Veien til et bedre personvern ligger i en kombinasjon av personlig og offentlig ansvar bygd på kunnskap og forståelse av felles verdier. Foto: Pixelvario/Shutterstock.

Vern om personlige opplysninger i vår digitale hverdag:

Hvorfor er personvern så vanskelig?

Staal A. Vinterbo

«*Jeg er ikke så bekymret, jeg har da ingenting å skjule*», er en kommentar man kan få når man spør om personvern på gata. Hvis du føler at personvern er vanskelig og overveldende, så er du ikke alene. Personvern *er* vanskelig og overveldende, men det er mange gode grunner til å engasjere seg, både for en selv og for samfunnet for øvrig.

Staal A. Vinterbo er professor ved Institutt for Informasjonssikkerhet og Kommunikasjonsteknologi ved NTNU og har forsket på personvern i kombinasjon med datagruvedrift og maskinlæring i 20 år. Han har blant annet også blitt invitert til diskusjon av personvern av Office of Civil Rights og Centers for Disease Control and Prevention i USA, samt Datatilsynet og Direktoratet for e-helse i Norge.

Allerede den 2000 år gamle hippokratiske ed inneholder et løfte om ikke å offentliggjøre pasientinformasjon. FN inkluderer personvern i sin menneskerettserklæring. Norge og mer enn 180 andre nasjoner har personvern omtalt i en eller annen form i Grunnloven. Hvis det er et tema som er så gammelt og blir ansett å være så viktig, hvorfor er det fremdeles så vanskelig?

For det første er personvern vanskelig fordi det er uenighet om hva personvern betyr. Grunnen til dette er at det i bunn og grunn er et verdispørsmål om hva slags samfunn vi vil ha og om personvern er nyttig for dette samfunnet. For eksempel, ønsker man et diktatur, vil personvern være i veien. Filosofer diskuterer om personvern er et nyttig begrep i det hele tatt. Ett standpunkt i diskusjonen er at alt det man ønsker fra begrepet allerede er gitt av andre begreper som frihet, verdighet og sikkerhet.

Figur 13.1 Personvern er vanskelig fordi det krever et felles verdigrunnlag, samarbeid og spesialistkunnskap. Foto: ra2 studio/Shutterstock.

I det siste har en økende mengde informasjon om oss blitt tilgjengelig gjennom teknologi. Som en følge av dette har tanken om personvern som en gruppe av begreper man ønsker vunnet frem. Viktig er her at disse begrepene og deres relative viktighet ikke er forhåndsbestemt, men tilpasses situasjonen. Eksempler på begreper som inngår i et slikt syn er vern av verdighet, unngå skade og vern av autonomi. Med autonomi menes da kontroll over egen person og det å kunne ta selvstendige beslutninger. Tap av autonomi har fått økende oppmerksomhet i mediene siden valget i USA i 2016, da det kom frem at falsk informasjon spredd gjennom blant annet sosiale medier hadde som mål å undergrave beslutningsgrunnlaget til velgere og dermed påvirke valget. Som vi skal se, henger dette også sammen med personvern.

Videre krever analyse av personvern og dets beskyttelse en spesiell tankegang som må læres. Dette er tankegangen der en motstander manipulerer omstendighetene til sin fordel. En slik motstander ønsker at det uforutsette skjer. Siden det uforutsette er nettopp uforutsett, kan man ikke utelukkende

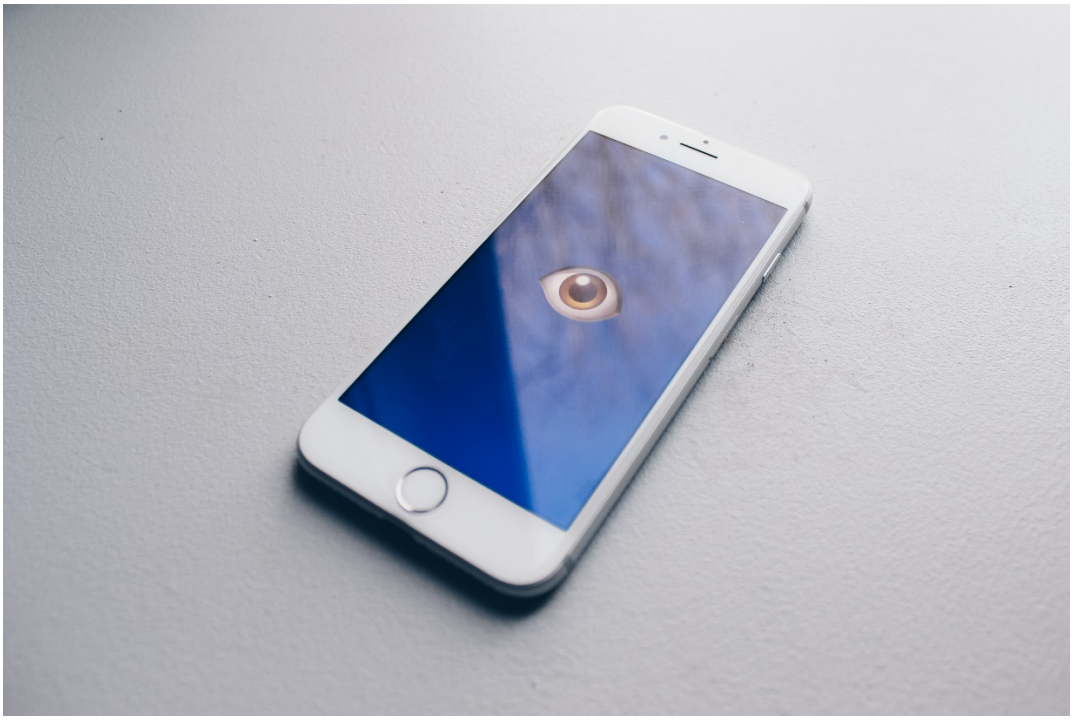
støtte seg på tidligere erfaring. For å beskytte seg fullstendig mot en hvilken som helst motstander må man være allvitende. Siden dette er umulig, må man gjøre antagelser som begrenser hva som kan oppstå, uforutsett eller ikke. Jo bedre man forstår sammenhengen mellom antagelser og hva motstanderen kan oppnå, jo bedre kan man beskytte seg.

Det beste er en formell, ofte matematisk definisjon av personvern som inneholder en beskrivelse av hva slags antagelser man gjør. Dette tillater to viktige ting: først at man kan bevise at en metode man bruker for å beskytte personvernet faktisk gjør det. Siden kan man analysere om definisjonen virkelig oppnår hva man ønsker og om antagelsene er realistiske. Hvis man støtter seg for mye på erfaringer uten en slik formell analyse, må man vente til noe skjer og oppdatere erfaringsgrunnlaget i etterkant. Dette siste kan sammenlignes med å sette bedre lås på låven etter at dyrene har rømt. I motsetning til rømte dyr som kan fanges inn, kan dessverre ikke offentliggjorte opplysninger gjøres hemmelige igjen.

Personvern er et bredt begrep og inneholder også fysisk beskyttelse av selve personen. I den digitale hverdagen er den delen av personvernet som dreier seg om personopplysninger sentral. I det følgende vil vi derfor konsentrere oss om vern av personopplysninger i digitalt format.

Hva truer beskyttelsen av personopplysninger?

Hvis du glemmer den bærbare datamaskinen din på bussen og ikke har kryptert dataene, kan andre få tak i alt som er lagret. Hvert år kommer store mengder av innsamlet data på avveie, enten ved uhell eller tyveri. Et eksempel er informasjon om 540 millioner brukere som i 2019 ble offentliggjort av to utviklere av apper på Facebook. Et annet er den indiske nasjonale biometridatabasen i Aadhaar-systemet som ikke var godt beskyttet over en årrekke, noe som ble offentlig kjent i 2017. Informasjon om 1,1 milliarder indere fra databasen kunne kjøpes billig på det svarte markedet.



Figur 13.2 Informasjon om den enkelte brukes i forsøk på å manipulere, både for å tjene penger og å påvirke samfunnet. Foto: www.shopcatalog.

Det disse eksemplene har til felles er at sikringen av dataene har vært mangelfull, noe som er straffbart under norsk og mange andre lands personvernlover når man er ansvarlig for informasjon om andre. Ikke uten grunn kalles personopplysninger også en giftig ressurs. Men det er ikke bare mangelfull sikring av data som kan skade personvernet.

Lovlig innsamling og bruk av data fra en person, såkalt lovlig prosessering, kan også skade personvernet. I Norge og EU gir loven flere muligheter til å gjøre prosessering lovlig. Tre av disse er at personen gir *tilsagn*, at data eller informasjon ikke er *personlige*, eller at den skjer i interesse av *nasjonal sikkerhet*. Vi skal kort se på disse etter tur.

Tilsagn. Du har sikkert sett en boks dukke opp på skjermen der det spørres om samtykke til bruk av data om deg. Ofte i form av «cookies» eller informasjonskapsler som tillater kobling av gjentatt tilgang til, eller bruk av, sider og tjenester på nett. Et prinsipp for gyldigheten av samtykke er at den som samtykker forstår hva det sies ja til. Problemer oppstår når bruken av dataene er så komplisert at konsekvensene av den ikke er overskuelige.

I bedriftssammenheng skiller man mellom bedrifter som primært har deg som kunde, for eksempel en møbelforhandler, og «datadrevne» bedrifter som lever av å selge informasjon om deg til en tredjepart. Møbelforhandleren kan sannsynligvis gjøre greit rede for hvordan kundedata kan hjelpe med å tilby et bedre utvalg av produkter. For datadrevne bedrifter, som nesten alltid tilbyr tjenester gratis for å få tilgang til persondata, er bruken av disse for komplisert til å forstås av utenforstående. Store datadrevne bedrifter som du kanskje har hørt om, er i reklamebransjen og heter Google og Facebook. Dette bildet blir også stadig mer komplisert ettersom flere og flere vanlige bedrifter ser at de kan tjene penger på å selge kundeinformasjon, dvs. bli litt «datadrevne» de også.

Personlige data. EUs, og dermed Norges, personvernforordning GDPR gjelder bare for data som er «personlige», dvs. kan knyttes til en reell person. Data som i utgangspunktet er personlige, kan gjøres upersonlige ved såkalt anonymisering. Det vil si at forbindelsene mellom data og personer gjøres tvetydige. Et problem er at forskning rundt personvern og data viser at det er umulig å sjekke at data virkelig er anonyme, dvs. at man ikke kan sjekke om data er personlige eller ikke. Grunnen er at informasjon som tilsynelatende ikke er personlig kan i sammenheng med annen informasjon gjøre det mulig å trekke slutninger om enkeltpersoner, med andre ord blottlegge personlig informasjon.

La oss si at Ola, som jobber ved lokalsykehuset, vil dele antallet pasienter ved sykehuset som er mannlige, 30 år gamle, har sukkersyke og ikke bruker Viagra, med Kari for å belyse sammenhengen mellom sukkersyke og seksuelle problemer. Ola bestemmer seg for at det er greit å dele antallet siden det er 0, og det dermed ikke finnes noen slike pasienter. Neste helg snakker Kari med Per på 31-årsdagen hans der han nevner at legen på lokalsykehuset stadig minner ham på at han må holde blodsukkeret under kontroll på grunn av sukkersyken. Kari vet nå umiddelbart at Per bruker Viagra, noe han kanskje ikke hadde lyst til å dele med henne.

Juristen Paul Ohm har sagt at personvernlovgivning der anonymiserte data ikke lenger omfattes av loven, er basert på en fundamental misforståelse av hva personvern krever. Forskningen viser også at hvis man vil sannsynliggjøre personvern, må man legge til en tilpasset mengde tilfeldig støy til informasjonen og at det er støyen som gir personvernet. Et hinder er at en slik mer forsvarlig tilnærming til personvern og anonymitet er et radikalt steg bort fra begrepene personlig informasjon, anonymiserte data og det nåværende veletablerte regelverket.

Nasjonal sikkerhet. I diskusjoner omkring nasjonal sikkerhet, overvåking og personvern blir det tydelig at personvern er et verdispørsmål. Én måte å se personvern på er at vernet knyttes opp til individet som en rett, og at overvåking er nødvendig for fellesskapets sikkerhet. Sett slik trumfer fellesskapet nesten alltid individet. Alternativt kan personvern sees som ikke spesielt knyttet til individet, men som en grunnleggende egenskap ved det samfunnet vi ønsker å sikre. Et slikt syn åpner for en diskusjon av det paradoksale ved å sikre samfunnet på en måte som forringer det.

En ting som gjør det vanskelig å diskutere personvern og overvåking, er at detaljene om overvåkingen nesten alltid er hemmelige. Som i diskusjonene rundt en ny norsk etterretningstjenestelov som trådte i kraft januar 2021, dannes det som regel et utvalg som skal være stedfortreder for offentligheten. Grunnen er at offentlig innsyn i E-tjenestens virke kan svekke tjenestens forsvar av landet.

Et punkt som ble diskutert i avisene i forkant, var at loven skulle gi mulighet for å innhente og lagre data om all elektronisk kommunikasjon over landegrensene, noe som i praksis ville bety masseinnsamling av data om norske borgere i Norge. Problemet med dette er at E-tjenesten er Norges nasjonale utenlandsetterretningstjeneste og skal ikke overvåke norske borgere i Norge uten grunn. Hvis du for eksempel bestiller matvarer fra kolonial.no tidlig i 2021, noe mange gjør under den pågående SARS-Cov-2-pandemien, så har E-tjenesten data om dette ettersom tjenestens bestillinger behandles i utlandet. Det samme gjelder om du bruker Office365.no, som er den norske varianten av Microsofts online variant av Office-produktene, eller besøker nettstedene ikea.no, google.no, og innovasjonnorge.no. Alle tilsynelatende med norsk nettadresse som ender i .no.

Selvfølgelig gjelder det også nesten alle store sky- og meldingstjenester i regi av Netflix, Google, Apple, Facebook (og WhatsApp), Azure, Amazon, Snap, Telegram og Signal. Selv trafikk som tilsynelatende bare går innenlands mellom deg og en norsk nettside kan fanges opp hvis nettsiden bruker analysetjenester som Google Analytics, som ligger i utlandet. Slike analysetjenester fremtvinger som regel en automatisk kontakt med analysetjenesten, såkalt tracking eller sporing på norsk.

For å forebygge både at overvåking fører til at folk kvier seg for å uttale seg, den såkalte avkjølende effekten, og et tap av tillit i befolkningen, er det viktig at styresmaktenes prosesser for å danne slike utvalg og bestemme deres mandat er åpne og gjennomsiktige slik at man unngår følelsen av at viktige beslutninger blir tatt «på kammerset». Som vi har sett under SARS-Cov-2-pandemien, og de stadige angrep på politiske valg gjennom bruk av falsk informasjon, er tillit til offentlige institusjoner veldig viktig for beskyttelse av nettopp nasjonal sikkerhet.

Faktiske konsekvenser. Hva har problemene over ført til av faktiske skader? For å forbedre de automatiske anbefalingene sine avholdt Netflix en konkurranse der utviklerne av den beste metoden for anbefalinger fikk en gjev pris. Som materiale til denne konkurransen offentliggjorde Netflix anonymiserte data om hva kunder mente om filmer de hadde sett. Det ble fort kjent at ved å sammenligne disse dataene med anmeldelser i IMDb (en filmdatabase på internett), kunne man gjenkjenne enkeltpersoner. Dette førte til en rettssak der en anonym lesbisk kvinne saksøkte Netflix for å ha gjort det mulig å finne ut hennes seksuelle legning.

America Online (AOL) offentliggjorde også anonymiserte data om kundene sine, denne gang var det ord brukt i websøk. En journalist i The New York Times brukte disse til å lete seg frem til Thelma Arnold, en eldre kvinne som sa seg villig til å stå frem.

Butikkjeden Target la merke til at kvinner som registrerte gaveønsker i forbindelse med kommende graviditet, også kjøpte spesielle ting som luktfri såpe og spesielle vitaminer. Tilgang til informasjonen som trengs for slike koblinger kan fås gjennom rabattkort. Ved å bruke denne kunnskapen sendte Target kuponger for babyutstyr hjem til en familie og avslørte dermed graviditeten til tenåringsdatteren i huset for resten av familien.

Slike historier om problemer med anonymisert informasjon blir kjent etter gravende journalistikk og ofte med støtte fra forskere med interesse for personvern. Men de er relativt sjeldne sammenlignet med de daglige tap av persondata ved uhell eller tyveri. Én grunn til dette er at loven ikke sier noe om hva som skal skje med informasjon etter at den er blitt anonymisert, dvs. man trenger ikke følge opp og sjekke at den ikke fører til skade. Dette gjør det enda vanskeligere å finne ut nøyaktig hva som førte til at du ble nektet kreditt eller fikk identiteten din stjålet.

Vi har likevel lært en del om hvordan systematisk innsamlet informasjon om mange mennesker misbrukes, til og med på lovlig vis. Du har kanskje hørt historier om, eller opplevd selv, at søk etter en vare på nettet har i ettertid resultert at denne eller lignende varer dukker opp forholdsvis ofte i reklame og søkeresultat. Dette er en versjon av et fenomen som har blitt kalt «filterboblen». Slike bobler oppstår når tjenester tilpasser seg etter hva de vet om deg. Dette kan være nyttig, for eksempel i at strømmingstjenesten du bruker kan foreslå bra musikk du ikke har hørt før, men det kan også brukes til å manipulere.

Mueller-rapporten om russisk intervensjon i det amerikanske presidentvalget i 2016 peker på systematiske kampanjer fra det Kreml-finansierte Internet Research Agency som hadde som mål å spre usikkerhet og polarisere amerikanere i forkant av valget. Falsk informasjon, eller «fake news», på Facebook og andre store sosiale medier var et av hovedvirkemidlene. Den falske informasjonen ble brukt effektivt ved å målrette den. Å kjøpe målrettet reklameplass for falske nyheter er et eksempel på hvordan dette ble gjort, og slik målretting bruker nettopp data om personer samlet inn av datadrevne selskaper.

I 2018 ble det kjent at Cambridge Analytica, et privat etterretningsselskap, hadde kjøpt informasjon om ca. 87 millioner brukere av Facebook gjennom en app på plattformen. Ifølge opptak av personer i ledelsen til Cambridge Analytica var selskapet involvert i å påvirke mer enn 200 politiske valg internasjonalt gjennom systematisk bruk av persondata i kampanjer for å spre falsk informasjon. Vi kan nå anse slike taktikker som standardverktøy for å skape mistro til myndigheter, vitenskap og tradisjonelle medier. Noe vi også kan observere i Norge, blant annet i debatten om klimakrisen.

Hva kan jeg personlig gjøre?

Her kan det være nyttig å skille mellom hva du kan gjøre for akkurat dine data og hva du kan gjøre som medlem av fellesskapet. Som det forhåpentligvis har blitt klart, har individet ikke mulighet til å beskytte sin informasjon uten hjelp fra fellesskapet. Med økende digital flyt av informasjon man rett og slett ikke kan unngå, er vi avhengige av gode regler og lover for personvern og gode nok budsjetter til forvaltningsorganer. I Norge er dette Datatilsynet. Vi trenger også transparente politiske beslutningsprosesser for å sikre tillit til de institusjoner vi har valgt å ha i demokratiet vårt. Disse tingene får vi ikke automatisk, vi må ville ha dem og bruke våre stemmer til dette. Både ved valgurnene og ellers.

Figur 13.3 Det er viktig å være bevisst i valg man treffer i dagens digitale hverdag, både som enkeltmenneske og medlem av fellesskapet. Foto: Jirsak/Shutterstock.

I tillegg til det nødvendige politiske initiativ er det ting man kan gjøre for å beskytte seg i det daglige. Et nøkkelord her er informasjonshygiene, det vil si at man tar godt vare på sitt digitale immunforsvar. Det innebærer for eksempel å ikke bruke det samme passordet til flere tjenester og nettsteder, spørre banken om de kan tilby engangs kredittkortnummer til handling på nett, bruke søketjenester og nettlesere som forebygger sporing, og lære hvordan man beskytter seg mot ting som «phishing».

Man bør være bevisst i bruken av datadrevne tjenester som typisk kan gjenkjennes i at de er gratis. Et eksempel er å unngå å organisere barnas aktiviteter som Facebook-gruppe, siden dette vil tvinge andre til å måtte velge mellom barnas sosiale vel og eget ønske om å unngå Facebook. Jeg bruker Facebook som eksempel siden det er det største datadrevne sosiale nettverket i verden og blir mye brukt til nettopp slikt. Det finnes mange bra, billige, eller til og med gratis, alternativer til mange datadrevne tjenester som ikke er datadrevne.

Til slutt brukes mangel på personvern til å styrke angrep på informasjonsgrunnlaget for våre beslutninger. Effekten av slike angrep kan også reduseres ved å abonnere på en tradisjonell avis og dermed hjelpe til å bevare kvalitetssikringen på mediene vi har gjennom journalistutdanning og Vær Varsom-plakaten.

Avrunding

Så hva kan vi nå svare på kommentaren vi begynte med – «*Jeg er ikke så bekymret, jeg har da ingenting å skjule*»? Vi har alle behov for å skjule ting. Å måtte bekymre seg over at vi skjuler ting passer ikke overens med det vi forbinder med blant annet hemmelige politiske valg. Selv om en føler at en selv ikke har noe behov for et sterkere personvern, så er personvern allikevel en viktig del av det samfunnet som vi kanskje ikke har råd til å miste.

Vi har sett at personvern er vanskelig, både filosofisk som verdi og i praksis når det gjelder å beskytte den enkeltes informasjon. Videre har vi sett hvordan systematisk innsamling av persondata kan føre til tap av personvern for oss enkeltmennesker, og hvordan mangel på personvern kan sette fellesskapet i fare. Det er viktig å være bevisst, både i hvordan vi i det daglige håndterer informasjon om oss selv, og hvordan vi kan påvirke det nødvendige personvernet vi er avhengige av at fellesskapet gir.

Både lokalt og globalt møter vi hele tiden store utfordringer som vi sammen arbeider med å overvinne. Eksempler er fattigdom, krig og sykdommer som Covid-19 og polio. Slik er det også med angrepene på personvernet. Å gi opp er rett og slett ikke noe alternativ.

Hvis du vil lese mer om personvern, er https://www.datatilsynet.no et godt sted å begynne.