Oppdragsrapport nr. 9 - 2018

Lisbet Berg og Arne Dulsrud

Tillit og sårbarhet på nett

Forbrukernes praksiser og vurderinger etter innføringen av den nye personvernforordningen (GDPR) i Norge 2018

OSLOMET

STORBYUNIVERSITETET
FORBRUKSFORSKNINGSINSTITUTTET SIFO

OsloMet – storbyuniversitetet
Oppdragsrapport nr. 9 – 2018

Forbruksforskningsinstituttet SIFO
OsloMet – storbyuniversitetet
Stensberggt. 26 – 7. etg.
Postboks 4 St. Olavs plass
0130 Oslo
www.oslomet.no/sifo

Oppdragsapport nr. 9 - 2018

STORBYUNIVERSITETET
FORBRUKSFORSKNINGSINSTITUTTET SIFO

Tittel: Tillit og sårbarhet på nett. Forbrukernes praksiser og vurderinger etter innføringen av den nye personvernforordningen (GDPR) i Norge 2018.	**Antall sider** 43	**Dato** 5.11.2018
Title: Trust and vulnerability online. Consumers' practices and considerations related to GDPR in Norway 2018.	**ISBN** 82-7063-475-1	**ISSN**
Forfatter(e) Lisbet Berg og Arne Dulsrud	**Prosjektnummer** 200772	**Faglig ansvarlig sign.** Anita Baron

Oppdragsgiver

Barne- og likestillingsdepartementet.

Sammendrag

De fleste har et passivt, ikke-refleksivt forhold til den nye personvernloven (GDPR). Det er stor forskjell i tillit til hvorvidt ulike nettaktører behandler persondata på en god måte. Høyest tillit har Altinn, banker og fastlegen. Minst tillit har Facebook, Snapchat og Amazon. Nasjonale plattformer har mer tillit enn globale. Mange synes det er vanskelig å ivareta eget personvern på nett. De unge er mest sårbare i forhold til personvern på nett. Og antageligvis mer sårbare enn de selv er klar over.

Summary

The majority of people aged 16 – 80, living in Norway, have a passive, non-reflective relation to GDPR. The majority of respondents think that it is difficult to manage their privacy options online. When it comes to privacy, young people are the most vulnerable online, and probably more vulnerable than they acknowledge themselves. The extent to which people trust that online actors will handle their personal data in a reliable way, is far higher for national than for global online actors.

Stikkord

Sårbarhet, sårbarhet på nett, personvernloven, datafangst, tillit.

Keywords

Vulnerability, vulnerability online, online privacy, trust.

Tillit og sårbarhet på nett

Forbrukernes praksiser og vurderinger etter innføringene av den nye personvernforordningen (GDPR) i Norge 2018

av

Lisbet Berg og Arne Dulsrud

2018

Forbruksforskningsinstituttet SIFO, OsloMet – storbyuniversitetet
Postboks 4 St. Olavs plass, 0130 Oslo

Forord

I denne rapporten presenteres resultater fra en landsrepresentativ studie i aldersgruppene 16-80 år. Utgangspunktet for studien var å samle kunnskap om hvordan vanlige forbrukere forholder seg til *de nye europeiske reglene for håndtering av personopplysninger GDPR (General Data Protection Regulation)*. Studien er finansiert av Barne- og likestillingsdepartementet, ved Forbruker-, rettighets- og likestillingsavdelingen.
Rapporten er kvalitetssikret av Eivind Jacobsen, SIFO

Oslo, 5. november 2019
Forbruksforskningsinstituttet SIFO,
Storbyuniversitetet – OsloMet

Innhold

Sammendrag

I denne rapporten har vi reist fem hovedspørsmål:

- *Er de nye personvernreglene - GDPR - kjent blant folk?*

De fleste (82%) har hørt om GDPR, men bare 9 prosent svarer at de 'vet godt' hva de nye personvernreglene innebærer. I tillegg svarer 47 prosent at de 'vet noe'.

- *Fungerer samtykke-erklæringene etter intensjonen; som personvern-beskyttelse?*

På et generelt spørsmål var det 40 prosent som sa de hadde gjort noe aktivt for å beskytte persondata og andre opplysninger knyttet til deres person. På spørsmål knyttet direkte til bruken av Facebook var det kun 13 prosent av de med Facebook-konto som sa at de hadde endret på innstillingene og reservert seg mot noe av det Facebook lagrer om dem. Vi kan regne med at i hvert fall to tredjedeler av de som er på Facebook ikke gjør annet enn å gi sitt samtykke, uten å se hva de samtykker til. På Google var det enda færre, bare fem prosent, som sa de har endret på innstillingene som gir Google anledning til å benytte deres persondata.

- *Er forbrukerne i stand til å bruke GDPR for å ivareta egne interesser?*

Det er stor skepsis til spørsmål om man evner ivareta eget personvern på nett. Hele 80 prosent mener det er vanskelig å finne ut hva som lagres om dem, og nesten 70 prosent sier personverninnstillingene er forvirrende og uoversiktelige. Samlet tolker vi dette til at følelsen av bruker-kontroll ikke er veldig stor, med andre ord at personvern-sårbarheten er betydelig.

- *Bidrar GDPR til mer **tillit** til digitale tjenester generelt? Og; Hvilke aktører anser forbrukerne som **mest risikable** – statlige, kommersielle, nasjonale, globale?*

Det er store forskjeller i tillit til ulike plattformer. Vi kan ikke si at offentlige plattformer nyter større tillit enn private. Men vi kan si at det er langt flere som har tillit til at nasjonale plattformer – både offentlige og private – behandler opplysninger knyttet til person på en tilfredsstillende måte, enn at store globale plattformer gjør det.
Litt over halvparten er helt eller litt enige i at GDPR gir forbrukerne bedre rettigheter. Men bare en av ti mener at GDPR er *tilstrekkelig* for å sikre en god håndtering av persondata. Hovedbildet er at svært mange er usikre på virkningene av GDPR. Ganske logisk; jo mindre følelse av kontroll med eget personvern, jo mindre tillit har forbrukerne til at GDPR løser personvernproblemet på nett. Troen på at GDPR gir økt tillit på nett, øker med hvor eksponert – eller erfaren - man er på nettet.

- *Er det grupper som er spesielt sårbare i forhold til personvern på nett?*

Vi har laget en Personvern-sårbarhet-indeks basert på hvordan den enkelte opplever at de klarer å ivareta eget personvern på nett. Vi finner en generell, usystematisk usikkerhet knyttet til personvern og GDPR i alle grupper – riktignok litt mer usikkerhet blant de yngre, de fra arbeiderklassen og de som ikke er i inntektsgivende arbeid, alt annet likt. Men det er først og fremst egen praksis på nett som har stor forklaringskraft på følelsen av personvern-sårbarhet. Samlet tyder analysen på at de unge, som er svært eksponert for datafangst på nett, underrapporterer egen personvernsårbarhet. Det er nemlig særlig aldersgruppene som oftest har konto på Facebook og Google, de mellom 16 og 20 år, som helt klart har lettest for å trykke på samtykke erklæringer, uten å lese gjennom informasjonen fra plattformene.

Summary: Trust and vulnerability online

This project investigates how Norwegian consumers responded to the new General Data Protection Regulation (GDPR) of May 2018. A web survey was carried out during July 2018 among 1000 people living in Norway, in the age groups between 16 and 80 years. GDPR, as well as the Cambridge Analytica scandal, was given lots of attention in media before and during the data collection period. The report focus on five main questions, the first one is:

- *Are people informed about the GDPR?*

The results demonstrate that most people (82%) have heard about GDPR, but only 9 percent said that they knew 'well' what the new privacy rules imply. In addition, 47 percent said they knew 'something'.

- *Do consent statements function as intended, according to privacy protection?*

On a general question, 40 percent said they had actively made efforts to protect personal data/deleted online accounts after receiving GDPR inquiries. On questions directly related to Facebook, only 13 percent among Facebook account holders said that they had changed their settings/made reservations about what Facebook stores about them. It is reason to believe that at least two thirds of those on Facebook just give their consent, without even looking at what they have agreed on. At Google, only five percent said they changed their settings or made reservations on what Google was allowed to use of their personal data.

- *Are consumers able to use GDPR to safeguard their own interests?*

People express far more skepticism than confidence concerning their capability to safeguard own privacy online. According to self-reports the feeling of user control is not very high. Almost 70 percent said that privacy settings are confusing and unclear. Even more, 80 percent agreed that it is difficult to find out what is stored about them. In other words, *online privacy vulnerability is significant*.

- *Does GDPR contribute to more trust in digital services in general? And what actors/platforms do consumers consider to be the most risky: public-, commercial-, national-, or global platforms/actors?*

There were big differences in people's confidence in different platforms. We cannot say that public platforms enjoy greater trust than private and commercial ones. But, more people believe that national platforms - both public and private - treat personal data in a satisfactory manner, than they believe that large, global platforms do.

More than every second respondent agreed, or somewhat agreed, that GDPR imply *better consumer rights*. But, only one in ten believed that GDPR is *sufficient* to ensure safe handling of personal data. The main picture is that many people are uncertain about the effects of GDPR. We cannot distinguish one demographic group that are more confident, or skeptical, to GDPR than others. The belief that GDPR boosts online trust increases with how exposed - or experienced - people are online, as well as how well they feel that they manage their own online privacy.

- *Are there any groups that are particularly vulnerable to online privacy?*

We have created a Privacy Vulnerability Index based on how individuals experience their (lack of) ability to manage their own online privacy. We find a general, unsystematic uncertainty related to privacy and GDPR in all groups - albeit somewhat more uncertainty among the younger ones, those of the working class and those who are not in gainful employment, all other variables kept constant. However, first and foremost it is *online practice*, more precisely sharing data because of *fear of loosing online functionality*, that is the strongest driver of the sense of Privacy Vulnerability. Also, the analysis suggests that young people, who are very exposed to online data capture, underestimate their own Privacy Vulnerability: It is the groups between the ages of 16 and 20, highly exposed online, who more frequent than others, tend to agree to consent statements without reading the information available on the platforms.

1 Innledning

I denne rapporten undersøker vi hvordan individer og forbrukere agerer i en digital hverdagskontekst, mer presist hvordan de forholder seg til de mulighetene og den myndigheten de har fått gjennom de nye personvernreglene – GDPR (General Data Protection Regulation).
Vi stiller følgende spørsmål:

- *Er de nye personvernreglene - GDPR - kjent blant folk?*
- *Fungerer samtykke-erklæringene etter intensjonen, dvs som personvern-beskyttelse?*
- *Er forbrukerne i stand til å bruke GDPR for å ivareta egen interesse?*
- *Bidrar GDPR til mer **tillit** til digitale tjenester generelt, i netthandel, på sosiale medier? Og; Hvilke aktører anser forbrukerne som **mest risikable** – statlige, kommersielle, nasjonale, globale?*
- *Er det grupper som er spesielt sårbare i forhold til personvern på nett?*

Økningen i de digitale sporene vi legger igjen i hverdagen har ført til et økt fokus på personvern. Nye nettjenester gir mulighet til å generere, lagre og analysere enorme datamengder knyttet til individer (stordata). Gjennom digitale plattformer samler selskaper data som forteller om våre 'likes', interesser, ønsker, politiske holdninger og seksuelle preferanser. Særlig gjelder det forhold der individet opptrer som forbruker. Data om forbrukere, i kombinasjon med nye digitale løsninger, gir muligheter til såkalt algoritmebasert markedsføring. Det betyr at bedrifter har mulighet til å tilpasse produktene, informasjon, tilbud og reklame mot hver enkelt kunde (Dulsrud og Alfnes 2018). Selskaper med omfattende forbrukerdata innen en bransje vil være i stand til å få en bedre markedsforståelse og utvikle mer treffsikre individualiserte tilbud til forbrukerne. Store internasjonale nettjenester slik som Google, Facebook og Amazon, har de beste mulighetene til å være ledende innen utvikling av nye analysemetoder og bruksområder, noe som har medført at persondata deles og omsettes mellom næringsdrivende.

Personvernforordningen GDPR

Det har vært en økende politisk erkjennelse av at forbrukeren er den sårbare parten. Spesielt viktig er EUs nye personvernforordning som strammer inn personvernreglementet for bedrifter som er aktive i Europa. Personvernforordningen (Forordning 2016/679), på engelsk General Data Protection Regulation, forkortet GDPR) er en forordning som skal styrke og harmonisere personvernet ved behandling av personopplysninger i Den europeiske union (EU). I EU trådte forordningen i kraft 25. mai 2018. Personvernforordningen gjelder også for EØS-landene, og i Norge trådte forordningen i kraft 20. juli 2018.

Bakgrunnen for forordningen er todelt: først og fremst et ønske om å bedre enkeltpersoners mulighet for å kontrollere opplysninger registrert om dem selv. Videre la EU vekt på at opprettelsen av like regler for alle medlemsland ville tjene den økonomiske utviklingen i dette området.

Direktivet utvider virkeområdet for EUs personvernlovgivning ved at det også dekker alle utenlandske selskaper som behandler data om innbyggere i EU. I praksis betyr det f eks at amerikansk eller asiatisk eide virksomheter som operer i Europa må forholde seg til de nye reglene.

Det legges opp til en ansvarliggjøring av selskapene også, brudd kan medføre strenge bøter på opptil 4% av en den samlede omsetningen til virksomheten.

Direktivet gjelder dersom den som behandler persondata (f eks en virksomhet) eller den registrerte (en person) befinner seg i EU. Personopplysningsbegrepet dekker alle opplysninger knyttet til en person, enten det gjelder hans eller hennes private, profesjonelle eller offentlige liv. Det kan være alt fra et navn, et bilde, en e-post-adresse, bankdetaljer, innlegg på sosiale nettverk nettsteder, medisinsk informasjon, eller en IP-adresse til datamaskinen. Innføringen av GDPR forutsetter et vesentlig ansvar fra brukeren også.

Personer må samtykke til bruk av informasjonene om deres aktiviteter. Det betyr at alle virksomheter som behandler persondata etter direktivets innføring må be den registrerte om tillatelse til å behandle deres persondata. Det gjelder alt fra sosiale media (Facebook) mv til organisasjoner som registrerer personopplysninger. Brukere av sosiale medier og nettsteder skal kunne kreve innsyn og kunne nekte deling av spesifikke persondata. Konsekvensen kan være at de mister tilgang til bestemte typer tjenester, eks personifisert reklame.

Personopplysninger skal bare samles inn til bestemte formål og disse må være uttrykkelig gitt og legitime. I tillegg må formålene for den videre behandling ikke avvike fra de formål opplysningene opprinnelig ble samlet inn for. Personopplysninger skal heller ikke utleveres til andre uten at det foreligger samtykke.

Dessuten ligger følgende prinsipper til grunn for personvernlovgivningen:

Minimalitet. Personopplysninger skal bare samles inn, lagres og behandles i den grad det er nødvendig for å oppnå formålet – innsamlede data som ikke lenger er nødvendig for formålet må anonymiseres eller slettes.

Kvalitet. Personopplysningene må være relevante, korrekte og fullstendige ut fra formålene de skal benyttes til. Dette for å unngå at beslutninger på grunnlag av personopplysninger ikke blir fattet på et feil eller ufullstendig grunnlag.

Informasjon og innsyn. Som registrert skal man ha rett til å bli informert om innsamling og bruk av sine personopplysninger.

Portabilitet. En person skal kunne overføre sine personopplysninger fra et elektronisk behandlingssystem til og inn i en annen, uten at det blir forhindret av dataansvarlig.

På mange måter gir det nye personvernforordningen GDPR forbrukeren både myndighet, fullmakt og beskyttelse gjennom prinsippet om at individet har full råderett over egne persondata (portabilitet) og at samtykke må være til stede dersom det skjer endringer i formålet med bruken av data. Men denne myndigheten forutsetter at brukeren har forutsetninger for å kunne vurdere hvilken verdi persondata har for selskaper som benytter disse, og hvilken potensiell risiko deling av persondata kan medføre. Ut fra et reguleringsmessig perspektiv hviler hensynet til beskyttelse i særdeles stor grad på individets egen evne til å foreta en fornuftig og rasjonell avveining mellom nytte ved å gi fra seg persondata på den ene siden (økt brukervennlighet), og kostnader og risiko på den andre.

Sårbarhet

Tidligere undersøkelser viser et noe sammensatt bilde når det gjelder hvordan brukere vurderer nytte og risiko ved de nye nettjenestene. En undersøkelse som Opinion AS foretok for Datatilsynet i 2015 (Datatilsynet 2016) tyder på at folk flest (nær 80 prosent) synes det er ubehagelig at nettaktører bruker persondata til kommersielle formål og personlig tilpasset reklame. Samtidig bruker de aller fleste gratistjenester på internett slik som Google og Facebook, og mange

bruker tjenester som bringer med seg kommersiell utnyttelse av personopplysninger. En forklaring, ifølge Datatilsynet (2016:41), kan ha vært at folk ikke ser alternativer, og at det ikke er aktuelt å gå av nettet. GDPR gir nettopp brukeren mulighet til å kontrollere utnyttelsen av personopplysninger.

Ut fra en prinsipiell vurdering er det likevel grunn til å spørre om GDPR vil gi forbrukere og individer tilstrekkelig beskyttelse. Det er flere grunner til det. Forbrukere representerer en sammensatt kategori med utsatte og sårbare grupper med svært ulike forutsetninger til å gjøre «fornuftige» valg på nettet og i en digital markedskontekst der kunnskap og innsikt er svært asymmetrisk fordelt mellom selger og forbruker. Tidligere forskning indikerer også at det er høyst varierende om forbrukerne forholder seg til brukervilkår (Kjørstad et al 2017). Datatilsynet fant at alder spilte en rolle. F eks syntes de yngre under 30 år (34 prosent) i mye større grad enn de eldre over 50 år (10 prosent) at det var greit at nettaviser benytter brukerdata for å tilpasse reklame. Yngre kan dermed være mer sårbare.

En annen grunn er at informasjon knyttet til brukervilkår ofte presenteres på måter som er vanskelig å forstå for forbrukeren (Slettemeås 2018). Det gjør at forbrukeren av hensyn til bekvemmelighet aksepterer vilkårene uten å ha kunnet sette seg inn i dem. Beslutningssituasjonen framstår som forvirrende og uklar, samtidig som brukeren i mange tilfeller mangler tilstrekkelig kunnskapsgrunnlag for å vurdere brukervennlighet mot risiko.

I tidligere undersøkelser har vi stilt spørsmål ved forbrukerens mulighet og evne til å ivareta sitt ansvar på en tilstrekkelig måte. Et stort reguleringsansvaret hviler på det svakeste leddet (Dulsrud og Alfnes 2018). Til sammen gir dette gode grunner for å følge utviklingen tett både fra tilsynsmyndigheter og forskning. Tidligere undersøkelser som er referert ovenfor, analyserte hvordan folks holdninger og hvordan de kunne tenke seg å agere i tenkte situasjoner.

3 Metode

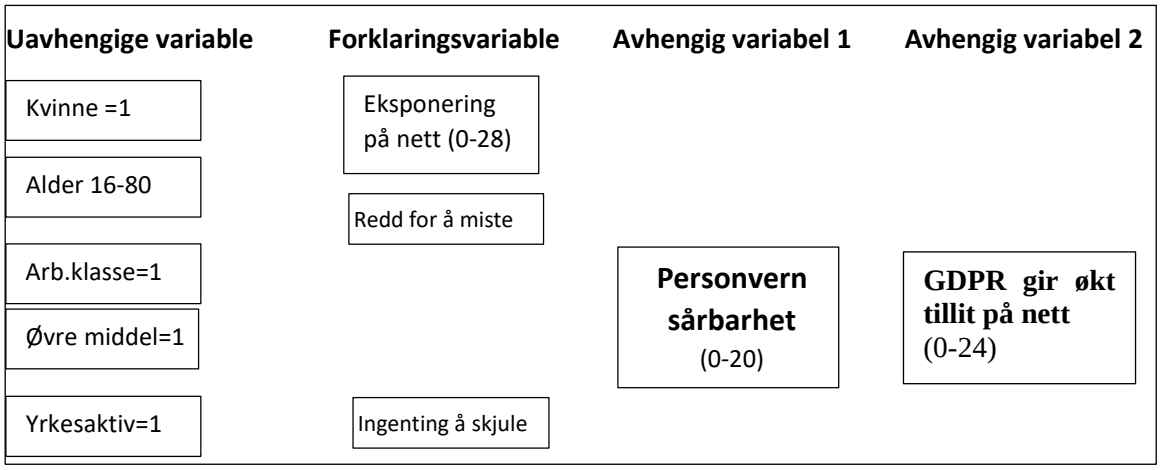
For å få innblikk i hvordan forbrukerne responderte på de nye personvernreglene (GDPR) gjennomførte Norstat på vegne av SIFO en web-survey primo juli 2018, altså omtrent en måned etter at GDPR ble gjeldene i EU den 25. mai 2018. Før og under innsamlingen av data fikk GDPR stor oppmerksomhet i pressen. Med denne studien ønsker vi å undersøke hvordan forbrukerne har mottatt det nye direktivet, og vi kan også gjenta studien etter en viss tid, for å undersøke om bevisstheten om, holdninger til, og praksiser knyttet til personvern på nett har endret seg.

Vi gjennomført en web-undersøkelse med litt over 1000 respondenter basert på Norstat's kvalitetssikrede panel. Fordi det er de unge som er mest aktive på nettet, og derfor kanskje mest sårbare for algoritme-styrt markedsføring, ønsket vi å inkludere respondenter helt ned til 16 år. Materialet er samlet inn på en slik måte at skjemaet sendes til et landsrepresentativt utvalg i aldersgruppene 16 – 80 år. Utvalget er forhånds-stratifisert, og i tillegg har vi vekter for kjønn, alder og geografi som sikrer at også det responderende utvalget skal være landsrepresentativt.

For å få et best mulig materiale har vi lagt vekt på at spørreskjemaet skulle være kort, med lettfattelige spørsmål, og ikke minst, så interessant som mulig å besvare for respondentene. Spørreskjemaet ligger som vedlegg.

3.1 Analytisk modell

I vår analytiske modell skiller vi mellom uavhengige variable, forklaringsvariable og avhengige variable. Hensikten med de uavhengige variablene er å kunne identifisere mulige grupperinger som er spesielt sårbare på nettet, med andre ord de som ikke klarer å nyttiggjøre seg de nye personvern reglene (Personvern-sårbarhet). Kjønn, alder etc. trekkes først inn i den avsluttende multivariate analysen. I den multivariate analysen vil vi også undersøke om det er grupper som er spesielt positive/negative til hvordan GDPR fungerer i forhold til trygghet og tillit på nettet (GDPR gir økt tillit på nett). I modellen har vi også med forklaringsvariable – eller mellomliggende variable – som eventuelt kan forklare hvorfor noen grupper fremstår som mer sårbare enn andre på nettet. Innledningsvis presenteres univariate fordelinger på variablene som senere skal brukes til å danne indekser i den avsluttende multivariate analysen.



Modell 1: Analytisk design.

Basert på modellen over kan vi undersøke hvilke grupper som er mest sårbare i forhold til personvern på nett, og hvilke grupper som har tro på at de nye personvern reglene (GDPR) bidrar til økt tillit og trygghet på nett. Vi kan også undersøke hvilke grupper som er mest eksponert på nett, hvilke grupper som gir lett fra seg personlig informasjon fordi de er redde for å miste funksjonalitet (Redd for å miste), og hvilke grupper som deler ubekymret fordi de mener at de ikke har noe å skjule (ingenting å skjule)? Ikke minst kan vi i multivariat stianalyse undersøke om i) eksponering på nett, eller ii) det å være redd for miste funksjonalitet, eller iii) det å dele ubekymret fordi de mener de ikke har noe å skjule, kan forklare personvernsårbarhet.

3.2 Uavhengige variable

Med analysen ønsker vi å undersøke om det er spesielle grupper som er spesielt sårbare i forhold til personvern på nett. Vi skiller derfor på kjønn, alder, klassebakgrunn og yrkesaktivitet. Grunnen til at vi ikke har med utdanningsnivå, som er en vanlig variabel for å måle sosial bakgrunn, er at utdanningsnivået henger sterkt sammen med alder. Vi vil da også få uriktig sosial bakgrunn for de yngste grupperingene, fordi de ikke har rukket å avslutte sine utdanningsløp. I stedet benytter vi selvopplevd klassebakgrunn som mål på sosial bakgrunn, der vi skiller mellom de som sier at de tilhører arbeiderklassen (26%), de som sier de tilhører middelklassen/lavere middelklasse (38%), og til slutt de som sier de tilhører overklassen (nesten ingen svarer dette i Norge) og øvre middelklasse (24%). Bare 11 prosent oppga ikke klassebakgrunn. Klassebakgrunn er ikke en kontinuerlig variabel, og i den multivariate analysen måles derfor klasse på dummy-variable, der arbeiderklasse (1) og øvre middelklasse (1) sammenlignes med middelklassebakgrunn (0).
Utvalget har med personer i aldersgruppene 16 – 80 år, og alder inngår i analysen som kontinuerlig variabel (16-80), bortsett fra i tilleggs- tabeller, som viser at den kontinuerlige aldersvariabelen er forsvarlig.
Til slutt har vi med en variabel som skiller på de som er yrkesaktive (heltid og deltid) mot de andre.

3.3 Avhengige variable

Hensikten med GDPR var å bidra til bedre personvern og økt trygghet og tillit på nettet. Vi har derfor to avhengige variable som skal måle hvordan GDPR fungerer i forhold til henholdsvis sårbarhet og tillit på nettet. For å undersøke om det er spesielle grupper som er sårbare i forhold til personvern på nett, har vi konstruert en *Personvern-sårbarhet-indeks* (avhengig variabel 1).

Indeksen bygger på fem utsagn respondentene tar stilling til, målt på skala 1-5:

- Jeg synes personverninnstillingene er forvirrende og uoversiktlige
- Jeg har dårlig kontroll med hva jeg gir fra meg av persondata (snudd 'god kontroll')
- Jeg forstår ikke hvordan jeg skal beskytte mine personopplysninger
- Jeg synes det er vanskelig å finne ut hvilke persondata som lagres om meg
- + I hvilken grad man sjekker hva slags persondata sosiale medier, kommersielle selskaper eller andre ber om tillatelse til å registrere om en. (snudd)

Med Personvern-sårbarhet-indeksen ønsker vi å fange opp respondentene som i liten grad ivaretar eget personvern. *Personvern-sårbarhet-indeksen gir et mål på respondentens selvopplevde følelse av mestring eller sårbarhet i forhold til de nye personvernreglene.* Dette er altså ikke et objektivt, men et subjektivt mål på personvern-sårbarhet.
For å undersøke hvem som har tro på at GDPR fungerer etter intensjonen om at de nye personvernreglene skal bidra til økt tillit og trygghet på nettet, har vi konstruert indeksen *GDPR gir økt tillit på nett* (avhengig variabel 2) basert på seks utsagn respondentene tar stilling til på skala 1-5:

De nye reglene for håndtering av personopplysninger….

- …..er tilstrekkelig
- …..gir forbrukerne bedre rettigheter
- …..gir større tillit til digitale tjenester generelt
- ….gjør det tryggere å dele på Facebook og andre sosiale medier
- ….gjør det tryggere å handle på nett
- Jeg tror det nytter å si nei til at selskaper på nettet lagrer og bruker mine persondata

Med *GDPR gir økt tillit på nett-indeksen* kan vi undersøke hvordan GDPR fungerer i forhold til tillit og trygghet sett fra ulike grupperinger av forbrukere.

3.4 Forklaringsvariable

De mellomliggende variablene – eller forklaringsvariablene – har til hensikt å forklare eventuelt *hvorfor* ulike grupper er mer sårbare enn andre i forhold til å dele person- og forbrukerdata på nettet. Modellen vil også vise om de valgte forklaringsvariablene kan være *drivere* av sårbarhet uavhengig av gruppetilhørighet. Vi antar at jo flere nettsteder respondentene er aktive på, jo mer utsatte er de i forhold til persondata-registreringer. Derfor har vi med en indeks som måler *Eksponering på nett*. Respondentene ble bedt om å svare 'nei' (0), 'ja det hender' (1) eller 'ja, ofte' (2) på hvor ofte de er på 14 navngitte digitale plattformer. Dette gir en index fra 0-28, en proxy, som skal speile hvor eksponert den enkelte er for å gi fra seg person- og forbrukerdata på nett.

Spesielt to utsagn representerer viktige *drivere* for å dele persondata på nett, og er derfor inkludert som forklaringsvariable i den multivariate analysen. På disse utsagnene kunne respondentene svare at dette 'Stemmer ikke', 'stemmer dårlig', de er 'usikre/vet ikke', det 'Stemmer litt', eller 'stemmer helt', med andre ord får vi to forklaringsvariable som går fra 1-5.

- Det spiller ingen rolle hva jeg deler på nettet for jeg har ingen ting å skjule
- Jeg er redd for å skru av deling av informasjon fordi jeg tror jeg kan miste funksjonalitet.

Den første gir en naiv, ubekymret forklaring på hvorfor man deler opplysninger om seg selv på nettet, mens den andre gir en mer tvungen forklaring, der respondenten deler opplysninger om seg selv, selv om de ikke liker det.

3.5 Analysen

For å besvarer våre problemstillinger presenteres først en univariat fordeling på variablene som måler kunnskap om, praksis og holdninger til GDPR.

For å undersøke om spesielle grupper av forbrukere er mer sårbare enn andre, og om vi finner forklaringer til hvorfor noen er mer sårbare enn andre, gjennomføres tre multivariate analyser (SPSS+). Vi undersøker om personvern-sårbarhet på nett kan knyttes til kjønn, alder, selvrapportert klassebakgrunn og hvorvidt man er i inntektsgivende arbeid eller ikke. I tillegg undersøker vi om noen grupper er spesielt skeptiske eller positive til hvorvidt GDPR bidrar til økt tillit på nettet. Vi undersøker også om personvernsårbarhet kan forklares gjennom høy eksponering på nett, altså at spesielle grupper er mer eksponert på nett enn andre, og hvorvidt sårbarhet kan knyttes til at spesielle grupper oftere deler opplysninger om seg selv ubekymret, eller tvangsmessig.

Vi estimerer tre multivariate modeller. I den første modellen ser vi både de to avhengige og de tre forklaringsvariablene som avhengige variable – og undersøker om de uavhengige variablene gir signifikante utslag på dem (fem lineære regresjoner). I tillegg viser vi hvordan disse – her fem avhengige variable – korrelerer (bivariate korrelasjoner).

I den andre modellen, for særlig å undersøke om det er spesielle grupper som er sårbare i forhold til personvern på nett, trekker vi inn de tre forklaringsvariablene som mellomliggende variable i en sti-analyse; altså undersøker vi om henholdsvis eksponering på nett, naiv deling av persondata, samt det vi kan kalle tvangsmessig deling av persondata, har betydning for selvopplevd personvernsårbarhet.

I den tredje modellen lar vi personvernsårbarhet inngå som mellomliggende forklaringsvariabel og undersøker hva som påvirker troen på de nye reglene for håndtering av personvern. Altså troen på at *GDPR gir økt tillit på nett*. Vi ønsker undersøke om det er spesielle grupper som, alt annet likt, er mer utsatte for personvernsårbarhet enn andre, hvem som har tro på de nye reglene, og eventuelle forklaringer til dette.

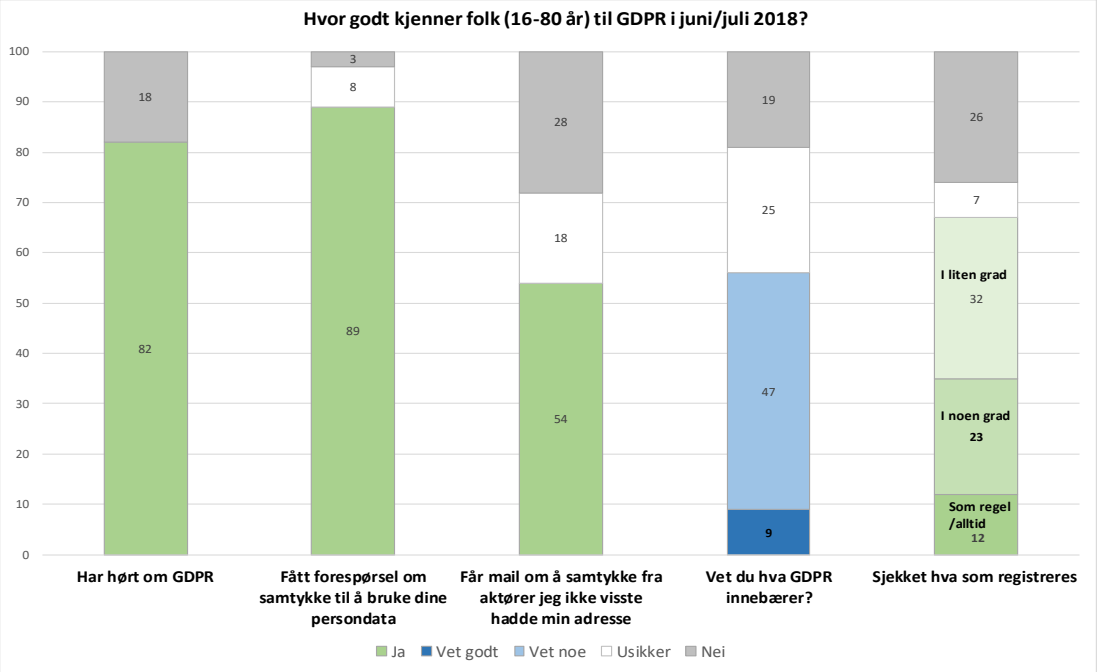
I presentasjonen av resultatene, basert på lineære regresjonsanalyser (SPSS+), viser vi kun de signifikante effektene (standardiserte regresjonskoeffisienter). Positive effekter tegnes med heltrukken linje, mens negative effekter tegnes med stiplet linje. Der det ikke går linjer, er det altså ingen signifikante effekter.

Resultatene presenteres visuelt i figurer, og som god praksis følger vi prinsippet om å vise *hele* prosent-skalaen (0-100) i prosentfordelinger. Og, igjen for ikke å overdrive forskjeller, når vi sammenlikner gjennomsnitt, viser y-aksen hele skalaen. Dette for at ikke variasjoner i resultatene skal overdrives.

4 Resultater

4.1 Er GDPR kjent blant folk?

Hvor godt kjenner folk til de nye reglene for håndtering av personopplysninger? GDPR har vært varslet og forberedt over en viss tid, og trådde i kraft i EU 25 mai 2018. Det var relativt mye presse om dette i måneden før og etter effektueringen av GDPR, så vi regnet med at de fleste hadde hørt om de nye personvernreglene, og at de dermed ville gjenkjenne varslinger om dette på nettsteder de besøkte. Det er rimelig å tenke seg at særlig Cambridge Analytica skandalen[1] har skapt økt oppmerksomhet rundt nettaktørers datafangst. Vi vet også fra tidligere studier at mange føler 'ubehag' ved at de for eksempel gir fra seg opplysninger om kjøpsadferd i bytte mot kjedenes fordelskort/lojalitetskort/app'er (Berg og Slettemeås 2017), noe som skulle tyde på at mange vil gripe muligheten og sette seg inn i hvordan GDPR kan gi dem bedre kontroll med sine persondata. Andre studier tyder imidlertid på at forbrukerrollen er tettpakket, og at de fleste har mangel på oppmerksomhet-kapasitet (Berg og Gornitzka 2012). Med andre ord er forbrukernes kapasitet under press, og ansvar for personvern kan dermed bli nedprioritert. I første figur skal vi se hvor mange som har hørt om de nye personvernreglene, om de vet hva reglene innebærer, og ikke minst om de har gjort noe aktivt, her å sjekke hva som registreres om dem:



Figur 1: Kjennskap til GDPR blant internettbefolkningen 16-80 år. Prosent. Landsrepresentativ vekt. (N=1003)

[1] https://www.aftenposten.no/tag/Cambridge_Analytica

Dette er en web-survey, så hele utvalget er på nettet. De fleste (82%) har hørt om GDPR, og enda flere, nesten alle (89%), har registrert at de har fått forespørsler om å samtykke til at nettaktører kan registrere og bruke deres persondata. De aller fleste har altså fått med seg – og erfart - at det er kommet nye personvernregler for plattformer og nettaktørene. Men resultatene viser likevel at bare litt over halvparten (56%) vet noe hva dette innebærer. Bare 9 prosent svarer at de 'vet godt' hva de nye reglene for håndtering av personopplysninger innebærer, 47 prosent svarer at de 'vet litt'.

På et generelt spørsmål om hvorvidt respondentene har sjekket hva slags persondata sosiale medier, kommersielle selskaper eller andre ber om tillatelse til å registrere om dem, svarer 26 prosent 'nei' og syv prosent er 'usikre'. Med andre ord har én av tre neppe sjekket hva som registreres om dem. I tillegg svarer én av tre at de 'i liten grad' har sjekket dette. Mange i denne gruppen har sannsynligvis heller ikke gjort stort. Fordi sannsynlighet er større for å overvurdere, enn å undervurdere, egne prestasjoner, kan vi anta at det bare er rundt en tredjedel som aktivt har gått inn og sjekket hva nettaktører samler av personopplysninger om dem: 23 prosent svarer 'i noen grad' og bare 12 prosent svarer at de 'som regel/alltid' sjekker hva nettaktører registrer på dem. Egne erfaringer kan tyde på at henvendelsene om samtykke etter innføring av GDPR er blitt så hyppige at det etter hvert blir en refleks å tillate slik lagring.

Resultatene i figur 1 viser også at over halvparten (54%) mottar mailer med forespørsler om å samtykke fra nettaktører de ikke viste hadde opplysninger om dem. Ved ikke å besvare disse, antar vi at mange får redusert aktørers tilgang på deres personopplysninger.

Samlet kan vi besvare første problemstilling: Ja, folk har hørt om GDPR, men nei, de er ikke godt informerte om hva GDPR innebærer, og bare et mindretall ser ut til å undersøke aktivt hva slags persondata som oppbevares om dem.

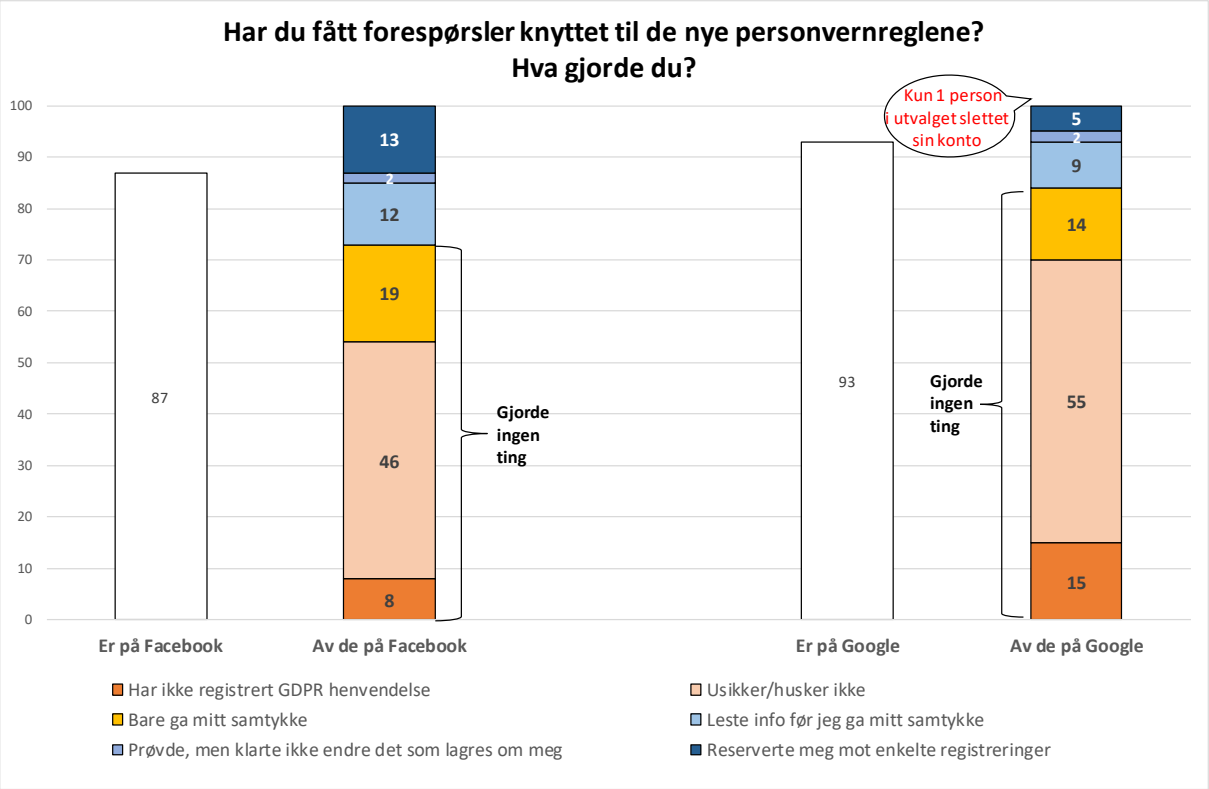
4.2 Fungerer samtykke-erklæringene etter hensikten?

Ingenting er gratis, heller ikke Facebook og Google, der man betaler med persondata, samt å stille seg åpen for reklame. Facebook og Google er noen av de største aktørene som selger tjenester der persondata er den sentrale varen. GDPR skal i prinsippet gi forbrukerne mer makt, gjennom å tvinge aktører som samler og benytter seg av persondata, til å opplyse om dette, og til å gi sine brukere/kunder muligheten til å reservere seg eller slette sine profiler. De nye personvernreglene gir brukere muligheter til å begrense hva slags data som sankes fra dem, f.eks gjennom å reservere seg mot Facebook's ansiktsgjenkjenning. Man kan også reservere seg mot personlig rettet reklame – og i stedet få tilfeldig reklame. I Datatilsynets undersøkelse var det 73 prosent som – på direkte spørsmål - fortrakk tilfeldig framfor personlig rettet reklame (Datatilsynet 2016). GDPR-henvendelsene vektlegger gjerne at tjenesten trenger persondata for å gi 'deg' et best mulig tilbud, tilpasset 'ditt' personlige behov. Og samtykket presenteres ofte som et valg mellom 'jeg forstår' og 'jeg vil vite mer'.

På et generelt spørsmål om respondentene hadde gjort noe aktivt for å beskytte sine persondata og andre opplysninger knyttet til sin person, var det 40 prosent som svarte at de enten hadde 'gått aktivt inn og endret på hva en avsender skal få registrere på meg' (30%), eller at de hadde 'slettet min profil hos nettaktør/tilbydere' (11%). Dette er litt flere enn da Ipsos MMI – rett etter Cambridge Analytica skandalen - spurte om respondentene hadde tilpasset hvor mye data som ble lagret om dem (32%) (Veberg 2018).

For å få bedre innblikk i hvorvidt GDPR-påbudte samtykke-erklæringer fungerer etter hensikten, har vi stilt spørsmål direkte knyttet til bruk av de største enkeltaktørene på nettet; Facebook og Google. Dette er aktører som leverer tjenester mange ikke kan se seg foruten. Begge aktørene har som følge av GDPR gitt sine brukere mulighet til å slette eller endre sine profiler før

de samtykker aktivt til at Facebook/Google kan bruke deres persondata. Fungerer samtykke erklæringen etter intensjonen? Registrerer brukere at de har fått slike henvendelser? Og gjorde de noe aktivt som følge av henvendelsene?



Figur 2: Hvordan forbrukerne responderer på forespørsler knyttet til personvernreglene (GDPR) på Facebook og på Google. Prosent. Landsrepresentativ vekt. (N=1001)

Hovedfunnet i Figur 2 er at svært mange har et lite reflektert, og heller passivt, forhold til de nye GDPR reglene. Figur 2 viser hvor mange som sier de er brukere på henholdsvis Facebook og Google, og hvordan de med konto har respondert på GDPR henvendelsen, som skal være sendt til alle. Den store majoritet (87%) i aldersgruppen 16 til 80 år som er på nett, sier at de har en Facebook-konto. Enda flere, nesten alle (93%) svarer at de er på Google. Resultatene viser tydelig at det bare er en liten andel av de som besøker disse to store plattformene som gjør noe aktivt for å beskytte sine persondata.

På Facebook var det bare 13 prosent som sa de hadde endret på innstillingene og reservert seg mot noe av det Facebook lagrer om dem. Ingen svarte at de hadde slettet sin konto. To prosent hadde prøvd, men ikke lykkes i, å reservere seg. Den klart største gruppen, 46 prosent, var usikre på om de har fått noen henvendelse og/eller husket ikke hvordan de hadde respondert. I tillegg var det 19 prosent som svarte at de bare hadde gitt sitt samtykke. Til slutt var det åtte prosent som mente de ikke hadde fått noen GDPR henvendelse på Facebook, som er mulig dersom de ikke har vært inne på sin konto de siste par månedene. Uansett kan vi regne med at i hvert fall to tredjedeler av de som er på Facebook ikke gjør annet enn å gi sitt samtykke, for raskest mulig komme inn på sin Facebook-vegg.

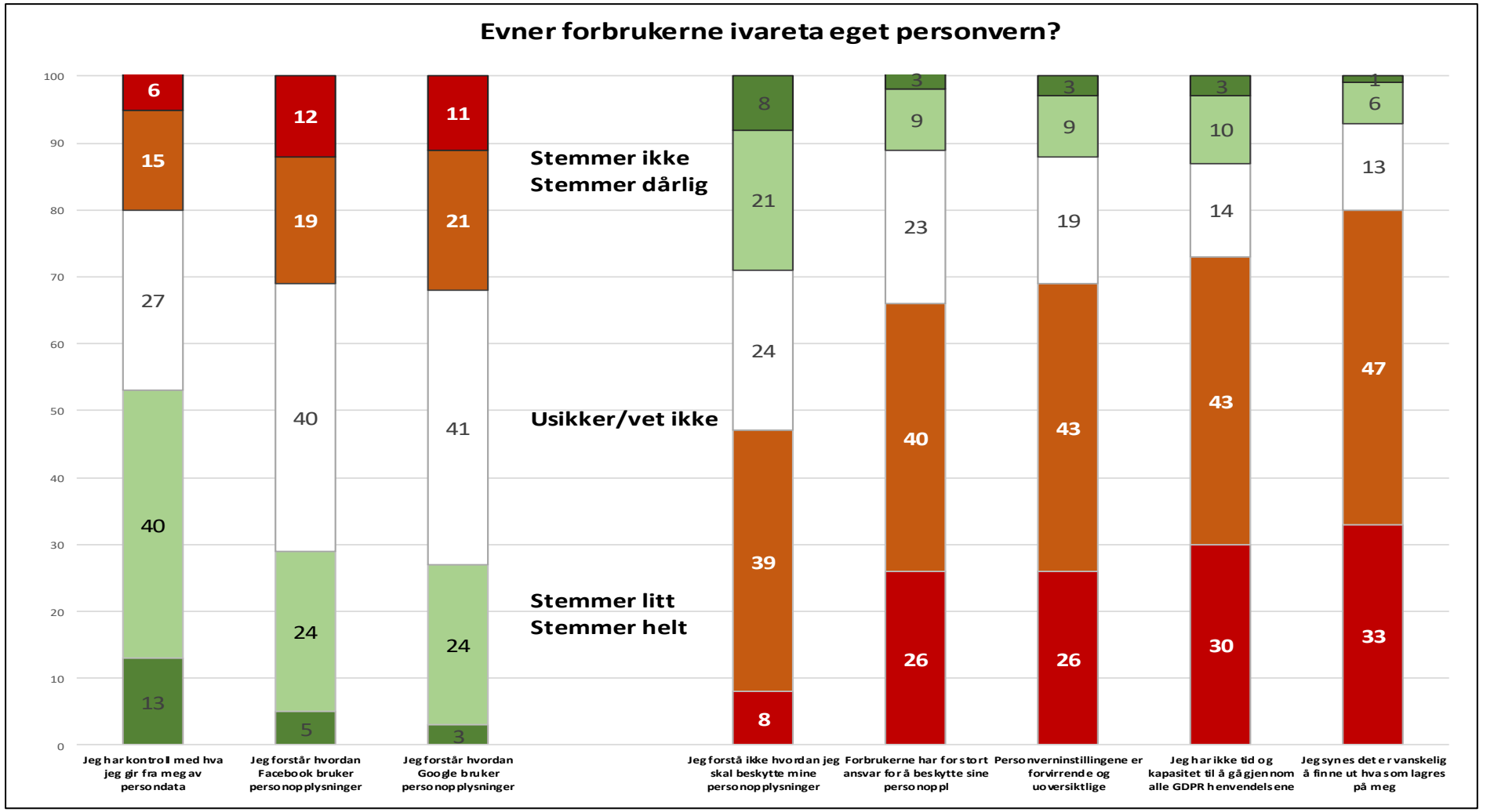
På Google er brukerne enda mindre aktive. Bare fem prosent av de som er på Google sier de har endret på innstillingene som gir Google anledning til å benytte deres persondata. To prosent hadde prøvd, men ikke lykkes. Så er det ni prosent som i hvert fall leser gjennom Googles GDPR informasjon før de samtykker til at Google kan fortsette å bruke deres data. Enda flere (55%) enn på Facebook (46%) var usikre eller husket ikke hva de gjorde når de mottok GDPR henvendelsen fra Google. I tillegg var det 14% som oppga at de bare hadde gitt Google sitt

samtykke. Femten prosent av de på Google mente de ikke hadde mottatt noen GDPR henvendelse, som er mulig hvis de ikke har vært på Google de siste par månedene. Av alle de som er på Google kan vi regne med at rundt regnet tre fjerdedeler ikke gjør annet enn å akseptere før de benytter Googles tjenester. Av Google-brukerne var de én person i vårt utvalg, altså én promille, som sa at GDPR henvendelsen gjorde at de slettet sin Google konto.

Så, fungerer GDPR etter hensikten ifølge forbrukernes rapporterte respons på Facebook og Google? Resultatene i Figur 2 er ikke spesielt betryggende eller overbevisende. Vi kan anta at rundt regnet to tredjedeler av de som er på Facebook, og tre fjerdedeler av de som er på Google, ikke en gang har lest gjennom informasjonen i forbindelse med GDPR-henvendelsen før de ga sine samtykker til at disse store nettaktørene kunne benytte deres persondata. Resultatene tyder altså på at de fleste har et ikke-refleksivt forhold til GDPR.

4.3 Er forbrukerne i stand til å bruke GDPR for å ivareta egne interesser?

I Figur 2 tok vi utgangspunkt i forbrukernes rapporterte respons. I spørreskjemaet ble respondentene også bedt om å ta stilling til ulike utsagn knyttet til hvordan de selv vurderer sin evne til å ivareta eget personvern. Noen utsagn var utformet positivt, andre negativt. I neste figur illustrerer de grønne feltene andeler som gir uttrykk for at de klarer å ivareta sitt personvern, mens de røde feltene trekker i retning av at forbrukerne ikke kan forventes å sikre håndhevelsen av GDPR. Neste figur viser med andre ord om forbrukerne – ifølge seg selv - fyller rollen som skal sørge for at GDPR fungerer etter hensikten:



Figur 3: Evner forbrukerne å ivareta eget personvern på nettet? (skala 1 – 5). Prosent. Landsrepresentativ vekt. (N=1003)

Hovedinntrykket fra Figur 3 er at det er større røde enn grønne felter, og i tillegg er mange usikre. Det er også slik at de fleste har lettere for å overvurdere, enn å undervurdere, seg selv i slike spørreundersøkelser. Dette tyder på at skepsisen er langt større enn tiltroen blant forbrukerne til at de makter å ivareta eget personvern.

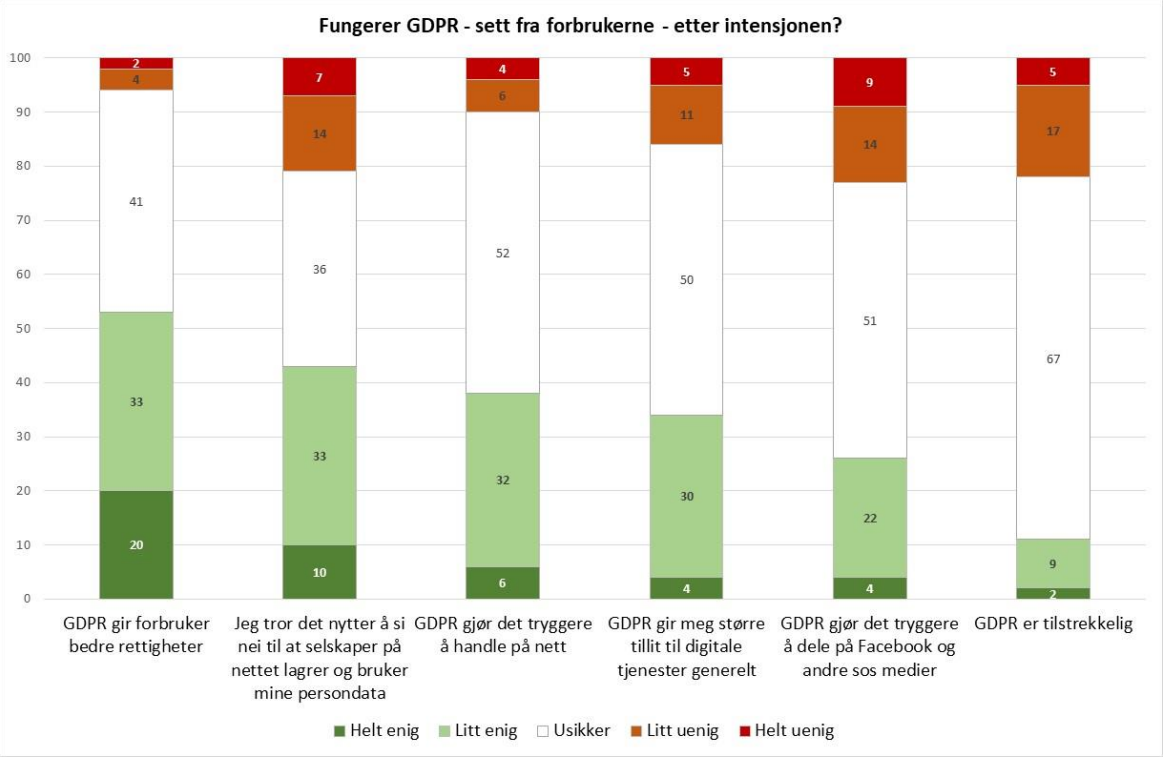
Mest optimistiske er respondentene i forholdet til egen kontroll. Men det er likevel bare litt over halvparten som sier at det 'stemmer helt' eller 'litt' at de har kontroll med hva de gir fra seg av persondata. Og samtidig viser søylen helt til høyre at 80 prosent er enige i at de synes det er vanskelig å finne ut hvilke persondata som lagres om dem. I Datatilsynets undersøkelse fra 2016 var det 70 prosent som sa at de er helt eller delvis uvitende om hva slags data som samles om dem online. Under tretti prosent svarer positivt på at de forstår hvordan henholdsvis Facebook og Google bruker deres personopplysninger. Samlet må vi tolke dette til at brukerkontrollen ikke er veldig stor.

Nesten 70 prosent mener personverninnstillingene er forvirrende og uoversiktlige. To tredjedeler (66%) sier at forbrukerne har for stort ansvar for å beskytte sine personopplysninger, kanskje fordi nesten halvparten sier de ikke forstår *hvordan* de skal beskytte sine personopplysninger, og at de fleste rett og slett ikke har tid eller kapasitet til å overvåke persondataene sine: 73 prosent sier de ikke har tid til å gå gjennom alle henvendelsene de får om de nye GDPR henvendelsene.

Resultatene i Figur 2 og 3 gir grunn til å stille seg kritisk til hvorvidt forbrukere flest klarer ivareta eget personvern. Personvern-sårbarheten ser ut til å være utbredt.

4.4 Bidrar GDPR til mer **tillit** til digitale tjenester generelt, i netthandel, på sosiale medier?

Men er da ikke GDPR til nytte sett fra forbrukerne? GDPR stiller klare krav om rutiner og opplysningsplikt knyttet til digital lagring av personopplysninger. Noe av hensikten med GDPR er å styrke forbrukermakten, bidra til større tillit, og innad i EU var det et ønske om å fremme EU's indre marked gjennom økt internetthandel. I neste figur viser vi hvordan respondentene vurderer GDPR som tiltak. Fungerer GDPR – sett fra forbrukerne – etter intensjonen om økt tillit på nett?



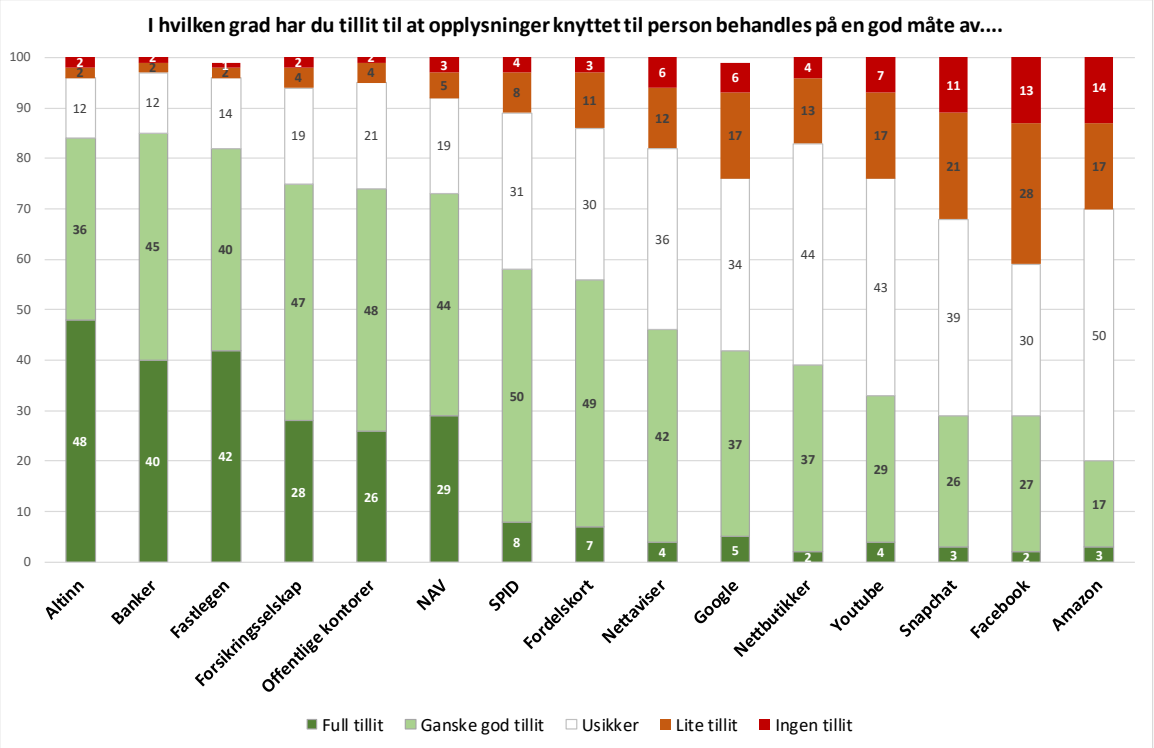
Figur 4: Hvor enig er du i følgende påstander om de nye reglene for håndtering av personopplysninger. Prosent. Landsrepresentativ vekt. (N=1003)

Hovedbildet her, er at svært mange er usikre på virkningene av GDPR. Likevel viser Figur 4 at flere er positive enn negative til effekten av GDPR. Men sjeldent mange er usikre (hvite felter). En av hensiktene med GDPR var å styrke forbrukermakten, og første kolonne i Figur 4 viser at litt over halvparten (53%) er helt eller litt enige i at GDPR gir forbrukerne bedre rettigheter. Riktig nok er ikke fullt så mange (43%) enige i at de tror det nytter å si nei til at selskaper på nettet lagrer og bruker deres persondata. Enda færre, men tross alt noen, 38 prosent, mener at GDPR gjør det tryggere å handle på nett. Og omtrent en av tre (34%) sier at GDPR gir dem større tillit til digitale tjenester generelt, og 26 prosent mener GDPR gjør det tryggere å dele på Facebook og andre sosiale medier. Men, bare en av ti mener at GDPR er *tilstrekkelig* for å sikre en god håndtering av persondata.

Enn så lenge, tolker vi resultatene i Figur 4 til at GDPR (fortsatt) bare bidrar til litt økt tillit til digitale tjenester, selv om ganske mange er enige i at GDPR bidrar til bedre forbrukerrettigheter.

4.5 Hvilke aktører anser forbrukerne som **mest risikable** – statlige, kommersielle, nasjonale, eller globale?

Det er ulike aktører som samler persondata på nett, og vi har stilt spørsmål om i hvilken grad respondentene har tillit til at femten ulike aktører, fra Facebook til fastlegen, behandler opplysninger knyttet til deres person på en tilfredsstillende måte. Er det for eksempel forskjell på tillit til private og offentlige aktører?



Figur 5: Tillit til ulike aktørers håndtering av persondata etter innføring av GDPR i aldersgruppen 16-80. Prosent. Uaktuelt = sysmis[2]. Landsrepresentativ vekt. (N varierer fra 996 (banker) til 623 (Amazon))

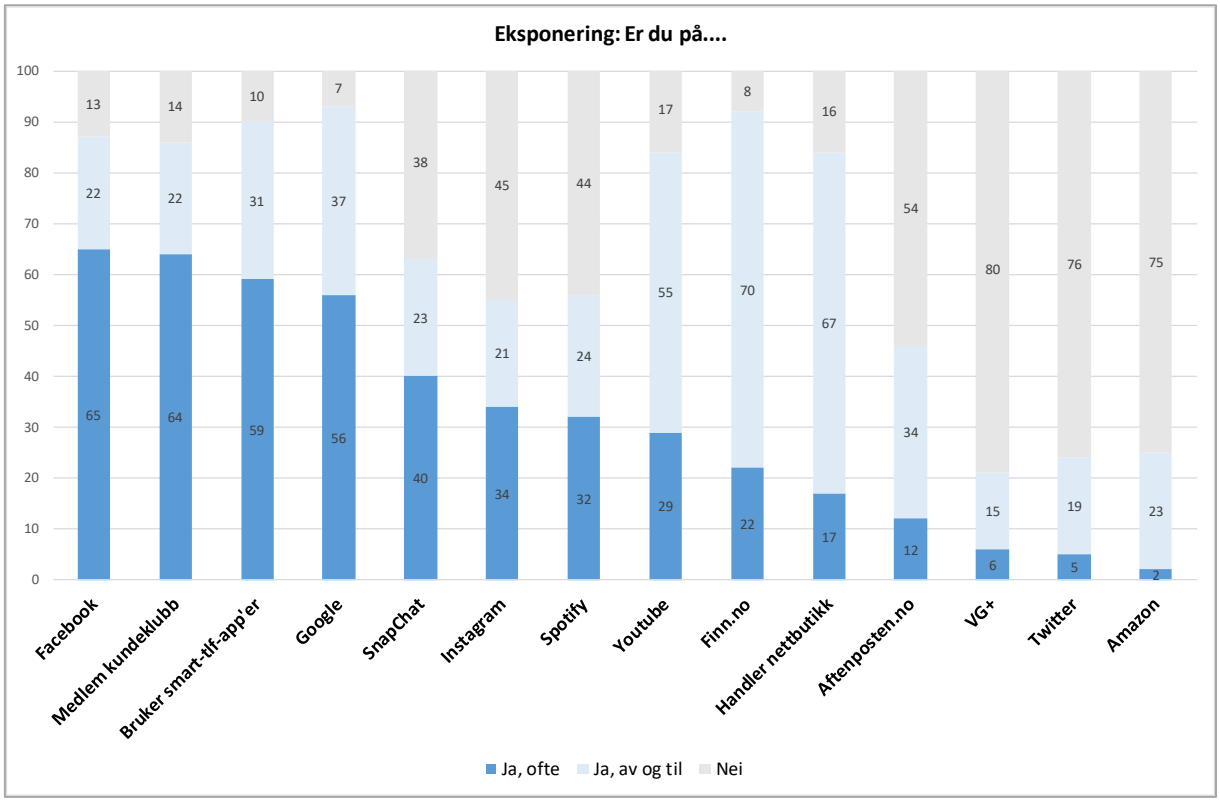
Som det framgår tydelig av figur 5, her er store forskjeller i tillit. Aller størst tillit har Altinn, den norske felles internettportalen for levering av elektroniske skjemaer til offentlige myndigheter, blant annet selvangivelsen og andre lovpålagte skjemaer. Bare fire prosent sier de har lite eller ingen tillitt, mens 84 prosent sier de har full tillit eller ganske god tillit til Altinn. Det er verd å merke seg, litt overraskende kanskje, at det er bankene som kommer som en god nummer to, faktisk et lite hakk foran fastlegen, som vi forventet ville rangere høyt. Bankene ivaretar en av våre viktigste samfunnsoppgaver, og det er derfor uhyre viktig at bankenes tillit, og enda mer deres tillitsverdighet, ligger høyt, særlig i møte med nye konkurrerende krypto-valuta-institusjoner. Det er også noe uventet at forsikringsselskapene faktisk kommer litt foran offentlige kontorer og NAV, men disse forskjellene er ikke signifikante. Så følger Schibsted-eide SPID (stor aktør innen persondata med tilgang på opplysninger fra blant annet Aftenposten, VG og Finn), der 58 prosent viser tillit, og bare 12 prosent mistillit. Butikkenes fordelskort og app'er nyter også rimelig tillit blant over halvparten av forbrukerne. For de resterende aktørene er det under halvparten som sier de har full eller ganske god tillit; nettavisene 46 prosent, Google 42 prosent tillit og 23 prosent mistillit, enda mindre tillit har nettbutikken med 39 prosent, så faller tilliten videre til 33 prosent tillit for Youtube, 29 prosent tillit for Snapchat og Facebook, og dårligst ut kommer Amazon – som nå skal etablere seg i Skandinavia – med 20 prosent. Mest mistillit tilfaller Facebook, der hele 41 prosent har lite eller ingen tillit til at Facebook behandler personopplysninger på en tilfredsstillende måte, et rimelig resultat i kjølvannet fra Cambridge Analytica skandalen.

Vi kan ikke, basert på figur 5, si at offentlige plattformer nyter større tillit enn private. Men vi kan si at det er langt flere som har tillit til at nasjonale plattformer – både offentlige og private – behandler opplysninger knyttet til person på en god måte, enn at store globale plattformer som Facebook, Google og Amazon gjør det.

[2] De som har svart 'uaktuelt' og ikke 'usikker' har som regel ikke konto, eller føler de ikke har grunnlag for å besvare spørsmålet.

4.6 Hvilke nettaktører har størst tilgang på personopplysninger?

Vi ville også undersøke hvilke aktører som i størst grad har tilgang på persondata og opplysninger knyttet til person aktiviteter på nett.



Figur 6: Hvilke aktører har best tilgang på personopplysninger? Prosent. Landsrepresentativ vekt. (N=1003)

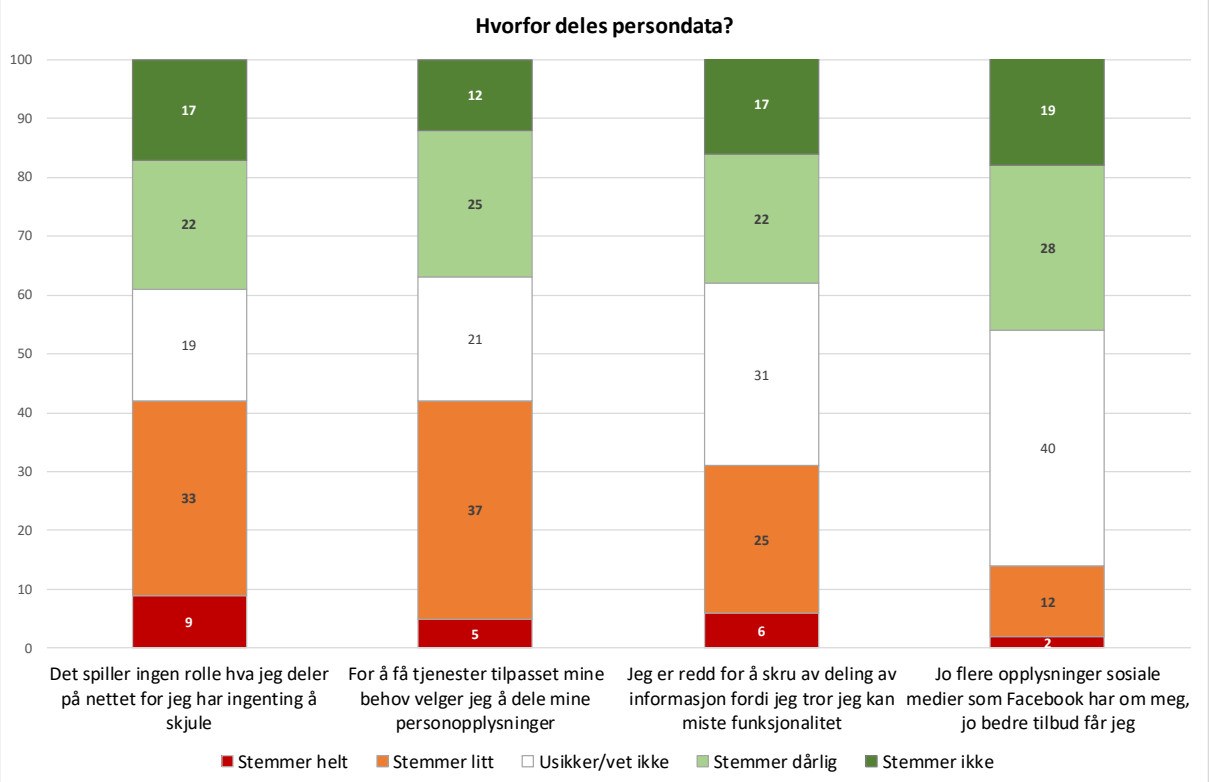
Hovedinntrykket fra Figur 6 er at mange er aktive på mange digitale kanaler som samler, bruker og kanskje videreselger persondata. Facebook, som ifølge forrige figur møter mest mistillit, er samtidig den største data-fangeren. Etter respondenters rapportereringer er Facebook, medlemskap i kundeklubber, app'er i smart-telefoner og Google de fire store data fangerne. Hvis vi rangerer etter de som svarer at de 'ofte' er på nett, følger SnapChat, Instagram og Spotify, men hvis vi rangerer etter de som er aktive 'ofte eller av og til', er det Youtube, Finn.no og nettbutikker som kommer høyt opp. Av våre nettsider er det VG+, Twitter og Amazon som rangerer lavest med bare litt over 20 prosent brukere. Vi ser også at av våre 14 digitale plattformer er minst 90 prosent av internettbefolkningen i aldersgruppen 16-80 år brukere av app'er på smarttelefonen, på google og på finn.no. I tillegg svarer over 80 prosent at de har konto på Facebook, er medlem i kundeklubber, er på Youtube og handler i nettbutikker. Det er rimelig å anta at jo mer nettaktivitet, jo mer utsatt er man for deling av persondata, og jo mer sårbar for algoritmestyrte påvirkninger. Men det er jo også mulig at de som er mye på nett, samler erfaringer og dermed er mindre utsatte for personvernsårbarhet.

4.7 Hvorfor deles personopplysninger?

Vi antar at mange, lenge, ikke har vært bevisst på at persondata de gir fra seg på nettet er en form for betaling, eller valuta, som byttes i nett-tjenester. I intervjuer med unge voksne i 2016 (Berg 2016) var bevisstheten rundt dette relativt lav. De fleste var 'på nett hele tiden' og anså seg som kompetente. De trykket rutinemessig og tillitsfullt 'enig' i at nettsteder registrerte informasjon om dem, vitende at uten å akseptere vilkårene kunne man ikke bruke produktet. Et

vanlig svar var at de ikke var engstelige for å være på nett, eller dele på nett, for de hadde uansett ingenting å skjule.

I Datatilsynets undersøkelse - *Personal data in exchange for free services: an unhappy partnership?* – svarte 76 prosent at de var klar over sammenhengen mellom nettaktivitet og reklamen de mottok på nettet. Likevel var 70 prosent usikre på hva slags data som ble samlet inn, og like mange var usikre på hvordan slike data ble utnyttet i personlig rettet reklame (Datatilsynet 2016). I intervjuene med unge voksne var også de fleste oppmerksomme på at reklamen de mottok på nett hadde sammenheng med egen nettaktivitet. Men de gikk ikke gjennom personvernerklæringene på Facebook – 'for det er jo skrevet sånn at vanlige folk ikke skal forstå det'. Og, selv om tilnærmet alle hadde Iphone, mente de stort sett at de selv var gode til å motstå reklame. Det ble påpekt at den som ville ha smart-telefon, og det vil jo alle, må finne seg i at mobiltelefonen samler personopplysninger. Du kan reservere deg mot noe, men ikke alt. Alle vil være på nett, så kampen om kontroll på egne persondata er kanskje allerede tapt? Er forbrukerne skeptiske mot å dele persondata? Deler de frivillig fordi de 'ikke har noe å skjule', eller fordi de er redd for å miste funksjonalitet og tilgang på tjenester? De røde feltene illustrer lav selvbeskyttelse, mens de grønne feltene illustrerer andeler som er mer varsomme med deling av egne data.



Figur 7: Drivere for villighet til å dele persondata. Prosent. Landsrepresentativ vekt. (N=1003)

Resultatene i figur 7 viser ikke et tydelig mønster. De røde feltene i de to første kolonnene viser andeler som deler ubekymret; Omtrent 40 prosent deler personopplysninger uten særlig bekymring, fordi de 'ikke har noe å skjule', like mange sier de 'velger å dele personopplysninger for å få tjenester tilpasset sine behov'. De grønne feltene viser at nesten like mange gir uttrykk for at de er uenige i dette. Befolkningen ser altså ut til å være delt; noen mener deling av persondata er uproblematisk, som kan gi dem fordeler på nett, mens andre er uenige i dette. Men igjen, andelene usikre er store. Mens de røde feltene i første, andre og fjerde kolonne viser til andeler som mer eller mindre ubekymret deler sine persondata, viser de røde feltene i kolonne tre til en mer uvillig, mer påtvungen, deling: Omtrent tretti prosent sier at de 'er redd for å skru av deling av informasjon fordi de tror de kan miste nett-funksjonalitet'. Men enda

flere sier dette stemmer dårlig eller ikke for dem, kanskje fordi de ikke er så opptatt av å beskytte seg mot deling av persondata. Disse variablene, som signaliserer henholdsvis ubekymret naivitet (kolonne 1) og noe uvillig, påtvungen, deling (kolonne 3), er spesielt interessant å undersøke i forhold til hvilke grupper som er spesielt sårbare.

Figur 7 viser også, noe overraskende, at det bare var 14 prosent som tror på nett-aktørenes forklaringer og forsikringer om at de vil få en mye bedre tjeneste dersom de gir fra seg persondata til for eksempel Facebook.

4.8 Er spesielle grupper mer sårbare enn andre?

For å få et mer samlende bilde av *tillit og sårbarhet på nett* har vi konstruert to indekser som skal inngå som avhengige variable i multivariate analyser; *Personvern-sårbarhet* og *GDPR gir økt tillit på nett*. Den analytiske modellen og konstruering av indeksene er beskrevet nærmere i Metodekapittelet.

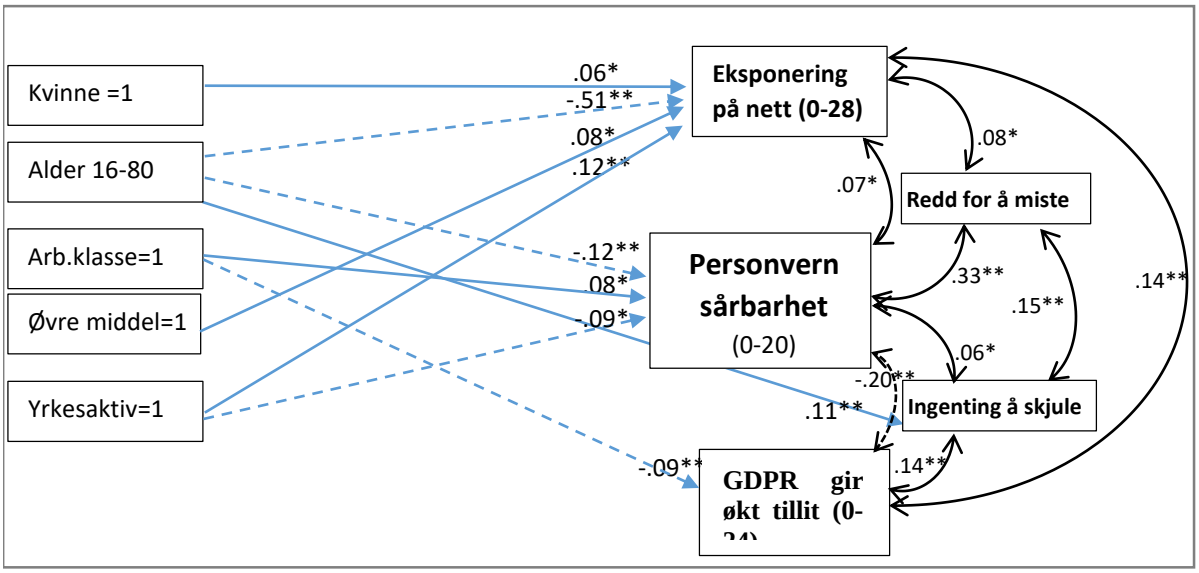
Hensikten med forklaringsvariablene er at de i de etterfølgende multivariate modellene skal kunne bidra til å forklare eventuelt *hvorfor* enkelte grupper er mer utsatt for personvernsårbarhet og/eller har mindre tillit til GDPR enn andre.

Grunnen til at vi har med *eksponering på nett* som forklaringvariabel er at vi tror den kan bidra til både personvern-sårbarhet og økt erfaring som kan gi (selv)tillit og tro på GDPR. Vi inkluderer også to forklaringsvariable som vi antar kan bidra til økt deling av person- og forbrukerdata på nett: For det første at man mener at det ikke er så farlig å dele på nettet fordi man ikke har noe å skule (*Ingenting å skjule*) og for det andre at man er engstelig for å miste nett-funksjonalitet hvis man nekter å gi fra seg informasjon (*Redd for å miste*).

Innledningsvis viser vi et oversiktsbilde der vi først og fremst ønsker undersøke hvorvidt kjønn, alder, selvrapportert klassebakgrunn, og hvorvidt man er i inntektsgivende arbeid eller ikke (uavhengige variable), har signifikante effekter på både de avhengige og de mellomliggende forklaringsvariablene. Hensikten er altså å undersøke betydningen av f.eks. kjønn på både sårbarhet, tillit, eksponering, samt data-delings-triggerne 'ingenting å skjule' og 'redd for å miste'. Vi undersøker samtidig de bivariate sammenhengene mellom de fem avhengige og mellomliggende variablene.

Figur 8 viser fem multivariate analyser[3] med signifikante effekter fra kjønn, alder, klasse og yrkesaktivitet på fem avhengige variable (blå piler til venstre), og i tillegg presenteres bivariate korrelasjoner mellom disse (svarte piler til høyre). Vi viser kun de signifikante effektene/korrelasjonene. Der det ikke går piler er det med andre ord ikke signifikante effekter/korrelasjoner. Stiplet linje illustrerer negative effekter, mens heltrukken linje illustrerer positive effekter.

[3] Multivariat analyse viser hvilke variable som har selvstendig effekt på den avhengige variabelen, når de andre uavhengige variablene holdes konstant. De standardiserte regresjonskoeffisientene (beta) kan tolkes som korrelasjonskoeffisienter mellom uavhengig og avhengig variabel når vi kontrollerer for de andre uavhengige variablene. Beta varierer mellom -1 og 1. I figur 8 viser vi også korrelasjonene (som tilsvarer beta-koeffisienten i en regresjonsanalyse med kun én uavhengig variabel) mellom de fem avhengige variablene.



Figur 8: Hvem er eksponert på nett? Hvem er sårbare i forhold til personvern? Hvem har troen på at GDPR gir økt tillit på nett? Hvem deler fordi de er redd for å miste funksjonalitet og hvem deler på nett fordi de mener at de ikke har noe å skjule? Signifikante standardiserte regresjonskoeffisienter (beta). Fem lineære regresjoner (r^2=.30, .00, .02, .01, .01) samt bivariate korrelasjoner mellom de avhengige variablene. (N=1003)

Vi ser umiddelbart at *ingen* av de uavhengige variablene har effekt på 'Redd for å miste'. Det er altså ikke slik at noen grupper i større eller mindre grad enn andre gir uttrykk for at de føler seg presset til å dele opplysninger om seg selv på nettet. Kun alder har effekt på 'Ingenting å skjule'. Og det er også bare alder som har effekt på 'GDPR gir økt tillit'. Den følgende sti-analysen vil imidlertid vise at disse variablene likevel fortjener oppmerksomhet.

Alder

Hovedfunnet i de innledende multivariate analysene tyder på at det først og fremst er de unge som er utsatte i forhold til personvern på nett. Aldersvariabelen slår ekstremt kraftig ut i forhold til hvor eksponert man er for datafangst på nett (-51**). De unge skårer også signifikant høyere enn de eldre, alt annet likt, på egen vurdering av personvern-sårbarhet (-.12**), men vi hadde trodd at denne effekten skulle vært høyere. Den bivariate sammenhengen (Figur 8) mellom grad av eksponering og personvern-sårbarhet (ut fra respondentenes selvrapporteringer) er signifikant, men svak (.07*). Og effekten blir helt borte når eksponeringsvariabelen trekkes inn i analysen som forklaringsvariabel (Figur 9). Man kan tenke seg to motsatte effekter knyttet til eksponering på nett; på den ene siden at de som er mye på nett er mer eksponert for kommersiell datafangst og dermed blir mer sårbare, på den andre siden at de som er mye på nett får mer erfaring og blir flinkere til å forsvare sine persondata. Dette kan bety at de to mekanismene, som trekker i hver sin retning, i noen grad oppveier hverandre. Men vi minner om at indeksen som skal måle personvern-sårbarhet er basert på respondentenes selvrapporteringer, og er på ingen måte et objektivt mål. Indeksen måler i prinsippet bare hvordan den enkelte føler de behersker eget personvern. Og vi skal ikke se bort fra at mange kan overvurdere egne evner.

Analysen viser også at det er de eldre, og ikke de yngre, som i størst grad deler ubekymret på nett fordi de mener at de ikke har noe å skjule. På bakgrunn av intervjuer med unge voksne i 2016 antok vi at dette var mest utbredt blant de yngste, men resultatene i Figur 8 viser altså at det i dag faktisk er motsatt. Men, naturligvis, de eldre er også sjeldnere enn de unge på nettet, og har dermed mindre grunn til å være bekymret. Det er også godt mulig at yngre og eldre deler ulike ting (transaksjonshistorikk/personopplysninger/egne tekster, bilder og videoer). Det har vært en god del media-oppmerksomhet rundt unges uheldige delinger av kompromitterende bilder, i tillegg til Cambridge Analytica-skandalen, hendinger som kan ha bidratt til økt nett-refleksivitet blant de unge.

Kjønn

Kjønn betyr forbausende lite. I følge vår analyse er kvinner litt mer eksponert – det vil si at de er aktive på litt flere nettsteder - enn menn (.06*). Men effekten er svak og nesten ubetydelig. Og av våre bakgrunnsvariable er det kun kjønn som *ikke* har egen effekt på personvernsårbarhet. Følelse av mestring, praksiser, holdninger og tillit, i forhold til GDPR, ser altså ikke ut til å være kjønnet.

Klassebakgrunn

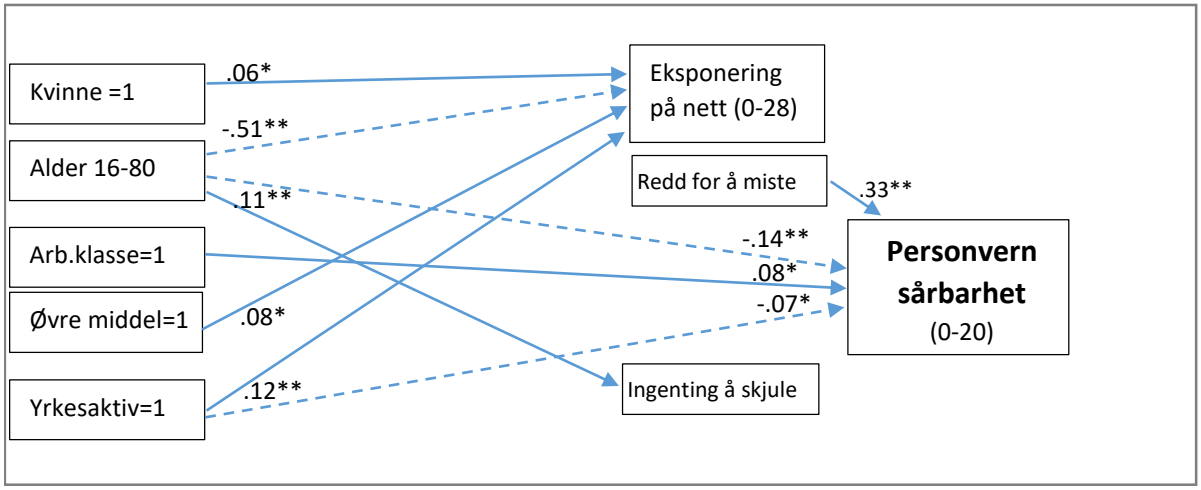
I og med at både utdannings- og inntektsnivå har svært stor sammenheng med alder, spesielt når utvalget strekker seg fra 16 til 80 år, har vi valgt å bruke selverklært klassebakgrunn som statusvariabel (i analysen sammenlignes arbeiderklasse og øvre middelklasse med middelklasse=0). Resultatene viser at de som assosierer seg med øvre middelklasse rapporterer høyere grad av eksponering på nett (.08*) enn middelklassen og arbeiderklassen. De som sier at de tilhører arbeiderklassen gir noe større uttrykk for personvern-sårbarhet (.08*) og de er litt mer skeptiske til GDPR (-.09**) enn de som sier de tilhører middelklassen og øvre middelklasse, alt annet likt.

Yrkesaktivitet

I vårt responderende utvalg oppgir 58 prosent at de er yrkesaktive (49% heltid, 9% deltid). Denne gruppen er ikke uventet mer eksponert på nett (.12**), de er dermed mer rutinerte og opplever sjeldnere enn andre, alt annet likt, at de ikke mestrer håndtering av sitt personvern på nett (-.09**).

4.9 Hva påvirker personvern-sårbarhet

I neste figur skal vi trekke inn forklaringsvariablene for å undersøke om dette kan øke modellens forklarte varians. Er det endringer i resultatene fra Figur 8, som viste relativt svake effekter av alder (-.12**) klasse (.08*) og yrkesaktivitet (-.09*) på respondentenes følelse av å mestre håndtering av sitt personvern på nett (personvern-sårbarhet), og kjønn hadde ingen effekt.



Figur 9. Hvem er mest sårbar i forhold til personvern på nett. Fem lineære regresjoner (r^2=.30, .00, .13, .02). Beta-koeffisienter. (N=1003)

Sti-analysen[4] i Figur 9, der forklaringsvariablene trekkes inn, viser – helt uventet - at grad av eksponering på nett ikke har signifikant effekt på personvern-sårbarhet. Muligens kan det her

[4] I en sti-analyse trekkes det inn ett eller flere sett med mellomliggende variable, eller forklaringsvariable. I vårt tilfelle kan vi f.eks. skille mellom direkte effekt fra f.eks. alder på personvernsårbarhet og eventuelle indirekte effekter fra alder gjennom forklaringsvariablene på personvernsårbarhet. Det helt uvanlige med resultatene i figur 9,

skjule seg en overvurdering av egen nettkapabilitet blant unge som er mye på nett. Heller ikke det vi har sett som et uttrykk for naiv, ubekymret deling (ingenting å skjule), har effekt på selverklært personvern-sårbarhet. Det som har effekt, og sterk effekt, er det vi har sett som mer tvangsmessig deling; mer presist de som er redde for å skru av deling av informasjon fordi de tror de kan miste nett-funksjonalitet (.33**). Men som vi ser; verken kjønn, alder, klasse eller yrkesaktivitet har effekt på denne variabelen. Å trekke inn forklaringsvariablene gir altså ingen hjelp i å peke ut sårbare grupper. Eller til å forklare *hvorfor* noen grupper har økt sannsynlighet for personvernsårbarhet enn andre.

Vi skal ikke se bort fra at de som er 'Redd for å miste' funksjonalitet faktisk har rett: Altså at det å skru av deling av informasjon faktisk gir dårligere funksjonalitet, eller at man mister tilgang til tjenesten/app'en. Det mange av oss trodde var gratis tjenester på nettet, er i så fall ikke gratis, valutaen er ikke penger, men personopplysninger.

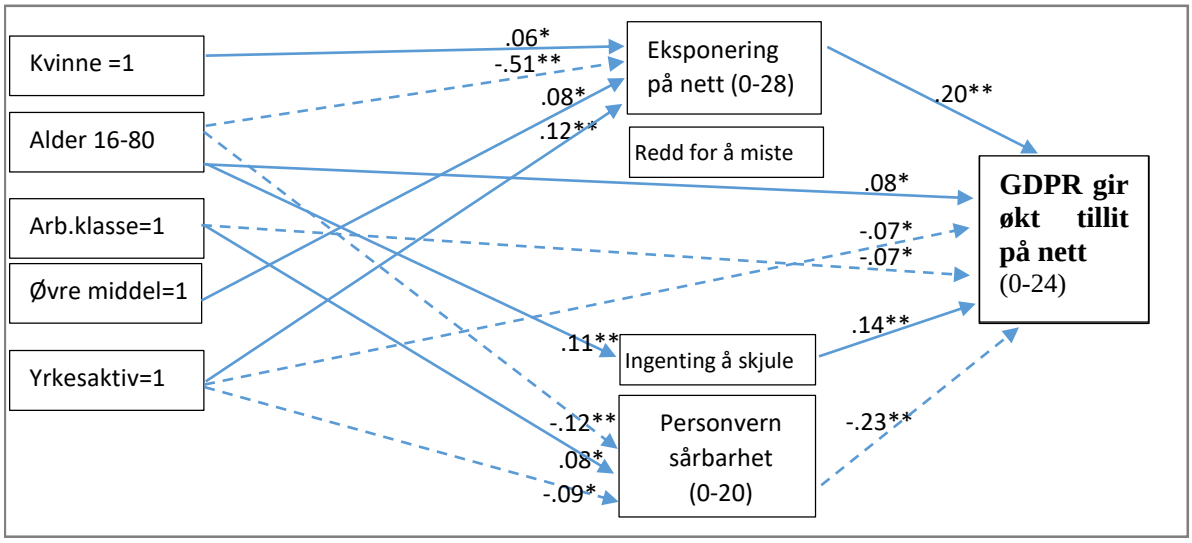
Metodisk oppsummert: Regresjonsmodellenes forklarte varians (r^2) øker fra .02 (nesten ingenting) til .13 når forklaringsvariablene – eller helt presist 'Redd for å miste' - inkluderes i modellen. Det at ingen av bakgrunnsvariablene hadde effekt på den svært sterke driveren 'Redd for å miste', kan være uttrykk for at det er en generell, usystematisk usikkerhet knyttet til personvern og GDPR i alle grupper – riktignok litt mer usikkerhet blant de yngre og de fra arbeiderklassen og de som ikke er i inntektsgivende arbeid, alt annet likt. Videre at det kanskje er de som har gjennomskuet mekanismen – men fortsetter å dele fordi de antar at de vil miste funksjonalitet hvis de ikke betaler med personopplysninger - som oftest føler seg sårbare i forhold til kontroll med hva de gir fra seg (.33**).

Vi har sett at alder har sjeldent sterk effekt (.51**) på hvor eksponert man er på nett, men at grad av eksponering – uventet – ikke hadde selvstendig effekt på selvopplevd personvernsårbarhet. Kanskje fordi det her knytter seg to mekanismer som trekker i ulik retning: De mest eksponerte er på den ene siden mest utsatte for datafangst, men på den andre siden har de mest netterfaring og opplever dermed kanskje at de er flinkere til å beskytte seg? Eller er dette resultatet kort og godt uttrykk for at de unge overvurderer egen nettkapabilitet?

4.10 Hvordan kan GDPR bidra til større tillit på nett?

I Figur 8 så vi at av de uavhengige variablene var det kun klasse som hadde effekt på hvordan GDPR ble vurdert: De som sier de tilhører arbeiderklassen har mindre tro på at GDPR gir større trygghet på nett enn middelklassen (-.09*), alt annet likt. I neste figur trekker vi inn forklaringsvariablene Eksponering på nett, Redd for å miste, Ingenting å skjule og Personvernsårbarhet:

er at vi ikke finner noen indirekte effekter, heller ikke fra alder. Rekkefølgen på variablene i en sti-analyse må følge tidslinjen.



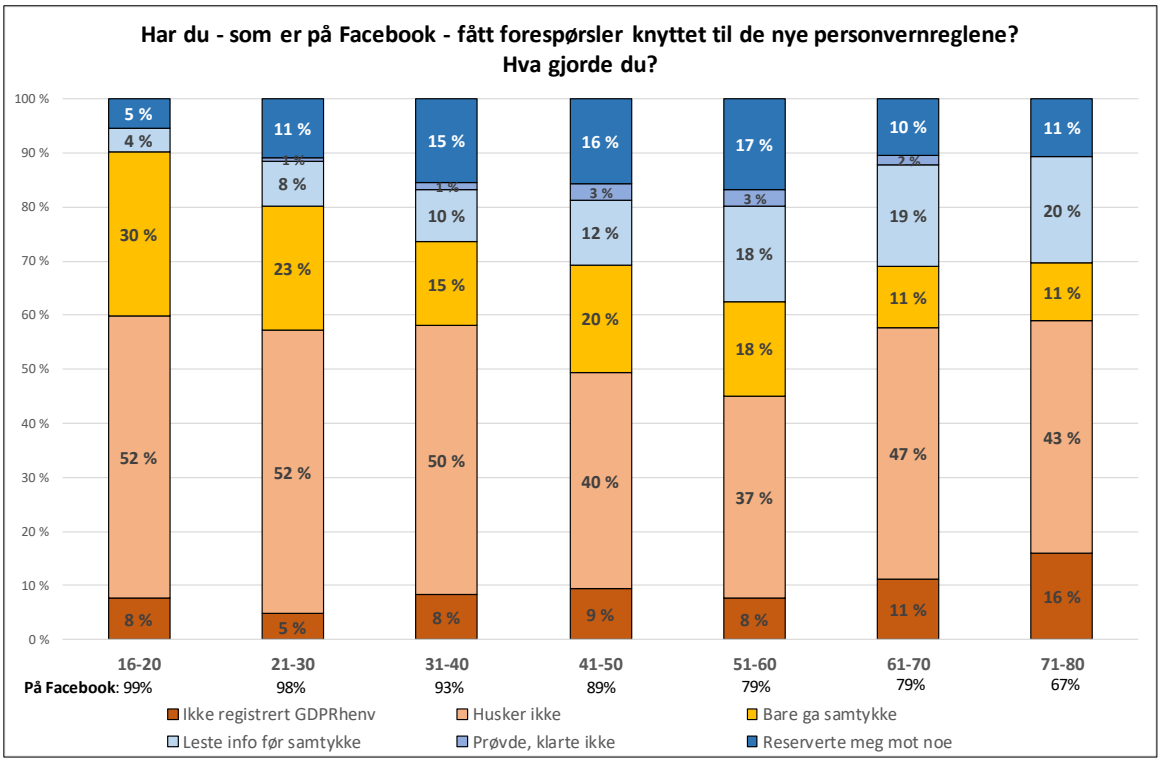
Figur 10: Hvem mener GDPR fungerer etter intensjonen og gir økt tillit på nett. Fem lineære regresjoner (r^2=.30, .00, .10, .01, .02). Beta-koeffisienter. (N=1003)

Også når vi undersøker hvilke grupper som mener GDPR gir økt tillit på nett, viser regresjonsmodellenes forklarte varians (som øker fra r^2=.01 til r^2=.10 når forklaringsvariablene inkluderes i modellen) at det først og fremst er forklaringsvariablene, og ikke de uavhengige variablene kjønn (0+(.06*.20)=.03), alder (.08*+ (-.51*.20)+(.11*.14)+(-.12*-.23)=.02), klasse (-.07*+(.08*-.23)=-.05) og yrkesaktivitet (-.07*+(.12*.20)+(-.09-.23)=-.04) som betyr noe for hvorvidt respondentene har tro på GDPR.

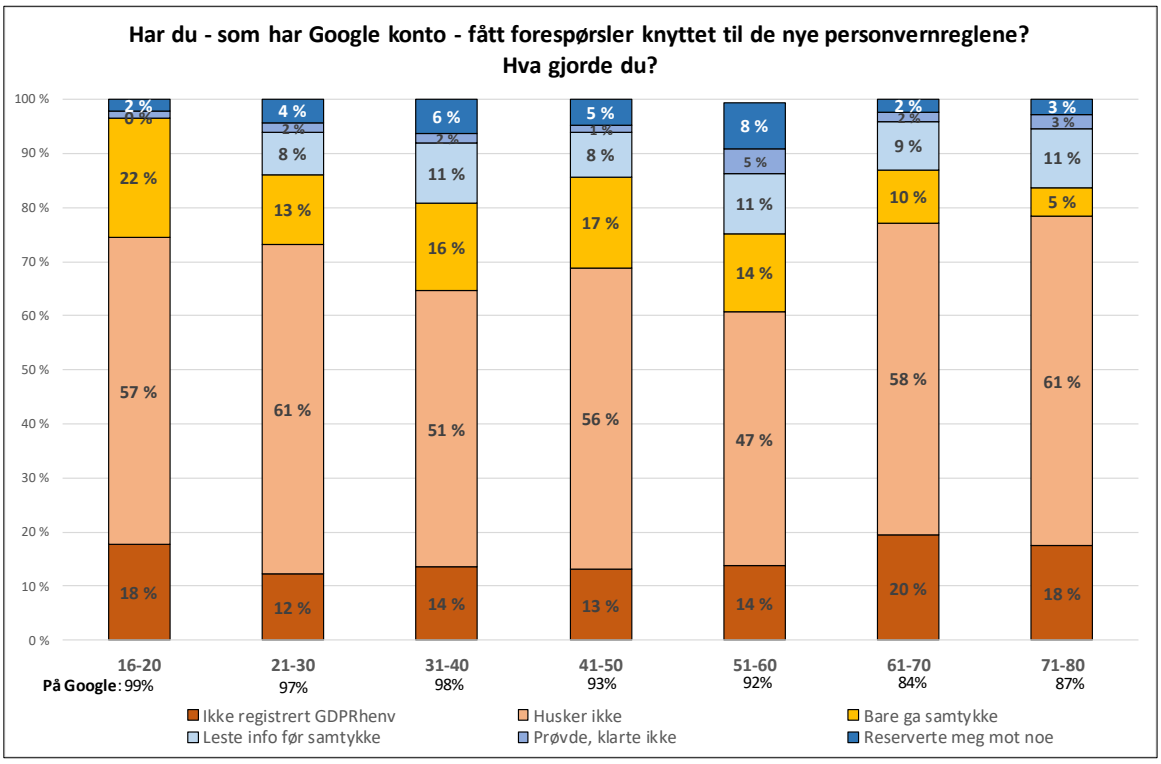
Troen på GDPR avhenger særlig av personvernsårbarhet, eksponering på nett og hvorvidt man mener å ha noe å skjule, en slags naivitets-proxy. Jo, mer eksponert på nett, jo større tro på GDPR (.20**). Og, jo mindre følelse av kontroll med eget personvern, jo mindre (-.23**) tillit har forbrukerne til GDPR løser personvernproblemet på nett. De som mener at de ikke har noe å skjule, og derfor kan dele ubekymret på nett, har samtidig noe større tro på GDPR (.14**), enn de som er uenige i dette utsagnet, alt annet likt. Hovedinntrykket – basert på Figur 8 & 10 er at verken kjønn, alder, klasse eller yrkesaktivitet har særlig betydning i seg selv for vurderingen av hvordan de nye personvernreglene fungerer.

4.11 Alder og respons på GDPR

I den foregående multivariate analysen var det alder som gjorde størst utslag. Spesielt hadde alder stor betydning for på grad av eksponering, langt mindre på selvopplevd personvernsårbarhet. I de to neste figurene går vi litt videre, og undersøker om ulike aldersgrupper har ulik praksis til hvordan de har respondert på GDPR henvendelsene (fra Figur 2).



Figur 11: Hvordan ulike aldersgrupper responderer på forespørsler knyttet til personvernreglene (GDPR) på Facebook (sig.). Prosent. Landsrepresentativ vekt. (N=1001)**



Figur 12: Hvordan ulike aldersgrupper responderer på forespørsler knyttet til personvernreglene (GDPR) på Google. Prosent. Landsrepresentativ vekt. (N=1001)

Figur 11 og 12 gir et tydelig hint om at de yngste aldersgruppene er spesielt lite aktive i forhold til de nye GDPR henvendelsene. Aldersgruppen 16 til 20 år er gruppen som oftest har konto på både Facebook og Google. Samtidig er dette aldersgruppen som helt klart har lettest for å trykke på samtykke erklæringer, uten å lese gjennom informasjon fra plattformen. Mye tyder på at

denne gruppen, som er svært eksponert på nettet, gir sine samtykker rutinemessig, nærmest uten at de legger merke til det.

Det er med andre ord grunn til å tro at den manglende alderseffekten gjennom eksponering skyldes subjektiv underrapportering av personvernsårbarhet blant yngre respondenter. Med andre ord er gir den samlede analysen grunn til å anta at de yngste forbrukerne er mest sårbare i forhold til deling av informasjon, person- og forbrukerdata på nettet. Og dette forsterkes kanskje av at de ofte ikke selv er klar over egen personvern-sårbarhet.

5 Oppsummering og konklusjoner

Etter vår vurdering representerer GDPR er stort framskritt når det gjelder å styrke forbrukerens innflytelse og myndighet over hvordan persondata distribueres og håndteres på internett. De som behandler persondata må forholde seg til langt flere regler og restriksjoner enn tidligere, og forbrukerens eiendomsrett til egne personopplysninger gis et rettsvern. Brudd på GDPR kan medføre svært omfattende bøter for de som behandler persondata. Ved hjelp av samtykke kan forbrukeren kontrollere om, og hvorledes, egne persondata kan deles av nettjenestene. Samtidig hviler det et stort ansvar på forbrukeren når det gjelder å forstå hva de nye reglene innebærer, hvordan persondata benyttes, og hvordan de selv kan regulere hvordan nettaktører bruker og distribuerer deres personopplysninger.
I denne rapporten har vi sett nærmere på hvordan forbrukere har agert i forbindelse med innføringen av GDPR i Norge. Rapporten baserer seg på en spørreskjemaundersøkelse blant litt over 1000 respondenter i alderen 16-80 år.
Vi har reist fem hovedspørsmål. Det første lyder:

- *Er de nye personvernreglene - GDPR - kjent blant folk?*

Ja, folk har hørt om GDPR, men nei, men mange er dårlig informert om hva GDPR innebærer. Selv om de aller fleste har fått med seg – og erfart - at det er kommet nye personvernregler for plattformer og nettaktører, er det bare 9 prosent som svarer at de 'vet godt' hva de nye reglene for håndtering av personopplysninger innebærer, 47 prosent svarer at de 'vet litt'.

- *Fungerer samtykke-erklæringene etter intensjonen (dvs som personvern-beskyttelse)?*

På et generelt spørsmål var det 40 prosent som sa de hadde gjort noe aktivt for å beskytte persondata og andre opplysninger knyttet til deres person. På spørsmål knyttet direkte til bruken av Facebook (87% hadde Facebook-konto), var det bare 13 prosent som sa de hadde endret på innstillingene og reservert seg mot noe av det Facebook lagrer om dem. Ingen svarte at de hadde slettet kontoen sin. To prosent hadde prøvd, men ikke lykkes i, å reservere seg. Den klart største gruppen, 46 prosent, var usikre på om de hadde fått noen henvendelse og/eller husket ikke hvordan de hadde respondert. I tillegg var det 19 prosent som svarte at de bare hadde gitt sitt samtykke. Vi kan altså regne med at i hvert fall to tredjedeler av de som er på Facebook ikke gjør annet enn å gi sitt samtykke, uten å se hva de samtykker til, for raskest mulig komme inn på sin Facebook-vegg.

På Google er bildet enda mer nedslående. Bare fem prosent av de som er på Google (93% er på Google) sier de har endret på innstillingene som gir Google anledning til å benytte deres persondata.
Det er mye som tyder på at henvendelsene om samtykke etter innføring av GDPR er blitt så hyppige at det etter hvert blir en refleks å tillate slik lagring.

- *Er forbrukerne i stand til å bruke GDPR for å ivareta egne interesser?*

Det er langt mer skepsis, enn tiltro, til at folk makter å ivareta eget personvern på nett. Hele 80 prosent er enige i at de synes det er vanskelig å finne ut hvilke persondata som lagres om

dem. Nesten 70 prosent mener personverninnstillingene er forvirrende og uoversiktlige. To tredjedeler (66%) sier at forbrukerne har for stort ansvar for å beskytte sine personopplysninger, kanskje fordi nesten halvparten sier de ikke forstår *hvordan* de skal beskytte sine personopplysninger. Og 73 prosent sier de ikke har tid til å gå gjennom alle henvendelsene de får om de nye GDPR reglene. Samlet må vi tolke dette til at følelsen av bruker-kontroll ikke er veldig stor, altså at personvern-sårbarheten er betydelig.

- *Bidrar GDPR til mer **tillit** til digitale tjenester generelt, i netthandel, på sosiale medier? Og; Hvilke aktører anser forbrukerne som **mest risikable** – statlige, kommersielle, nasjonale, globale?*

En av hensiktene med GDPR var å styrke forbrukermakten, og resultatene viser at litt over halvparten (53%) er helt eller litt enige i at GDPR gir forbrukerne bedre rettigheter. Riktignok er ikke fullt så mange (43%) enige i at de tror det nytter å si nei til at selskaper på nettet lagrer og bruker deres persondata. Enda færre, men tross alt noen, 38 prosent, mener at GDPR gjør det tryggere å handle på nett. Og omtrent en av tre (34%) sier at GDPR gir dem større tillit til digitale tjenester generelt, og 26 prosent mener GDPR gjør det tryggere å dele på Facebook og andre sosiale medier. Men, bare en av ti mener at GDPR er *tilstrekkelig* for å sikre en god håndtering av persondata. Hovedbildet er at svært mange er usikre på virkningene av GDPR.

Det er store forskjeller i tillit til ulike plattformer. Vi kan ikke si at offentlige plattformer nyter større tillit enn private. Men vi kan si at det er langt flere som har tillit til at nasjonale plattformer – både offentlige og private – behandler opplysninger knyttet til person og forbrukertransaksjoner på en god måte, enn at store globale plattformer som Facebook, Google og Amazon gjør det.

Størst tillit har Altinn, den norske felles internettportalen for levering av elektroniske skjemaer til offentlige myndigheter, blant annet selvangivelsen og andre lovpålagte skjemaer. Hele 84 prosent sier de har full tillit eller ganske god tillit til Altinn. Det er verd å merke seg, litt overraskende kanskje, at det er bankene som kommer som en god nummer to, faktisk et lite hakk foran fastlegen, som vi forventet ville rangere høyt. Mest mistillit tilfaller Facebook, Snapchat og Amazon.

- *Er det grupper som er spesielt sårbare i forhold til personvern på nett?*

Personvern-sårbarhet-indeksen måler en subjektiv følelse basert på hvordan den enkelte opplever at de ivaretar eget personvern på nett. Vi finner en generell, usystematisk usikkerhet knyttet til personvern og GDPR i alle grupper – riktignok litt mer usikkerhet blant de yngre, de fra arbeiderklassen og de som ikke er i inntektsgivende arbeid, alt annet likt. Men det er først og fremst egen praksis på nett som har stor forklaringskraft på følelsen av personvern-sårbarhet. Særlig er det mange er redde for å skru av deling av informasjon fordi de tror de kan miste nettfunksjonalitet, noe som øker følelsen av sårbarhet i forhold til personvern på nett.

Hovedfunnet i analysen tyder likevel på at de unge er svært utsatte i forhold til personvern på nett. Aldersvariabelen slår ekstremt kraftig ut i forhold til hvor eksponert man er for datafangst på nett. Men – helt uventet – gir eksponering ingen effekt på følelsen av personvern-sårbarhet. Det er god grunn til å tro at den manglende alderseffekten gjennom eksponering skyldes underrapportering av personvernsårbarhet blant yngre respondenter. Vi finner nemlig at det særlig er aldersgruppene 16 til 20 år, aldersgruppene som oftest har konto på Facebook og Google, som helt klart har lettest for å trykke på samtykkeerklæringer, uten å lese gjennom informasjon fra plattformen.

På bakgrunn av disse resultatene stiller vi spørsmål om forbrukerne i tilstrekkelig grad er i stand til å vurdere og å agere fornuftig i henhold til det som er intensjonen i det nye personvernregulativet. Kunnskapen om GDPR er fortsatt mangelfull, og for de store nettjenestene

som Google og Facebook er det bare et lite mindretall som har forsøkt å regulere bruken av egne personopplysninger. Vi finner derfor at mange forbrukere – på tross av GDPR – vurderer sin egen situasjon som sårbar, og at de i mindre grad har tatt forholdsregler ved å beskytte persondata på nettjenester. Prosesser knyttet til digitalisering av vårt hverdagsliv har skjedd i stor skala på svært kort tid. Det kan således være en forklaring på at mange i vår undersøkelse svarte «vet ikke» på en rekke av spørsmålene knyttet til nettjenester, og spørsmål om egen situasjon. Det tar tid å utvikle erfaringsbasert kunnskap og 'nettvett'. Samtidig burde dette resultatet være en spore til oppmerksomhet fra myndigheter og forbrukerinstitusjonene i tiden som kommer. En særlig oppmerksomhet bør rettes mot de unges nettbruk.

6 Referanser

Berg, L. & Gornitzka, Å. (2012): The Consumer Attention Deficit Syndrome: Consumer choices in complex markets. *Acta Sociologica* **55(2)**, 159-178.

Berg (2016): *Hvordan mestrer de unge forbrukerrollen*? En fortelling basert på fjorten informanters vurderinger og funderinger. Oppdragsrapport 2-2016, SIFO-Hioa, Oslo.

Berg, L. & Slettemeås, D. (2017) App'ifisering av dagligvaremarkedet. I Lavik & Borgeraas (red) *Forbrukstrender 2017*. Prosjektnotat 8-2017.

Datatilsynet (2016): Personal data in exchange for free services: an unhappy partnership? https://www.datatilsynet.no/globalassets/global/english/privacy-trends-2016.pdf

Dulsrud, A & Alfnes, F (2018) Når stordata blir Big Business. SIFO rapport, OsloMet.

Slettemeås, D. (2018). «Big Data og tingenes internett – om den tilkoblede forbruker» i *Markedsføring og forbrukerne – samfunnsvitenskapelige blikk* (red Storm Mathisen, A, Jacobsen, E og Helle Valle, J) Universitetsforlaget, Oslo.

Veberg, A. (2018) Brukerdata på avveie skremmer ikke folk vekk fra Facebook. *Aftenposten* 10.07.2018.

7 Vedlegg

7.1 Spørreskjema

Intro:

Problemstillinger (fargene viser til hvilke spørsmål som besvarer de ulike problemstillingene):

A) Er GDPR kjent blant folk?

B) Fungerer samtykke-erklæringene etter intensjonen (dvs som personvern-beskyttelse)?

C) Bidrar GDPR til mer **tillit** til digitale tjenester generelt, i netthandel, på sosiale medier? Og; Hvilke aktører anser forbrukerne som **mest risikable** – statlige, kommersielle, nasjonale, globale

D) Er forbrukerne i stand til å bruke GDPR for å ivareta egen interesse? Er forbrukene seg oppgaven bevisst?

E) Hvor sårbare er ulike grupper målt etter eksponering/praksis/refleksivitet?

Intro: I denne undersøkelsen vil vi samle kunnskap om hvordan vanlige forbrukere forholder seg til ***de nye europeiske reglene for håndtering av personopplysninger GDPR (General Data Protection Regulation)***.

A1
Har du hørt om de nye reglene for håndtering av personopplysninger (GDPR)?
0 **Nei, har ikke hørt om** det før nå
1 **Ja**

A2
Vet du hva de nye personvernreglene innebærer?
0 **Nei**
1 Usikker
2 **Vet noe** om hva det innebærer
3 **Vet godt** hva de nye reglene for håndtering av personopplysninger innebærer

B1
Har du – pga de nye personvernreglene - **fått forespørsel om å gi samtykke til** at sosiale medier, kommersielle selskaper eller andre kan lagre og bruke opplysninger om deg?
0 **Nei**
1 Usikker
2 Ja

B3
Har du sjekket hva slags persondata sosiale medier, kommersielle selskaper eller andre **ber om tillatelse til å registrere** om deg?
0 Nei
1 Usikker
2 Ja, men i liten grad
3 Ja, i noen grad
4 Ja, som regel
5, Ja, alltid

B2
Har du **gjort noe aktivt** for å beskytte dine persondata og andre opplysninger knyttet til din person?
0 **Nei**
1 Usikker
2 **Ja, jeg har gått aktivt inn og endret på hva en avsender skal få registrere på meg**
3 Ja, jeg har slettet min profil hos nettaktør/tilbydere
9 Ikke aktuelt

Alle:

	Nei	Ja, det hender	Ja, ofte
Benytter du fordelskort/medlemskap i matvarehandelen's kundeklubber som Trump, Æ, Coops medlem, etc?			
Handler du i nettbutikker?			
Bruker du smart-telefon app'er?			

E1)
Er du på følgende digitale plattformer: (karusell)

	Nei	Ja, det hender	Ja, ofte
Facebook			
Instagram			
Google			
SnapChat			
Youtube			
Twitter			
Spotify			
Amazon			
Finn.no			
VG+			
Aftenposten.no			

Select: De som er på facebook:
B4
Har du fått forespørsler knyttet til de nye personvernreglene **på din Facebookside/konto?**
0 Nei
1 Usikker
2 Ja

Hvis ja **B5: Hva gjorde du?**
0 Husker ikke
1 bare ga mitt samtykke
2 leste informasjonen før jeg ga mitt samtykke
3 prøvde, men klarte ikke endre hva Facebook lagrer om meg
4 reserverte meg mot enkelte registreringer
5 slettet min Facebook konto

Select de som er på Google:
B6
Har du fått forespørsler knyttet til de nye personvernreglene **på Google?**
0 Nei
1 Usikker
9 Ja

Hvis ja B7: Hva gjorde du?
0 Husker ikke
1 bare ga mitt samtykke
2 leste informasjonen før jeg ga mitt samtykke
3 prøvde, men klarte ikke endre hva Facebook lagrer om meg
4 reserverte meg mot enkelte registreringer
5 slettet min Google konto

C1): I hvilken grad har du tillit til at opplysninger knyttet til din person behandles på en god måte av… (karusell)

	Ingen tillit	Lite tillit	Usik-ker	Ganske god tillit	Full tillit	Vet ikke
…Facebook						
….Google						

…Amazone						
…Youtube						
…Snapchat						
…nettaviser						
…SPID (aftenposten.no, Finn.no, m.fl)						
…nettbutikker						
….fordelskort/kundeklubb i vanlig butikk						
…Altinn						
….forsikringsselskap						
…banker						
…offentlige kontorer						
…NAV						
…fastlegen						

Er du uenig eller enig i følgende påstander om de nye reglene for håndtering av person-opplysninger (som; mailadresse, kjøpsadferd og bilder på mobil, etc.) (karusell)

De nye reglene for håndtering av person-opplysninger…..	Helt uenig 1	Litt uenig 2	Verken enig eller uenig 3	Litt enig 4	Helt enig 5	Vet ikke 9
…gir forbrukerne bedre rettigheter						
…gjør det tryggere å dele på Facebook og andre sosiale medier						
…gjør det tryggere å handle på nett						
…er utilstrekkelig						
..gir meg større tillit til digitale tjenester generelt						
Jeg tror det nytter å si nei til at selskaper på internett(nettet) lagrer og bruker mine persondata						

I hvilken grad stemmer følgende påstander for deg? (spørres i karusell):

	Stemmer ikke 1	stemmer dårlig 2	Usikker/ Vet ikke 3	Stemmer litt 4	Stemmer helt 5	Uaktuelt 9
Det spiller ingen rolle hva jeg deler på nettet for jeg har ingenting å skjule						
For å få tjenester tilpasset mine behov velger jeg å dele mine personopplysninger						
Jeg synes personvern-innstillingene er forvirrende og uoversiktlige						
Jeg er redd for å skru av deling av informasjon fordi jeg tror jeg kan miste funksjonalitet						
Jeg har god kontroll med hva jeg gir fra meg av persondata						
Forbrukerne har for stort ansvar for å beskytte sine personopplysninger						
Jeg forstår ikke hvordan jeg skal beskytte mine personopplysninger						
Jeg forstår hvordan Google bruker personopplysninger						
Jeg forstår hvordan Facebook bruker personopplysninger						
Jeg har ikke tid og kapasitet til å gå gjennom alle henvendelsene jeg får om de nye reglene for håndtering av personopplysninger						
Jeg synes det er vanskelig å finne ut hvilke persondata som lagres om meg						
Jo flere opplysninger sosiale medier som Facebook har om meg, jo bedre tilbud får jeg						
Jeg får mail om samtykke fra aktører jeg ikke visste hadde min adresse						
Jeg vil heller betale mer enn å bytte fordeler mot personopplysninger						

Bakgrunnsvariable:

Alder: I hvilket årstall er du født?

Kjønn: Kvinne/Mann

Klasse:
Man snakker noen ganger om forskjellige samfunnsklasser. Hvilken klasse vil du si du tilhører?

Arbeiderklassen
Middelklasse……. Hvis middelklasse: øvre eller nedre middelklasse + usikker.
Overklassen
Vet ikke/usikker

Hvordan vil du beskrive din daglige situasjon?

Dersom det er flere alternativ som passer, velger du det som ut fra din egen mening stemmer best.

- ❍ Studier (1)
- ❍ Heltidsansatt (2)
- ❍ Deltidsansatt (3)
- ❍ Jobber i eget firma (4)
- ❍ Militærtjeneste/siviltjeneste (5)
- ❍ Fødselspermisjon (6)
- ❍ Pensjonert (7)
- ❍ Arbeidssøker (8)
- ❍ Hjemmeværende (9)
- ❍ Permittert (10)
- ❍ Trygdet (11)

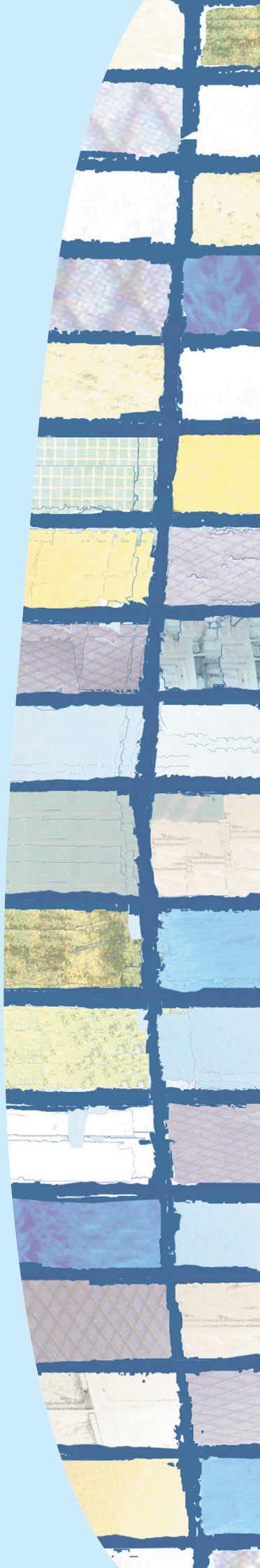
Nye variable: Respons på GDPR-henvendelsene fra Facebook og Google:
Compute **faceResp** = B5.
If (b4=0)faceResp=8.
if(b4=1)faceResp= 0.
compute **googResp**=B7.
if (b6=0)googResp=8.
if (b6=1)googResp=0.
value label faceResp, googResp 0'husker ikke' 1'Bare samtykke' 2'leste info før samtykke' 3'prøvde,klarte ikke' 4'reserverte noe' 5'slettet' 8'ikke reg GDPRhenv'.
Freq var =faceResp, googResp.

```
compute faceAll =0.
if (faceResp = 8)faceAll=1.
if (faceResp =0)faceAll=2.
if (faceResp=1)faceAll=3.
if (faceResp=2)faceAll=4.
if (faceResp=3)faceAll=5.
if (faceResp=4)faceAll=6.
compute googAll=0.
if (googResp = 8)googAll=1.
if (googResp =0)googAll=2.
if (googResp=1)googAll=3.
if (googResp=2)googAll=4.
if (googResp=3)googAll=5.
if (googResp=4)googAll=6.
value label faceAll, googAll 0'har ikke konto' 1'ikke reg GDPDhenv'
2'husker ikke' 3'bare samtykke' 4'leste før samtykke' 5'prøvde klarte
ikke' 6'reserverte noe'.
freq var = faceAll, googAll.
```

Forbruksforskningsinstituttet SIFO ved OsloMet – storbyuniversitetet har et spesielt ansvar for å bidra til kunnskapsgrunnlaget for forbrukerpolitikken i Norge og skal utvikle ny kunnskap om forbruk, forbrukerpolitikk og forbrukernes stilling og rolle i samfunnet.

Sentrale forskningstema er:

- forbrukerne i markeder og forbrukervalg
- husholdningenes ressursdisponeringer
- forbrukerøkonomi - gjeldsutvikling og fattigdom
- teknologisk utvikling og forbrukernes hverdag
- digitalt hverdagsliv og mestring
- miljøeffekter av ulike typer forbruk
- mat- og spisevaner
- tekstiler - verdikjeder - konsekvenser for hverdagsliv og miljø
- forbrukets betydning for inkludering i sosialt hverdagsliv
- forbrukerpolitikk



OSLOMET

STORBYUNIVERSITETET
FORBRUKSFORSKNINGSINSTITUTTET SIFO

Boks 4 - St. Olavs plass - N-0030 Oslo. **Besøksadresse:** Stensberggata 26, 7. etg. **Telefon:** +47 67 23 50 00
E-mail: post@oslomet.no **Internett:** www.oslomet.no/sifo