bilskilt (ANPR), og Neighborhood Watch-ordningen var de fenomenene som ble undersøkt) (Ball, K. mfl. 2014). Rapporten kan i sin helhet leses her: http://irissproject.eu/wp-content/uploads/2014/06/D3.2-Surveillance-Impact-report1.pdf1.pdf

9 Praksisen reguleres gjennom personopplysningsforskriften. Alle som har, eller har hatt, skattbar inntekt i Norge bidrar til denne databasen som blant annet henter data fra Brønnøysundregistrene, skattelistene og Norsk Lysningsblad. Ordlyden i personopplysningsforskriften § 4-3 er relativt vag, da «saklig behov» ikke konkretiseres ytterligere. Dette etterlater i siste instans tilgangen til denne typen overvåkning relativt åpen, da det er opp til den som bestiller kredittopplysningen å gjøre denne vurderingen, og ikke nødvendigvis virksomhetene med konsesjon.

10 I tillegg ble det første spadetaket som førte til implementeringen av personregisterloven i 1978

(som også inkluderte retten til innsyn), utløst av bekymringer for utviklingen knyttet til de nye mulighetene for elektronisk databehandling, særlig i kredittsektoren, og kreditt fortsatte å spille en viktig rolle i som premissleverandør i utviklingen av lovverket.

11 Datatilsynet (2013) tilbyr en guide til dette på sine hjemmesider: http://www.datatilsynet.no/Sektor/Kreditt-finans-forsikring/Hvordan-sperre-for-kredittvurdering/

12 I Storbritannia har for eksempel såkalte «pay-day loans» skapt store kontroverser (Ball mfl. 2014). Dette er en kommersiell finansiell tjeneste der en ved noen få tastetrykk kan låne penger til en veldig høy rente. Dette tilbudet er først og fremst rettet mot, og benyttet av, individer som ikke er kredittverdige i tradisjonell forstand og via tradisjonelle kanaler. Selv om disse lånene er enkle å få, er de økonomiske konsekvensene store dersom en ikke betaler i tide. I tillegg kommer skjulte implikasjoner, som det paradoksale faktum at å ta opp et slikt lån, i tur har negativ innvirkning på ens kredittscore (Ball mfl. 2014).

13 Automatiske avgjørelser refererer til personopplysningsloven § 22, og er betegnelsen på en avgjørelse som fullt ut er basert på automatisk behandling av personopplysninger.

14 Ifølge Datatilsynets retningslinjer, *Kameraovervåkning – hva er lov?* skal skiltene skal ha en størrelse, en plassering og være i et antall som gjør det lett å få med seg at en overvåkes (Datatilsynet 2014).

15 Her kan det legges til at da vi forsøkte å etablere kontakt med behandlingsansvarlige, la vi stor vekt på å opptre forståelsesfullt, og i de aller fleste innledende samtaler var det utelukkende en post- eller e-postadresse der innsynsbegjæringen kunne sendes til vi var ute etter.

16 Etter at denne delen av IRISS var avsluttet ble vi imidlertid gjort oppmerksomme på at Datatilsynet hadde innført en mal for innsynsbegjæringer. En slik mal kan forhåpentligvis bidra til å gjøre slike henvendelser enklere, både for behandlingsansvarlig og den registrerte. På den andre siden er det en mulighet for at i konkrete tilfeller vil formkravene i malen kunne virke hemmende på mengden informasjon som kreves for å rette en tilstrekkelig spesifikk henvendelse.

17 I følge *Store norske leksikon* er metadata (2009), «data om data, informasjon som beskriver annen informasjon, gjerne en elektronisk fil (tekstdokument, bilde, film). Typiske metadata er emneord, fagkategorisering og tidspunkt for opprettelse og endring av dokumentet. Et sett med metadata ordnes som regel i en søkbar database sammen med metadata for andre filer».

18 Legg spesielt merke til dette siste ordet, *aktivitet*, hvilket vil kunne innebære hvilke nettsider en besøker, hvilke søk en foretar, og så videre.

LITTERATUR

Ball K., Bellanova R., Bergersen S., Bonß W., Burgess J. P., Ceresa A., Clavell G. C., Dahm S., Fischer D., Fonio C., Friedevald M., Galletta A., Goos K., Jones R., Kreissl R., Lamina J. S., Lastic E., LeLeux C., Neumann A., Norris C., Peisll W., Raab C., Rothman R., Spiller K., Szekely I., Vissy B., Webster

W., Zurawski N. (2014). Chapter 3. Credit scoring, s. 78- 137 i Ball, K. & K. Spiller (red.), *Deliverable D3.2: Surveillance impact report*. Tilgjengelig på: http://irissproject.eu/wp-content/uploads/2014/06/D3.2-Surveillance-Impact-report1.pdf1.pdf

Bellanova, R., Bergersen S., Burgess, J. P., Mirshahi M., Moe-Pryce, M. (2014). Norway country reports. I Norris, C. & X. L'Hoiry (red.), *Deliverable D5: Exercising democratic rights under surveillance regimes*. Tilgjengelig på: http://irissproject.eu/wp-content/uploads/2014/06/Norway-Composite-Reports-Final.pdf

Bye, R. & F. Sjue (2008). *Overvåket*. Oslo: Gyldendal Akademisk.

Court of Justice of the Europen Union (2014). *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*. Case C-131/12. 2014. Tilgjengelig på: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d644d05bf64bd7411e91338550575 90c48.e34KaxiLc3qMb40RchoSaxuOaxj0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=29115

Datatilsynet (2013). Slik sperrer du deg for kredittvurderinger. Tilgjengelig på: http://www.datatilsynet.no/Sektor/Kreditt-finans-forsikring/Hvordan-sperre-for-kredittvurdering/

Datatilsynet (2014). Kameraovervåkning - hva er lov? Tilgjengelig på: http://www.datatilsynet.no/Global/04_veiledere/Kameraoverv%C3%A5kingsveileder_2014.pdf

Datatilsynet. Ordliste. Tilgjengelig på: http://www.datatilsynet.no/verktoy-skjema/Ordbok-A-til-A

Den europeiske menneskerettskonvensjon, EMK. Tilgjengelig på: http://www.echr.coe.int/Documents/Convention_ENG.pdf

European Data Protection Directive (Directive 95/46EC). Tilgjengelig på: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Gandy, O. H. (2009). *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Farnham, Surrey: Ashgate Publishing.

Google 2014: Europeiske personvernsforespørsler om sletting av søk. Tilgjengelig på: http://www.google.com/transparencyreport/removals/europeprivacy/

Lomell, H. M. (2011). Bedre føre var? Menneskerettslige konsekvenser av en pre-aktiv strafferett. I B. Barland, M. Egge & T.G. Myhrer (red.), *Men er det rett? Om politiet og menneskerettighetene*. Forskningskonferansen 2011. Oslo: Politihøgskolen.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.

Lyon, D. (red.) (2002): *Surveillance as social sorting: Privacy, risk and automated discrimination*. London: Routledge.

Menneskerettsloven (1999). *Lov om styrking av menneskerettighetenes stilling i norsk rett*. Art. 8. Retten til respekt for privatliv og familieliv. Tilgjengelig på: http://lovdata.no/dokument/NL/lov/1999-05-21-30/KAPITTEL_emkn-1#emkn/a8

Metadata (2009). I *Store norske leksikon*. Hentet 08.08.2014 fra: http://snl.no/metadata

Norris, C. & X. L'Hoiry (2014): *Exercising democratic rights under surveillance regimes: Executive Summary*. Tilgjengelig på: http://irissproject.eu/wp-content/uploads/2014/06/IRISS-WP5-Executive-Summary-for-Press-Release.pdf

NOU 2009:15. (2009). *Skjult informasjon – åpen kontroll*. Oslo: Justis- og politidepartementet. Tilgjengelig på: http://www.regjeringen.no/pages/2210108/PDFS/NOU200920090015000DDDPDFS.pdf

Personopplysningsforskriften. (2000). *Forskrift av 15. desember 2000 nr. 1265 om behandling av personopplysninger.*

Personopplysningsloven. (2000). *Lov av 14. april 2000 nr. 31 om behandling av personopplysninger.*

Thon, B. E. & T. Tennøe (2014a). Personvernet etter Snowden. Tilgjengelig på: http://www.personvernbloggen.no/2014/01/28/personvernet-etter-snowden/

Thon, B. E. & T. Tennøe (2014b). Personvern 2014. Tilstand og trender. Tilgjengelig på: https://www.datatilsynet.no/Global/04_planer_rapporter/Persovern_tilstandogtrender_2014.pdf

Wessel-Aas, J. (2011). Kan ideen om den liberale, demokratiske rettsstat overleve hvis samfunnsvern blir politikkens overordnede mål? *Tidsskrift for strafferett – 10 år jubileumsnr. mars 2011.*