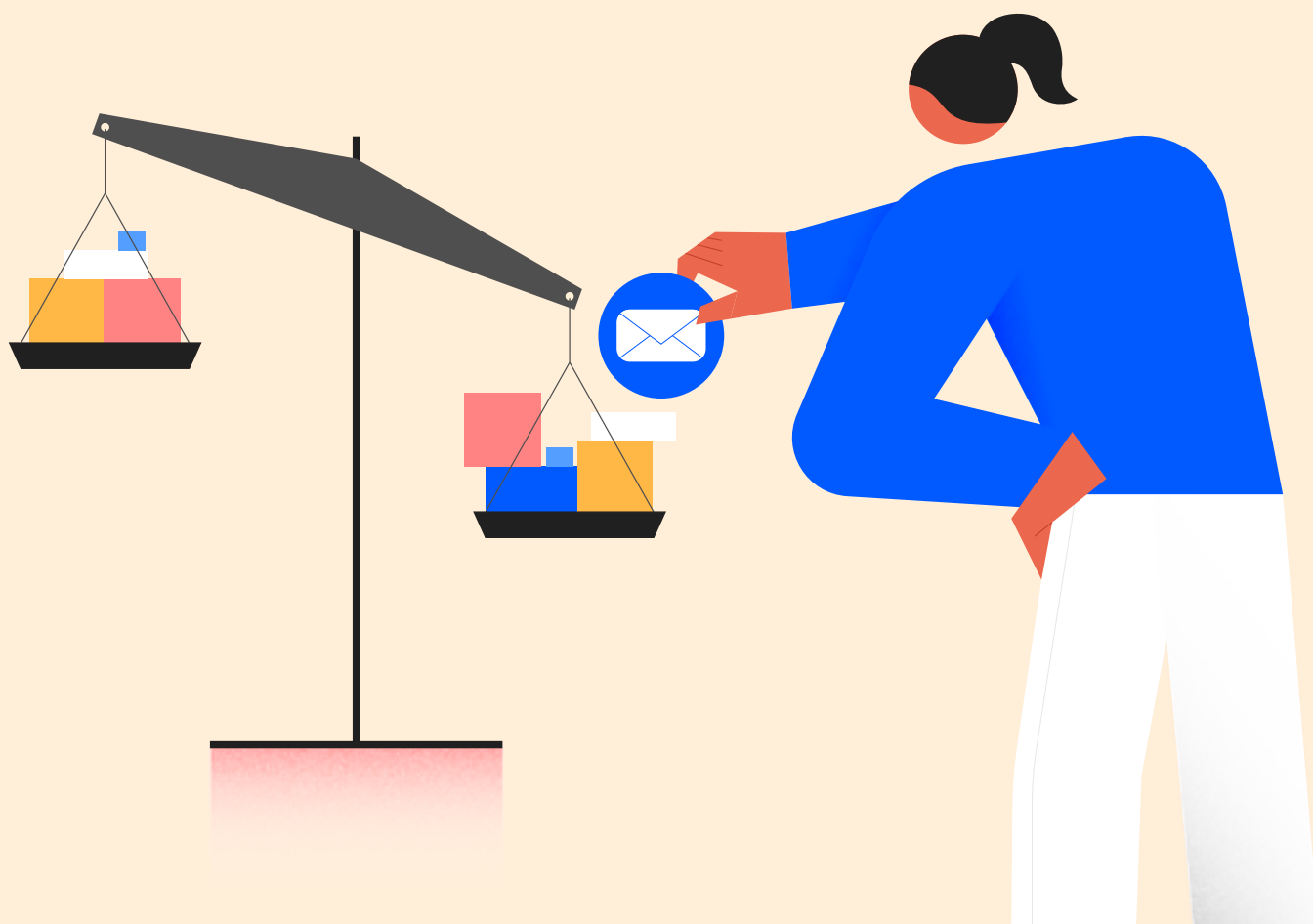


TECHSPLAINER

Dataetik og privatliv



Dataetik og privatliv

Vores smartphones samler data om hvilke apps vi bruger. Teleselskaberne gemmer oplysninger om hvor vi opholder os, ved at se på hvilke mobilmaster telefonerne er logget på, og om hvem vi ringer og skriver til. Vores browsere bruger cookies til at registrere, hvad vi laver på internettet. Når vi færdes i det offentlige rum bliver vi ofte filmet, og nogle gange bliver billederne analyseret for at genkende vores ansigter eller vurdere vores følelser. Og når vi er på arbejde kan kameraer, telefoner, nøglekort, og software på arbejdscomputeren hjælpe os med at registrere hvor vi er og hvad vi laver.

De nye digitale teknologier, som er blevet en fast del af vores hverdag, bruger data. Ofte behandler de meget store mængder data, og ofte handler i hvert fald nogle af disse data om os. Når digitale teknologier indsamler, skaber eller deler personlige informationer kan det påvirke vores privatliv.

De fleste mener, at privatliv er vigtigt. Derfor kan man blive bekymret for, at vores privatliv indskrænkes af teknologier som samler, skaber og deler data om os. Og man kan mene, at vi på forskellige måder bør beskytte menneskers privatliv med lovgivning, sådan som Europæiske lande for eksempel har gjort med EU's databeskyttelsesforordning (GDPR). Hensynet til privatliv spiller en central rolle i dataetikken.

Men hvad er privatliv? Hvad vil det sige, at noget er privat? Og hvorfor er privatliv dataetisk set vigtigt?

Når man skal arbejde med dataetik, er det værd at overveje sådanne spørgsmål. Hvis man afklarer hvad privatliv betyder, bliver det lettere at forstå hvordan digitale teknologier som indsamler, skaber og deler data påvirker vores privatliv. Og hvis man afklarer hvorfor privatliv er dataetisk vigtigt, bliver det lettere at vurdere de dataetiske problemstillinger, hvor privatliv er på spil.

I denne tekst præsenterer Dataetisk Råd et overblik over nogle af de forskellige måder man kan forstå privatliv, og den rolle det spiller i dataetikken.

Hvad er privatliv

Når vi taler om privatliv eller at noget er privat, så kan det betyde flere forskellige ting.¹

Vi snakker for eksempel om, at en beslutning kan være privat, at et sted kan være privat, og at informationer kan være private.

Private beslutninger

En første betydning af privatliv drejer sig om, at beslutninger kan være private. Når vi siger at en beslutning er privat mener vi, at det er en beslutning, som den enkelte har ret til at træffe, uden at andre blander sig. Det kan for eksempel virke grænseoverskridende, hvis andre blander sig i hvordan man klæder sig, hvilke hobbyer man dyrker, eller hvem man vælger at være kæreste med.

Private beslutninger beskytter personers selvbestemmelse. Hvis andre tager beslutninger på ens vegne, eller forsøger at true eller manipulere en til at træffe en bestemt beslutning, så er beslutningen ikke fri, og ikke i egentlig forstand ens egen beslutning. De fleste mener, at der er grunde til, at personer skal have mulighed for frit at træffe visse beslutninger om, hvordan de vil leve deres liv, selvom der kan være forskellige opfattelser af hvilke grunde, og hvornår de optræder. Når der er sådanne grunde, er det dataetisk vigtigt, at beskytte private beslutninger.

Private steder

En anden betydning af privatliv drejer sig om, at visse rum kan være private. Når vi siger at et sted er privat mener vi, at vi har ret til at være i fred der, og at andre kun har adgang med vores tilladelse. De fleste mennesker betragter deres hjem som et privat område, hvor det kun er en selv og den nærmeste familie som hører til. Andre mennesker er gæster.

Men også indenfor et hjem kan for eksempel et teenagebarns værelse være privat i denne betydning – et sted hvor teenageren har ret til at være i fred, og hvor andre familiemedlemmer ikke uden videre kan opholde sig.



¹ På engelsk anvendes begrebet "privacy", som ikke er helt identisk med det danske begreb om "privatliv". Ikke desto mindre kan betragtninger om "privacy" i vidt omfang oversættes til at gælde det vi på dansk kalder privatliv. De forskellige betydninger af privatliv diskuteres blandt andet i Tavani 2007; Rubel 2011.

Rum kan også være private udenfor hjemmet, for eksempel et kontor på en arbejdsplads.

Selv et offentligt toilet kan være et privat rum, imens en person benytter det.

Private steder beskytter personers ejendom og fysiske sikkerhed. Men private rum beskytter også det behov de fleste mennesker har, for at kunne vælge hvornår de vil være sociale, og hvem de vil omgås. Derfor kan det være dataetisk vigtigt, at beskytte private steder.

Private informationer

Den tredje betydning af privatliv drejer sig om, at personlige informationer kan være private.² Personlige informationer fortæller noget om en bestemt person, for eksempel hvad de hedder, hvordan de ser ud, deres alder, beskæftigelse, og så videre. Personlige informationer kan også handle om ting, som er knyttet til en person, eller relationer. Det er for eksempel personlige informationer, hvad farven på en persons bil er, og hvem en person er i familie med.

Selvom de andre betydninger også kan spille en rolle, er det især private informationer som er centrale i dataetikken. Det skyldes, at moderne digitale teknologier ofte samler, skaber og deler personlige informationer. Derved kan disse teknologier påvirke personers privatliv. Men hvad vil det sige, at en personlig information er privat? Og hvorfor er denne form for privatliv dataetisk vigtig?

² På engelsk tales om "informational privacy".

Hvornår er en personlig information privat?

Dét, at en personlig information er privat, kan forstås på flere måder. Der kan være forskellige forståelser af blandt andet:

- Betyder privat at andre ikke kender eller har adgang til en information?
Eller at de ikke bør kende eller have adgang til den?
- Er en information enten privat eller ikke privat?
Eller kommer privatliv i forskellige grader?
- Kan en hvilken som helst information være privat?
Eller er det kun nogle informationer, som kan være private?
- Holder en information op med at være privat, når andre får adgang til den?
Eller først når de kender til den?

Er "privat" beskrivende eller etisk?

Når vi siger at en information er privat, handler det så om hvem som kender eller har adgang til informationen? Eller handler det om, hvilke dataetiske forpligtelser vi har, for eksempel til at beskytte informationen?³

Nogle gange, når vi taler om, at en information er privat, bruger vi begrebet på en rent beskrivende måde. I denne betydning kan en information holde op med at være privat, for eksempel fordi den bliver delt med andre personer.

Andre gange taler vi om en privat information i en værdiladet eller etisk betydning. En person kan for eksempel afvise at besvare et spørgsmål, ved at sige, at "det er privat". Når en information er privat i denne betydning holder den ikke op med at være privat ved for eksempel at blive delt – den er stadig en information, som vi har dataetiske grunde til at beskytte.

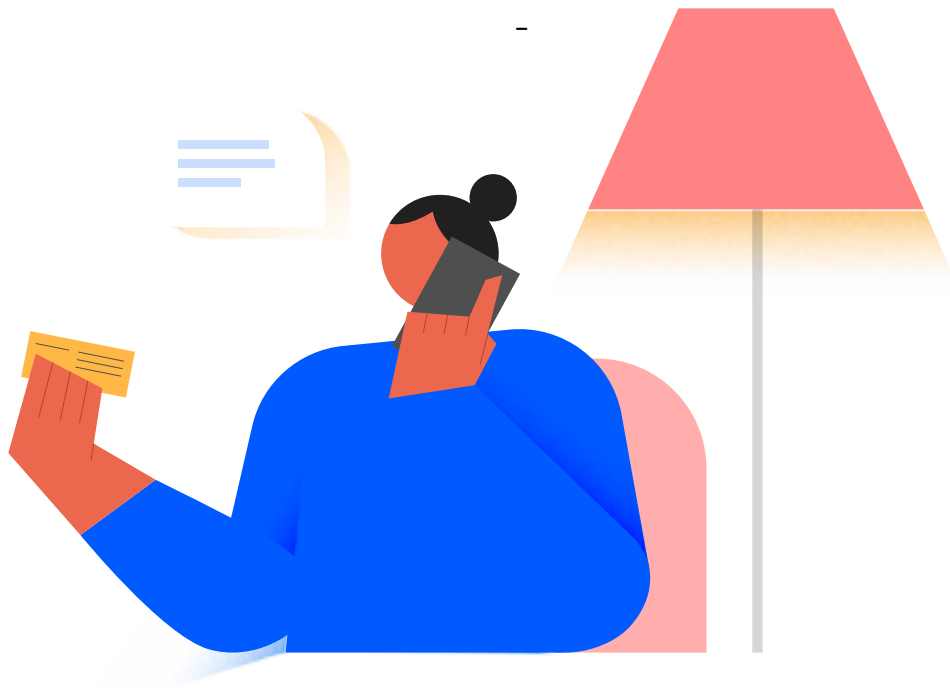
En information kan i nogle tilfælde være privat i begge betydninger samtidig, men det kan ofte være en fordel at skelne mellem dem, så det er klart hvad man mener, hvis man for eksempel siger, at "en information ikke er privat".

Kan informationer være mere og mindre private?

Ofte taler vi om privatliv (i den beskrivende forstand) som noget man mister, så snart en personlig information bliver delt: Hvis en anden person kender til informationen, så er den ikke længere privat. Ifølge denne forståelse af privatliv, så er en personlig information kategorisk enten privat eller ikke privat.

³Se Davis 2009; Gavison 1980; McCloskey 1980; Powers 1996; Parent 1983.

Man kan også mene, at privatliv er et spørgsmål om grader.⁴ Man kan for eksempel mene, at en hemmelighed er mere privat, hvis man kun har delt den med én nær ven, end hvis man har fortalt den til mange forskellige personer. Hvor privat en information samlet set er, afhænger ifølge denne forståelse af hvor mange andre personer som kender eller har adgang til informationen. En information er meget privat, hvis få eller ingen andre mennesker kender eller har adgang til den, og ikke særlig privat, hvis mange personer kender eller har adgang til den.



Kan alle slags informationer være private?

Når vi taler om private informationer, så fokuserer vi ofte på særlige, følsomme informationer. Én måde man kan forstå privatliv drejer sig kun om disse særlige informationer, mens andre informationer ifølge denne forståelse ikke kan være private. For nogle kan det måske lyde underligt, at tale om privatliv i forbindelse med helt dagligdags informationer, som man rutinemæssigt deler med andre, når man færdes i det offentlige rum. Giver det mening at sige, at sådanne informationer kan være private, og at man derfor mister privatliv, når man går en tur? Man kunne også mene, at sociale normer er med til at afgøre, hvornår informationer er eller kan være private. Sådanne normer kan variere med konteksten. For eksempel kunne ens sundhedsinformationer være ikke-private, når man taler med sin læge, men private i andre sammenhænge.

Omvendt kan man mene, at alle informationer kan være private. I denne forstand er dagligdags informationer private indtil man går en tur, og sundhedsinformationer private indtil man deler dem med lægen. Hvis man forstår privatliv på denne måde, så kunne man forsøge at forklare hvorfor vi ofte fokuserer på visse informationer med, at disse

⁴ Se Rubel 2007.

informationer er særligt dataetisk vigtige. Ifølge denne forståelse er spørgsmålene om en information er privat eller ej, og hvornår vi bør interessere os for om en information er privat eller ej, to forskellige spørgsmål.

Hvornår er en information ikke privat længere?

Man kan også spørge hvad der skal til, for at en information er privat? Der findes to udbredte svar på dette spørgsmål: kontrolteorien og kendskabsteorien.⁵

Kontrolteorien siger at en personlig information er privat, hvis personen kan kontrollere andres adgang til informationen.⁶ Når digitale teknologier indsamler, skaber og deler ens personlige informationer, så mister man ofte kontrol over andres adgang til disse informationer. Hvis et kamera filmer en person på gaden, et smartur måler puls- og søvnrytmer, eller en cookie registrerer aktivitet på internettet, så kan disse informationer blive tilgængelige for andre. I nogle tilfælde kan de blive tilgængelige, uden at man har mulighed for at vælge om data skal deles, måske fordi man slet ikke ved, at de bliver delt. Det betyder, ifølge kontrolteorien, at man mister privatliv.

Kontrolteorien om privatliv:
En personlig information er privat, når vedkommende har kontrol over andre personers adgang til informationen.

Kontrolteorien er blevet kritiseret for, at blande dataetiske grunde til at beskytte personers kontrol over privatliv sammen med spørgsmålet om, hvad privatliv er.⁷ I nogle situationer, hævder kritikerne, holder informationer ikke op med at være private, selvom man ikke har kontrol over andres adgang til dem.⁸ I sådanne situationer kunne det alligevel være dataetisk vigtigt, at personen har kontrol over adgang til sine personlige informationer.

Kendskabsteorien siger at personlig information er privat, når andre personer ikke har kendskab til informationen.⁹ Information holder derfor først op med at være privat, når andre får kendskab til den. Digitale teknologier indsamler, skaber og deler ofte personlige data. Disse data kan give andre kendskab til ens personlige informationer. Når det sker, så mister man ifølge kontrolteorien privatliv.

⁵ Se Asgarinia 2023; Menges 2021; Mainz 2021; Lundgren 2020; Munch & Mainz 2023; Nissenbaum 2004; Roessler 2005. På engelsk tales om "control" og "access" teorier. "Access" oversættes mest direkte til det danske "adgang". Men det er et anerkendt problem, at også kontrolteorien handler om adgang. Vi benytter derfor "kendskab" som en mere retvisende og mindre potentielt forvirrende betegnelse.

⁶ Se Westin 1967; Marmor 2015; Rachels 1975; Moore 2003.

⁷ Se Davis 2009; Mainz 2021.

⁸ Et illustrativt eksempel handler om en person, som glemmer sin dagbog på en café. En venlig cafégæst passer på dagbogen, uden at læse i den, indtil ejeren kommer tilbage og henter den. Ifølge kontrolteorien er de personlige informationer i dagbogen ikke private, fordi cafégæsten kunne have læst i den, og ejeren derfor ikke havde kontrol over adgang til informationerne. For mange vil det nok virke mere oplagt at sige, at informationerne fortsat er private, fordi cafégæsten ikke brugte adgangen til faktisk at få kendskab til dem. Se Macnish 2018.

⁹ Parent 1983; Powers 1996; Mainz 2021.

Kendskabsteorien er blevet kritiseret for, at give det forkerte svar i situationer, hvor en person frivilligt deler sine personlige informationer.¹⁰

Giver det i denne situation mening at sige, at personen mister privatliv? Fortalere har svaret, at udfordringen blander spørgsmålet om hvornår vi mister privatliv sammen med spørgsmålet om, hvornår det er dataetisk problematisk at miste privatliv. De har endvidere peget på, at udfordringen også synes at ramme kontrolteorien, fordi man dårligt kan siges at have kontrol over adgangen til personlig information, efter at man har delt den.¹¹

Kendskabsteorien om privatliv:
En personlig information er privat, når andre personer ikke har kendskab til informationen.



¹⁰ Inness 1992.

¹¹ Parent 1983; Lundgren 2020.

Hvorfor privatliv for personlige informationer?

De fleste af os mener, at privatliv i en eller anden grad er vigtigt. Men hvor vigtigt? I mange situationer kan der være grunde til at indsamle, skabe eller dele personlige informationer, selvom man derved reducerer en persons privatliv. Hvordan skal man i disse situationer vurdere hvilke hensyn, der vejer tungest – privatliv eller grundene til at indsamle, skabe og/eller dele informationer? Svarene på disse spørgsmål afhænger af hvorfor man mener, at privatliv er dataetisk vigtigt.

Der kan være forskellige holdninger til spørgsmålet om, hvorfor privatliv er dataetisk vigtigt.¹²

Seks almindelige begrundelser er:

- Tab af privatliv kan stride mod en dataetisk rettighed
- Tab af privatliv kan være ydmygende og ubehageligt
- Tab af privatliv kan være stressende
- Tab af privatliv kan gøre det svært at forme relationer
- Tab af privatliv kan afskrække uskyldig adfærd
- Tab af privatliv kan gøre en sårbar

Forskellige personer kan have forskellige opfattelser af hvilke begrundelser, som er gode og dårlige. Man kan også have forskellige forståelser af, hvordan begrundelser bedst forstås, og hvad grundlaget for dem er. Endelig kan man, blandt andet i kraft af sådanne forskelle, have forskellige holdninger til, hvornår vi dataetisk set bør beskytte privatlivet. Selvom begrundelserne her præsenteres relativt abstrakt, så vil det ofte være nødvendigt at præcisere og kritisk vurdere dem, når man tager stilling til en konkret dataetisk problemstilling.

Privatliv og rettigheder

En første begrundelse, som mange henviser til, når man diskuterer dataetik og privatliv, er retten til privatliv. Retten til privatliv kan forstås på forskellige måder.

Først og fremmest er retten til privatliv en juridisk grundrettighed. I Danmark er den juridiske ret til respekt for privatliv fastsat i Grundlovens paragraf 72, som en beskyttelse af boligens ukrænkelighed og brevhemmeligheden. Retten til privatliv er også beskyttet i de internationale menneskerettighedskonventioner, som forbyder vilkårlige indgreb i en persons privatliv, familieliv, hjem og korrespondance, samt angreb på ære og omdømme. EU Charterets artikel 7 og 8 og den europæiske menneskerettighedskonventions artikel 8 folder beskyttelsen mere ud,

En juridisk grundret

Et sæt af love og konventioner, som beskytter personers kropslige og mentale integritet, familieliv, hjem, korrespondance, omdømme, og personlige oplysninger.

¹²For overblik, se eksempelvis Macnish 2015; Solove 2006.

og omfatter – udover integritet, familie, hjem og korrespondance – også personoplysninger.¹³

Den juridiske ret til respekt for privatliv begrundes typisk ved, at den bygger på og skal forstås i lyset af det etiske princip om menneskets personlige autonomi og selvbestemmelsesret.

Den beskytter selve evnen til at leve det liv, man ønsker.¹⁴

Retten til privatliv anses også bredt som en grundsten i demokratiske samfund, der muliggør realiseringen af andre rettigheder. Retten er for eksempel med til at beskytte personers mulighed for at ytre sig, indhente information, deltage i foreninger og forsamlinger, stemme til demokratiske valg, og træffe selvstændige beslutninger om uddannelse, arbejde og sundhed.¹⁵

I mange diskussioner om dataetik er det ikke kun den juridiske rettighed, som er på spil. Ind imellem kritiserer personer eksempelvis eksisterende lovgivning for, at den ikke tilstrækkeligt sikrer retten til privatliv. I sådanne tilfælde mener de antageligt, at den juridiske ret til privatliv ikke giver den nødvendige beskyttelse af en *moralsk* ret til privatliv.

En anden måde at forstå retten til privatliv, er således som en *grundlæggende moralsk* rettighed. Hvis man forstår retten til privatliv

på denne måde, så er den ikke begrundet i

andre, bagvedliggende dataetiske hensyn

– retten er grundlæggende, fordi det i sig

selv er dataetisk problematisk at reducere

en persons privatliv. Typisk vil man tilføje, at det ikke er dataetisk problematisk at reducere en

persons privatliv, hvis vedkommende frivilligt afgiver det. Til gengæld kan man mene, at den

grundlæggende moralske ret til privatliv *trumfer* andre dataetiske hensyn.¹⁶ Det betyder, at

man ikke behøver at veje forskellige hensyn mod hinanden – hvis retten til privatliv trumfer

andre hensyn, så er det altid samlet set forkert, at reducere en persons privatliv.

En grundlæggende moralsk ret:
Det er i sig selv dataetisk problematisk, at reducere en persons privatliv.

¹³ Se Olsen 1997.

¹⁴ Se Olsen & Jørgensen 2008.

¹⁵ Resolution 75/176 om The right to privacy in the digital age, vedtaget af FN's Generalforsamling den 16. December 2020.

¹⁶ I faglitteraturen kaldes moralske rettigheder, som kan tilsidesætte andre etiske hensyn, ofte "absolutte". Fortolkningen af moralske rettigheder som etiske hensyn, der trumfer andre typer etiske hensyn, forbindes især med den amerikanske retsfilosof Ronald Dworkin. Se: Dworkin 2005.

Selvom det er relativt almindeligt at forstå retten til privatliv som en grundlæggende moralsk rettighed, så findes der indvendinger imod denne fortolkning. Kritikere har argumenteret for, at der er situationer, hvor retten til privatliv må vige for andre hensyn, og situationer, hvor det slet ikke er dataetisk problematisk at reducere personers privatliv.¹⁷

En sammenfattende moralsk ret:
Det er dataetisk problematisk at reducere en persons privatliv, når der er dataetiske grunde til at lade være.

En moralsk ret til privatliv kan også forstås som en sammenfatning af de moralske hensyn i en situation. Hvis man forstår retten til privatliv på denne måde, så har en person en ret til privatliv, hvis der er dataetiske grunde til at ikke at reducere personens privatliv, især hvis disse grunde samlet set gør det forkert at reducere privatlivet.¹⁸

En fordel ved denne fortolkning er, at det er plausibelt at der kan være grunde til ikke at reducere personers privatliv. Ved at pege på disse grunde kan man forklare, hvorfor det er moralsk problematisk at reducere en persons privatliv.

Opgaven for denne fortolkning er til gengæld at præcisere de dataetiske hensyn, som kan give personer en moralsk ret til privatliv.

Privatliv og ydmygelse

En anden almindelig begrundelse for at tage dataetisk hensyn til privatliv er, at det kan være ydmygende eller ubehageligt, når andre får kendskab til visse personlige informationer. Oplevelsen af at få afsløret yd-

mygende eller ubehagelig personlig information kan endvidere skade personers selvværd, sociale status og relationer.

I visse tilfælde kan personlig information være ydmygende, fordi den afslører at man har handlet kritisabelt. I disse tilfælde kan man føle begrænset sympati med vedkommende. Men mange informationer har en karakter, hvor det kan være ydmygende, at andre får kendskab til dem, selvom de ikke viser, at man har gjort noget forkert.¹⁹

Ydmygelse og ubehag:

Det er dataetisk problematisk at reducere en persons privatliv, når det er ydmygende eller ubehageligt for personen.

Præcis hvilke personlige informationer det er ydmygende eller ubehageligt at dele, kan variere med konteksten og den enkeltes personlighed. Men hvis man mener, at vi i almindelighed bør forhindre, at personer oplever ydmygelse og ubehag, så giver denne risiko én grund til ikke at reducere personers privatliv.

¹⁷ Se Ryberg 2007; og Doyle 2009.

¹⁸ For en kritisk variant af denne udlægning, se Thomson 1975.

¹⁹ Se Solove 2007.

Privatliv og observationsstress

En tredje mulig begrundelse for at tage dataetisk hensyn til privatliv er, at det for de fleste mennesker kan være stressende at føle sig observeret eller overvåget. Det, at udføre en opgave, mens man oplever at blive observeret eller overvåget, har veldokumenterede mentale og fysiologiske stresseffekter.²⁰

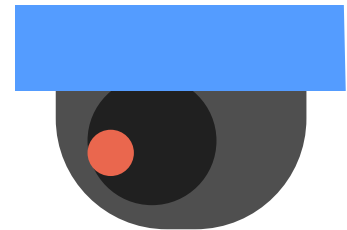
Mange vil nok også have erfaret sådanne effekter i deres eget liv. Der kan eksempelvis være stor forskel på at øve en tale eller et stykke musik når man er alene, og på at fremføre det, når man bliver observeret af en større forsamling. Indsamling, skabelse og deling af data med personlige informationer risikerer således at skabe eller øge observationsstress, simpelthen ved at udbrede eller intensivere oplevelsen af at blive observeret eller overvåget.

Observationsstress

Det er dataetisk problematisk at reducere en persons privatliv, når det er stressende for personen.

Et oplagt spørgsmål er hvor stor effekt det har, at føle sig observeret. Forskningen peger på, det kan afhænge af en række faktorer, blandt andet hvor mange data man deler, hvilke data man deler, og hvad formålet med at indsamle data er. Den negative effekt af stress kan også

variere. Mange mennesker oplever stress ind imellem, når der er travlt på arbejdet eller med familien, uden at det har alvorlige konsekvenser. Men stress kan have alvorlige konsekvenser, når det er intenst eller varer i længere perioder, både for det fysiske og psykiske helbred, og som afledte negative konsekvenser for eksempelvis sociale relationer, studier, eller karriere. Sandsynligheden for at tab af privatliv fører til observationsstress, og de negative effekter af stress, må vurderes i den konkrete sammenhæng. Men hvis man mener, at vi bør undgå at påføre andre personer stress, så udgør risikoen for observationsstress én mulig begrundelse for det dataetiske hensyn til privatliv.



²⁰

Giacosa, et al. 2023; Backhaus 2019; Smith, et al. 1992; Ravid, et al. 2023. Et beslægtet og mere komplekst spørgsmål er, om sådanne stresseffekter hæmmer eller gavner præstationer. Her tyder moderne forskning på, at dette både kan afhænge af hvilken type opgave, den pågældende person skal løse, og variere med personlighed. Aiello & Kolb 1995; Bhave 2014; Hills, et al. 2019.

Privatliv og relationer

Den fjerde mulige begrundelse for at tage dataetisk hensyn til privatliv er, at privatliv kan være vigtigt for, at personer kan forme og opretholde sociale relationer til andre.²¹

Relationer:

Det er dataetisk problematisk at reducere en persons privatliv, når det gør det vanskeligt, at forme eller opretholde værdifulde sociale relationer.

De fleste kender til, at personer deler forskellige dele af deres liv og forskellige sider af deres personlighed i forskellige relationer. Man viser én side af sig selv til sine venner, en anden til kollegaer, en tredje til sin romantiske partner, og en fjerde til familiemedlemmer, for eksempel til sine børn. Argumentet for privatliv er, at en del af grundlaget for at man kan have forskellige slags relationer er, at vi netop kan vælge at dele eller ikke dele forskellige sider af os selv. Og det kan være en vigtig del af en social relation, at man i netop denne relation deler visse intime personlige informationer, som man ikke deler med andre.

En indvending kunne være, at det ikke er klart, at personers mulighed for at forme relationer ved at holde information privat altid er moralsk værdifuld. Eksempelvis kunne en person som krænker en anden person, have et stærkt ønske om at begrænse andres kendskab til denne adfærd. Det kan netop skyldes, at det ville skade krænkerens sociale relationer, hvis krænkelserne blev almindeligt kendte. Sådanne eksempler synes at vise, at det måske kun er når muligheden for at forme relationer er moralsk værdifuld, at den kan begrunde det dataetiske hensyn til privatliv.

Privatliv og afskrækkelse

En femte mulig begrundelse for at tage dataetisk hensyn til privatliv er, at truslen om tab af privatliv, kan have en negativ, afskrækkende effekt på personers adfærd.

Afskrækkelse:

Det er dataetisk problematisk at reducere en persons privatliv, når det afskrækker uskyldig eller gavnlig adfærd.

Det er en almindelig antagelse i mange sammenhænge, at indsamling af data kan påvirke den måde personer handler. I nogle tilfælde kan det være gavnligt at bruge truslen om tab af privatliv til at afskrække adfærd. Videoovervågning i det offentlige rum begrundes eksempelvis ofte med, at overvågningen afskrækker potentielle kriminelle fra at begå forbrydelser.²² Indsamling skabelse og deling af personlige informationer kan imidlertid også tænkes at afskrække adfærd, som der er grund til at beskytte eller fremme. I faglitteraturen omtales dette som en "afkølende effekt" (eng. "chilling"). Truslen om tab af privatliv kunne eksempelvis tænkes at afskrække borgere fra demokratiske aktiviteter, såsom deltagelse i politisk debat på internettet og demonstrationer i det offentlige rum.²³

²¹ Se Marmor 2015; Nagel 1998; Rachels 1975.

²² Det er værd at bemærke, at det diskuteres i forskningen, om videoovervågning i det offentlige rum faktisk har en kriminalpræventiv effekt. Se Welsh & Farrington 2009; Alexandrie 2017.

²³ Se Stoycheff, et al. 2019; Penney 2017; Penney 2016.

En udfordring for begrundelsen er, at det har vist sig at være meget vanskeligt at måle de negative afskrækkende effekter. Det er derfor endnu uklart både hvornår de optræder, og hvor store de er. Men hvis indsamling, skabelse og deling af personlige informationer afskrækker adfærd, og vi har grund til at beskytte denne adfærd, så kan denne effekt begrunde det dataetiske hensyn til privatliv.

Privatliv og sårbarhed

Den sidste mulige begrundelse for at tage dataetisk hensyn til privatliv handler om, hvordan kendskab til personlig information kan gøre personer sårbare. Det skyldes at de måder, vi behandler hinanden på, ofte afhænger af hvad vi ved om andre, og at nogle måder personer kan behandle hinanden på er uetiske.²⁴

Sårbarhed:

Det er dataetisk problematisk at reducere en persons privatliv, når det gør personen sårbar for uetiske handlinger.

De fleste mener, at sårbarhed er en væsentlig grund til at beskytte personers privatliv. Et simpelt eksempel er at en person bliver sårbar, hvis andre får kendskab til vedkommendes adgangskoder til e-mail- og bankkonti, fordi disse informationer kan misbruges. Et andet velkendt eksempel er forbuddet mod at opsøge information om aktuel eller planlagt graviditet i forbindelse med ansættelse, som er motiveret af, at ansøgeren bliver sårbar for diskrimination, hvis arbejdsgiveren får kendskab til disse informationer. Personer kan også blive sårbare overfor afpresning, manipulation, og sammenstilling af data, som afslører ny, følsom information.²⁵

Sårbarhed handler om risikoen for at andre agenter kan bruge information til at handle uetisk, for eksempel ved at skade personen. Det vil derfor variere med konteksten hvilke personlige informationer en person bliver sårbar af at dele.

Men når indsamling, skabelse og deling af personlige informationer gør en person sårbar, og vi har grund til at beskytte personen mod denne sårbarhed, så kan sårbarheden begrunde det dataetiske hensyn til privatliv.



²⁴ Velíz 2019.

²⁵ Se Solove 2006; Macnish 2015.

Litteratur

- Aiello, J. R. & Kolb, K. J. (1995). "Electronic performance monitoring and social context: Impact on productivity and stress." *Journal of Applied Psychology* 80: 339–353 DOI: 10.1037/0021-9010.80.3.339.
- Alexandrie, G. (2017). "Surveillance cameras and crime: a review of randomized and natural experiments." *Journal of Scandinavian Studies in Criminology and Crime Prevention* 18(2): 210–222 DOI: 10.1080/14043858.2017.1387410.
- Asgarinia, H. (2023). "Convergence of the source control and actual access accounts of privacy." *AI and Ethics* DOI: 10.1007/s43681-023-00270-z.
- Backhaus, N. (2019). Context Sensitive Technologies and Electronic Employee Monitoring: a Meta-Analytic Review. 2019 IEEE/SICE International Symposium on System Integration (SI).
- Bhave, D. P. (2014). "The Invisible Eye? Electronic Performance Monitoring and Employee Job Performance." *Personnel Psychology* 67(3): 605–635 DOI: <https://doi.org/10.1111/peps.12046>.
- Davis, S. (2009). "Is there a right to privacy?" *Pacific Philosophical Quarterly* 90(4): 450–475.
- Doyle, T. (2009). "Privacy and perfect voyeurism." *Ethics and Information Technology* 11(3): 181–189 DOI: 10.1007/s10676-009-9195-9.
- Dworkin, R. (2005). *Taking Rights Seriously*. London, Gerald Duckworth & Co. Ltd.
- Gavison, R. (1980). "Privacy and the Limits of Law." *The Yale Law Journal* 89(3): 421–471 DOI: 10.2307/795891.
- Giacosa, E., Alam, G. M., Culasso, F. & Crocco, E. (2023). "Stress-inducing or performance-enhancing? Safety measure or cause of mistrust? The paradox of digital surveillance in the workplace." *Journal of Innovation & Knowledge* 8(2) DOI: 10.1016/j.jik.2023.100357.
- Hills, P. J., Dickinson, D., Daniels, L. M., Boobyer, C. A. & Burton, R. (2019). "Being observed caused physiological stress leading to poorer face recognition." *Acta Psychol (Amst)* 196: 118–128 DOI: 10.1016/j.actpsy.2019.04.012.
- Inness, J. (1992). *Privacy, intimacy, and isolation*. Oxford, Oxford University Press.
- Lundgren, B. (2020). "A Dilemma for Privacy as Control." *The Journal of Ethics* 24(2): 165–175 DOI: 10.1007/s10892-019-09316-z.
- Macnish, K. (2015). "An Eye for an Eye: Proportionality and Surveillance." *Ethical Theory and Moral Practice* 18(3): 529–548.
- Macnish, K. (2018). "Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World." *Journal of Applied Philosophy* 35(2): 417–432.
- Mainz, J. (2021). "An Indirect Argument for the Access Theory of Privacy." *Res Publica* 27(3): 309–328 DOI: 10.1007/s11158-021-09521-4.
- Marmor, A. (2015). "What Is the Right to Privacy?" *Philosophy and Public Affairs* 43(1): 3–26.
- McCloskey, H. J. (1980). "Privacy and the Right to Privacy." *Philosophy* 55(211): 17 – 38.
- Menges, L. (2021). "A Defense of Privacy as Control." *The Journal of Ethics* 25(3): 385–402 DOI: 10.1007/s10892-020-09351-1.

Moore, A. D. (2003). "Privacy: Its Meaning and Value." *American Philosophical Quarterly* 40(3): 215-227. <http://www.jstor.org/stable/20010117>.

Munch, L. & Mainz, J. (2023). "To Believe, or Not to Believe – That is Not the (Only) Question: The Hybrid View of Privacy." *The Journal of Ethics* DOI: 10.1007/s10892-023-09419-8.

Nagel, T. (1998). "Concealment and Exposure." *Philosophy and Public Affairs* 27(1): 3-30.

Nissenbaum, H. (2004). "Privacy as contextual integrity." *Washington Law Review* 79(1): 101-139.

Olsen, B. K. (1997). "Den menneskeretlige privatlivsbeskyttelse og ny teknologi." *Grundloven og menneskerettigheder*. Morten Kjærum, Djøf 125-143.

Olsen, B. K. & Jørgensen, R. F. (2008). "The right to respect for privacy." *Human Rights Monitoring – A Field Mission Manual*. Anette Faye Jacobsen, Martinus Nijhoff Publishers: 403-430.

Parent, W. A. (1983). "Privacy, morality, and the law." *Philosophy and Public Affairs* 12(4): 269-288.

Penney, J. W. (2016). "Chilling effects: Online surveillance and Wikipedia use." *Berkeley Technology & Law Journal* 31(1): 118-182.

Penney, J. W. (2017). "Internet surveillance, regulation, and chilling effects online: a comparative case study." *Internet Policy Review* 6(2): 1-39.

Powers, M. (1996). "A cognitive access definition of privacy." *Law and Philosophy* 15(4): 369 - 386.

Rachels, J. (1975). "Why privacy is important." *Philosophy & Public Affairs* 4(4): 323-333.

Ravid, D. M., White, J. C., Tomczak, D. L., Miles, A. F. & Behrend, T. S. (2023). "A meta-analysis of the effects of electronic performance monitoring on work outcomes." *Personnel Psychology* 76(1): 5-40 DOI: <https://doi.org/10.1111/peps.12514>.

Roessler, B. (2005). *The Value of Privacy*, Polity Press.

Rubel, A. (2007). "Claims to Privacy and the Distributed Value View." *San Diego Law Review* 44(4): 921-956. <http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=31197946&site=ehost-live>.

Rubel, A. (2011). "The Particularized Judgment Account of Privacy." *Res Publica* 17(3): 275-290.

Ryberg, J. (2007). "Privacy Rights, Crime Prevention, CCTV, and the Life of Mrs. Aremac." *Res Publica* 13(2): 127-143.

Smith, M. J., Carayon, P., Sanders, K. J., Lim, S. Y. & LeGrande, D. (1992). "Employee stress and health complaints in jobs with and without electronic performance monitoring." *Applied Ergonomics* 23(1): 17-27 DOI: [https://doi.org/10.1016/0003-6870\(92\)90006-H](https://doi.org/10.1016/0003-6870(92)90006-H).

Solove, D. J. (2006). "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154(3): 477-560.

Solove, D. J. (2007). "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." *San Diego Law Review* 44: 745-772.

Stoycheff, E., Liu, J., Xu, K. & Wibowo, K. (2019). "Privacy and the Panopticon: Online mass

surveillance's deterrence and chilling effects." *New Media & Society* 21(3): 602–619 DOI: 10.1177/1461444818801317.

Tavani, H. T. (2007). "Philosophical theories of privacy: Implications for an adequate online privacy policy." *Metaphilosophy* 38(1): 1–22.

Thomson, J. J. (1975). "The Right to Privacy." *Philosophy & Public Affairs* 4(4): 295–314 DOI: 10.2307/2265075.

Velíz, C. (2019). "The Internet and Privacy." *Ethics and the Contemporary World*. David Edmonds. Abingdon, Routledge: 149–159.

Welsh, B. C. & Farrington, D. P. (2009). "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis." *Justice Quarterly* 26(4): 716–745.

Westin, A. F. (1967). *Privacy and Freedom*. New York, Ig Publishing.

Dataetisk Råd

Dataetisk Råd er en offentlig myndighed, som rådgiver om etiske udfordringer ved nye digitale teknologier.

Læs mere på **dataetiskraad.dk**

Illustrationer ved Grobowski

København 6. Oktober 2025.