



PERSONVERNUNDERSØKELSEN 2019/2020

Om befolkningens holdninger til personvern og
kjennskap til det nye personvernregelverket

Innhold

INNLEDNING	3
SAMMENDRAG	4
ET NYTT PERSONVERNREGELVERK	6
Kjennskap til det nye personvernregelverket	6
Kjennskap til personvernrettighetene	7
Sosioøkonomisk status påvirker kjennskap til regelverket	8
TAP AV KONTROLL OG HOLDNINGER TIL PERSONVERN	10
Personvern er en viktig verdi	10
Opplevelse av tap av kontroll og maktesløshet	11
Hvilke opplysninger er særlige beskyttelsesverdige?	12
HVEM STOLER VI PÅ? VARIERENDE GRAD AV TILLIT.	16
Offentlige virksomheter nyter stor tillit	17
Lav tillit til meldingstjenester, søkemotorer og sosiale medier	18
Unngår å bruke tjenester på grunn av usikkerhet	18
PERSONOPPLYSNINGER TIL REKLAME, TJENESTER OG PRODUKTER	20
Negative til målrettet annonsering	20
Skeptiske til målretting av politiske budskap	22
Negative til å dele finansielle opplysninger	23
Google og Facebook i finansmarkedet	24
Lite interesse for banktjenester fra Google eller Facebook	25
Tingenes internett og smarte hjem	25
NEDKJØLINGSEFFEKTEN	28
Tendenser til nedkjølingseffekt i frykt for overvåking fra offentlige myndigheter	28
Endrer adferd på grunn av usikkerhet om hvordan private virksomheter bruker opplysningene	30
REFERANSER	33
VEDLEGG – INTERVJUGUIDE	36

Innledning

Personvernforordningen (General Data Protection Regulation, GDPR) trådte i kraft i Norge 20. juli 2018, som en del av den nye personopplysningsloven. Innføringen av dette regelverket styrket og harmoniserte personvernet for borgerne i EU og EØS-landene.

I Norge har regelverket ført til store endringer. Både private selskap og offentlige myndigheter har vært nødt til å gjennomgå rutiner og praksis knyttet til deres behandling av personopplysninger for å tilfredsstille kravene i den nye loven. Regelverket styrker rettighetene til norske og europeiske borgere når våre personopplysninger samles inn og brukes.

Vi lever i digitaliseringens tidsalder. Stadig større deler av hverdagen, handlingene og kommunikasjonen vår flyttes over i sfærer tilkoblet internett. Nesten alle bærer til enhver tid med seg en smarttelefon med kapasitet til å overvåke oss døgnet rundt. Det er vanskelig å ha full kontroll over hvilke opplysninger vi gir fra oss, hvem som samler dem inn og hva de brukes til.

Samtidig har vi i dag en helt annen forventning til hvordan våre data brukes enn for noen år tilbake. Persondata har stor verdi, og vi er bare i begynnelsen av en utvikling der nye tjenester og produkter utvikles og tilpasses den enkelte. I de fleste tilfeller forutsetter personalisering av tjenester bruk av store mengder personopplysninger. Da er det viktig at dataene blir brukt riktig, ansvarlig og i tråd med våre forventninger.

Noe av datainnsamlingen er en forutsetning for at selskapene skal kunne tilby tjenestene som leveres, men selskapene tjener også store penger på den kunnskapen de utvinner fra analyse av de enorme datamengdene som samles inn. En av vår tids store utfordringer er å finne den rette balansegangen mellom datadrevet verdiskaping og individets grunnleggende rett til personvern.

I november 2019 gjennomførte vi en spørreundersøkelse om befolkningens holdninger til personvern og kjennskap til det nye personvernregelverket. I denne rapporten presenterer vi de viktigste funnene fra undersøkelsen.

Rapporten har fem deler der vi ser nærmere på aktuelle problemstillinger i dagens personverndebatt, slik som:

- Hvor godt kjenner befolkningen det nye personvernregelverket og rettighetene de har?
- Føler folk at de har kontroll over sine egne personopplysninger?
- Hvem stoler befolkningen på at samler inn og behandler personopplysningene deres?
- I hvor stor grad er folk villige til å dele personopplysningene sine for å få tilgang til nye tjenester og produkter?
- Og, endrer folk på vaner og gjøremål når de er usikre på hvem som ser hva de gjør og hvordan opplysningene de legger igjen blir brukt?

Om undersøkelsen

Opinion utførte undersøkelsen på vegne av Datatilsynet. Datainnsamlingen ble gjennomført i perioden 15. til 28. november 2019. Respondentene svarte på web. Målgruppen var befolkningen i Norge fra 15 år og oppover. Utvalget er et representativt tilfældighetsutvalg med 1501 respondenter (n=1501). Resultatene er vektet på kjønn, alder og geografi. Feilmarginene i undersøkelsen ligger innenfor 1,1 og 2,5 prosentpoeng.

Det har tidligere vært gjennomført flere personvernundersøkelser på vegne av Datatilsynet. De største var i [1997](#), [2005](#), [2008](#) og [2013/14](#). Denne undersøkelsen bygger på kunnskap fra disse, og i noen tilfeller viser vi til trender over tid.

Sammendrag

Nordmenn har god kunnskap om det nye personvernregelverket. Sosioøkonomisk status påvirker kjennskapen

To av tre nordmenn kjenner til det nye personvernregelverket som ble innført i 2018. Det er svært positivt at regelverket er så godt kjent i befolkningen. Likevel, en bekymringsverdig tendens er at kjennskapen til regelverket og rettighetene har nær sammenheng med sosioøkonomisk status. Hvis man har høy inntekt og universitetsutdanning, er det langt mer sannsynlig at man kjenner til regelverket og rettighetene. Uten kjennskap til grunnleggende personvernrettigheter slik som innsyn, retting, informasjon, begrensning og dataportabilitet, kan man heller ikke utøve rettighetene sine i den utstrekningen som regelverket skal legge til rette for.

Fødselsnummer, kommunikasjon og biometri oppleves som mest beskyttelsesverdig

Folk opplever ikke alle personopplysninger som like beskyttelsesverdige. Fødselsnummer, biometriske data og innholdet i privat kommunikasjon vurderes som mest beskyttelsesverdig av respondentene. Befolkningens syn på hvilke opplysninger som er mest beskyttelsesverdige samsvarer ikke alltid med lovverket. Opplysninger om religiøs og politisk tilhørighet, samt fagforeningsmedlemskap, nyter et særlig vern i loven, men anses som minst beskyttelsesverdig av de spurte. Den andelen som anser slike opplysninger som beskyttelsesverdige, har imidlertid økt de siste årene.

Tilliten til offentlige virksomheter er høyere enn til private virksomheter

Undersøkelsen viser at nordmenn gjennomgående har høy tillit til hvordan offentlige virksomheter behandler personopplysninger. NAV, skoler og barnehager er unntakene, hvor tillitsnivået relativt sett er lavere. Svarene viser at tilliten er lavest til virksomheter som driver med sosiale medier, meldingstjenester og søkemotorer.

Halvparten av de spurte har avstått fra å bruke en tjeneste på grunn av manglende tillit

At en virksomhet ikke har tillit, har konsekvenser for folks bruk av tjenestene de leverer. Over halvparten av respondentene har avstått fra å bruke en tjeneste fordi de er usikre på hvordan personopplysningene deres blir håndtert.

Svært mange føler at de har liten kontroll over personopplysningene på internett

Nær syv av ti av de spurte føler at de har lite kontroll over hvordan personopplysningene deres lagres og brukes på internett. Seks av ti svarer at de føler seg maktesløse når det gjelder å ha kontroll over egne personopplysninger på internett. Følelsen av å ha liten kontroll og å føle seg maktesløs er lik på tvers av generasjoner og sosioøkonomiske skillelinjer.

Folk er negative til målretting av annonser

I tråd med tidligere undersøkelser vi har gjennomført, ser vi en tydelig skepsis mot forretningsmodellen som dagens internett bygger på. Tre av fire er negative til at personopplysninger samles inn av private selskaper for å personalisere annonser på internett. Kun åtte prosent er positive. Om lag like mange er negative til at politiske partier målretter politiske budskap basert på personlig informasjon hentet fra internett. Aksepten for denne måten å drive politisk påvirkningsarbeid er svært lav, samtidig som dette er en valgkampmetode norske partiene har begynt å ta i bruk.

Flertallet er negative til å dele å dele kontoopplysningene sine med aktører utenfor bank- og finanssektoren for å få tilgang til nye banktjenester

Et nytt europeisk regelverk (betalingstjenestedirektivet) legger til rette for at vi skal kunne dele våre kontoopplysninger med andre virksomheter enn bankene, og dermed fremme konkurranse i markedet

for betalingstjenester. Fire av fem nordmenn er imidlertid negative til å dele disse opplysningene med andre aktører enn bankene, selv om formålet er å utvikle betalingstjenester de kan ha nytte av.

Skepsisen til Google og Facebooks inntreden i bankmarkedet er spesielt tydelig. 84 prosent av de spurte er negative til at disse virksomhetene skal ha tilgang til de finansielle opplysningene deres.

Halvparten av de spurte er utrygge på hvordan internettilkoblet teknologi i hjemmet behandler og lagrer personinformasjon

Tingenes internett muliggjør at hjemmene våre fylles av internettilkoblede gjenstander som «snakker» med hverandre, slik som støvsugere, kjøleskap, strømmålere og smartassistenter. Nesten halvparten av de spurte sier at de føler seg utrygge på om smarthusteknologi samler inn og behandler informasjon på en måte som ivaretar personvernet.

Sterk nedkjølingseffekt som følge av usikkerhet knyttet til private selskapers bruk av personopplysninger

Usikkerhet knyttet til at vi ikke vet hvordan opplysninger som samles om oss blir brukt, kan føre til at vi endrer atferd. Denne selvreguleringen som følge av overvåkingsfrykt kalles «nedkjølingseffekten». Undersøkelsen avdekker at svært mange svarer at de endrer atferd eller unnlater å gjøre en rekke aktiviteter på grunn av usikkerhet knyttet til selskapenes bruk av deres personopplysninger.

Halvparten av de spurte avstår fra å delta i fri meningsutveksling på nett som følge av denne usikkerheten. Det er også én av tre som avstår fra å søke informasjon på internett og én av to unnlater å gjennomføre netthandel. Den store andelen som endrer atferd som følge av usikkerhet knyttet til hvordan deres opplysninger blir brukt, må også sees i sammenheng med den lave tilliten til de store teknologiselskapene.

Undersøkelsen viser også at en betydelig andel utøver selvsensur som følge av usikkerhet knyttet til myndighetsovervåking.

Et nytt personvernregelverk

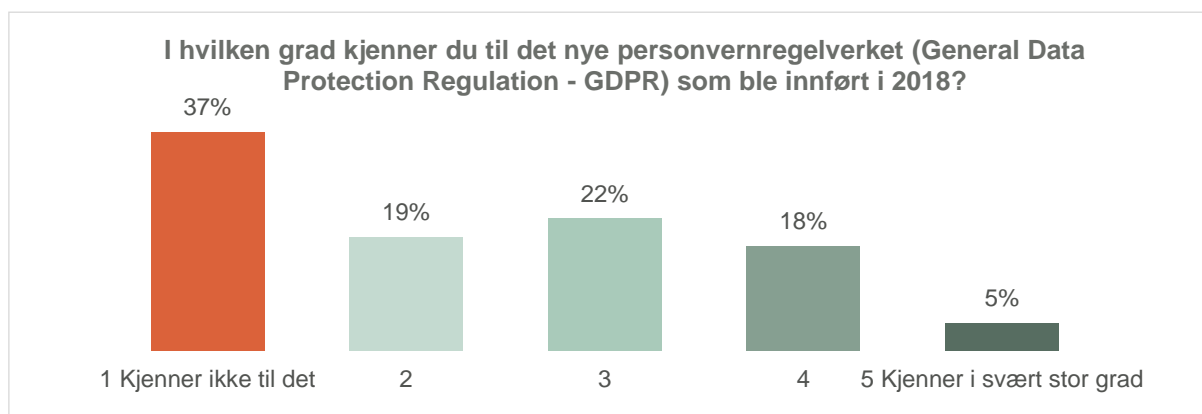
I 2018 fikk Norge en ny personopplysningslov. Loven består av nasjonale regler og EUs personvernforordning (General Data Protection Regulation, GDPR). Personvernforordningen inneholder et sett med regler som gjelder for alle EU/EØS-land, og gir virksomhetene flere plikter når de behandler personopplysninger. Regelverket har også gitt nye personvernrettigheter til norske borgere, samt videreført mange av rettighetene fra det gamle regelverket.

Virksomhetenes etterlevelse av det nye regelverket har vært varierende. Det har vært en sterk økning i antall innmeldte brudd på personopplysningssikkerheten (avviksmeldinger) i etterkant av at regelverket ble innført. Det har også vært vedtatt store overtredelsesgebyrer for brudd av loven, både i Norge og Europa for øvrig.

Datatilsynet mottar mange spørsmål fra enkeltpersoner om personvern og deres rettigheter. Vi har derfor undersøkt hvor godt folk kjenner til regelverket og rettighetene sine, og hvorvidt de mener at personvernet har blitt styrket som følge av innføringen av personvernforordningen.

Kjennskap til det nye personvernregelverket

En grunnleggende forutsetning for å kunne utøve rettighetene regelverket gir, er at man kjenner til det. Vi har spurt om i hvilken grad folk kjenner til det nye personvernregelverket.

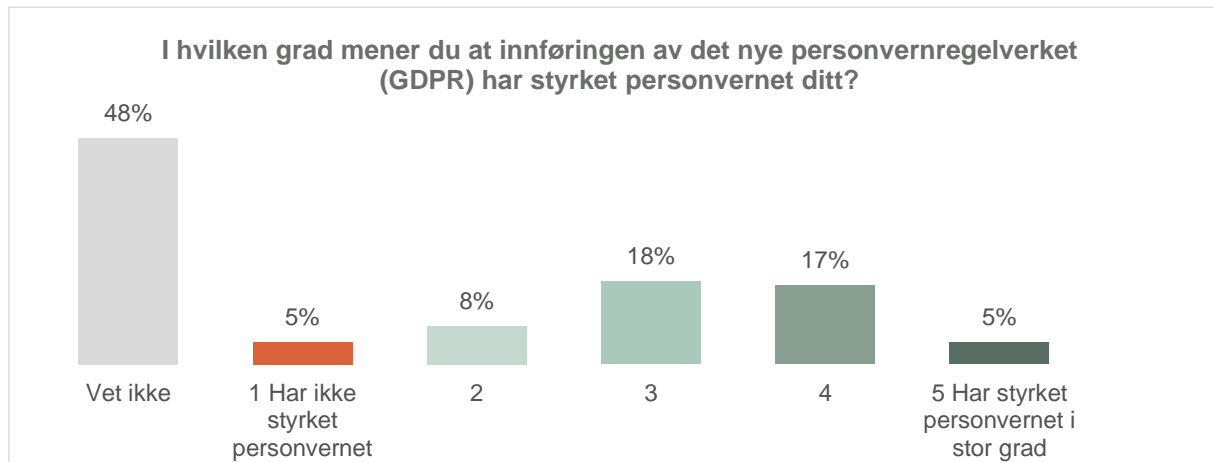


Svarene viser:

- Om lag to av tre nordmenn kjenner til det nye personvernregelverket. 37 prosent svarer at de ikke kjenner til regelverket.
- Kjennskapen til regelverket er lavest blant de under 30 og de over 60 år.
- Høyt utdannede har best kjennskap til regelverket. Åtte av ti nordmenn med mer enn fire års universitets- eller høyskoleutdanning kjenner til regelverket, mens det samme gjelder for kun seks av ti med videregående skole som høyeste utdanning.
- Av de som har en årslønn på over 600 000,- kroner har 86 prosent kjennskap til regelverket. 54 prosent av de som tjener mindre enn 400 000,- kroner oppgir at de ikke kjenner til regelverket.

Det er positivt at et stort flertall av norske borgere kjenner til det nye europeiske regelverket. Den store mediedekningen og det store antallet e-poster mange fikk før forordningen ble innført – knyttet til fornying av samtykke til å behandle personopplysningene deres – har sannsynligvis bidratt til dette. Det er likevel et stort antall av befolkningen (37 prosent) som ikke kjenner til regelverket. Dette kan ha betydning for om folk har kunnskap om sine rettigheter, og er i stand til å utøve dem. [Ifølge en studie](#)

utført på vegne av EU-kommisjonen, kjenner 67 prosent av europeere til personvernforordningen (GDPR). Kjennskapen i Norge ligger med andre ord litt under det europeiske gjennomsnittet.



Svarene viser:

- Nesten halvparten av respondentene (48 prosent) mener at innføringen av det nye personvernregelverket har styrket deres personvern fra liten og opp til stor grad.
- Like mange (48 prosent) svarer at de ikke vet.
- Fem prosent oppgir at det ikke har styrket personvernet.

Med unntak av de som svarer «vet ikke», så oppgir de fleste at innføringen av det nye regelverket har styrket deres personvern. Det er få som mener at regelverket ikke har styrket deres personvern.

Det er likevel nesten halvparten av respondentene som ikke har tatt et standpunkt til spørsmålet. At det er et så stort antall som svarer «vet ikke», reflekterer delvis at det er en relativt stor andel som ikke kjenner til regelverket. Mange kan nok også synes at det er vanskelig å ta stilling til spørsmålet ettersom de ikke har hatt tid til å opparbeide seg en personlig erfaring med regelverket, eller at de synes at det er for komplisert å gjøre en vurdering.

Kjennskap til personvernrettighetene

Personvernforordningen gir enkeltpersoner en rekke rettigheter. For eksempel går retten til innsyn ut på at enkeltpersoner kan spørre en virksomhet om hvilke personopplysninger som er lagret om dem og hvordan opplysningene behandles. Retten til informasjon innebærer at virksomheter har en plikt til blant annet å gi kort og forståelig informasjon om hvordan de behandler personopplysningene de samler inn. Retten til retting betyr at man kan kreve at opplysninger rettes eller suppleres hvis de er uriktige. Retten til sletting innebærer at man i enkelte tilfeller kan kreve at personopplysninger slettes. Dette kalles noen ganger «retten til å bli glemt».

En av de nye rettighetene er retten til dataportabilitet. Denne retten innebærer at man kan få utlevert personopplysningene sine fra en virksomhet og gjenbruke disse som man vil, på tvers av ulike systemer og tjenester. Dette vil gjøre det lettere å bytte tjenesteleverandører, siden man enkelt kan ta med seg opplysningene sine til den leverandøren som tilbyr de beste vilkårene. Retten til dataportabilitet gjelder kun opplysninger som man selv har gitt fra seg bevisst og aktivt.

En grunnleggende forutsetning for å benytte seg av disse rettighetene, er at man kjenner til dem. Derfor har vi spurt respondentene om hvilke rettigheter i personvernregelverket de har hørt om. Siden respondentene blir informert om rettighetene i spørsmålsformuleringene, kan prosentene være høyere enn dersom de ikke ble hjulpet.



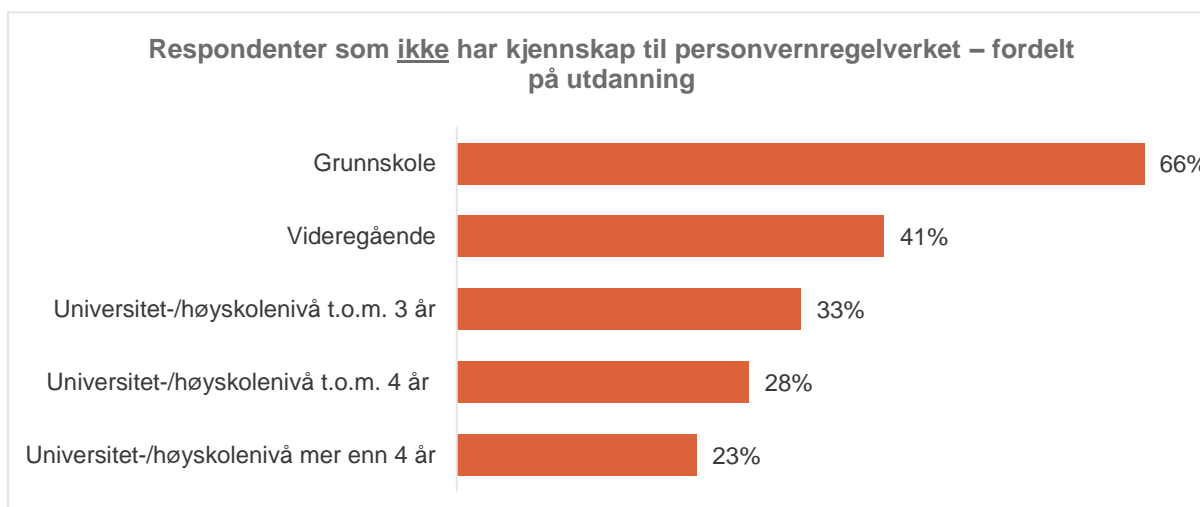
Svarene viser:

- Med unntak av retten til dataportabilitet kjenner over halvparten av befolkningen til de ulike rettighetene.

Om lag to av tre er klar over at de har en lovfestet rett til innsyn. Omtrent like mange har kjennskap til at de i visse tilfeller kan be en virksomhet som behandler personopplysninger om å få disse slettet, eller nekte behandlingen av disse opplysningene. Selv om retten til dataportabilitet er minst kjent, oppgir en betydelig andel å vite om den. Vi har imidlertid ikke tall på hvor mange som faktisk benytter seg av denne nye rettigheten.

Sosioøkonomisk status påvirker kjennskap til regelverket

Undersøkelsen viser også at kjennskap til regelverket og rettighetene samsvarer sterkt med inntekt og utdanning. Hvis man har høy inntekt og høyskole-/universitetsutdanning, er det mer sannsynlig at man kjenner til regelverket og rettighetene som følger av det. Hvis man har lavere inntekt og høyeste utdanning fra grunn- eller videregående skole, har man generelt lavere kjennskap til regelverket og de rettighetene loven fastslår at man har.





Uten kjennskap til grunnleggende personvernrettigheter, kan man heller ikke utøve rettighetene slik regelverket legger til rette for. Det er problematisk at de med lavere utdanning og inntekt i så stor grad har mindre kjennskap til regelverket. I ytterste konsekvens betyr det at ressurssterke personer har et sterkere rettsvern enn ressursvake, fordi de har bedre kjennskap til regelverket og rettighetene sine. Datatilsynet får mange henvendelser om overvåking i arbeidslivet fra ufaglærte og arbeidstakere i lavtlønnsyrker. At vår undersøkelse viser at personer uten høyere utdanning har mindre kunnskap om sine rettigheter, er bekymringsverdig med tanke på folks personvern på slike arbeidsplasser.

Forbruksforskningsinstituttet (SIFO) har også vist til at sosioøkonomiske forhold er utslagsgivende for enkeltpersoners forhold til personvern og personvernregelverket. I undersøkelsen «[Tillit og sårbarhet på nett](#)» viste de at folk som identifiserte seg som «arbeiderklasse», har mindre tro på at personvernforordningen vil gi større trygghet på nett enn de som identifiserte seg som «middelklasse». Samtidig fant de at mens det finnes generell usikkerhet knyttet til personvern og personvernforordningen i alle grupper, er usikkerheten størst blant de yngre, de fra arbeiderklassen og de som ikke er i inntektsgivende arbeid. I [en rapport utført på vegne av EU-kommisjonen](#) fant de også at personer med minst økonomiske problemer hadde en større sannsynlighet for å ha hørt om GDPR.

Holdninger til personvern og tap av kontroll

Personvern handler blant annet om at vi skal ha kontroll over våre egne personopplysninger. Mengden opplysninger som samles inn når vi bruker digitale tjenester, utfordrer denne kontrollen. Vi deler personopplysninger bevisst og ubevisst når vi handler på nett, bruker tid i sosiale medier, eller når vi tar i bruk ulike digitale kunde- og publikumstjenester. Vår aktivitet på internett blir sporet av kommersielle virksomheter som bruker informasjonen til å sende oss persontilpasset reklame. Mange opplysninger blir også brukt og delt mellom veldig mange selskap, aktører og tjenester. Informasjon som du kanskje ikke engang visste at du hadde gitt fra deg, kan bli brukt til å lage profiler på deg. Det er lett å miste oversikt og kontroll.

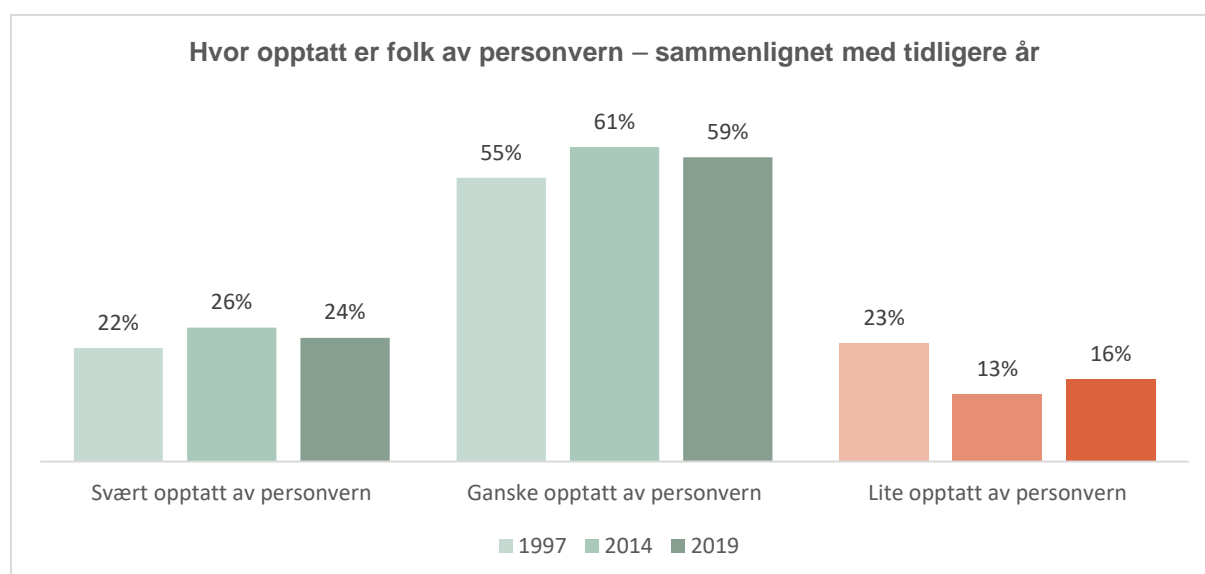
Personvernregelverket skal hjelpe enkeltpersoner til å ta kontroll over opplysningene sine, gi folk større makt til å skjerme opplysningene sine og styrke retten til å vite hvordan opplysningene brukes. At man legger igjen så mange spor at man mister oversikten over hva andre vet, er en stor utfordring for personvernet.

I dette kapitlet vil vi se nærmere på hvor opptatt folk er av personvern, og i hvilken grad de opplever at de har kontroll over personopplysningene sine. Vi har også spurt om hvilke opplysninger respondentene mener er særlig beskyttelsesverdige.

Personvern er en viktig verdi

Stadig større deler av livene våre er gjenstand for sporing og registrering. Smarttelefonen de fleste bærer med seg til enhver tid deler informasjon om hvor man beveger seg. Nettsider og applikasjoner selger opplysninger om oss til selskap vi ikke kjenner. I sosiale medier deler folk villig sine tanker, følelser, interesser, verdier og sosiale nettverk. Hjemmet, definisjonen på den innerste private sfære, fylles opp av smarte strømmålere, stemmeassistenter og annen internettilkoblet forbrukerelektronikk som sporer atferden vår.

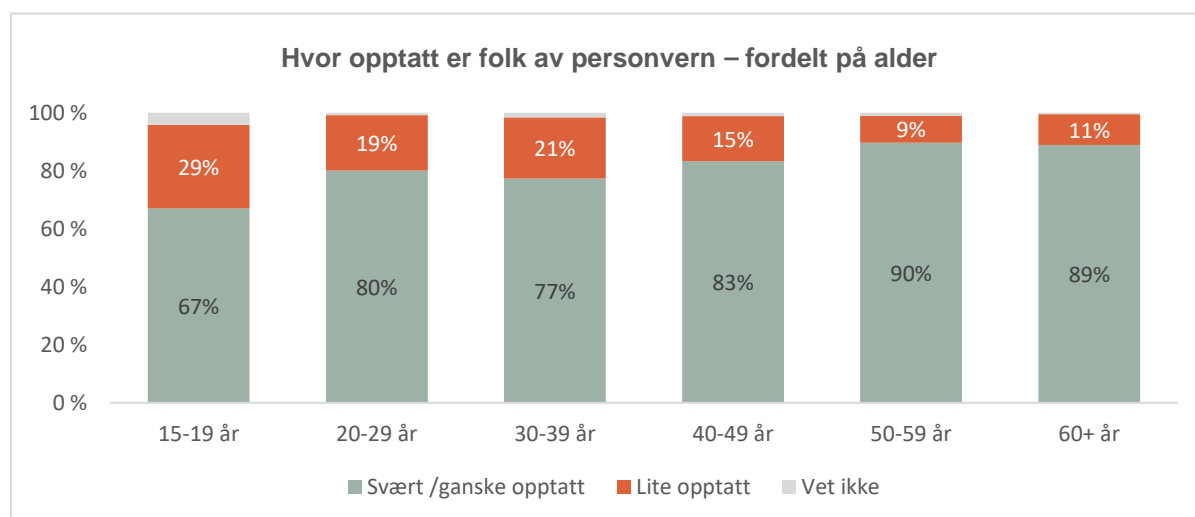
Er personvern fortsatt en verdi folk flest bryr seg om, eller er det en rettighet og verdi folk villig ofrer for tilgang til brukervennlige tjenester og produkter? Hadde Facebook-grunnlegger Mark Zuckerberg rett da han i 2010 proklamerte at [personvern ikke lenger er en sosial norm](#)? Vi har spurt hvor opptatt befolkningen er av personvern, og sammenlignet svarene med undersøkelser gjennomført i 1997 og 2014.



Svarene viser:

- 83 prosent er svært eller ganske opptatt av personvern.
- En litt større andel er opptatt av personvern i 2019 forhold til 1997.
- En litt mindre andel er opptatt av personvern i 2019 i forhold til 2014.

I forhold til 1997, deler befolkningen i dag enorme mengder opplysninger om seg selv. Samtidig viser svarene at folk var noe mer opptatt av personvern i 2014. Tallene viser uansett tydelig at personvern er en levende og viktig verdi i dagens samfunn, og at det lenge har vært det.



Svarene viser at:

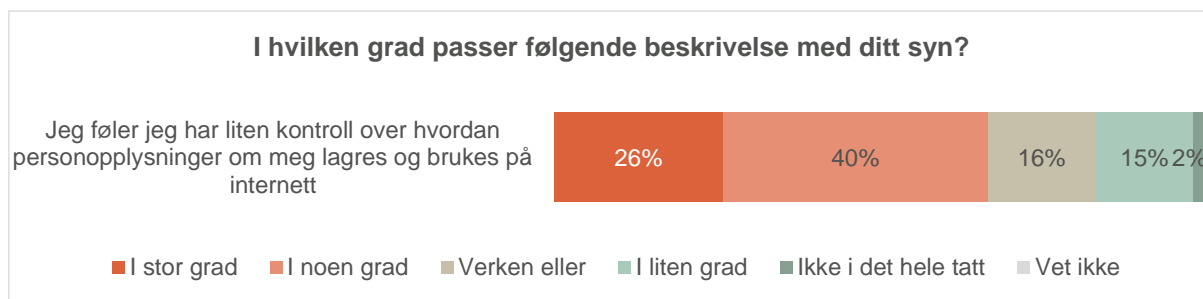
- De som er eldst oppgir å være mest opptatt av personvern.

29 prosent av de som er mellom 15 og 19 år, oppgir å være lite opptatt av personvern. Dette er 18 prosentpoeng flere enn de som svarer det samme og er 60 år og eldre. Den store majoriteten av den yngste aldersgruppen i undersøkelsen, nesten 70 prosent, er likevel ganske eller svært opptatt av personvern. Dette er funn som samsvarer med tidligere personvernundersøkelser. Forskning på barn og unges mediebruk viser imidlertid at mange unge [tar grep for å beskytte personvernet sitt på internett](#).

Opplevelse av tap av kontroll og maktesløshet

Ulike nettsamfunn og nettsider gir ulik kontroll over hva man deler med andre, og hva man gir fra seg av personopplysninger. Delingen av personopplysninger skjer ofte frivillig, for eksempel når man vil ha tilgang til digitale tjenester og produkter. Ulike sporingsmetoder på internett fører likevel ofte til at man ubevisst deler informasjon om egne karaktertrekk og interesser. Når man daglig interagerer med en lang rekke tjenester, selskap og plattformer som samler inn personopplysninger både åpent og i det skjulte, er det lett å miste oversikt.

Vi ønsket å finne ut i hvilken grad folk føler at de har kontroll over sine personopplysninger når de ferdes på nett. For å måle graden av opplevd kontroll har vi bedt respondentene om å ta stilling til to påstander:

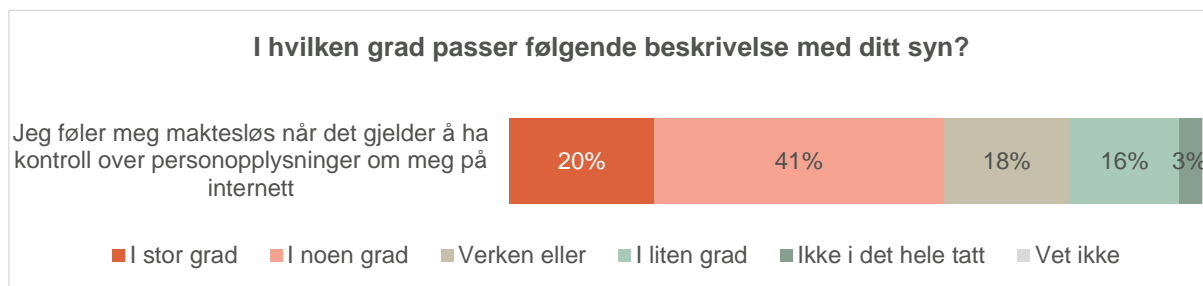


Svarene viser:

- 66 prosent, nesten syv av ti, føler at de har liten kontroll over hvordan personopplysninger lagres og brukes på internett.
- Opplevelsen av å ha liten kontroll er relativt lik på tvers av alder, kjønn, inntekt og utdanning.

Selv om mange føler liten kontroll over flyten av personopplysninger på internett, betyr ikke dette nødvendigvis at alle er negative til at opplysninger samles inn og brukes. Det er fullt mulig å føle at man mangler kontroll, uten at det oppleves som problematisk. Verdien av å få tilgang til gode og brukervennlig tjenester kan oppleves så stor at man godtar kontrolltapet som del av en byttehandel.

Vi spurte derfor respondentene om å ta stilling til om de føler seg maktesløse når det gjelder å ha kontroll over personopplysninger om seg selv på internett. Maktesløshet kan forstås som en følelse av at man ikke har muligheten til å ta kontroll over personopplysningene som er delt via internett, selv om man kanskje ønsker det.



Svarene viser:

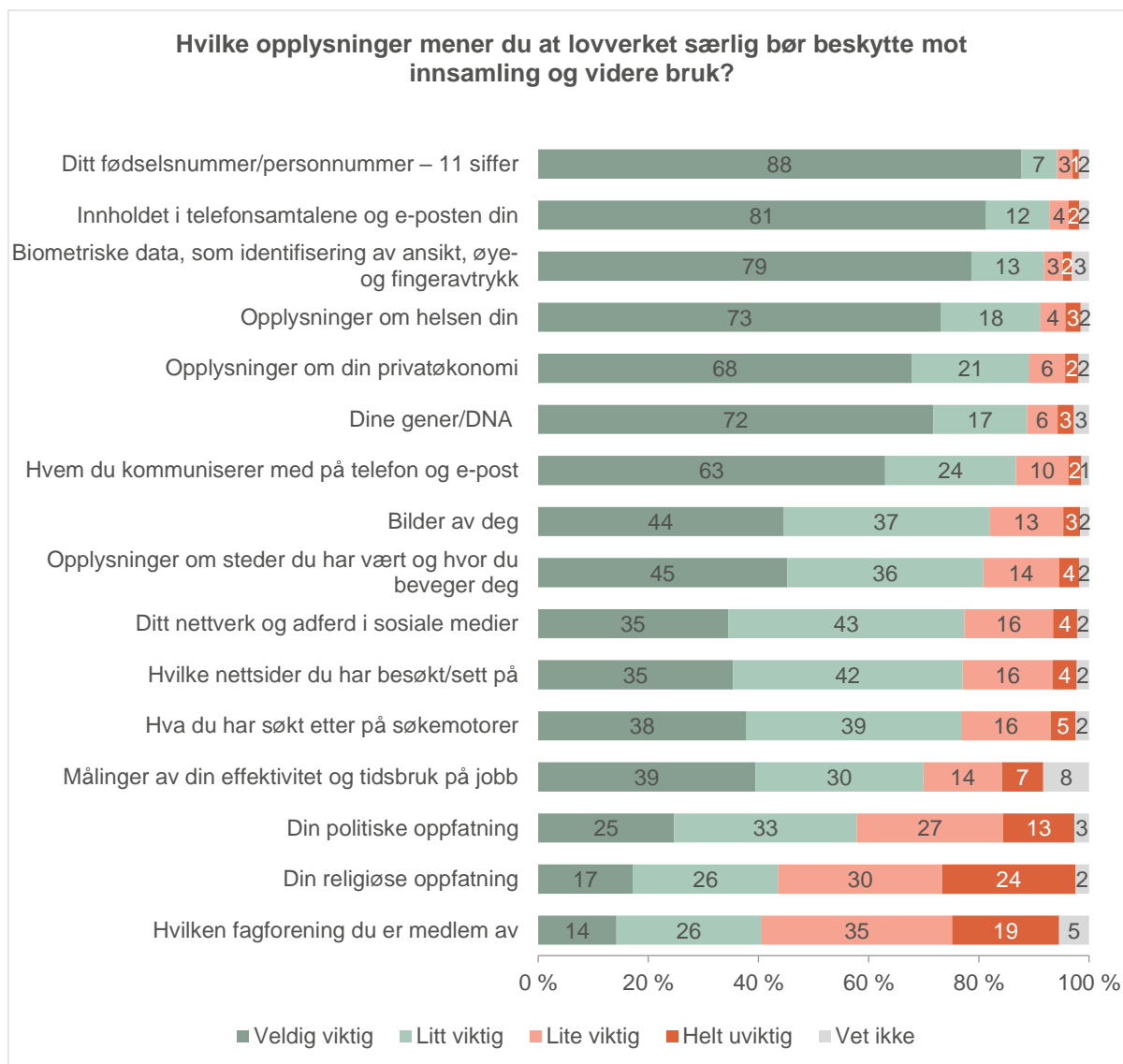
- Seks av ti oppgir å føle seg maktesløse når det gjelder å ha kontroll over personopplysninger på internett.

Vi ser altså at det er en utbredt følelse av maktesløshet når det gjelder å ha kontroll over personopplysninger på internett. Dette viser at følelsen av å ikke ha kontroll ikke oppleves som uproblematisk. Tendensen er relativt lik på tvers av alder, kjønn, inntekt og utdanning. Følelsen av maktesløshet kan dermed sies å gjelde på tvers av generasjoner og sosioøkonomisk status.

Mange av virksomhetene som styrer de digitale plattformene som samler inn store mengder av opplysninger om vår digitale atferd på nett (slik som søkemotorer, sosiale medier og meldingstjenester), høster svært lav tillit i befolkningen. Dette vil vi se nærmere på i neste kapittel.

Hvilke opplysninger er særlige beskyttelsesverdige?

Hvilke opplysninger vi ser på som private er kulturelt betinget, og hva vi synes er viktig å beskytte kan endre seg over tid. Vi har bedt respondentene ta stilling til beskyttelsesverdigheten til 16 ulike typer personopplysninger. Vi stilte tilsvarende spørsmål i personvernundersøkelsene i 2005 og 2014.



Svarene viser:

- Nordmenn mener i stor grad at alle typer persondata er beskyttelsesverdige.
- Fødselsnummer/personnummer er den personopplysningen som vurderes som viktigst at lovverket beskytter.
- Alle typer helse- og biometriske data oppleves som svært beskyttelsesverdige.
- Opplysninger om privatøkonomi rangerer også høyt. Hele 89 prosent svarer at det er viktig at lovverket beskytter slike data.
- Politisk og religiøs oppfatning, samt fagforeningstilhørighet oppleves som minst beskyttelsesverdige.

Vi ser at folk oppfatter de fleste personopplysningene som beskyttelsesverdige, og det er i stor grad de samme opplysningene som vurderes som mest beskyttelsesverdige i dag som i 2005 og 2014. I tråd med tidligere undersøkelser, viser svarene også at oppfatningen av hva som oppfattes som spesielt beskyttelsesverdige, ikke nødvendigvis sammenfaller med hva loven kategoriserer som særlige kategorier av personopplysninger (sensitive personopplysninger).

Fødsels-/personnummer

Fødsels-/personnummer er den personopplysningen som vurderes som mest beskyttelsesverdige av befolkningen. Dette korresponderer med undersøkelser fra 2005 og 2014. I personvernregelverket

defineres imidlertid ikke fødselsnummer som en såkalt særlig kategori av persondata (tidligere kalt sensitive personopplysninger). Likevel anser flere at det er viktigere at fødselsnummeret vernes enn innholdet i deres private kommunikasjon. Noe av grunnen til at fødsels-/personnummer oppleves som så beskyttelsesverdig kan handle om at det ofte har blitt omtalt i forbindelse med ID-tyverier. Ved hjelp av fødselsnummer, ofte i kombinasjon med andre identifikasjonspapirer, har det for eksempel vært mulig å ta opp lån i andres navn eller tegne falske mobilabonnementer. Slike hendelser har vært omtalt bredt i media, og var i spørreundersøkelsen i 2014 den trusselen mot personvernet som flest oppga at de fryktet.

Datatilsynet erfarer imidlertid at ID-tyveri ved bruk av fødselsnummer var mer vanlig tidligere da det også var enklere å misbruke, og svarene viser at spesielt de over 60 år (97 prosent) mener at lovverket særlig burde beskytte denne typen informasjon. Samtidig er også de under 30 år (90 prosent) opptatt av at fødsels-/personnummer gis særlig beskyttelse.

Kommunikasjon

De spurte mener videre at både hvem man kommuniserer med, og innholdet i kommunikasjonen, er svært beskyttelsesverdig. 87 prosent mener at det er viktig at lovverket beskytter informasjon om hvem man kommuniserer med på telefon og e-post, mens 93 prosent mener at det er viktig at lovverket særlig beskytter innholdet i kommunikasjonen. Disse tallene er nesten uendret siden 2014. Innsamling av denne type data har ofte vært diskutert i sammenheng med overvåkingen til etterretningstjenesten.

Nettverk og adferd i sosiale medier

Om lag fire av fem mener at nettverk og atferd i sosiale medier er høyt beskyttelsesverdig. I likhet med i 2014, mener nesten åtte av ti at hva de har søkt etter i søkemotorer er særlig beskyttelsesverdig, og 77 prosent, fire prosentpoeng flere enn i 2014, oppgir det samme for nettsidehistorikk. Disse tallene viser at et stort flertall av de spurte anser at opplysningene de etterlater seg på internett er høyt beskyttelsesverdige. Dette kan ha flere grunner. Hva man søker etter på nett kan være av svært privat karakter og potensielt avsløre sensitive ting. Også offentlige tjenester har publikumsrettede nettsider og lagrer personlig informasjon som ofte kan oppfattes som svært sensitiv.

Biometriske data

I denne undersøkelsen har vi for første gang spurt om lovverket særlig bør beskytte biometriske data. Biometriske data er kjennetegn som utgår fra kroppen, som er unike for deg og som du i liten grad kan endre. Biometriske data kan være et godt og effektivt identifiseringsverktøy, og blir i økende grad benyttet i forbrukerteknologi. For eksempel har det blitt mer vanlig å bruke ansiktsgjenkjenning og fingeravtrykk istedenfor å taste passord for å åpne mobiltelefonen.

Selv om bruk av biometriske data blir mer og mer vanlig, anses det altså som meget beskyttelsesverdig av respondentene, faktisk mer beskyttelsesverdig enn helseopplysninger og opplysninger om gener og DNA. Det er mulig at de iboende egenskapene til biometriske data bidrar til dette. Fingeravtrykk, ansikts- og retinaprofil er unike kjennetegn som bæres på utsiden av kroppen. I motsetning til geninformasjon, som kun kan kartlegges ved hjelp av tester, er det så godt som umulig å beskytte seg mot å bli profilert av et overvåkingskamera med innebygd ansiktsgjenkjenningsteknologi.

Privatøkonomi

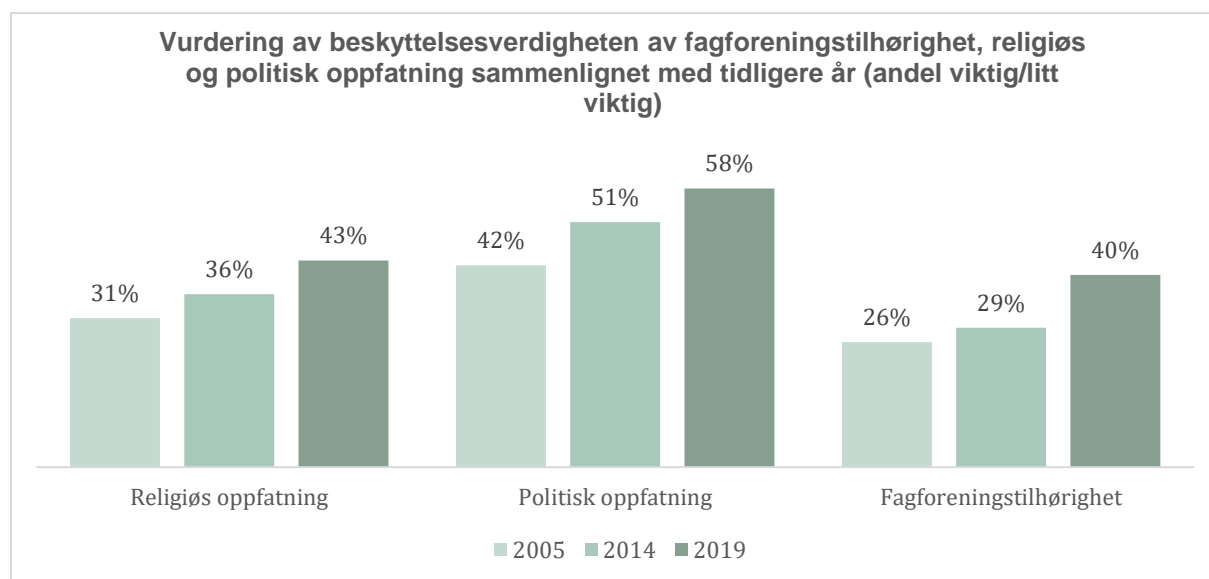
Nesten ni av ti svarer også at det er viktig at lovverket beskytter opplysninger om privatøkonomi. Dette er en økning på tre prosentpoeng fra 2014 og elleve prosentpoeng fra 2005. At privatøkonomi anses som så beskyttelsesverdig er interessant, sett i lys av at slike opplysninger ikke nyter et særlig vern i personvernregelverket. Skattelister er åpne i Norge og finansteknologi er i tillegg et felt i rivende utvikling. Nyere europeiske lovgivning har åpnet opp for et voksende marked for overføring og bruk av

finansielle personopplysninger for å utvikle og tilby nye tjenester til forbrukere. Vi vil se nærmere på denne problemstillingen i kapittelet «Personopplysninger til reklame, tjenester og produkter».

Fagforeningsmedlemskap, politisk tilhørighet og religion

I personvernregelverket har enkelte personopplysningskategorier, som informasjon om etnisitet, politisk oppfatning, religion og helse, et særlig vern. Slike opplysninger skal kun behandles når det foreligger et særskilt grunnlag. Både helseopplysninger og gener/DNA oppleves av de spurte som svært beskyttelsesverdige. De rangerer likevel lavere enn fødsels-/personnummer, som lovverket ikke anser som sensitive data. Informasjon om religiøs og politisk tilhørighet, samt fagforeningsmedlemskap, oppfattes derimot som relativt lite beskyttelsesverdig, til tross for at de nyter et spesielt sterkt vern.

Selv om enkelte sensitive personopplysninger havner langt ned på listen over hvilke opplysninger folk oppfatter som mest viktig å beskytte, har det skjedd en gradvis endring fra 2005 til 2019. Jevnt over anses i dag mange typer sensitive personopplysninger som mer beskyttelsesverdige enn for 15 år siden. Endringen er størst for opplysninger om politikk, religion og fagforeningstilhørighet.



Dette er personopplysninger som kan være avgjørende å beskytte i mindre frie samfunn enn det norske. At nordmenn anser slike opplysninger som relativt sett lite beskyttelsesverdige bør derfor sees i lys av at det for de fleste i Norge ikke medfører noen særlig risiko å åpent tilkjenne et politisk eller religiøst ståsted. Svarene viser likevel at fagforeningsmedlemskap, samt politisk og religiøs tilhørighet anses som mer beskyttelsesverdig i 2019 enn i 2005 og 2014.

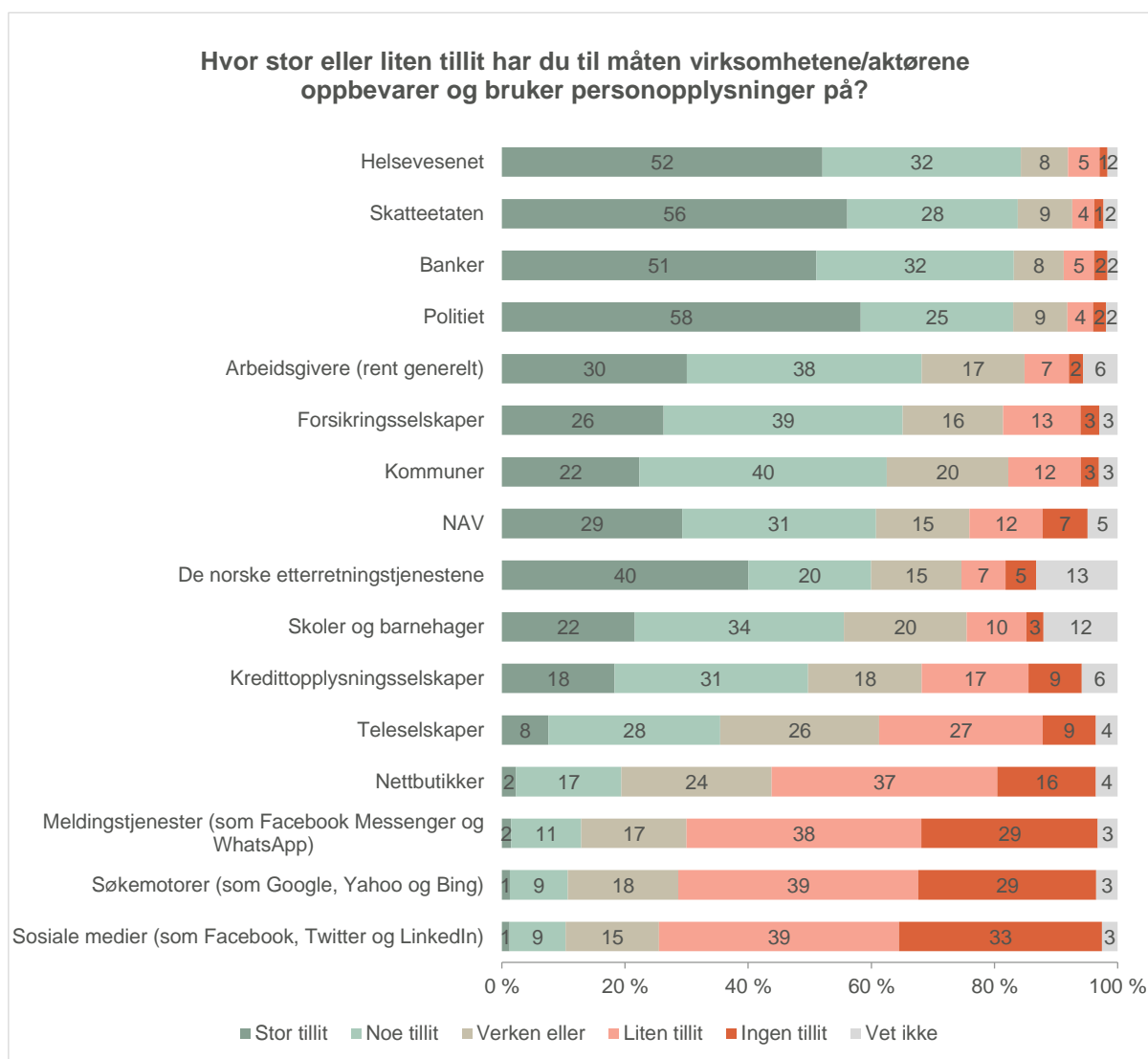
Hvorfor har nordmenn blitt mer restriktive når det gjelder slike opplysninger? Det kan tenkes at denne økningen speiler bredere utviklingstrekk, slik som økt polarisering, religionskonflikt og et hardere arbeidsliv. Mange land i Europa opplever en tiltakende polarisering, noe som gjør at det kan oppleves som mer risikabelt å proklamere et politisk ståsted. På samme måte opplever mange at debatten og retorikken rundt religiøs tilhørighet har hardnet til de siste årene. Kanskje opplever også flere at fagforeningstilhørighet er et mer betent tema i arbeidslivet som følge av den endrende dynamikken mellom arbeidstagere og arbeidsgivere.

Økningen i antallet respondenter som mener disse kategoriene av personopplysninger er veldig viktige å beskytte, kan også henge sammen med økt bevissthet omkring innsamling og bruk av opplysninger for profileringsformål og en uro knyttet til hvordan denne type opplysninger skal benyttes.

Hvem stoler vi på? Varierende grad av tillit

Tillit er viktig for ivaretagelse av personvernet. Det bør i størst mulig grad være et godt tillitsforhold mellom de som gir fra seg personopplysningene sine og de som behandler opplysningene. Man skal med andre ord i minst mulig grad ha grunn til å føle usikkerhet og frykt når man deler personopplysninger med en virksomhet, privat så vel som offentlig.

Vi har spurt om i hvilken grad folk har tillit til hvordan ulike private og offentlige virksomheter behandler deres personopplysninger.



Svarene viser:

- Med enkelte unntak har respondentene større tillit til offentlige enn private virksomheter.
- Helsevesenet og Skatteetaten nyter størst tillit. Hele 84 prosent svarer at de har stor eller noe tillit til hver disse. Bare én prosent svarer at de ikke har noen tillit, mens få svarer at de har liten tillit.
- Politiet kommer også høyt opp ved at hele 83 prosent oppgir at de har stor eller noe tillit. (Disse tallene er stabile siden 2014, og samsvarer også med funnene i [Politiets innbyggerundersøkelse fra 2018.](#))

- Tilliten til etterretningstjenestene er på 60 prosent.
- Tilliten til NAV på 60 prosent er lavere enn til de fleste andre offentlige virksomheter.
- Tilliten til måten skoler og barnehager oppbevarer og bruker personopplysninger på er slående lav. Bare 56 prosent svarer at de har tillit til skoler og barnehager, noe som er langt lavere enn tillitsnivået til andre offentlige aktører.

Det er gledelig å finne en gjennomgående høy tillit i befolkningen når det gjelder dette. Folk har imidlertid høyere tillit til offentlige virksomheter enn private, og sosiale nettsteder og de store globale teknologigigantene skiller seg ut ved at et stort flertall ikke har tillit til deres behandling av personopplysninger.

Offentlige virksomheter nyter stor tillit

Nordmenn har gjennomgående høy tillit til hvordan offentlige virksomheter behandler deres personopplysninger. Den høye tilliten til helsevesenet er spesielt viktig, ettersom de behandler svært sensitive personopplysninger om vår helse. Det er også viktig at tilliten mellom pasient og behandler helsepersonell er høy, ettersom dette er en forutsetning for å yte god helsehjelp, og det er viktig at pasienter føler at de kan gi viktig informasjon til helsevesenet. På samme måte behandler Skatteetaten, som har nest størst tillit blant befolkningen, store mengder økonomiske opplysninger om den enkelte. De fleste nordmenn har kontakt med Skatteetaten minst én gang i året, når skattemeldingen blir publisert. Andelen som har tillit til Skatteetaten har økt med fem prosentpoeng siden 2014, og kan muligens reflektere tilliten til etatens digitale løsninger og publikumstjenester.

Tilliten til etterretningstjenesten har falt med åtte prosentpoeng siden 2014. I 2019 la Forsvarsdepartementet frem et forslag om å etablere et nytt «digitalt grenseforsvar», som innebærer at det kan innhentes grenseoverskridende elektronisk kommunikasjon. I [Datatilsynets høringsvar](#) mente vi at forslaget om «tilrettelagt innhenting» var altfor inngripende og ikke burde innføres. Det er mulig at debatten rundt denne saken har påvirket tilliten til denne tjenestens behandling av personopplysninger.

Tilliten til NAV er lav sammenlignet med andre offentlige forvaltningsorganer. Siden 2014 har andelen som har stor eller noe tillit til NAV gått ned med seks prosentpoeng. I perioden hvor denne undersøkelsen ble gjennomført var NAV gjenstand for sterk kritikk for trolig å ha feilbehandlet en rekke saker som følge av en feiltolkning av EØS-reglene. Dette kan ha bidratt til å påvirke befolkningens tillit.

Slående lav tillit til skoler og barnehager

Skoler og barnehager har markant lavere tillit enn andre offentlige virksomheter. Bare 56 prosent av respondentene oppgir å ha høy eller noe tillit til disse virksomhetene, noe som er på nivå med etterretningstjenesten og kredittopplysningsselskaper.

Både skoler og barnehager behandler store mengder opplysninger om elevene, slik som informasjon om atferd, karakterer og språkutvikling. Datatilsynet har imidlertid ved flere anledninger de siste årene pekt på at norske kommuner har en jobb å gjøre når det gjelder å sikre at barnas personvern blir ivaretatt i skolen. De første og største overtredelsesgebyrene tilsynet har gitt etter innføringen av det nye personvernregelverket, har gått til kommuner som ikke har lyktes i denne jobben.

Barn defineres i personvernregelverket som en spesielt sårbar gruppe. Barn kan ikke velge å ikke gå på skole, og barna og deres foreldre er avhengige av at kommunen de bor i sikrer elevenes personopplysninger på en forsvarlig måte. At tilliten til en offentlig etat som er en så sentral del av samfunnet er såpass lav, er oppsiktsvekkende.

De siste årene har også flere og flere skoleelever blitt utstyrt med et personlig læringsbrett utviklet av enten Google eller Apple. Det er nærliggende å tro at usikkerheten og mangelen på kontroll som vi har omtalt tidligere også gjør seg gjeldende for teknologien barn får tilgang til gjennom den norske skolen. Vi har ikke spurt om tilliten til skoler og barnehager i tidligere undersøkelser, så vi har ikke tall på hvordan dette eventuelt har utviklet seg de siste årene.

Lav tillit til meldingstjenester, søkemotorer og sosiale medier

Det går en tydelig skillelinje mellom tilliten til private og offentlige virksomheter. Folk har gjennomgående lav tillit til hvordan private virksomheter behandler og bruker personopplysninger, med banker og til dels forsikringsselskaper som de eneste unntakene. Lavest tillit har folk til tjenester som i hovedsak leveres av de store teknologiselskapene i USA. Kun ti prosent oppgir å ha tillit til søkemotorer og sosiale medier, mens 13 prosent har tillit til meldingstjenester.

Vi stoler altså langt mindre på private virksomheter enn offentlige. Dette kan trolig delvis forklares ved at intensjonen bak behandlingen av våre opplysninger er ulik: private virksomheter bruker ofte opplysningene våre for kommersielle hensyn, mens offentlige virksomheter ofte trenger dem for å kunne utføre sitt samfunnsoppdrag.

Tilliten til sosiale nettsteder har falt med fem prosentpoeng siden 2014. Det lave tillitsnivået har trolig flere årsaker. Først og fremst har vi de siste årene sett at de store, amerikanske teknologiselskapene har blitt konfrontert og stilt til veggs av blant annet politikere, presse og interesseorganisasjoner i mye større grad enn tidligere. Flere og flere får øynene opp for den enorme makten et knippe Silicon Valley-selskap besitter, en makt de har oppnådd ved å samle inn mest mulig informasjon om flest mulig og selge annonseplass basert på denne informasjonen. Den mye omtalte [Cambridge Analytica-skandalen](#) som ble rullet opp i 2018, viste hvilken makt som kan ligge i å bruke Facebooks enorme datamengder til politisk påvirkningsarbeid.

Vi skriver mer om politisk målretting i neste kapittel.



Les mer

I 2015 så Datatilsynet nærmere på markedet for kjøp og salg av personopplysninger i den digitale annonseindustrien. Funnene er oppsummert i rapporten «[Det store datakappløpet](#)».

I rapporten «[På parti med teknologien – Digital målretting av politiske budskap i Norge](#)» fra 2019 har vi sett nærmere på hvordan slike annonseringsverktøy tas i bruk av politiske partier.

Unngår å bruke tjenester på grunn av usikkerhet

Usikkerhet knyttet til håndteringen av personopplysninger kan påvirke hvilke tjenester og produkter man velger å ta i bruk, og hvilke man avstår fra å bruke. Hvis folk ikke stoler på hvordan virksomheter behandler personopplysninger, kan det resultere i at de ikke tar i bruk løsningene.

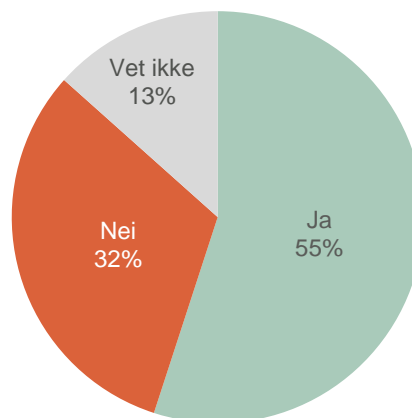
Vi spurte om respondentene noen gang har valgt å ikke ta i bruk et produkt eller en tjeneste på grunn av usikkerhet knyttet til behandlingen av personopplysninger.

Svarene viser:

- Et flertall har avstått fra å bruke en tjeneste eller et produkt som følge av at de er usikre på hvordan personopplysningene vil bli håndtert.
- Seks prosentpoeng flere menn enn kvinner har unnlatt å bruke en tjeneste.
- Det er flest personer i aldersgruppen 40 til 49 år (64 prosent) som oppgir å ha avstått fra å benytte tjenester.

En majoritet oppgir altså å ha avstått fra å bruke en tjeneste på grunn av usikkerhet knyttet til personvern. Spørsmålet skiller ikke mellom tjenestetilbydere. Hvis tjenesten som mister brukere er offentlig, kan de potensielle konsekvensene bli store for enkeltpersoner. For kommersielle virksomheter kan det tenkes at konsekvensene vil være størst for virksomheten selv, ved at de taper kunder som følge av å ikke ha den nødvendige tilliten til hvordan de behandler deres personopplysninger. Vi ser nærmere på konkrete følger av dette i kapitlet om nedkjølingseffekt.

Har du avstått fra å bruke en tjeneste eller produkt fordi du er usikker på hvordan dine personopplysninger vil bli håndtert?



Personopplysninger til reklame, tjenester og produkter

Produktene, tjenestene og løsningene vi bruker i hverdagen høster inn flere opplysninger om oss enn noen gang før. Basert på analyse av innsamlede personopplysninger, blir produkter og tjenester tilpasset den enkelte.

En gjennomsnittsnordmann brukte i 2018 nær [tre timer på internett](#) hver dag. En stor del av denne tiden tilbringes på digitale plattformer styrt av selskaper som har intensiv datainnsamling som bærende forretningsmodell. Verdens lagrede datamengde vokser i et voldsomt tempo. 5G-nettet, som vil tas i bruk i Norge i løpet av 2020, vil dramatisk øke mobilnettets kapasitet og kraft. Dette vil gi et kraftig dytt til utbredelsen av tingenes internett og smarte hjem.

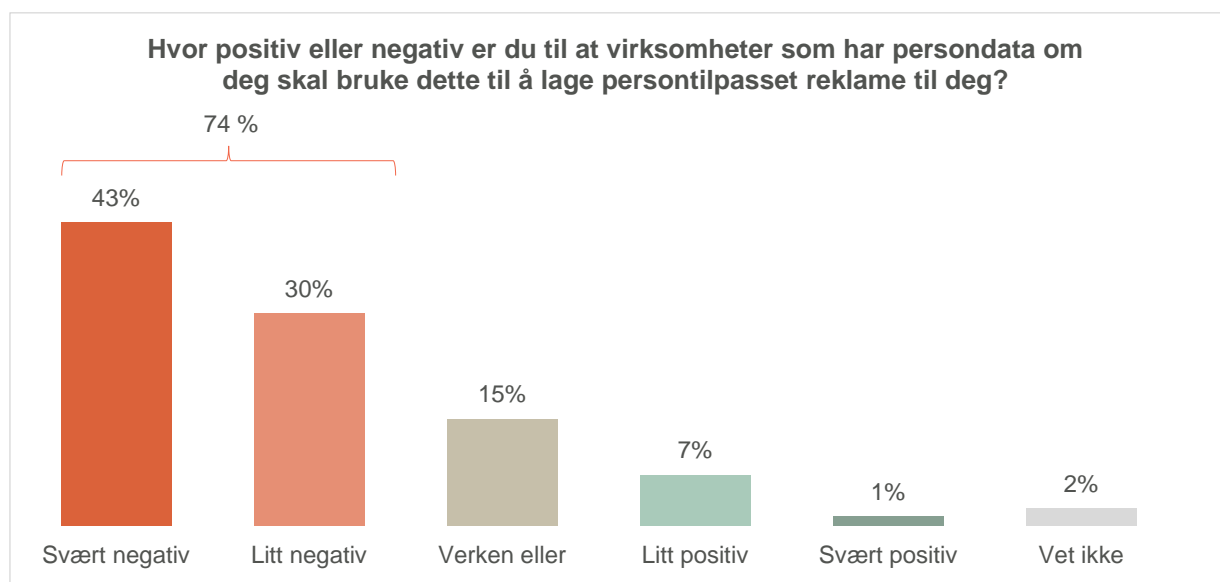
Vi ser også nye sektorer åpner opp for å tilrettelegge for økt bruk av personopplysninger. Nye europeiske regelverk har endret rammebetingelsene i banksektoren. Dette har ført til at økonomiske personopplysninger også kan brukes til å utvikle nye banktjenester.

I dette kapittelet ser vi på noen utvalgte problemstillinger knyttet til hvordan virksomheter bruker personopplysninger. Vi har stilt spørsmål om holdninger til målretting av digitale annonser, politiske partiers bruk av slik digital målretting, tingenes internett og smarte hjem. I lys av innføringen av det nye betalingstjenestedirektivet fra EU har det også blitt stilt spørsmål om holdninger til å dele data om personlig økonomi i bytte mot brukervennlige banktjenester.

Negative til målrettet annonsering

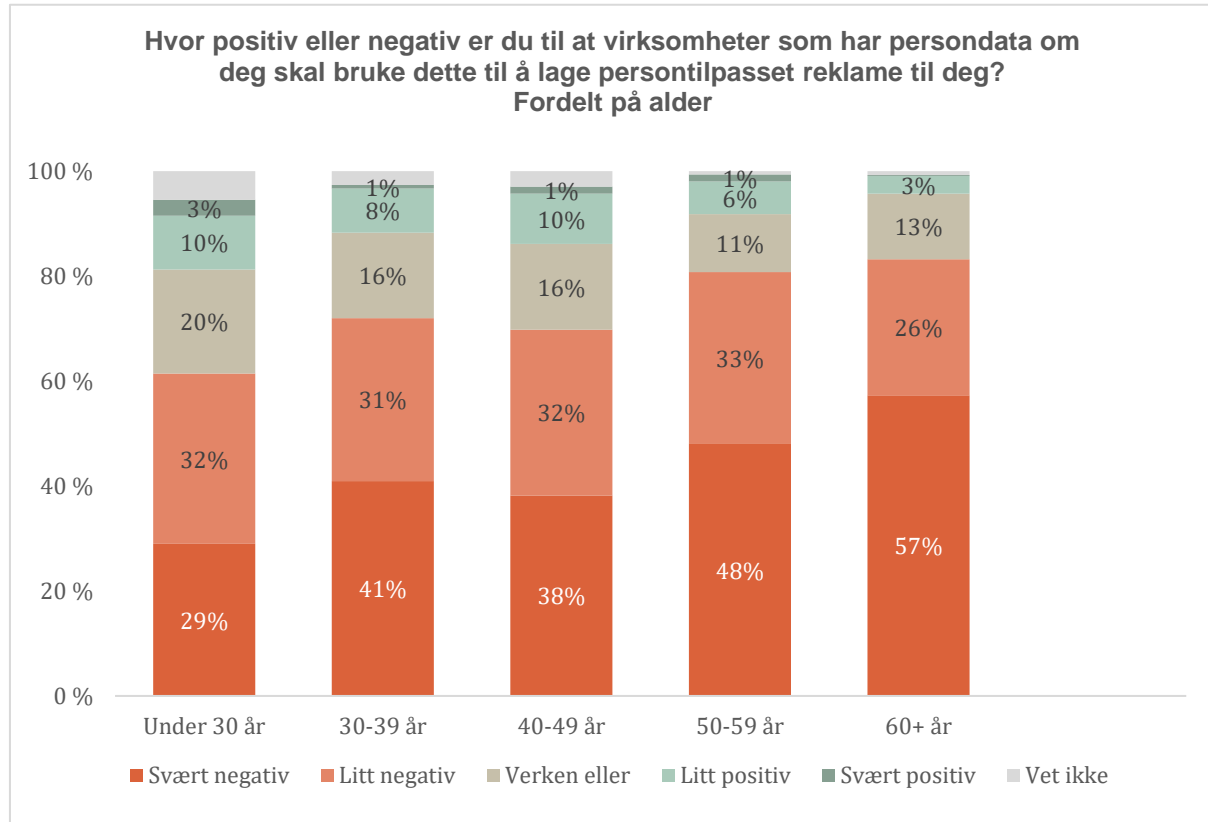
En lang rekke selskaper følger med på og samler informasjon om folks individuelle preferanser og atferd når de bruker internett. Denne informasjonen blir kjøpt og solgt på store, internasjonale børser for at markedsførere skal kunne treffe best mulig med sine skreddersydde annonser. Den digitale annonseindustrien er lukket, kompleks og tilbaketrukket. Facebook og Google er de største aktørene, men det finnes mange tusen andre selskaper som profitterer på kjøp og salg av personopplysninger. Folks privatliv blir dermed i stadig større grad nærgående kartlagt av kommersielle aktører som er fullstendig ukjente for de fleste.

For å undersøke folks holdninger til målrettet annonsering, har vi spurt om hvor positive eller negative de er til at nettsteder, søkemotorer og sosiale medier samler inn informasjon om nettaktivitet for å selge målrettede annonser.



Svarene viser:

- Tre av fire er negative til at virksomheter samler inn personopplysninger for å målrette annonser.
- Kun åtte prosent svarer at de er positive.



Når vi bryter svarene ned på alder, ser vi at:

- blant de over 50 år er åtte av ti negative til målrettede annonser.
- de yngste, som er mellom 15 til 19 år, er betydelig mindre negative til målrettet reklame i forhold til andre aldersgrupper. Likevel er nesten halvparten (48 prosent) av de yngste negative.

Svarene viser at et stort flertall av befolkningen er skeptiske til målrettet reklame. Disse tallene er konsistente med tidligere undersøkelser vi har gjennomført. I en undersøkelse til rapporten «[Personvern – tilstand og trender 2016](#)» spurte vi et representativt utvalg av befolkningen om de ville valgt å se reklame som er tilpasset atferd eller interesser, eller om de ville se «dum» reklame som viser tilfeldige produkter. Svaret viste at tre av fire nordmenn ville valgt å få tilfeldig reklame. Flere undersøkelser peker mot en voksende kløft mellom den digitale annonseindustriens metoder og folks oppfatning av hva som er greit. En undersøkelse gjennomført av [cybersikkerhetsfirmaet RSA Security](#) viser for eksempel at kun 17 prosent av de spurte anser personalisert reklame som etisk.

Som tidligere nevnt, så vi i 2015 på økosystemet i den digitale annonseindustrien i rapporten «Det store Datakappløpet». Siden den gang har denne industrien vokst ytterligere, men også blitt satt under sterkere press. Datatilsynsmyndigheter i flere europeiske land har mottatt klager rettet mot denne bransjens bruk av personopplysninger. De ulike klagene er ikke helt ensartede, men felles for dem alle er at de peker på at den bærende forretningsmodellen for kjøp og salg av annonseplasser på nett, sannsynligvis bryter med en lang rekke av prinsippene i personvernforordningen.

Skeptiske til målretting av politiske budskap

Verktøyene som kommersielle aktører bruker for å målrette annonser, blir også brukt for å påvirke velgermasser og vinne valg verden over. Politiske partier og kandidater, pressgrupper og organisasjoner har mulighet til å benytte informasjon som er samlet inn om velgernes aktivitet på internett og i sosiale medier for å kunne sende politiske annonser rettet mot de antatt mest mottakelige personene.

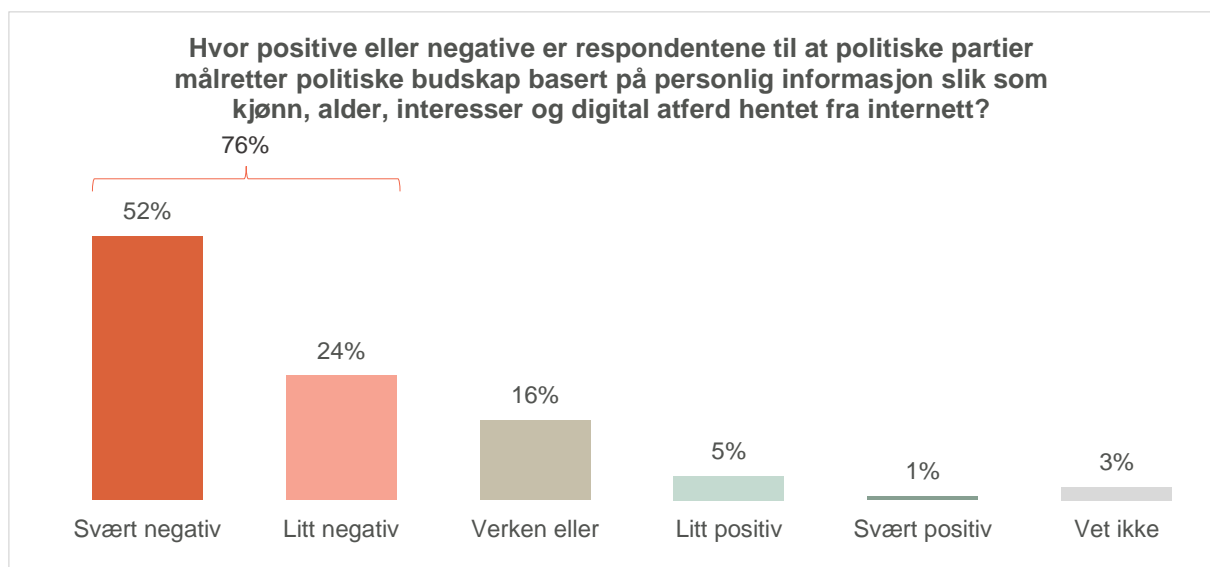
Politiske partier i Norge har gradvis flyttet annonsekroner fra aviser til sosiale medier, og først og fremst til Facebook. [Datatilsynets rapport](#) om hvordan politiske partier målrettet politiske budskap i forkant av lokalvalget i 2019, viste at de fleste annonsene, både de målrettede og de som siktet bredt, ble distribuert på Facebook. Dette innebærer at en større og større del av vår felles politiske offentlighet er flyttet over på denne plattformen, og avgjørelser som tas i deres styrerom får direkte konsekvenser for hvordan vår politiske offentlighet fungerer. Hvor grensene går for lovlig og etisk velgerprofilering er ikke hugget i stein, men mest mulig effektiv kommunikasjon i sosiale medier anses av alle partier som en av de viktige suksessfaktorene for en vellykket valgkamp.

Cambridge Analytica

Digital målretting av politiske annonser ble for alvor satt på agendaen da avisen The Guardian avslørte praksisen til analyseselskapet [Cambridge Analytica](#).

Selskapet hadde, på oppdrag fra Donald Trumps valgkampanje, på ulovlig vis innhentet data om 87 millioner amerikanere fra Facebook, og kombinerte denne informasjonen med en lang rekke andre datakilder for å bygge detaljerte psykologiske profiler. Videre matet de denne informasjonen tilbake i Facebooks annonsesystem, og målrettet annonser mot små målgrupper bestående av de mest sannsynlige svingvelgerne i de viktige vippestatene. Det ble også avdekket utstrakt bruk av budskap som oppfordret velgergrupper til å ikke bruke stemmeretten sin. Avsløringene ble et vendepunkt for bevisstheten rundt hvordan politikere, partier og andre interessegrupper med politisk agenda bruker personopplysninger for å vinne valg.

Siden målretting av politiske budskap har blitt en viktig del av partienes valgkamp, har vi spurt hva respondentene synes om at politiske partier bruker informasjon personene har registrert på internett og i sosiale medier for å sende dem politisk reklame.



Svarene viser:

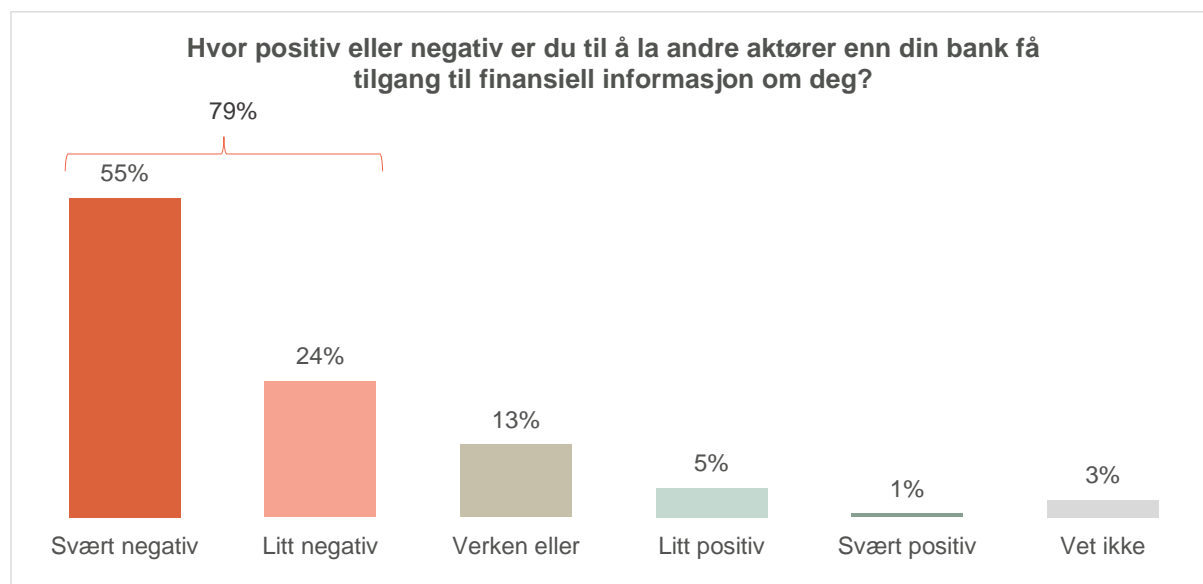
- Tre av fire nordmenn er negative til politisk målretting av budskap basert på personlig informasjon hentet fra internett.
- Den negative holdningen til politisk målretting av budskap er den samme uavhengig av alder, kjønn, inntekt og utdanning.

Aksepten for denne måten å drive politisk påvirkningsarbeid er med andre ord svært lav, samtidig som det er en valgkampmetode som alle norske partier satser tungt på. Det er grunn til å tro at motstanden har sammenheng med Cambridge Analytica-saken og en generell økende skepsis mot den datadrevne forretningsmodellen til de store teknologiselskapene.

Facebooks algoritmestyrte annonseløsning kan gi politiske partier en helt annen spredningskraft enn en annonse i lokalavisen. Partier styrer ofte ressursene mot plattformene som gir best uttelling. Politiske partier bør likevel merke seg den utbredte skepsisen mot algoritmedrevet valgkamp i sosiale medier.

Negative til å dele finansielle opplysninger

Finans- og banksektoren i Norge, som i resten av verden, gjennomgår store endringer. I 2018 ble det europeiske betalingstjenestedirektivet (Revised Payment Services Directive, PSD2), innført i EU og i Norge. Formålet med direktivet er blant annet å harmonisere regelverket i EU og legge til rette for økt konkurranse i markedet for betalingstjenester. Betalingstjenestedirektivet gir forbrukerne større eierskap over opplysningene som bankene har om dem. Nå kan forbrukeren samtykke til at virksomheter utenfor banksektoren kan få tilgang til kontoopplysningene deres. Med tilgang til disse opplysningene får virksomhetene muligheten til å bygge tjenester på toppen av bankenes data og infrastruktur.



Svarene viser:

- Fire av fem er negative til at andre aktører enn banken skal få tilgang til deres finansielle informasjon. Kun seks prosent er positive.
- Holdningene varierer etter respondentenes alder. Mens nesten 90 prosent av de over 60 år er negative til at nye aktører skal få tilgang til personlig finansiell informasjon, viser tallene at bare 64 prosent av de under 30 år er negative.
- Menn er mer positive til å dele finansielle opplysninger enn kvinner. Mens åtte prosent av menn er positive, gjelder dette bare tre prosent av kvinnene.

Undersøkelsen viser en utbredt skepsis til å dele finansielle opplysninger med andre virksomheter enn banken. Yngre personer er litt mindre negative til å åpne opp for andre aktører. Dette kan delvis forklares med at yngre forbrukere ofte har mindre lojalitet til tradisjonelle institusjoner som banker, og er mer vant til å ha tilgang til nye tjenester via smarttelefonen. For aldersgruppene som hele livet har forholdt seg til banken primært som en nettjeneste, vil trolig ikke spranget til en ekstern tjenesteleverandør være like stort som for aldersgruppene som har opplevd tiden da man fysisk troppet opp i banken for å betale regninger.

Google og Facebook i finansmarkedet

Med betalingstjenestedirektivet forsvinner altså bankenes monopol på kundenes kontoopplysninger, noe som åpner opp for at nye aktører fra inn- og utland kan konkurrere i et marked som tidligere var kontrollert av bankene.

Vi vil i tiden fremover trolig se flere applikasjoner og tjenester som tilbyr rask og enkel betaling, samt hjelper oss med å spare eller samordne gjelds- og kredittopplysninger. Norske banker har investert tungt i utvikling av slike tjenester, men vil nå møte tøff konkurranse fra andre aktører, inkludert de store internasjonale teknologiselskapene. Facebook, Google, Apple og Amazon tilbyr alle løsninger for rask og sømløs betaling. Disse selskapene omsetter for milliardbeløp hvert år og har i tillegg et enormt konkurransefortrinn i kraft av antall brukere. Som vi skrev om tidligere nyter imidlertid norske banker høy tillit i den norske befolkningen, noe Facebook og Google ikke gjør.

Vi spurte om hvor problematisk respondentene synes det er for personvernet å gi Google eller Facebook tilgang til våre finansielle opplysninger, hvis de kan tilby oss en nyttig banktjeneste.

Svarene viser:

- Et overveldende flertall synes det er problematisk at Google og Facebook skal ha tilgang til finansielle opplysninger.
- Omtrent like mange kvinner (87 prosent) som menn (83 prosent) mener at det er problematisk.
- Skepsisen går på tvers av aldersgrupper.

Et stort flertall mener altså at det er problematisk for personvernet å gi Google eller Facebook tilgang til sine finansielle opplysninger. Dette samsvarer med funnene i Datatilsynets rapport «[Personvern 2017 – Persontilpassing og kunstig intelligens](#)» hvor 79 prosent av respondentene svarte at de var negative til å benytte seg av en banktjeneste fra Google eller Facebook.



En nærliggende forklaring er at tradisjonelle banker over mange år har knyttet lojalitetsbånd til kundene sine, og at folk er fornøyde med tjenestene de tilbyr. Som nevnt, har folk stor tillit til hvordan banker behandler personopplysninger, og svært liten tillit til teknologiselskaper som leverer søkemotorer og sosiale medier. Norske bankers høye tillit i befolkningen vil med andre ord være et stort konkurransefortrinn når Facebook og Google ruller ut sine løsninger. På den annen side har disse selskapene enorme fortrinn i kraft av økonomiske muskler, brukermasse og funksjonalitet.

Det vil derfor bli spennende å se hvordan dette markedet utvikler seg de neste årene. Banker og sosiale medier-selskap befinner seg i hver sin ende av tillitsskalaen, men vi vil se flere og flere nye selskap som vil forsøke å ta markedsandeler. Hvordan vil for eksempel nordmenn stille seg til en norskutviklet betalingstjeneste som kan friste med både ivaretagelse av personvernet og sømløs mobilbetaling?

I Norge gikk norske banker, anført av DNB, tidlig sammen om å utvikle betalingsløsningen Vipps, som i dag benyttes av om lag tre av fire nordmenn. Det gjenstår å se hvilke selskap og løsninger som er i stand til å utfordre denne markedsposisjonen. Kanskje vil vi se at flere utfordrere sikter seg inn mot rådgivningstjenester ved å samle informasjon om lån, gjeld og spareavtaler på tvers av ulike banker.

Lite interesse for banktjenester fra Google eller Facebook

De fleste er skeptiske til å la nye aktører få tilgang til finansielle opplysninger, men dette kan endre seg. Noen vil la seg overtale av en venn, andre vil vurdere fordelene ved de nye tjenestene som større enn ulempene.

Vi spurte derfor de som mener at det er problematisk å gi Google eller Facebook tilgang til deres finansielle opplysninger, om de likevel er interessert i å benytte seg av en nyttig banktjeneste fra disse selskapene.

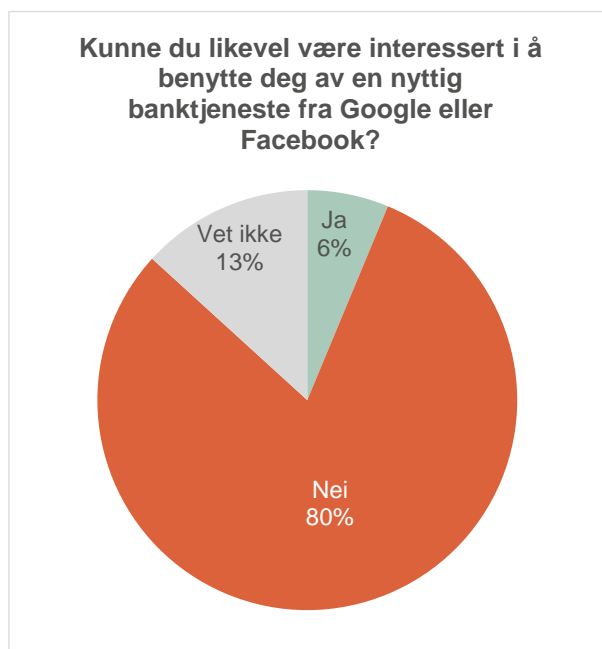
Svarene viser:

- Av de som beskriver det som problematisk for personvernet å gi Google og Facebook tilgang til sine finansielle opplysninger, oppgir åtte av ti at de heller ikke ville tatt i bruk en slik tjeneste fra disse selskapene.
- Fire av fem i gruppen som mener at det er problematisk å gi finansielle opplysninger til Facebook og Google, ønsker ikke å ta i bruk en betalingstjeneste fra disse selskapene. Samtidig svarer seks prosent at de gjerne tar i bruk en slik tjeneste og 13 prosent unnlater å ta stilling.

Det kan tenkes at løsningene som norske banker allerede har utviklet er så gode at det ikke oppleves som nødvendig å gi Facebook og Google innpass i nok en del av våre liv. Ofte finnes det ikke reelle alternativer til kjernetjenestene som Facebook og Google tilbyr. Innenfor finanssektoren opplever sannsynligvis flere at de har et reelt valg. I tillegg tilbys hurtig mobilbetaling i dag av institusjoner vi har høy tillit til. Det store spørsmålet blir hvor mange som vil ta i bruk direktebetaling i meldingstråden på Messenger eller lignende hvis det gjør hverdagen enda litt enklere.

Tingenes internett og smarte hjem

Tingenes internett er et samlebegrep for nettverket av gjenstander som er utstyrt med elektronikk og sensorer som muliggjør internetttilkobling og deling av data. Slik teknologi preger, og vil fortsette å prege, moderne samfunn på en lang rekke områder, inkludert transport, medisin og infrastruktur. For folk flest er tingenes internett som regel assosiert med forbrukerelektronikk og smarte hjem. Kjølleskap som sender en autogenerert handleliste basert på analyser av innholdet, stemmeassistenter som sjekker været mens man kler på seg og stereoanlegg som spiller favorittlåten mens man lager middag,



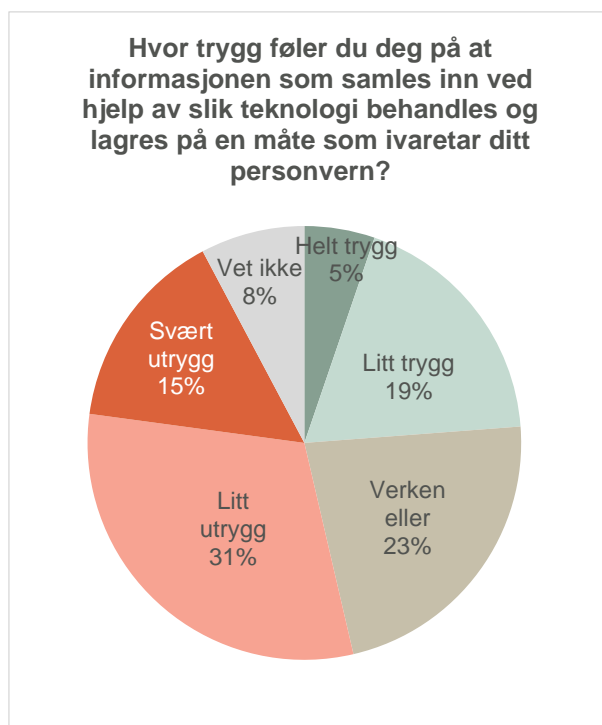
blir vanligere og vanligere. Utbredelsen av smarte ting til hjemmet forventes å øke i takt med utbredelsen av neste generasjons mobilnett, også kjent som 5G.

Fordelene med smarte produkter er mange. De kan gi mer tilrettelagte tjenester, og ha enorm betydning for energisparing og effektiv samfunnsplanlegging. I tillegg er potensialet stort for et mer tilrettelagt hjemmemiljø for eldre og syke. Flere internettilkoblede dingser fører like fullt til at virksomheter samler inn større mengder opplysninger om enkeltpersoners atferd i hjemmet.

Vi spurte om hvor trygge folk føler seg på at informasjon som samles inn ved hjelp av smart forbrukerteknologi (robotstøvsugere, smarte kjøleskap, målere for innendørsklima, strømmålere og lignende) behandles på en måte som ivaretar personvernet.

Svarene viser:

- 46 prosent føler seg, i forskjellig grad, utrygge på om teknologien samler inn og behandler informasjon på en måte som ivaretar personvernet.
- 24 prosent svarer at de føler seg litt eller helt trygge.
- Nesten én av fire har svart «verken eller», mens åtte prosent har svart at de ikke vet. Det kan antyde at mange fremdeles ikke er kjent med teknologien.
- Utryggheten man føler i møte med teknologien, øker litt med alderen. Av de over 60 år, svarer nesten halvparten (49 prosent) at de føler seg utrygge på teknologien, sammenlignet med 40 prosent av de under 30.
- Det er særlig de med høyere inntekt som svarer at de føler seg utrygge. Mens 33 prosent av de med inntekt under 400 000,- kroner svarer at de føler seg utrygge, svarer 53 prosent av de med inntekt over 600 000,- kroner at de føler seg utrygge.



Nesten halvparten av befolkningen føler seg altså utrygge på at informasjon som samles inn via tingenes internett blir behandlet og lagret på en måte som ivaretar personvernet. Dette samsvarer med [en undersøkelse til rapporten «Personvern, tillit og følelser 2018»](#), hvor vi spurte om folk er bekymret for informasjonssikkerheten og personvernet i smarte produkter. Nesten halvparten av respondentene svarte ja.

På grunn av utbyggingen av 5G-nettet står vi på terskelen av et potensielt stort taktskifte i tempoet og utbredelsen av denne typen teknologi. Flere og flere nybygg vil inkludere internettilkoblede dingser med sensorer som måler, registrerer og analyserer store datamengder, og forbrukerelektronikk med de samme egenskapene vil bli billigere og mer utbredt. Produkter koblet til tingenes internett muliggjør en lang rekke funksjonaliteter, men det finnes mange eksempler på at de ikke sikrer personopplysninger på en god måte.

[Da Forbrukerrådet testet internettilkoblede leketøy for barn](#), avslørte de flere svakheter ved sikringen av personopplysninger. Hvem som helst kunne med enkle grep ta kontroll over lekene og avlytte det som ble sagt. Dukkene kunne også bli brukt til skjult markedsføring, ved at de inneholdt forhåndsprogrammerte fraser hvor utvalgte varer og tjenester ble positivt omtalt. [På lignende vis har Google, Amazon og Apple latt analytikere boltre seg i stemmeopptak](#) fra privathjem. Amazon-eide

Ring, som tilbyr internettilkoblede kameraer som skal installeres ved inngangsdøren, ble også [avslørt i å sende personopplysninger, som navn, IP-adresser, teleoperatør, og sensordata, videre til tredjeparter.](#)

Nedkjølingseffekten

Frykten for å bli overvåket, eller at noen skal bruke opplysninger om oss til formål vi ikke er klar over, kan føre til endret atferd. Når vi mister kontroll over hvem som vet hva om oss, blir vi tvunget til å ta hensyn til usikkerhetsfaktoren. Konsekvensene kan være at vi tenker gjennom og revurderer hva vi skriver, hvem vi har kontakt med og hva vi foretar oss. Denne selvreguleringen som følge av overvåkingsfrykt kalles «nedkjølingseffekten».

En konsekvens av en slik nedkjøling i et åpent, demokratisk samfunn er en svekkelse av den reelle ytringsfriheten. Selv om Norge er blant landene i verden hvor ytringsfriheten står sterkest, kan usikkerhet knyttet til konsekvensene av å ytre seg føre til at flere velger å la være. Dette vil igjen føre til at fri meningsutveksling, et bærende fundament i et velfungerende demokrati, blir litt mindre fri. I tillegg kan overvåkingsfrykt føre til endret atferd på individnivå, for eksempel ved at mennesker avstår fra å søke hjelp om tabubelagte forhold av frykt for at informasjonen ikke forblir konfidensiell.

Å måle dette fenomenet kan være utfordrende. Det er i hovedsak lettere å måle aktive handlinger enn fravær av handlinger. I tillegg inntreffer gjerne selvregulerende atferd gradvis og ubevisst.

Overvåking kan beskrives som «systematisk observasjon» og har tradisjonelt vært mest forbundet med aktiviteter utført av myndigheter, etterretningsvesen og politi. I vår nære, europeiske historie står Øst-Tysklands Stasi som det mest fryktingytende eksempelet på et totalitært overvåkingsorgan med kapasitet til, og ambisjon om, å vite alt om alle borgere.

De siste årene har det imidlertid vokst frem en annen potensiell trussel mot ytrings- og informasjonsfriheten. Når man bruker internett samles det inn opplysninger i stor skala for å forstå folks interesser og preferanser. Denne informasjonen blir fortløpende kjøpt og solgt på store, internasjonale børser. Den omfattende mengden data som samles inn om fører til en svært nærgående kartlegging av enkeltpersoners liv. Internettøkonomien kan dermed sies å ha blitt en overvåkingsøkonomi. Hundretalls virksomheter vet svært mye om enkeltpersoner, mens personene selv ikke vet hvem som vet og hva de vet.

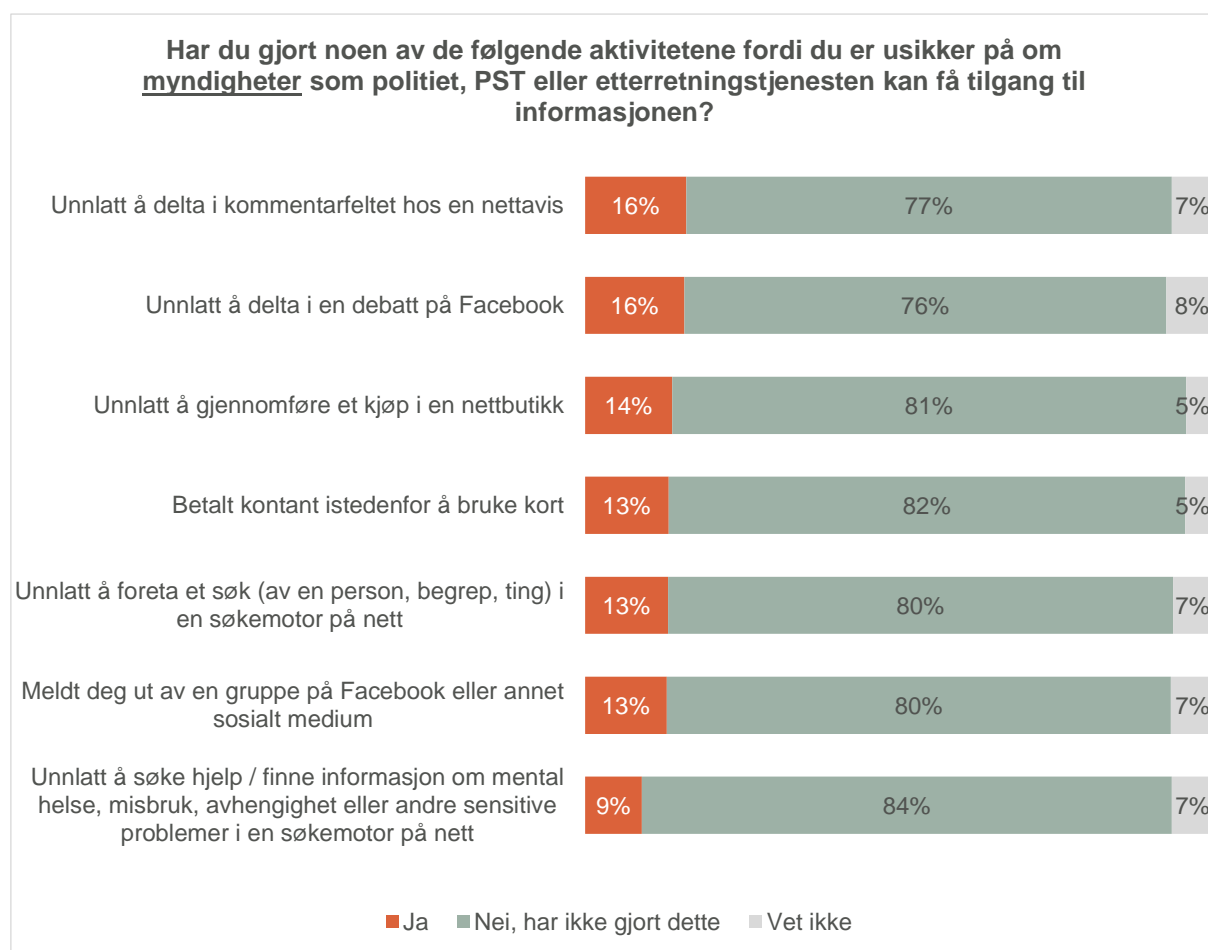
Flere og flere innser at de fleste gratistjenester på nett er gratis fordi selskapene tjener store penger på å samle inn personopplysninger. Skyggesiden av internettøkonomien blir stadig tydeligere.

Har usikkerheten knyttet til hvordan persondata blir brukt en nedkjølende effekt på folks oppførsel på nett? Hindrer det befolkningen i å skrive under en spørreundersøkelse eller å foreta et bestemt google-søk? Og påvirker usikkerheten knyttet til hvordan kommersielle selskaper bruker personopplysninger befolkningen mer enn hvordan myndighetene bruker opplysningene?

I 2014 ba vi respondentene svare på om de hadde unnlatt å gjøre en rekke handlinger av frykt for hvordan opplysningene kunne bli brukt senere. I år har vi skilt mellom myndighetsovervåking på den ene siden og kommersielt drevet sporing og registrering av private selskaper på den andre, for å få innsyn i ikke bare om folk moderer seg, men også overfor hvem.

Tendenser til nedkjølingseffekt i frykt for overvåking fra offentlige myndigheter

For å vite hvordan man reagerer på usikkerhet rundt overvåking fra offentlige myndigheter, har respondentene blitt spurt om å ta stilling til om de har gjort eller unnlatt å gjøre visse aktiviteter fordi de er usikre på om myndigheter slik som politiet, PST eller etterretningstjenesten, kan få tilgang til informasjonen.



Svarene viser:

- 16 prosent har unnlatt å delta i kommentarfeltet i en nettavis eller i en Facebook-debatt fordi de er usikre på om myndighetene har tilgang til informasjonen de legger igjen. Dette er et svært høyt tall i et liberalt demokrati som det norske.
- 13 prosent har unnlatt å foreta et søk på nett på grunn av usikkerhet knyttet til om myndighetene har tilgang til informasjonen. Nesten én av ti har av samme årsak unnlatt å søke hjelp eller søke etter informasjon om problemer knyttet til psykisk helse, misbruk, avhengighet eller andre sensitive problemer.
- Det er de i aldersgruppene fra 30 til 49 år som i høyest grad oppgir at de har unnlatt å gjøre aktivitetene listet opp i tabellen eller endret atferd.
- Det er gjennomgående menn som i størst grad avstår fra å utføre aktiviteter eller endrer sin atferd.
- De med mer enn fire års universitets- eller høyskoleutdanning oppgir i minst grad å ha endret atferd.

Selvsensur på meningsutveksling

Tallene viser at selv om de fleste ikke endrer sin atferd som følge av at de er usikre på om myndighetene kan få tilgang til informasjonen, utøver en betydelig andel selvsensur. Det er spesielt aktiviteter som har sammenheng med fri meningsutveksling flest unnlater å gjøre. Dette inkluderer å delta i et kommentarfelt eller i en Facebook-debatt. Politikere og meningsbærere tyr ofte til tastaturet og publiserer debattinnlegg på sin private Facebook-profil istedenfor å gå omveien rundt de redaktørstyrte mediene. Slik kan de i større grad sette premissene for debatten og engasjere flere på en rask og effektiv måte. Det kan argumenteres for at denne utviklingen har positive trekk, men at så

mange som én av åtte unnlater å delta på grunn av frykt for myndighetsovervåking, er dypt bekymringsfullt. I ytterste konsekvens kan man argumentere for at den reelle ytringsfriheten er under press som følge av at den offentlige debatten i økende grad foregår på nett.

Unnlater å lete etter informasjon om sensitive problemer

Nesten én av ti har unnlatt å søke hjelp eller finne informasjon om mental helse, misbruk, avhengighet eller andre sensitive problemer på nett. Bakgrunnstallene viser at litt flere menn (elleve prosent) unnlater å gjøre slike søk, i forhold til kvinner (syv prosent).

Offentlige helsemyndigheter og hjelpeorganisasjoner er ofte helt avhengige av at de som søker hjelp finner frem. Mennesker som søker informasjon om psykisk helse, avhengighet eller misbruk er som regel i en sårbar situasjon, og hvis man ikke allerede er i kontakt med helsevesenet, er et Google-søk ofte den eneste, reelle muligheten man har til å finne hjelp. At ti prosent oppgir å ha unnlatt å søke etter denne hjelpen på grunn av frykt for myndighetsovervåking er illevarslende og noe helsemyndigheter og hjelpeorganisasjoner må ta med i betraktningen når de utformer kommunikasjonsstrategier.

Overordnet må tallene om nettdebatt og internettsøk om sensitive tema forstås i sammenheng med den ekstremt lave tilliten folk har til selskapene som står bak de viktigste internettjenestene, som søk og sosiale medier.

Er forsiktige med netthandel og betaling med kort

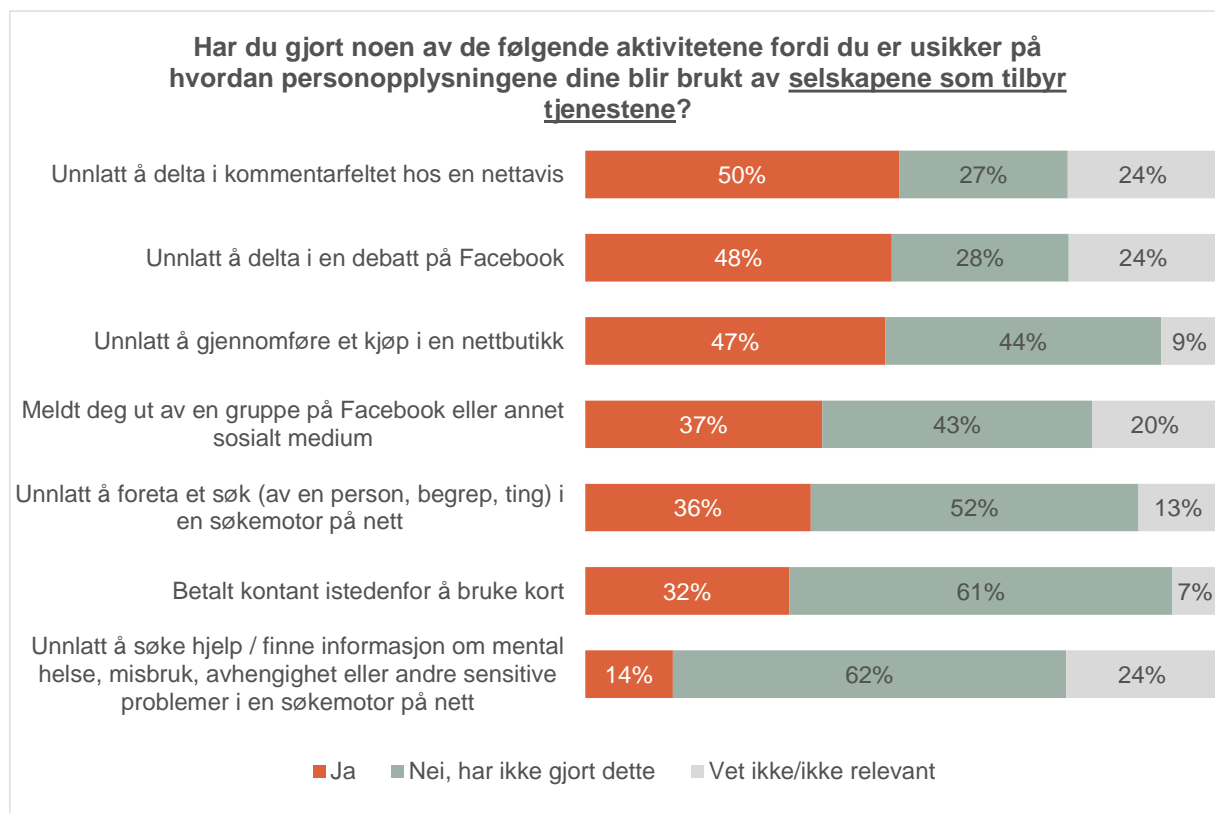
14 prosent av de spurte har unnlatt å handle på nett og 13 prosent har betalt kontant istedenfor med kort på grunn av usikkerhet knyttet til myndighetsovervåking. Kontanter er en stadig mindre brukt betalingsform i Norge, og vil sannsynligvis på et eller annet tidspunkt fases helt ut. Overgangen til det kontantfrie samfunn vil sannsynligvis bidra til å svekke den svarte økonomien og skape dårligere vekstvilkår for enkelte former for kriminalitet.

På den annen side forsvinner muligheten til sporingsfri handel. Alle korttransaksjoner registreres, det samme gjelder for transaksjoner i nettbutikker. De som i dag bevisst velger å betale kontant for å verne seg, vil miste denne muligheten. At såpass mange bevisst har valgt å betale kontant istedenfor med kort kan sies å være overraskende, med tanke på hvor høy tillit befolkningen har til at banker beskytter personopplysninger på en god måte. Det kan tenkes at ønsket om å beskytte opplysninger om privatøkonomi bidrar til forsiktighet, til tross for at vi i utgangspunktet stoler på bankene.

Endrer adferd på grunn av usikkerhet om hvordan private virksomheter bruker opplysningene

Nedkjølingseffekten er tradisjonelt forbundet med myndighetsovervåking, fordi det lenge først og fremst var stater som hadde kapasitet til å drive utstrakt overvåking. I dag interagerer vi daglig med selskap som samler inn så mye informasjon som mulig om så mange som mulig. Livene våre er i økende grad totalovervåket. Denne forretningsmodellen har vist seg å være ekstremt lønnsom, men har de siste årene møtt mer og mer motstand. Som omtalt tidligere opplever svært mange liten kontroll over flyten av personopplysninger på internett, og svært mange føler på maktesløshet knyttet til dette.

For første gang har Datatilsynet også sett på om usikkerhet knyttet til hvordan private selskaper bruker personopplysninger kan bidra til en nedkjølingseffekt ved at man unnlater å gjøre visse ting eller endrer atferd.



Svarene viser:

- Langt flere unnlater å gjøre visse aktiviteter eller endrer atferd på grunn av usikkerhet knyttet til private selskapers bruk av personopplysninger, sammenlignet med myndighetsovervåking.
- Rundt halvparten av respondentene har unnlatt å delta i en diskusjon i et kommentarfelt eller på Facebook fordi de er usikre på hvordan opplysningene vil bli brukt.
- Nesten halvparten har unnlatt å gjennomføre et kjøp i en nettbutikk fordi de er usikre på hvordan opplysningene vil bli brukt.
- Menn endrer oftere atferd på grunn av frykt for myndighetsovervåking. Kjønn spiller en mindre rolle når det gjelder usikkerhet knyttet til selskapenes bruk av personopplysninger.
- Vi ser en tendens til en omfattende nedkjølingseffekt som følge av at folk ikke har kontroll over flyten av personopplysninger på internett. En svært stor andel begrenser seg selv eller endrer atferd på grunn av usikkerhet knyttet til kommersielle aktørers bruk av personopplysninger.

Unngår å delta i debatt og kommentarfelt

Flest unnlater å delta i kommentarfelt i nettaviser og på Facebook. At om lag halvparten har avstått fra å delta i disse aktivitetene er oppsiktsvekkende. Langt flere modererer seg og endrer atferd på grunn av usikkerhet knyttet til hvordan private selskap bruker personopplysninger, sammenlignet med myndighetsovervåking. Som diskutert tidligere har dette følger for hvordan vår demokratiske offentlighet fungerer. Når politikere og meningsbærere migrerer til disse plattformene ekskluderes mange på grunn av overvåkingsfrykt og en utbredt mangel på kontroll over plattformenes bruk av personopplysninger.

Samtidig unnlater omtrent like mange å delta i nettavisenes kommentarfelt som i en Facebook-debatt. Det indikerer at folk heller ikke har tillit til norske mediers ansvarlighet. [En kartlegging gjort av NRKbeta](#) viste nylig at mediebransjen er blant de som sporer folk mest på nett, noe vi også påpekte i rapporten «Det store datakapløpet» i 2015. Samme redaksjon avslørte også i 2019 at [Disqus, en](#)

[tjeneste som leverer kommentarfelt på en lang rekke anerkjente nettsteder, lenge hadde brutt personvernregelverket.](#)

Unnlater å bruke søkemotorer til enkelte søk

36 prosent av respondentene svarer at de har unnlatt å foreta et internettsøk. Hva som skrives inn i søkefeltet forsvinner ikke, men lagres og analyseres fortløpende. Innsikten som kan hentes fra denne enorme datamengden blir blant annet brukt til å forbedre søkemotoren, og kombineres med en lang rekke andre datapunkter for å blant annet personalisere annonser som følger enkeltpersoner rundt om på nettet. Det er få som vet hva som foregår i kulissene når søkemotorer benyttes. Markedet som styrer annonsering basert på hva folk søker på preges av informasjonsasymmetri, lukkethet og hemmelighold.

Tusenvis av virksomheter i denne bransjen vet svært mye om befolkningen, mens folk flest ikke vet hvem som vet og hva de vet. Google har et tilnærmet monopol i markedet for nettsøk i Norge, og er i praksis ensbetydende med informasjonssøk. Når én av tre har unnlatt å søke informasjon fordi de er usikre på søkemotorleverandørenes bruk av personopplysninger, får det konsekvenser for den reelle informasjons- og ytringsfriheten.

Avstår fra å søke om sensitive problemer

Spesielt problematisk er det når folk unngår søke om informasjon eller hjelp om sensitive problemer. Undersøkelsen viser at 14 prosent av de spurte har unnlatt å søke hjelp eller finne informasjon om mental helse, misbruk, avhengighet eller andre sensitive problemer i en søkemotor på nett. Undersøkelsen viser også at de i aldersgruppen 20 til 29 oftest unnlater å gjøre slike søk, og at det er fire prosentpoeng flere menn (elleve prosent) enn kvinner (syv prosent).

Som diskutert over er mennesker som søker informasjon om psykisk helse, misbruk og avhengighet ofte i en svært sårbar situasjon. Et Google-søk er for de aller fleste det første steget mot å få hjelp. Helsemyndigheter og hjelpeorganisasjoner bruker følgelig nettet aktivt til utadrettet virksomhet og førstelinjehjelp, og det er viktig at slike aktører er ekstra bevisste det ansvaret de har for å sikre sine klienters personopplysninger. Kunnskap om et menneskes grad av sårbarhet er ekstremt verdifullt i den digitale annonseindustrien. [En kartlegging gjennomført av Privacy International](#) viste at den digitale annonseindustrien kartlegger aktivitet på nettsider om psykisk helse i Storbritannia, Frankrike og Tyskland. Blant annet fant de at en rekke slike sider, som gjerne dukker opp hvis man søker etter slik informasjon, lekket resultater fra depresjonstester.

Unngår å handle på nett

Svarene viser også at hele 47 prosent har unnlatt å gjøre et kjøp i en nettbutikk. Nettbutikker har gjerne mange opplysninger om kundene sine, blant annet passord, kredittkortinformasjon, navn og adresse. Når folk skal gi fra seg så viktige opplysninger, er det viktig med et godt utviklet tillitsforhold. At nesten halvparten av oss har unnlatt å gjennomføre et kjøp i en nettbutikk, viser at denne tilliten ofte ikke er til stede. Svaret må også forstås i lys av at økonomiske opplysninger anses som svært beskyttelsesverdig. I tillegg kan det tenkes at det fremdeles er like enkelt for mange å oppsøke en butikk som å handle på nett.

Referanser

- Beaton, M., Cortesi, S., Duggan, M., Gasser, U., Lenhart, A., Madden, M., & Smith, A. (2013, 21. mai). *Teens, Social Media, and Privacy*. Pew Research Centre. Hentet fra <https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/>
- Berg, L., & Dulstrud, A. (2018). *Tillit og sårbarhet på nett. Forbrukernes praksiser og vurderinger etter innføring av den nye personvernforordningen (GDPR) i Norge 2019*. Forbruksforskningsinstituttet SIFO. Oppdragsrapport; 9-2018. Hentet fra <https://fagarkivet.oslomet.no/en/item/tillit-og-sarbarhet-pa-nett-forbrukernes-praksiser-og-vurderinger-etter-innforingen-av-den-nye-personvernforordningen-gdpr-i-norge-2018>
- Budington, B. (2020, 27. januar). Ring Doorbell App Packed with Third-Party Trackers. *Electronic Frontier Foundation*. Hentet fra <https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers>
- Cadwalladr, C., & Graham-Harrison, E. (2018, 17. mars). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Hentet fra <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Datainspektionen. (2019). *Nationell Integritetsrapport 2019*. Hentet fra <https://www.datainspektionen.se/om-oss/integritetsrapport/>
- Datatilsynet. (2013/14). *Personvernundersøkelsen 2013/14*. Hentet fra <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-2013-delrapporter/>
- Datatilsynet. (2014). *Personvern 2014 – tilstand og trender*. Hentet fra <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvern-2014-tilstand-og-trender/>
- Datatilsynet. (2015). *Det store datakappløpet*. Hentet fra <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personopplysninger-og-det-digitale-annonsermarkedet/>
- Datatilsynet. (2017). *Personvern 2017 – Persontilpassing og kunstig intelligens*. Hentet fra <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personverndagen-2017-persontilpassing-og-kunstig-intelligens/>

- Datatilsynet. (2018) *Personvern 2018 – Tillit og følelser*. Hentet fra <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvern---tilstand-og-trender-2018/>
- Datatilsynet. (2018). *Personlige finanser – Hvordan utviklingstrekk i finanssektoren påvirker personvernet*. Hentet fra <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/fintech-og-personvern/>
- Datatilsynet. (2019). *På parti med teknologien – Digital målretting av politiske budskap*. Hentet fra <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/malretting-av-politiske-budskap/>
- Den europeiske kommisjon. (2019). *Special Eurobarometer 487a*. Hentet fra <https://www.privacy-web.nl/cms/files/2019-06/ebs487a-en.pdf>
- Forbrukerrådet. (2016, 6. desember). Cayla og i-Que bryter flere norske lover. Hentet fra <https://www.forbrukerradet.no/siste-nytt/cayla-og-i-que-bryter-flere-norske-lover>
- Gulløy, E. (1997). Undersøkelse om personvern: Holdninger og erfaringer 1997. *Statistisk sentralbyrå*, 97/48. Hentet fra https://www.ssb.no/a/histstat/not/not_9748.pdf
- Gundersen, M. (2019, 18. desember). Disqus delte persondata om titalls millioner internettbrukere uten at nettsidene visste om det. *NRK*. Hentet fra <https://nrkbeta.no/2019/12/18/disqus-delte-persondata-om-titalls-millioner-internettbrukere-uten-at-nettsidene-visste-om-det/>
- Gundersen, M. (2019, 28. mai). Dette er de norske nettsidene som sporer deg mest. *NRK*. Hentet fra <https://nrkbeta.no/2019/05/28/dette-er-de-norske-nettsidene-som-sporer-deg-mest/>
- Johnson, B. (2010, 11. januar). Privacy no longer a social norm, says Facebook founder. *The Guardian*. Hentet fra <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>
- Kantar TNS. (2018). *Politiets innbyggerundersøkelse 2018*. Hentet fra <https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/innbyggerundersokelsen/innbyggerundersokelsen-2018.pdf>
- Lynskey, D. (2019). Alexa, are you invading my privacy? – The dark side of our voice assistants. *The Guardian*. Hentet fra <https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants>
- Mazetti, M., & Schmidt, M. S. (2013, 9. juni). Ex-Worker at C.I.A. Says He Leaked Data on Surveillance. *The New York Times*. Hentet fra <https://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html>

Privacy International. (2019). Your mental health for sale. How websites about depression share data with advertisers and leak depression test results. Hentet fra <https://privacyinternational.org/node/3193>

Ravlum, I. (2005). *Setter vår lit til Storebror... og alle småbrødre med? Befolkningens holdning til og kunnskap om personvern. Transportøkonomisk institutt 789/2005*. Hentet fra <https://www.toi.no/getfile.php/13913/Publikasjoner/T%C3%98I%20rapporter/2005/789-2005/789-2005.pdf>

Regjeringen. (2018). *Høring – forslag til ny lov om Etterretningstjenesten*. Hentet fra <https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/>

Regjeringen. (2018). *Høringssvar fra Datatilsynet*. Hentet fra <https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=e0b87829-2c74-4f2c-8066-c75801bcd0d5>

RSA Security. (2019). *RSA Data Privacy & Security Survey 2019: The Growing Data Disconnect Between Consumers and Businesses*. Hentet fra <https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf>

Statistisk Sentralbyrå. (2019). *04495: Tid brukt til ulike massemedier en gjennomsnittsdag (minutter), etter medietype, statistikkvariabel og år*. Hentet fra <https://www.ssb.no/statbank/table/04495/tableViewLayout1/>

Vedlegg – Intervjuguide

Introduksjon

Denne undersøkelsen handler om personvern. Personvern handler om din rett, så langt det er mulig, til selv å bestemme over egne personopplysninger. Kontroll med hvordan opplysninger om en selv blir brukt, hvordan informasjonen sikres og vern om privatlivet, står sentralt.

Bakgrunnsvariabler

Kjønn

Alder

Geografi

Utdanning

Inntekt

Spørsmål 1

I hvilken grad er du opptatt av personvern?

Svaralternativer:

1. Svært opptatt
2. Ganske opptatt
3. Lite opptatt
4. Vet ikke

Spørsmål 2

I hvilken grad passer følgende beskrivelser med ditt syn?

- a. Jeg føler jeg har liten kontroll over hvordan personopplysninger om meg lagres og brukes på internett
- b. Jeg føler meg maktesløs når det gjelder å ha kontroll over personopplysninger om meg på internett
- c. Jeg føler jeg har god kontroll over hvordan personopplysninger om meg brukes på internett
- d. Jeg føler ubehag når jeg tenker på hvor mye personopplysninger om meg som finnes på internett

Svaralternativer:

1. I stor grad
2. I noen grad
3. Verken eller
4. I liten grad
5. Ikke i det hele tatt
6. Vet ikke

Spørsmål 3

Er det noen opplysninger om deg eller andre som du mener lovverket særlig bør beskytte mot innsamling og videre bruk? Hvor viktig er det at lovverket beskytter:

- a. Opplysninger om helsen din
- b. Dine gener/DNA (opplysninger om arvestoff og sannsynlighet for ulike sykdommer)
- c. Ditt fødselsnummer/personnummer – 11 siffer
- d. Din politiske oppfatning
- e. Din religiøse oppfatning
- f. Opplysninger om din privatøkonomi
- g. Hvilken fagforening du er medlem av
- h. Opplysninger om steder du har vært og hvor du beveger deg
- i. Hvilke nettsider du har besøkt/sett på

- j. Bilder av deg
- k. Biometriske data, som identifisering av ansikt, øye- og fingeravtrykk.
- l. Hvem du kommuniserer med på telefon og e-post
- m. Innholdet i telefonsamtalene og e-posten din
- n. Hva du har søkt etter på søkemotorer
- o. Målinger av din effektivitet og tidsbruk på jobb
- p. Ditt nettverk og adferd i sosiale medier

Svaralternativer:

- 1. Helt uviktig
- 2. Lite viktig
- 3. Litt viktig
- 4. Veldig viktig
- 5. Vet ikke

Spørsmål 4

I hvilken grad kjenner du til det nye personvernregelverket (General Data Protection Regulation - GDPR) som ble innført i 2018?

Svaralternativer:

- 1. 1 Kjenner ikke til det
- 2. 2
- 3. 3
- 4. 4
- 5. 5 Kjenner i svært stor grad

Spørsmål 5

I hvilken grad mener du at innføringen av det nye personvernregelverket (GDPR) har styrket ditt personvern?

Svaralternativer:

- 1. 1 Har ikke styrket personvernet
- 2. 2
- 3. 3
- 4. 4
- 5. 5 Har styrket personvernet i stor grad
- 6. Vet ikke

Spørsmål 6

Det nye personvernregelverket (GDPR) viderefører de eksisterende rettighetene, og gir i tillegg nordmenn enkelte nye rettigheter.

Har du hørt om følgende rettigheter som du har?

- a. Du har rett på å få vite hva slags personopplysninger en virksomhet, myndighet eller organisasjon har om deg.
- b. Du har rett på å vite hvordan en virksomhet, myndighet eller organisasjon bruker dine personopplysninger.
- c. Du kan i visse tilfeller be en organisasjon om å slette personopplysninger som de har om deg.
- d. Du kan i visse tilfeller nekte bruk av dine personopplysninger.
- e. Du har rett til å få dine personopplysninger overlevert til deg eller overført til en annen virksomhet (kalt retten til dataportabilitet).

Svaralternativer:

- 1. Ja
- 2. Nei

Spørsmål 7

Nedenfor er en liste over virksomheter og aktører som kan ha personopplysninger om deg. Hvor stor eller liten tillit har du til måten de oppbevarer og bruker personopplysninger på?

- a. Helsevesenet
- b. Forsikringsselskaper
- c. Kredittopplysningsselskaper
- d. Banker
- e. Teleselskaper
- f. Arbeidsgivere (rent generelt)
- g. Sosiale medier (som Facebook, Twitter og LinkedIn)
- h. Meldingstjenester (som Facebook Messenger og WhatsApp)
- i. Søkemotorer (som Google, Yahoo og Bing)
- j. Politiet
- k. De norske etterretningstjenestene
- l. NAV
- m. Skatteetaten
- n. Kommuner
- o. Nettbutikker
- p. Skoler og barnehager

Svaralternativer:

1. Ingen tillit
2. Liten tillit
3. Verken eller
4. Noe tillit
5. Stor tillit
6. Vet ikke

Spørsmål 8

Hvor positiv eller negativ er du til kameraovervåking på følgende steder:

- a. Inne på bussen eller toget
- b. I drosjer
- c. I barer og restauranter
- d. Ved vaskene på offentlige toaletter
- e. I butikker
- f. Inne i barnehager eller barneskoler
- g. Ved inngangen til egen arbeidsplass eller skole/studiested
- h. Der du utfører dine arbeidsoppgaver/studerer
- i. I parker, på stranda og andre offentlige rekreasjonsområder
- j. På gata
- k. I venterommet på legevakta

Svaralternativer:

1. Svært negativ
2. Litt negativ
3. Verken eller
4. Litt positiv
5. Svært positiv
6. Vet ikke

Spørsmål 9

Under er en liste med tjenester/teknologier som vi ber deg svare om du som privatperson bruker i dag, kunne tenke deg å bruke eller ikke kunne tenke deg å bruke.

- a. GPS-sporing av barna dine
- b. GPS-sporing av eldre eller andre familiemedlemmer med spesielt omsorgsbehov
- c. Kameraovervåking i eget hjem eller hytte
- d. Kameraovervåking utenfor eget hjem eller hytte

Svaralternativer:

1. Bruker i dag
2. Kunne tenke meg å bruke
3. Kunne ikke tenke meg å bruke
4. Vet ikke

Spørsmål 10

Ansiktsgjenkjenningsteknologi kan brukes for å identifisere personer, samt anslå blant annet alder og kjønn. Hvor positiv eller negativ er du til bruken beskrevet nedenfor?

- a. At myndigheter bruker ansiktsgjenkjenningsteknologi til å overvåke offentlige rom for å lete etter etterlyste personer?
- b. At videoopptak av deg i en butikk eller kjøpesenter blir analysert slik at en skjerm i butikken viser reklame som passer ditt utseende, kjønn og alder?
- c. At overvåkingsanlegg på arbeidsplasser gjenkjenner og registrerer ansatte?
- d. At overvåkingsanlegg på skoler gjenkjenner og registrerer barn og lærere?

Svaralternativer:

1. Svært negativ
2. Litt negativ
3. Verken eller
4. Litt positiv
5. Svært positiv
6. Vet ikke

Spørsmål 11

Hvilke typer informasjon mener du at det er greit at en arbeidsgiver har tilgang til?

- a. Innholdet i ansattes jobbepost
- b. Oversikt over innholdet i telefon som er eid av jobben, som ringehistorikk og tekstmeldinger.
- c. Oversikt over netthistorikk på ansattes PC som er eid av jobben
- d. Oversikt over informasjon over din tidsbruk i arbeidstiden
- e. Oversikt over helsestatistikk via smartklokke i arbeidstiden

Svaralternativer:

1. Ja, alltid
2. Ja, i enkelte tilfeller
3. Nei
4. Vet ikke

Spørsmål 12

I hvilken grad mener du følgende er akseptabelt eller uakseptabelt?

- a. At foreldre legger ut bilder av egne barn under 13 år på egen Facebook-side, uten å spørre barnet først
- b. At foreldre legger ut bilder av andres barn under 13 år på egen Facebook-side, uten å spørre barnet eller deres foreldre først

- c. At skolene benytter digitale tjenester fra IT-selskaper som Google, Apple og Microsoft som samler inn og bruker elevenes opplysninger til egne formål

Svaralternativer:

1. Helt uakseptabelt
2. Ganske uakseptabelt
3. Verken eller
4. Ganske akseptabelt
5. Helt akseptabelt
6. Vet ikke

Spørsmål 13

Det utvikles stadig flere ting til hjemmet (robotstøvsugere, smarte kjøleskap, målere for innendørsklima, strømmålere og lignende) som sender informasjon over internett. Hvor trygg føler du deg for at informasjonen som samles inn ved hjelp av slik teknologi behandles og lagres på en måte som ivaretar ditt personvern?

Svaralternativer:

1. Helt trygg
2. Litt trygg
3. Verken eller
4. Litt utrygg
5. Svært utrygg
6. Vet ikke

Spørsmål 14

Har du avstått fra å bruke en tjeneste eller et produkt fordi du er usikker på hvordan dine personopplysninger vil bli håndtert?

Svaralternativer:

1. Ja
2. Nei
3. Vet ikke

Spørsmål 15

De fleste nettsteder, søkemotorer og sosiale medier samler inn informasjon om din nettaktivitet for å kunne selge annonser som er tilpasset din atferd.

Hvor positiv eller negativ er du til at virksomheter som har persondata om deg skal bruke dette til å lage persontilpasset reklame til deg?

Svaralternativer:

1. Svært negativ
2. Litt negativ
3. Verken eller
4. Litt positiv
5. Svært positiv
6. Vet ikke

Spørsmål 16

Politiske partier bruker ofte informasjon du har registrert på internett og i sosiale medier, for å kunne sende deg politisk reklame. Informasjonen de bruker kan inneholde informasjon om kjønn, alder, interesser og digital atferd.

Hvor positiv eller negativ er du til at politiske partier målretter politiske budskap til deg basert på personlig informasjon hentet fra internett?

Svaralternativer:

1. Svært negativ
2. Litt negativ
3. Verken eller

4. Litt positiv
5. Svært positiv
6. Vet ikke

Spørsmål 17

Har du gjort noen av de følgende aktivitetene fordi du er usikker på hvordan personopplysningene dine blir brukt av selskapene som tilbyr tjenestene?

Kryss av for alle relevante alternativ. [Randomiser]

- a. Unnlatt å foreta et søk (av en person, begrep, ting) i en søkemotor på nett
- b. Unnlatt å søke hjelp / finne informasjon om mental helse, misbruk, avhengighet eller andre sensitive problemer i en søkemotor på nett
- c. Unnlatt å gjennomføre et kjøp i en nettbutikk
- d. Betalt kontant istedenfor å bruke kort
- e. Unnlatt å delta i en debatt på Facebook
- f. Unnlatt å delta i kommentarfeltet hos en nettavis
- g. Meldt deg ut av en gruppe på Facebook eller annet sosialt medium

Svaralternativer

1. Ja
2. Nei, har ikke gjort dette
3. Vet ikke/ikke relevant

Spørsmål 18

Har du gjort noen av de følgende aktivitetene fordi du er usikker på om myndigheter som politiet, PST eller etterretningstjenesten kan få tilgang til informasjonen?

Kryss av for alle relevante alternativ.

- a. Unnlatt å foreta et søk (av en person, begrep, ting) i en søkemotor på nett
- b. Unnlatt å søke hjelp / finne informasjon om mental helse, misbruk, avhengighet eller andre sensitive problemer i en søkemotor på nett
- c. Unnlatt å gjennomføre et kjøp i en nettbutikk
- d. Betalt kontant istedenfor å bruke kort
- e. Unnlatt å delta i en debatt på Facebook
- f. Unnlatt å delta i kommentarfeltet hos en nettavis
- g. Meldt deg ut av en gruppe på Facebook eller annet sosialt medium

Svaralternativer:

1. Ja
2. Nei, har ikke gjort dette
3. Vet ikke

Spørsmål 19

Dersom du samtykker til det, er det mulig for virksomheter å få tilgang til finansiell informasjon om deg fra din bank. Med tilgang til din finansielle informasjon, kan andre virksomheter enn din bank utvikle betalingstjenester du kan ha nytte av.

Hvor positiv eller negativ er du til å la andre aktører enn din bank få tilgang til finansiell informasjon om deg?

Svaralternativer:

1. Svært negativ
2. Litt negativ
3. Verken eller
4. Litt positiv
5. Svært positiv
6. Vet ikke

Spørsmål 20

Synes du det er problematisk for personvernet ditt å gi Google eller Facebook tilgang til dine finansielle opplysninger i banken (hvis de kan tilby deg en nyttig banktjeneste)?

Svaralternativer:

1. Ja
2. Nei
3. Vet ikke

Spørsmål 20 - FILTER: Spm 20=1

Kunne du likevel være interessert i å benytte deg av en nyttig banktjeneste fra Google eller Facebook?

Svaralternativer:

1. Ja
2. Nei
3. Vet ikke

Spørsmål 21

Hvor positiv eller negativ er du til følgende scenarioer:

- a. Hvis Skatteetaten tok i bruk et automatisk system for å identifisere hvem som har stor risiko for å bedrive svindel. Dette kan baseres på sammenhenger mellom personers alder, økonomiske forhold og andre opplysninger fra selvangivelsen.
- b. Hvis det brukes mer data for å automatisk identifisere elever som står i fare for å droppe ut av videregående skole. Dette kan være informasjon om elevens sosiale bakgrunn og data fra digitale læremidler.
- c. Hvis NAV tok i bruk et system som analyserte jobbsøkeres bakgrunn og deres ledighetshistorikk for å lage persontilpassede tiltak for å få folk ut i arbeid.

Svaralternativer:

1. Svært positiv
2. Litt positiv
3. Verken eller
4. Litt negativ
5. Svært negativ
6. Vet ikke



Postadresse:

Postboks 458 Sentrum
0105 Oslo

postkasse@datatilsynet.no

Telefon: +47 22 39 69 00

datatilsynet.no

personvernbloggen.no

twitter.com/datatilsynet