Personlige finanser

Hvordan utviklingstrekk i finanssektoren påvirker personvernet.

Rapport, februar 2018

Datatilsynet

Innhold

INNLEDNING 4

Hva er fintech og hvorfor nå? 4

Høy tillit til banker og forsikringsselskaper 5

TRE SENTRALE UTVIKLINGSTREKK 6

Persontilpasning 6

Automatisering og profilering 10

Plattformer og partnerskap 14

PERSONVERNUTFORDRINGER 17

Nærgående kartlegging 17

Mangel på valgmuligheter – bli sporet eller betal 17

All informasjon er relevant 18

Ugjennomsiktige algoritmer 18

Beslutninger basert på gale data 19

Diskriminering og økt sosial ulikhet 19

Tap av kontroll – hvem vet hva i plattformøkonomien? 20

Vanskelig å sammenligne tjenester 21

Økt sårbarhet for cyberangrep 21

Håndtering av sikker identifisering 21

Svak sikkerhet i smarte ting 22

Endrer vi atferd når noen ser oss over skulderen? 23

NYE REGLER FOR BEHANDLING AV PERSONOPPLYSNINGER 24

Mer ansvar til virksomhetene 24

Skjerpet krav til samtykke 24

Dataportabilitet 25

Automatiserte avgjørelser 26

Rett til å protestere 26

Vurdering av personvernkonsekvenser 27

Innebygd personvern 28

Er PSD2 og forordningen godt harmonisert? 28

OPPSUMMERING OG ANBEFALINGER 29

REFERANSELISTE 30

Innledning

Banker, forsikringsselskaper og andre finansvirksomheter spiller en sentral rolle i livene våre. De leverer tjenester vi ikke klarer oss uten, og de tar beslutninger som kan få store praktiske konsekvenser for oss.

Finans- og forsikringsbransjen er kjent for å være ganske tradisjonelle i måten å drive virksomhet på. Dette er nå i endring. Stordata, kunstig intelligens og sensorteknologi driver frem nye forretningsmodeller og finansteknologi (fintech). Tilgangen til data fra blant annet sosiale medier, mobilapplikasjoner og ulike typer sensorer, har ført til kappløp om å ha mest mulig data om kundene. Dataene brukes til å forutsi kundenes oppførsel, ønsker og behov. I tillegg til dette beveger teknologigiganter seg inn i finanssektoren. For å ikke bli utkonkurrert av nye aktører, utvikler banker og forsikringsselskaper nå nye forretningsmodeller og inngår nye allianser og partnerskap.

I denne rapporten ser vi på hvordan endringene i finans- og forsikringsbransjen vil påvirke vårt personvern.

I banksektoren vil opplysninger om vår privatøkonomi bli behandlet på nye måter og av langt flere aktører enn i dag. Klarer vi som forbrukere å holde oversikt over hvilke aktører som vet hva om oss? Til hvilke formål vil opplysninger om vårt handlemønster bli utnyttet? Blir informasjonen behandlet på en trygg måte, eller blir vi mer sårbare for misbruk eller andre uønskede hendelser?

Prisen på forsikringen vil fremover beregnes ut ifra vår unike atferd. Hvor tett inn på livet skal vi slippe forsikringsselskapene med sine sensorer? Hvor mange opplysninger skal vi gi i fra oss i bytte mot en rimeligere forsikring? Forsikringsselskapene er avhengige av å samarbeide med produsenter av smarte sensorer i utviklingen av persontilpassede forsikringsprodukter. Vil dette skape en mer uoversiktlig bruk og deling av data mellom selskapene?

I arbeidet med rapporten har vi vært i kontakt med aktører i finans- og forsikringsbransjen, konsulenter, Finans Norge, Finanstilsynet og relevante forskningsmiljøer. Vi har også støttet oss på utredninger, rapporter og nyhetsartikler som er skrevet om utviklingstrekk i finansnæringen.

Hva er fintech og hvorfor nå?

Finanstekologi (fintech) er en samlebetegnelse for ny teknologi og design som utfordrer tradisjonelle finanstjenester for lån, betaling, finansiering, handel og forsikring. Nye selskaper, såkalte «fintech-selskaper», vokser frem og endrer konkurransesituasjonen og de tradisjonelle verdikjedene i finansnæringen.

Utviklingen i finanssektoren er drevet av ny teknologi, nye forventninger blant forbrukerne og nye reguleringer:

Muliggjørende teknologi: For det første drives utviklingen av at det er blitt lettere og rimeligere å samle inn, lagre og analysere enorme datamengder. Nye tjenester og forretningsmodeller kan utvikles med bruk av stordata, sensorteknologi og kunstig intelligens.

Nye forventninger: For det andre er økte forventninger blant forbrukerne en drivkraft. Forbrukerne er blitt vant til å ha rask og enkel tilgang til tjenester på smarttelefonen. God tilgjengelighet og brukervennlighet er avgjørende for at forbrukerne skal ta i bruk nye tjenester. Yngre forbrukere, de såkalte digital natives, har ikke samme grad av lojalitet til tradisjonelle institusjoner som banker og forsikringsselskaper. De er mer åpne for å ta i bruk tjenester levert av nye aktører.

Ny regulering: For det tredje bidrar regulatoriske endringer til å drive frem innovasjon og nye forretningsmodeller. Det blir store endringer i banksektoren når det reviderte betalingstjenestedirektivet, PSD2, trer i kraft i 2018. Hovedformålene med PSD2 er å:

- understøtte et mer integrert og effektivt europeisk betalingsmarked
- åpne markedet for mer konkurranse
- bidra til at betalingen blir sikrere.
- beskytte forbrukerne
- legge til rette for lavere priser

Med innføringen av PSD2 mister bankene sitt monopol over kundenes transaksjonsopplysninger. Med samtykke fra kunden kan nye aktører få direkte innsyn i kontoer og transaksjoner. Selskaper utenfor banksektoren kan da bygge nye tjenester på toppen av bankenes data og infrastruktur. PSD2 legger til rette for utvikling av to nye tjenester:[1]

- **Betalingsinitieringstjenester:** Dette er tjenester som initierer betalingstransaksjoner på vegne av brukeren. For eksempel kan et selskap tilby en betalingsapplikasjon på smarttelefonen som en selvstendig tjeneste, eller som en del av sitt øvrige tjenestetilbud. Det er en forventning om at det vil

[1] Tilbydere av betalingsinitieringstjenester og kontoinformasjonstjenester blir underlagt tilsyn, regulering og overvåking av myndighetene. Aktørene må søke godkjenning hos Finanstilsynet, som vil publisere en liste over godkjente aktører.

dukke opp svært mange aktører som leverer denne typen tjenester. Tilbyder av slike tjenester kalles for Payment Initiation Service Provider, forkortet PISP.

- **Kontoinformasjonstjenester:** Dette er tjenester som gir forbrukeren nye måter å håndtere sine finanser og forbruk på. For eksempel kan det være et verktøy som holder oversikt over hva man bruker penger på og som gir hjelp og tips til hvordan du kan spare penger. En slik tjeneste kan også gi forbrukeren mulighet til å samle kontoopplysninger fra flere ulike banker på ett sted. Tilbyder av slike tjenester kalles for Account Information Service Provider, forkortet AISP.

I nær fremtid vil vi altså kunne bruke Facebook, Google eller et nyoppstartet fintechselskap til å betale regninger eller analysere forbruksmønstret vårt, mens vi fortsatt har pengene trygt plassert i banken.

25. mai 2018 erstattes dagens personvernlovgivning av en ny EU-forordning. Den nye personvernforordningen setter også rammer for hvordan personopplysninger kan samles inn og brukes til utvikling av persontilpassede forsikrings- og banktjenester.

Høy tillit til banker og forsikringsselskaper

Banker og forsikringsselskaper behandler store mengder informasjon om oss. Noen ganger også sensitive opplysninger. Når vi oppretter et kundeforhold til banken, må det registreres informasjon for å administrere kundeforholdet. Søker vi om lån eller andre finansielle tjenester, vil banken ha informasjon om blant annet vår økonomiske situasjon. Informasjonen brukes til å vurdere om vi skal få lånet, og i så fall på hvilke betingelser. Hver gang penger går inn eller ut av din konto registreres det informasjon om det. I tillegg må banken foreta kundekontroll av deg etter reglene i hvitvaskingsloven, og de har ulike rapporteringsplikter overfor myndighetene.

Forsikringsselskaper behandler også personopplysninger i stor utstrekning. De behandler blant annet informasjon om oss som kunde og, etter omstendighetene, hvem som er tilgodesett etter forsikringen for å administrere avtaleforholdet. Avhengig av hva slags type forsikring du tegner, behandler selskaper ulike former for personopplysninger for å beregne risiko og fastsette prisen på forsikringen. Ved skadeoppgjør må det behandles enda mer informasjon om oss.

En undersøkelse Datatilsynet gjennomførte i 2013 viste at befolkningen opplever opplysninger om privatøkonomi som følsomme.[2] Økonomiske opplysninger var i undersøkelsen listet som den sjette mest følsomme opplysningsgruppen, etter fødselsnummer, helseopplysninger og innholdet i telefonsamtaler og epost. Folk opplever opplysninger om privatøkonomi som mer beskyttelsesverdige enn opplysninger om for eksempel politisk og religiøs oppfatning. Banker og forsikringsselskaper har likevel høy tillit. Hele 80 prosent av de spurte har stor eller noe tillit til bankers behandling av personopplysninger. Det er bare helsevesenet og politiet som har høyere tillit. Litt færre, 70 prosent, har stor eller noe tillit til forsikringsselskapenes behandling av personopplysninger.

Finanssektoren er i rask endring. Opplysninger om vår privatøkonomi vil bli behandlet på nye måter, til nye formål og av nye og flere aktører enn i dag. Hvordan vil dette påvirke vår tillitt til sektoren?

[2] Datatilsynet, Personvernundersøkelsen 2013/2014, https://www.datatilsynet.no/globalassets/global/om-personvern/planer-strategier/personvernundersokelsen/samlerapport-personvernundersokelsen.pdf

Tre sentrale utviklingstrekk

Aktørbildet og forretningsmodellene i finanssektoren er i rask og kontinuerlig endring. Det er et omskiftelig og komplekst landskap å holde oversikt over. I denne rapporten har vi valgt å se på endringene i sektoren i lys av tre overordnede trender. Disse er:

1. Persontilpassing av tjenester og produkter
2. Automatisering av tjenester og oppgaver
3. Samarbeid og nye partnerskap

I følge World Economic Forum er banksektoren den sektoren som *raskest* vil føle effekten av disse driverne. Forsikringsbransjen er den bransjen som vil bli mest *endret*.[3]

Ved å se på endringene i lys av disse tre driverne ønsker vi å belyse de mest sentrale utviklingstrekkene. Vi vil også diskutere noen personverndilemmaer som endringene skaper. Deretter ser vi på hvilke rammer den nye personvernlovgivningen setter for utviklingen i finansnæringen fremover, før vi kommer med noen anbefalinger.

Persontilpasning

Virksomheter som Netflix, Amazon og Facebook har lenge brukt data de samler inn om oss til å tilpasse sine tjenester til den enkelte bruker. Som forbrukere forventer vi det samme nivået av brukertilpasning også av bank og forsikringstjenester. Muligheten til å samle inn kunde-opplysninger via blant annet apper og sensorer gjør det mulig for banker og forsikringsselskap å personalisere tjenestene de leverer. Ved å persontilpasse tjenestene, ønsker banker og forsikringsselskap å komme tettere på kunden og skape brukervennlige tjenester som igjen gir økt kundelojalitet.

Betalingstjenester gir verdifulle data

Når det reviderte betalingstjenestedirektivet (PSD2) innføres, står nye aktører klare til å bygge betalingstjenester på toppen av bankenes data og infrastruktur. Selskapene som har tilgang til flest opplysninger om oss – om vår inntekt, vårt forbruk og vennenettverk, samt våre hverdagsrutiner, interesser og meninger – er best rustet til å levere oss de mest målrettede og persontilpassede banktjenestene.

For bankene er det viktig å ikke miste betalingstjenestene til konkurrenter utenfor banksektoren. Hvis bankene taper kampen om den direkte kontakten med kundene, kan de i verste fall risikere å kun bli et hvelv for oppbevaring av penger.

Det har vært et kappløp mellom bankene i Norge om å være den aktøren som tilbyr den dominerende betalingstjenesten. Vipps, utviklet av DNB, har siden den ble lansert for tre år siden, lykkes i å bli den enerådende betalingsapplikasjonen i det norske markedet. Tjenesten har 2,6 millioner brukere.[4] Vipps har etablert seg som et eget selskap og har etter hvert knyttet til seg over 100 banker. Konkurrentene Nordea og Danske Bank har også inngått partnerskap med Vipps, og konkurrenten MobilPay er lagt ned.[5]

Selv om markedet foreløpig har konsolidert seg rundt Vipps, er markedet svært omskiftelig og det er ikke utenkelig at Vipps sin posisjon kan utfordres av aktører som er store utenfor Norge. (For å stå imot konkurransen fra de globale teknologigigantene, inngikk bankene i Norge i november 2017 en intensjonsavtale om å slå sammen Vipps, BankAxept og BankID Norge. Det tas sikte på at det nye selskapet skal være i drift innen 1. august 2018, forutsatt godkjenning fra norske myndigheter.)

Verdien i en mobil betalingstjeneste ligger ikke primært i transaksjonsinntektene den genererer. Den virkelige verdien ligger i opplysningene den samler inn. En mobil betalingstjeneste gir mulighet til å samle inn verdifulle opplysninger om kundenes forbruksmønster. Dette kan for eksempel være opplysninger om:[6]

- hva kunden kjøpte og hvor mye hun eller han betalte
- hvor kunden kjøpte noe
- når kunden kjøpte noe
- hvordan været var da han/hun handlet
- hva han/hun postet på sosiale medier før eller etter handelen
- hvor kunden var før han/hun handlet
- hvem han/hun var sammen med under handelen
- hva andre som handlet på samme tidspunkt

[3] World Economic Forum, «The Future of Financial Services – How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed», 2015, http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf

[4] Kampanje, «Nordea og Vipps inngår samarbeid – konkurrent legger ned», 11.10.2017, http://kampanje.com/tech/2017/10/nordea-og-vipps-inngar-samarbeid--konkurrent-legger-ned/

[5] Aftenposten, «Alle bankene er snart med i Vipps», 11.10.2017, https://www.aftenposten.no/okonomi/i/Pk2k0/Alle-bankene-er-snart-med-i-Vipps

[6] PWC, «Customer centric banking. Aligning the GDPR and PSD II», 2017, https://www.pwc.co.uk/banking-capital-markets/assets/documents/customer-centric-banking-aligning-gdpr-psd-ii.pdf

For leverandører av betalingstjenester, er disse opplysningene interessante å bruke for å videreutvikle tjenesten. De kan for eksempel brukes for å tilby personifisert forbrukerveiledning. Opplysningene er også nyttige for målrettet markedsføring av andre produkter og tjenester som selskapet tilbyr, slik som for eksempel forbrukslån eller kredittkort. Ettersom opplysninger om folks kjøpevaner er svært verdifulle, kan banker og andre tilbydere av betalingstjenester også selge disse videre til markedsførere.

Betalingstjenester integreres i andre tjenester

Betalingstjenester er i ferd med å integreres i tjenester vi bruker til daglig. For brukerne er det lettvint å slippe å logge seg inn på en separat tjeneste for å foreta betalingen. For aktører som har integrert en betalingsløsning i tjenesten sin, gir det en mulighet til å samle inn verdifulle betalingsdata fra brukerne, i tillegg til de andre opplysningene de kan samle inn.

Apple, Amazon, Google og Facebook har alle utviklet betalingsløsninger som er integrert i deres økosystem av tjenester. Apple Pay ble nylig gjort tilgjengelig i Sverige og Danmark, men Norge står fortsatt på vent. Facebook lanserte nylig vennebetaling i Storbritannia og Frankrike. Det er den første utvidelsen av vennebetalingsløsningen, som har vært tilgjengelig i USA siden 2015. Via Facebook Messenger kan brukerne sende og motta penger. Tjenesten hadde i 2017 over 1,2 milliarder brukere.[7]

Nordea har som første aktør i Norden, lansert en betalingstjeneste for eFaktura i Facebook Messenger i samarbeid med Nets. Systemet er lagt opp slik at man må logge seg inn med BankID første gang, men etter dette vil Nordeas chatte-robot sende en melding i Messenger for hver nye regning. Brukeren får et varsel, akkurat som for andre samtaler, og kan godkjenne uten ny BankID-innlogging.[8]

Vi ser også fremveksten av betalingstjenester som ikke er myntet på betaling alene. Det er livsstilsapper med et bredt spekter av funksjonalitet. Det kan være forbruker-veiledning, sosialt nettsamfunn eller en e-handelsapplikasjon. Verdens mest brukte mobile betalingsløsning, kinesiske Alipay, er et eksempel på en slik livsstilsapp der du i tillegg til å bruke den til betaling også kan bestille blant annet drosje og take-away med appen. Alipay er eid av e-handelsgiganten Alibaba og inngår som en integrert del av Alibabas e-handelstjenester.[9]

Apple Pay

Apple Pay ble lansert i oktober 2014. Løsningen er basert på NFC-teknologi. Selv om dette ikke var den første mobile betalingstjenesten som ble lansert, var det ansett som et betydningsfullt vendepunkt at et av verdens største teknologiselskap lanserte en slik tjeneste. Apple Pay kan benyttes i over en million utsalgssteder i USA, og systemet er støttet av Visa, Mastercard og American Express. I tillegg kan Apple Pay brukes i mange apper og in-app kjøp, samt i andre ting slik som Coca Cola-automater. Apple Pay er også inkorporert i Apple Watch. Apple ser store muligheter for å skape en brukervennlig betalingstjeneste når brukeren får anledning til å betale med klokken.

Apple Pay er tilgjengelig i flere europeiske land, deriblant Sverige og Danmark. Tjenesten er ikke tilgjengelig i Norge. En mulig årsak til dette kan være at Apple Pay ikke fyller et behov her til lands, foreløpig. Vi har et velfungerende, og fremfor alt billig betalingssystem sammenlignet med andre land. I tillegg har banksektoren samlet seg rundt en felles mobilbetalingsløsning med stor oppslutning blant forbrukerne. Aktørbildet er imidlertid i rask endring og det er mulig Apple Pay bare venter på rett tidspunkt til å entre det norske markedet.

Med banken i lomma

Tradisjonelle banker møter også konkurranse fra banker som kun er tilgjengelige via mobilen. Å bygge en bank med smarttelefonen som plattform, gir gode muligheter til å lage personaliserte banktjenester.

Den britiske app-banken Atom Bank har som mål å bygge en bank tilpasset kundens unike behov. For å kunne levere en mest mulig tilpasset tjeneste, henter banken ut data fra alle sensorene i mobiltelefonen:

«Another thing that sets us apart is our determination to ensure that we're eventually hooked into the whole mobile OS sub-structure, to take advantage of the whole device.» (Nick Wiles, Head of User Experience at Atom Bank.)

---

[7] E24, «Kan snu opp ned på nordmenns vennebetalingsvaner», 06.11.2017, http://e24.no/digital/facebook/facebooks-betalingstjeneste-inntar-europa-neppe-noen-gledens-dag-for-bankene/24181011

8 Dagens Næringsliv, «Betaler regningen på syv sekunder med Facebook Messenger», 29.11.2017, https://www.dn.no/nyheter/2017/11/29/0840/Finans/betaler-regningen-pa-syv-sekunder-med-facebook-messenger

[9] TechinAsia, «Why Alipay is more than just the Chinese equivalent of PayPal», 03.08.2015, https://www.techinasia.com/talk/online-payment-provider-alipay-chinese-equivalent-paypal

Monzo er en annen britisk bank laget for smarttelefonen. I tillegg til å fungere som en vanlig banktjeneste, sender Monzo varsel til mobilen din hvis du har overtrukket kontoen, minner deg på å betale regninger, gir informasjon om hvordan du bruker penger (nå har du handlet lunsj på Starbucks ti ganger siste måned!) og holder styr på dine kvitteringer. Målet til Monzo er å bli en smart og forutseende bank som kan gi deg hjelp før du selv vet at du trenger det.[10]

Forsikring – betal som du lever

Forsikring har siden ordningen så dagens lys vært basert på spredning av risiko. Prisen på forsikringen har blitt fastsatt med utgangspunkt i statistisk kunnskap om hvordan andre vi har likhetstrekk med har oppført seg tidligere.

Ny teknologi og muligheten til å samle inn data i sanntid, er nå i ferd med å endre denne forretningsmodellen. Ved hjelp av sensorer i bilen, hjemmet og på kroppen vår, kan forsikringsselskapene samle inn data om hvordan vi lever og hvordan vi oppfører oss. Prisen på forsikringen vil i fremtiden beregnes ut ifra vår unike atferd.

Forsikring endres fra å være basert på historiske data og med beskjeden kundekontakt, til å basere seg på sanntidsdata og aktiv og tett kontakt med kundene:

Historiske data	->	**Sanntidsdata**
Kunnskap om grupper	->	**Kunnskap om enkeltindivid**
Sjelden kundekontakt	->	**Løpende kundekontakt**
Passivt kundeforhold	->	**Aktivt kundeforhold**

Personaliserte forsikringsprodukter har foreløpig hatt størst utbredelse innen **bilforsikring**. Storebrand, gjennom forsikringsagent Rema 1000 Forsikring, var det første norske selskapet som tilbød persontilpasset bilforsikring. Kunder som bestiller bilforsikring hos Rema 1000, får tilbud om rimeligere forsikring hvis de installerer en brikke som overvåker bilførerens kjøreatferd. Brikken registrerer blant annet hastighet, om man akselererer raskt og bremser hardt eller om man kjører om natten. Opplysningene sendes til en databehandler som beregner kjørescore, og så sendes ferdig analyserte kjørescoredata tilbake til appen, slik at kunden kan få se sin score der.[11] Sparebank 1 tilbyr også bilforsikring basert på sensordata samlet inn fra bilen.

Selskapene oppgir at de kun bruker sensordataene til å fastsette pris og til å gi tilbakemelding på din kjørestil, slik at du kan forbedre den. De bruker ikke de innsamlede opplysningene til oppgjørsformål. De norske forsikringsselskapene samler ikke inn GPS-data som forteller hvor du kjørte. Sparebank 1 sier de har konkludert med at det er mye de ikke vil vite om kunden av personvernhensyn.[12]

Livs- og helseforsikringer er også i ferd med å personaliseres. Ved bruk av ulike typer sensorteknologi i for eksempel skrittellere, sportsarmbånd og mobilapplikasjoner, samler forsikringsselskapene inn data. Disse dataene brukes forløpende for å vurdere den enkeltes helse og livsstil.

Å basere utregningen av forsikringsprisen på slike data, vil kunne være mer effektivt og kostnadsbesparende for selskapene, enn å måtte hente inn opplysninger om helsetilstand via leger og pasientjournaler. Det forenkler og forkorter også prosessen med å søke og få livs- og helseforsikring for kundene.

I USA og Australia kan forsikringsselskapene personalisere forsikringsprisen basert på genetiske data. Genetiske selvtester blir stadig billigere. Hos 23andMe, et selskap som selger genetiske selvtester på internett, kan du kjøpe en test for tusen kroner. Når prisen på selvtester har blitt så lav, er det mulig for forsikringsselskapene å legge gentester til grunn for prissetting av helse-forsikringen. I Norge forhindrer imidlertid bioteknologi-loven muligheten til å bruke gendata til forsikringsformål.

Hus- og innboforsikringer vil også personaliseres. Våre hjem fylles av internett-tilkoblede sensorer som skal automatisere, effektivisere og trygge hjemmet.

Det finnes allerede forsikringsselskap som dekker kostnader forbundet med installering av sensorbaserte enheter, slik som for eksempel røykvarslere eller kameraovervåking. Dette gjør de dersom selskapet får overført data fra enhetene slik at de kan følge med på hva som skjer i hjemmet og eventuelt bruke informasjonen til å forebygge og hindre at skader inntreffer. I fremtiden kan forsikringsselskapet ringe rørleggeren før du selv har oppdaget vannlekkasjen.[13]

---

[10] http://monzo.com/

[11] https://www.remaforsikring.no/forsikringer/bil/

[12] Teknisk ukeblad, «Et halvt år med overvåking: Denne dingsen bekrefter mytene om unge sjåfører», 26.09.2017, https://www.tu.no/artikler/denne-dingsen-overvaker-bilisters-kjorestil-na-vil-de-bruke-kjoredataene-pa-helt-nye-omrader/408082

[13] MIT Technology Review, «Why Insurance Companies Want to Subsidize Your Smart Home», 12.10.2016, https://www.technologyreview.com/s/602532/why-insurance-companies-want-to-subsidize-your-smart-home/

Upersonlig forsikring

Samtidig som forsikringsløsninger blir mer personaliserte, peker en annen trend i motsatt retning: Etter hvert som hjemmet og bilen blir smartere og tryggere, blir individuell risiko i økende grad standardisert og omgjort til en vare – løsrevet fra personen som kjøper den.

Delingsøkonomien endrer konseptet med eierskap og utfordrer dermed den rådende forsikringsmodellen basert på et en-til-en eierskap til tingene. Det finnes allerede forsikringsselskap som tilbyr forsikring knyttet til aktivitet, heller en eierskap.

(Kilde: World Economic Forum, «The Future of Financial Services - How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed», 2015)

Forsikringsselskapet hjelper deg til bedre livsstil

Forsikringsselskapene ønsker også å bruke sensorteknologi til aktivt å påvirke kundenes livsstil. Ved å stimulere kunden til en best mulig livsstil, kan forsikringsselskapet spare store summer. Et slikt samspill med kunden legger også til rette for hyppig kundekontakt. Dette gir igjen en mulighet til å øke kundelojaliteten. Generali Group, et av verdens største forsikringsselskap, tilbyr sitt såkalte Vitality program i blant annet Tyskland, Italia, Frankrike og Østerrike.[14] Under programmets motto «Litt sunnere for hver dag», får kunden rabatt på helseforsikringen og på helserelaterte produkter, mot å dele data om sitt aktivitetsnivå og sine spisevaner.

Manulife i Hong Kong gir nye kunder avslag på Apple Watch mot at de kobler klokken til selskapets helseapp. Jo mer aktiv kundene er, jo rimeligere blir forsikringsprisen.

Amerikanske Beam Technology, tilbyr kundene en internett-tilkoblet tannbørste som kan gi tilbakemeldinger om pussevaner og hvordan kunden kan forbedre disse.[15]

Dataene som samles inn ved hjelp av sensorteknologi gir et omfattende bilde av kunden. Opplysningene kan også benyttes til andre, verdiøkende tjenester – for eksempel for å forutsi hendelser som kommer. I fremtiden kan forsikringsselskapet varsle at bildekkene begynner å bli slitt og kan samarbeide med bilforhandlere om gode tilbud.

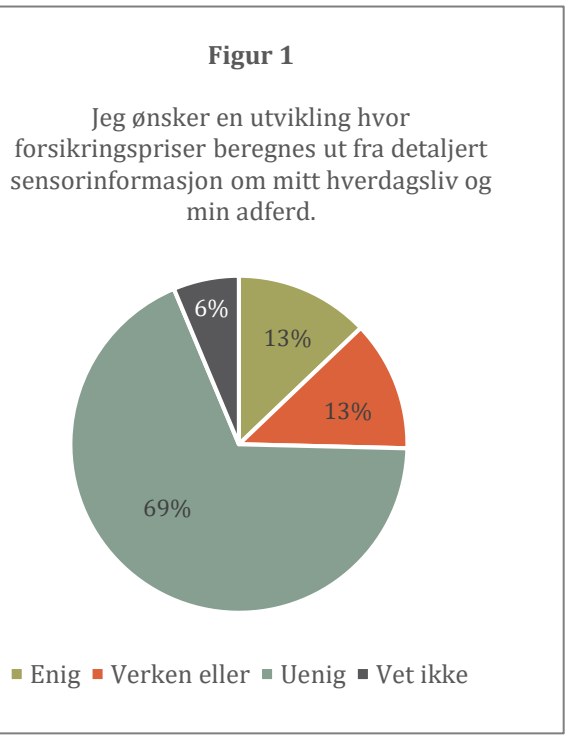
Ønsker folk persontilpasset forsikring?

I personvernundersøkelsen 2017 undersøkte vi hvilke holdninger folk har til persontilpassede forsikringsordninger.[16]

Det kom frem at nesten 70 prosent av de spurte uttrykte at de *ikke* ønsker seg en utvikling der forsikringspriser beregnes ut fra detaljert sensorinformasjon om deres hverdagsliv og atferd. Bare 13 prosent svarte at de var positive til dette.

Det er imidlertid verdt å merke seg at andelen negative blant de som er over 50 år (77 prosent) var mye høyere enn hos gruppen under 30 år (52 prosent negative):

Figur 1



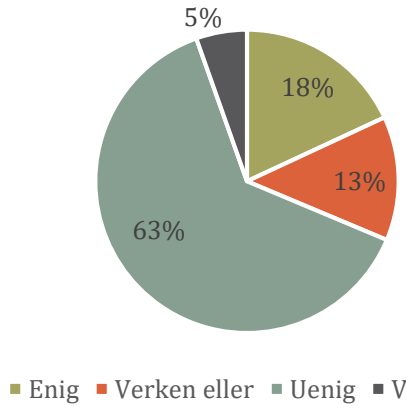
[14] Christl, Wolfie og Spiekermann, «Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy», facultas, 2016

[15] Capgemini, «Value-added services in insurance», 2017, https://www.capgemini.com/wp-content/uploads/2017/07/value_added_services_in_insurance_2017_2_web.pdf

[16] I forbindelse med rapporten Tilstand og trender 2017 gjennomførte Opinion en undersøkelse blant 1001 nordmenn om deres holdninger til bruk av data i finansbransjen. Datatilsynet, «Tilstand og trender 2017», 2017, https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/tilstand-og-trender-2017.pdf

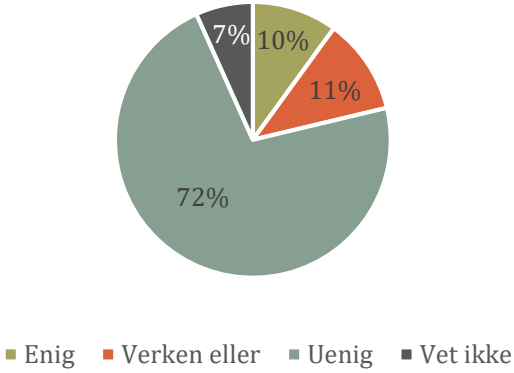
Figur 2

Så lenge prisen blir vesentlig lavere, kan jeg godt gi forsikringsselskapet tilgang til detaljerte sensordata om mitt hverdagsliv og min atferd



Figur 3

Jeg ønsker at forsikringsselskapet tar en aktiv rolle overfor min helse, eksempelvis ved å sende sms-varsler ved lite fysisk aktivitet eller tips om sunt hverdagsliv tilpasset meg.



Vi lurte videre på om folk var mer positive hvis forsikringsordningene som bruker informasjon om vår atferd, gir rimeligere forsikring. Flertallet av de spurte, 63 prosent, ville likevel ikke gi forsikringsselskapet tilgang til detaljerte sensordata fra sitt hverdagsliv – selv om det gir vesentlig rimeligere forsikring (se figur 2).

Igjen var de over 50 år mer skeptiske til å oppgi sensordata (69 prosent) sammenlignet med de under 30 år (48 prosent).

Vi stilte også spørsmål om folk ønsker en bilforsikring som beregner pris basert på data om hvordan de faktisk kjører. Rundt 40 prosent svarte at de er negative til dette, og omtrent like mange var positive.

Folk er mer skeptiske til å gi tilgang til helsedata som kan gi rimeligere livs- og helseforsikring enn de er til å dele kunnskap om egen kjøring. På spørsmål om folk ønsker at prisen på livs- eller uføreforsikringen blir beregnet etter helserelaterte sensordata, svarte kun 17 prosent at de var positive til dette. Dette gjelder data som fysisk aktivitet/ trening, puls, kaloriforbruk og søvn. Så mange som 64 prosent vil ikke dele slik informasjon.

På spørsmål om i hvor stor grad respondentene ønsker at forsikringsselskapene tar en aktiv rolle overfor deres helse – for eksempel ved å sende SMS-varsler ved lite fysisk aktivitet eller tipse dem om hvordan du kan få et sunt hverdagsliv – var hele 72 prosent negative (se figur 3). Kun 10 prosent svarte positivt. Tallene indikerer at det er stor skepsis mot å involvere forsikringsselskaper i forhold knyttet til egen helse og fysisk aktivitet.

Automatisering og profilering

Bruk av stordata og kunstig intelligens endrer hvordan finansnæringen arbeider. Tilgang til flere og nye typer data hentet fra sosiale medier, mobilapplikasjoner og sensorer, gjør det mulig å utvikle nye modeller for å forutsi forbrukernes atferdsmønster. Dette påvirker alle typer aktiviteter og tjenester, slik som profilering og segmentering av kundene, risiko og kredittvurdering, markedsføringskampanjer, produktutvikling, prissetting av produkter og tjenester, avverging av svindel og hvitvasking, kundeidentifisering og kundebehandling.

Ved hjelp av maskinlæring og kunstig intelligens, kan også datamaskiner løse oppgaver vi før måtte overlate til mennesket. Banker og forsikringsselskaper automatiserer nå prosesser knyttet til blant annet lånesøknader og skadeoppgjør.

Stordata og risikoprofilering

Forsikringsbransjen var blant de første til å bruke statistiske modeller basert på demografiske data til å forutsi atferden til forbrukerne. Allerede på slutten av 1800-tallet forsøkte forsikringsselskapene å anslå folks antatte livslengde og relative dødsrisiko.[17] Å samle inn data for å beregne individuell risiko, har alltid vært i

17 Christl, Wolfie, «Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade and Use Personal Data on Billions», Wien, 2017

kjernen av forsikringsselskapenes virksomhet. Også kredittopplysningsforetak har lang erfaring i å benytte statistiske modeller for å beregne folks risikoatferd.

Hvilke personopplysninger kredittopplysningsforetak kan bruke, er i dag regulert gjennom konsesjon fra Datatilsynet. Kredittopplysningsforetakene har blant annet anledning til å bruke opplysninger fra folkeregisteret, Brønnøysundregistrene, domstolene, selvangivelse og lønnsslipp. Kredittopplysningsforetak kan for eksempel ikke hente opplysninger fra massemedier, fordi opplysningens kvalitet ikke er ansett som god nok.[18]

I Europa, og verden for øvrig, dukker det nå opp selskaper som tenker nytt rundt hvilke data og datakilder som kan brukes i vurderingen av folks risikoprofil. Det finnes fintech-selskaper som vurderer kredittverdighet basert på såkalte atferdsdata, det vil si analyse av kundens nettaktivitet. Ved å samle inn og analysere atferdsdata hevder de at de trener opp algoritmer som kan forutsi om kunden er en god betaler eller ikke. Sporene på nett kan avsløre om du er en impulsiv rotekopp eller ansvarsfull og pliktoppfyllende.

Det tyske selskapet Kreditech kredittvurderer kunder ved bruk av maskinlæring som analyserer mer enn 20 000 ulike datapunkter om hver kunde. Kreditech angir ikke lenger på sine nettsider hvilke datakilder de benytter. Tidligere oppga de imidlertid at de baserte seg på opplysninger om blant annet hvilke nettsteder som ble besøkt, lokasjonsdata, aktivitet i sosiale medier, kontaktliste, historikk over varer kjøpt på nett, samt aktivitet i sosiale medier.[19]

Det finnes også selskaper som oppgir at de benytter data om kundenes batteristatus på mobilen til å estimere kredittrisiko.[20] Cignfi, et amerikansk fintech-selskap vurderer kredittverdighet blant annet basert på når og hvor hyppig folk benytter mobiltelefonen.[21]

Det kan være mange årsaker til at kredittvurderings-virksomheter velger å bruke atferdsdata i stedet for offentlige registerdata. En av dem kan være at det er raskere og dermed kostnadsbesparende å regne ut kredittscore på denne måten. Nesten alle selskaper som baserer kredittvurderingen på atferdsdata, legger vekt på at de gjør dette for å hjelpe mennesker som ellers ikke har tilgang til banktjenester fordi det ikke finnes opplysninger om dem i offisielle registre.[22]

Kina utvikler nasjonalt kredittvurderingssystem

Hvor du har vært, hva du kjøper, hvem du kjenner, prikker på førerkortet ditt, hvordan elevene dine rangerer deg – dette er noe av det kinesiske myndigheter ønsker å bruke for å gi en vurdering av alle sine innbyggere. Systemet heter Social Credit System (SCS) og skal gjøre vurderinger ved å kombinere personopplysninger fra banker, e-handel og sosiale medier. I tillegg til å gjøre kredittvurdering, kan systemet også brukes av utleiere, arbeidsgivere og potensielle kjærester til å vurdere hva slags type menneske du er.

Sesame Credit er en av de første funksjonene til systemet og er utviklet av Ant Financial, et datterselskap av den kinesiske e-handelgiganten Alibaba. Sesame Credit er et vurderingssystem som gir borgerne en score mellom 350 og 950 poeng basert på blant annet borgerens økonomiske bakgrunn. Hvis du bruker mye penger via Alibabas betalingsapp Alipay, eller du gjennomfører økonomiske transaksjoner som involverer venner gjennom Sesame Credit, øker scoren din. Jo høyere score du har, jo flere muligheter åpner seg. Hvis du har mer enn 600 poeng, kan du leie biler uten depositum. Har du mer enn 650 poeng kan du sjekke ut av hoteller raskere, mens mer enn 700 poeng gir deg visum til Singapore lettere.

Målet med SCS er å lage et nasjonalt system som henter opplysninger fra mange kilder, både fra offentlige registre og kommersielle kilder som for eksempel sosiale medier, og skal gjelde alle borgere. Systemet skal være på plass innen 2020. Kinesiske myndigheter har allerede en nettside der hvem som helst sjekke ut andre sin kredittvurderingsscore. Nettsiden bruker data fra 37 sentrale registre og opererer med hjelp fra Baidu, som er Kinas største søkemotor.

(Kilde: Wired, «Big data meets Big Brother as China moves to rate its citizens», 21.10.2017, http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion)

[18] Blixrud, Katrine Berg og Christine Ask Ottesen, «Personvern i finanssektoren», Gyldendal, Oslo, 2010

[19] Datatilsynet, «Big Data – personvernprinsipper under press», 2013

[20] CNNTech, «This startup uses battery life to determine credit scores», 24.08.2016 http://money.cnn.com/2016/08/24/technology/lenddo-smartphone-battery-loan/index.html

[21] https://cignifi.com/company/

[22] Ibid.

Store selskaper som Mastercard og kredittopplysningsforetak som Experian og Equifax, har inngått partnerskap med fintech-selskaper som bruker data og analysemetoder som nevnt over. [23]

Forsikringsselskaper og såkalte insuretech-selskaper utforsker også hvordan nye datakilder kan erstatte eller supplere data samlet inn direkte fra kunden og offentlige registre.

Admiral, et av de største forsikringsselskapene i Storbritannia, lanserte i november 2016 et forsikringsprodukt der kunder kunne samtykke til at selskapet analyserer deres Facebook-konto. Slik kunne bileiere som ikke hadde hatt forsikring tidligere få billigere bilforsikring. Admiral ville analysere kundenes oppførsel på Facebook, blant annet ville de se på hvilke ord og uttrykk de brukte for å avgjøre hvor samvittighetsfulle og velorganiserte de var.[24]

Facebook uttalte imidlertid umiddelbart etter lanseringen av dette produktet at de ikke ville tillate en slik bruk av deres brukeropplysninger, selv om deres brukere samtykket til dette.[25]

Lærende maskiner tar over

Kunstig intelligens er et begrep som beskriver hvordan datasystemer er i ferd med å tilegne seg egenskaper som vi tidligere har tenkt er unike for mennesker. De kan lære av egne erfaringer og løse komplekse problemer uten at de har fått presise instrukser. Mens algoritmer er regler som tradisjonelt har vært programmert for hånd, skjer utviklingen av kunstig intelligens nå innen maskinlæring. Maskinlæring gjør at maskiner lærer ved å bli vist en rekke eksempler, eller ved å prøve seg frem selv.[26]

Å kjøpe forsikring er en omstendelig og tidkrevende prosess. Kunden må ofte fylle ut lange spørreskjemaer som deretter behandles manuelt av forsikringsselskapet. Bruk av kunstig intelligens kan gjøre denne måten å kjøpe forsikring til historie.[27] Taksering av skadeoppgjør er også et område hvor bruk av maskinlæring og bildegjenkjenning kan automatisere prosessen og få behandlingstiden ned til sekunder.

Selskapet Epigram, som driver med maskinlæring og bildegjenkjenning, har hjulpet Gjensidige med å utvikle en helteknologisk skade- og takseringsprosess ved bilskader. En million bilder av bilskader er lastet opp i løsningen. Ved hjelp av kunstig intelligens og bildegjenkjenning kan systemet automatisk kjenne igjen og taksere ulike typer av bilskader. Kunder som har fått en bilskade kan ta bilde av bilen og sende det til Gjensidige. Innen kort tid er skaden taksert og oppgjøret i gang. Gjensidige mener de sannsynligvis er det første forsikringsselskapet i verden som tilbyr denne tjenesten.[28]

Det har dukket opp flere fintech-selskaper som tar i bruk kunstig intelligens for å automatisere risikovurderingene, skadeoppgjøret og kundepleien.[29] Det amerikanske selskapet Lapetus har utviklet en algoritme for bildegjenkjenning som anslår antatt levealder for å automatisere tilbud på livsforsikring. Kunden kan laste opp en «selfie» på selskapets nettside. Basert på bildet og noen få bakgrunnsspørsmål, beregner selskapet i løpet av få sekunder prisen på livsforsikringen.

Banker ser også på hvordan de kan automatisere prosesser knyttet til kundebehandling. I Norge har SFI BigInsight, sammen med partner DNB, utviklet et system for automatisert behandling av lånesøknader basert på en metode innen maskinlæring, kalt deep learning. Forskerne har ved hjelp av maskinlæring og data om kundens kontobevegelser laget en algoritme som kan brukes til å sannsynliggjøre hvorvidt en kunde vil betale tilbake lånet sitt eller ikke.[30] Resultatene av studien er svært lovende og metoden vil bli overført til DNB.[31]

Universitetet i Tromsø samarbeider med en bank om et lignende prosjekt. De ser på hvordan maskinlæring kan brukes til å forutsi risiko knyttet til utlån og nedbetalingsevne.[32] I prosjektet ser de blant annet på om det er en sammenhengen mellom hvilken nettleser brukeren har og hvor lang tid de bruker på å fylle ut

---

[23] Christl, Wolfie, «Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions», Wien, 2017

[24] The Guardian, «Admiral to price car insurance based on Facebook posts», 02.11.2016, https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts

[25] The Guardian, «Facebook forces Admiral to pull plan to price car insurance based on posts», 02.11.2016, https://www.theguardian.com/money/2016/nov/02/facebook-admiral-car-insurance-privacy-data

[26] Datatilsynet og Teknologirådet, «Tilstand og trender 2017», 2017, https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/tilstand-og-trender-2017.pdf

[27] Financial Times, «Insurance and the big data technology revolution», 24.02.2017, https://www.ft.com/content/bb9f1ce8-f84b-11e6-bd4e-68d53499ed71

[28] Dagens Næringsliv, «Gjensidige vil kaste ut konsulenter og hente inn it-hoder», 21.04.2017, https://www.dn.no/nyheter/2017/04/21/1152/Finans/gjensidige-vil-kaste-ut-konsulenter-og-hente-inn-it-hoder

[29] Financial Times, «Ten fintech start-ups that are causing a stir in insurance», 03.10.2016, https://www.ft.com/content/db833e5a-6eb1-11e6-a0c9-1365ce54b926

[30] BigInsight, Annual Report 2016

[31] Dagens Næringsliv, «Roboten gir lån hvis den får gode vibrasjoner fra kontoen din», 30.04.2017, https://www.dn.no/nyheter/2017/04/30/1817/Privatokonomi/roboten-gir-lan-hvis-den-far-gode-vibrasjoner-fra-kontoen-din

[32] Universitetet i Tromsø, «UiT samarbeider med storbank om datanalyse», 10.06.2016, https://uit.no/om/enhet/aktuelt/nyhet?p_document_id=472218&p_dimension_id=88136

søknadspapirene på nett og sannsynligheten for at vedkommende er en god betaler.

Et annet område innen bank hvor bruk av kunstig intelligens vil få betydning, er for å avdekke hvitvasking. Bankene er gjennom regulering forpliktet til å føre kontroll med og avdekke hvitvasking. Dette er en ressurskrevende og komplisert aktivitet. En utfordring ved metodene som brukes i dag, er at de plukker ut for mange falske positiver.[33]

IBM er i ferd med å trene opp sin programvare for kunstig intelligens, Watson, til å bli god på å avdekke hvitvasking.[34] BigInsight har også et forskningsprosjekt gående på dette området i samarbeid med DNB.

Personlige assistenter

Kunstig intelligens brukes også til å utvikle såkalte chatbots. En chatbot er kunstig intelligens du kan snakke med. Neste generasjon bank vil trolig ta form av en personlig assistent, som ved hjelp av kunstig intelligens vil utføre tjenester for oss før vi selv vet at vi trenger dem. De vil følge med på vårt forbruk, gi tips om rabatter på produkter de vet vi liker, sørge for at vi bruker den strømleverandøren som er rimeligst og flytte sparepengene våre dit de gir mest avkastning.

Nordea har lansert sin chatbot Nova og Swebank sin virtuelle assistent Nina. Begge er utstyrt med kvinnestemme, ettersom forsking viser at kunder føler seg mest komfortable med kvinnestemmer. Nova og Nina vil ha en bratt læringskurve og vil gi bedre råd og anbefalinger etter hvert som de samler inn data fra brukerne.[35]

Også innen forsikring tas virtuelle assistenter i bruk. Hos insuretech-selskapet Lemonade behøver ikke kunden fylle ut noen skjemaer for å få forsikring. Kunden må bare se inn i kamera og snakke med den virtuelle assistenten. Selskapet lover også at deres virtuelle assistent kan ferdigbehandle deres skadeoppgjør i løpet av tre sekunder.[36]

Eva - den usynlige banken

KPMG har utviklet fremtidsscenarioet «EVA – the invisible bank». Eva er en virtuell assistent basert på kunstig intelligens. Assistenten mates med bankens kundeopplysninger og opplysninger banken samler inn via partnerskap med en leverandør av aktivitetsarmbånd, tilgang til opplysninger på smarttelefonen og fra sosiale medier.

EVA vekker deg om morgenen, minner deg på at en venn av deg har bursdag, og spør om hun skal komme med gaveforslag. Rundt lunsjtider spør EVA hvordan det går med deg. «Du har spist mer junk food enn du pleier, du har ikke trent på en uke og du virker stresset», sier EVA. Hun foreslår at du begynner på yoga og kommer med forslag til et kurs som er i nærheten av der du bor. «Ja takk, det høres fint ut», sier du, «meld meg på.» «Kanskje Frode og Kari også vil være med på yoga?», spør Eva, «jeg ser de har ledig tid i kalenderen, og jeg tror yoga er noe for dem.» «Nei,» sier du, «jeg vil helst gå alene.» «Ok», sier EVA, og forteller deg før du legger på at hun har flyttet litt rundt på sparepengene dine slik at du får bedre rentevilkår.

(Kilde: KPMG, «Meet EVA - the future face of the invisible bank", 2016, https://home.kpmg.com/uk/en/home/insights/2016/10/meet-eva.html)

[33] GTNews, «False positives a growing headache», 08.10.15, https://www.gtnews.com/articles/false-positives-a-growing-headache/

[34] Techcrunch, «Watson Financial Services is born out of IBM's purchase of Promontory Financial Group», 29.09.2016, https://techcrunch.com/2016/09/29/watson-financial-services-is-born-out-of-ibms-purchase-of-promontory-financial-group/

[35] Independent, «Swedish banks embrace artificial intelligence as a cure to closures", 31.07.17, http://www.independent.co.uk/news/business/news/sweden-banks-robots-ai-artificial-intelligence-closures-financial-industry-online-digital-banking-a7868471.html

[36] Accenture, «Amplifyou. Technology for people. The Era of the Intelligent Insurer», 2017, https://www.accenture.com/gb-en/_acnmedia/C6F35436B1B2461F84C6A766968B701C.pdf

Plattformer og partnerskap

Grensene mellom ulike sektorer og bransjer er i ferd med å viskes ut som følge av digitaliseringen. Det blir vanskeligere i tiden fremover å definere hvem som tilhører finanssektoren. Starbucks har gjennom sin betalingsløsning tilgang til større oppsparte verdier enn det mange banker har.[37] Å tilby mobile finansielle tjenester er en sentral del av Telenors strategi.

Facebook har fått lisens til å drive betalingstjenester, og Google er inne på eiersiden i flere forsikringsselskaper.

Vi er vitne til fremveksten av plattformøkonomien. De selskapene som lykkes best, er de som ekspanderer inn i nye sektorer eller går sammen i partnerskap med aktører utenfor egen sektor. Drivkraften bak utviklingen er nødvendigheten av å nå ut til flest mulig brukere og å få tilgang til mest mulig data. Å eie distribusjon – i tillegg til data – er avgjørende i den nye økonomien.

Finansforetak vil enten bygge egne plattformer med seg selv som kjerne, eller koble seg opp mot eksisterende plattformer drevet av Amazon, Google, Alibaba, Apple eller Facebook.

Nytt aktørbilde

Uavhengig av betalingstjenestedirektivet møter bankene konkurranse fra aktører utenfor sektoren. Teknologigigantene Apple og Google lanserte allerede for flere år siden sine egne mobile betalingsløsninger. Et av formålene med betalingstjenestedirektivet PSD2 er å sikre at utviklingen av nye finansielle tjenester skjer innen regulerte rammer. Direktivet er derfor både en respons på utviklingen, og en katalysator for den. Med digitaliseringen av banksektoren og innføringen av PSD2, vokser det frem tre hovedgrupper av aktører som leverer finansielle tjenester. Felles for alle aktørene er at de leter etter forretningsmodeller som gir dem tilgang til data, samt distribusjon til mange brukere.

1. Nye teknologiselskaper

De nye fintech-selskapene, med ekspertise på digital tjenesteutvikling og data-analyse fokuserer gjerne på en nisje i markedet og har ikke intensjoner om å levere et bredt spekter av banktjenester. Dette gjør det mulig for dem å unngå begrensningene som ligger i å bli regulert som bank.[38] Eksempler på nordiske fintech-tjenester er Payr, Klarna, MeaWallet, Spiff og Zwipe.

Det holder imidlertid ikke med god teknologi og mye data for å lage en suksessfull tjeneste. Det er også nødvendig å få mange brukere raskt. For å nå kritisk brukermasse, inngår derfor mange fintech-selskaper strategiske partnerskap med etablerte banker, aktører innen varehandel eller med teknologigigantene.

2. Etablerte finansinstitusjoner

Bankene har i dag fordelen av å sitte på store mengder data som beskriver den finansielle situasjonen og atferden til kundene. Denne fordelen kan de tape. Det kan enten skje ved at de mister den direkte kontakten med kundene til andre aktører, eller ved at andre aktører får tilsvarende forbrukerinnsikt. Dette gjør de gjennom å sammenstille data fra andre kilder, for eksempel sosiale medier.

For å møte konkurransen fra Google, Apple, Facebook og Amazon, må bankene selv bli digitale plattformer. Ved å åpne opp sine systemer og dele data i form av API-er (se faktaboks), ønsker bankene å knytte til seg innovative selskaper og teknologitalent, slik at disse kan videreutvikle tjenestene deres. Dette strategien omtales som «open banking».

Hva er et API?

API (application programming interface) er et grensesnitt i en programvare som gjør at spesifikke deler av denne kan aktiveres fra en annen programvare. API-et er abstrakt og skjuler kompleksiteten i applikasjonen bak, og fungerer som en regelbok for kall til applikasjonen. Dette gjør det enkelt for tredjeparter å hente ut informasjon, gjøre endringer eller på annen måte behandle data i en større kontekst uten å kjenne til detaljene om hvordan applikasjonen bak er programmert. Et API kan ha funksjonalitet for å ivareta krav til tilgangskontroll og informasjonssikkerhet.

Eksempler på åpne norske API-er, er de som leveres av Statistisk Sentralbyrå og Metrologisk institutt, og som gjør det mulig for tredjeparter å enkelt hente ut statistikk- og værdata til bruk i egne applikasjoner.

[37] Forbes, «Starbucks Holds More Cash Than Many Banks», 01.08.2016, https://www.forbes.com/sites/niallmccarthy/2016/08/01/starbucks-holds-more-cash-than-many-banks-infographic/#5ca0d2ce231a

[38] McKinsey&Company, «The Age of Analytics: Competing in a Data-Driven World», desember, 2016, https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world

Alle de store norske bankene har satt i gang programmer der de inviterer nystartede fintech-selskaper til å utvikle nye digitale tjenester basert på sine bankdata. Nordea har for eksempel lansert en utviklerportal, eller markedsplass som del av sin «open bank-strategi». Den britiske banken Starling har lansert en API-markedsplass der tredjeparter kan bruke deres data til å utvikle tjenester på toppen av Starlings plattform. Tredjeparter er invitert til å legge til chatbots, forbrukerrådgivningstjenester eller oppkobling til sensorteknologi. Banken har allerede integrert Amazons Alexa i sin plattform, slik at kundene kan foreta betalinger og få tilgang saldoen via stemmestyring.[39]

3. Aktører utenfor finanssektoren

Blant bankenes fremste konkurrenter er teknologigantene Google, Apple, Facebook, Amazon og Microsoft med sine enorme ressurser på innovasjonssiden, samt tilgang til omfattende mengder med forbrukerdata.

Teknologikjempene kan utnytte nettverksfordeler blant brukerne. Nettverksfordelene innebærer at én eller flere av disse aktørene kan bli svært store innen betalingstjenester på internasjonalt nivå. Hvis vi ser på annonsemarkedet, så har Google og Facebook i løpet av få år lykkes i å ta to tredjedeler av det norske markedet.[40] Konkurransetrusselen fra disse aktørene er med andre ord høyst reell også for norske aktører.

Bankene møter ikke bare konkurranse fra aktører i Silicon Valley. Kina er i dag verdensledende på finansiell teknologi. Kinesiske Alipay er verdens største mobile betalingstjeneste med 520 millioner brukere. Alipay er eid av Alibaba, som i lilkhet med Amazon bygger opp en verdensomspennende plattform av ulike forbrukertjenester. Alipay ble gjort tilgjengelig i norske butikker i 2017, men kan foreløpig kun benyttes av kinesere på besøk i Norge. [41] På sikt vil trolig også norske forbrukere kunne bruke Alipay både hjemme i Norge og på ferie i utlandet. Det er ikke utenkelig at Alipay blir den dominerende betalingsappen globalt og dermed den foretrukne for folk på reise.

Foruten teknologikjempene etablerer også leverandører av kapitalvarer egne betalingstjenester. I dag betaler nettbutikkene en transaksjonsavgift til banker og kortselskaper ved betaling. Med PSD2 kan de få direkte tilgang til kundenes kontoer via tredjeparter, og dermed få redusert disse avgiftene. En aktør slik som Vipps eller Google vil kunne tilby butikkene en gratis betalingstjeneste (butikkene trenger ikke betale kortavgift til bankene) mot at de får tilgang til kjøpsdataene.

Partnerskap en forutsetning

Forsikringsselskapene møter også konkurranse fra nye aktører. I likhet med bankene møter de konkurransen med å inngå partnerskap med andre selskaper. Forsikringsselskapene bygger egne plattformer der de inviterer innovative teknologiselskaper med sine nye forretningsmodeller, eller de kobler seg til plattformer drevet av aktører utenfor egen sektor.

Forsikringsselskapene er særlig avhengige av å samarbeide med teknologiselskaper. For å kunne tilby persontilpassede forsikringsprodukter, må de benytte ulike former for sensorteknologi. Det er kostnadskrevende for forsikringsselskapene å utvikle slik teknologi selv. I tillegg er det en fordel for forsikringsselskapene å bruke teknologi som allerede er populær og allment tilgjengelig, slik som for eksempel Fitbit eller Applewatch.

Teknologi- og forsikringsselskapene har gjensidig interesse av å finne sammen. Verdien i smarte produkter ligger ikke primært i salg av produktet i seg selv. Det er i dataene som produktene samler inn at den store verdien ligger. En sentral del av forretningsmodellen til leverandører av internettoppkoblede produkter er derfor å tjene penger på videresalg av de opplysningene som utstyret samler inn, eller å dele dem med andre aktører gjennom strategiske partnerskap.

Fitbit, en markedsleder innen helse- og treningsarmbånd, har inngått partnerskap med en rekke amerikanske forsikringsselskaper. Forsikringsselskapet Vitality Group belønner kunder som bruker Apple Watch og som deler opplysningene klokken samler inn med forsikringsselskapet.[42]

Selskapet Beam Dental har utviklet en tannhelseforsikring i samarbeid med en produsent av en sensorbasert tannbørste som sender opplysninger om tannhelsen til forsikringsselskapet.

Google er inne på eiersiden i Nest som leverer selvlærende, internettoppkoblede termostater, røykvarslere og andre sikkerhetssystemer. Nest har etablert partnerskap med American Family Insurance og Liberty Mutual Insurance. Forsikringsselskapene

---

[39] Finextra, «Starling releases Open API, talks up marketplace model», februar 2017, https://www.finextra.com/newsarticle/30183/starling-releases-open-api-talks-up-marketplace-mode

[40] Aftenposten, «Facebook har trolig milliardoverskudd i Norge - betalte under 500.000 kroner i skatt», 06.07.2017, https://www.aftenposten.no/okonomi/i/jqOAA/Facebook-har-trolig-milliardoverskudd-i-Norge---betalte-under-500000-kroner-i-skatt

[41] E24, «Verdens største betalingsløsning lanseres i Norge – men ikke for nordmenn», 08.09.2017, http://e24.no/naeringsliv/teknologi/verdens-stoerste-betalingsloesning-lanseres-i-norge-men-ikke-for-nordmenn/24133447

[42] Financial Times, «Wearable technology: gathering data from tooth to toe», https://www.ft.com/content/9b00b05c-70fe-11e6-a0c9-1365ce54b926

subsidierer installering av utstyret mot at de mottar data fra enhetene.

Flere av de store teknologiselskapene er i ferd med å bygge opp standardiserte plattformer for å forbedre koordineringen av ulike typer smarte enheter. Plattformene skal gjøre det lettere å samle inn, utveksle og analysere data. Apple og Google har for eksempel utviklet hver sin plattform (henholdsvis AppleCarPlay og Open Automotive Alliance) myntet på bilbransjen, der ulike bilmerker kan laste opp sine apper. Det vokser også frem tilsvarende plattformer innen helsedata og smarte hjem.[43] For å nå ut til flest mulig brukere vil det være interessant for forsikringsselskapene å koble seg til disse plattformene.

Forsikringsselskapene bygger også opp sine egne plattformer for å knytte til seg nyoppstartede teknologiselskaper med innovative ideer og forretningsmodeller. Det er særlig i distribusjonsleddet ut mot kundene at det dukker opp nye aktører som samarbeider med de tradisjonelle forsikringsselskapene.

For nyoppstartede selskaper er det interessant å fungere som forsikringsagent fordi de da får tilgang til verdifulle kundedata. Samtidig slipper de kostnadene forbundet med å utvikle selve produktene, samt de regulatoriske forpliktelsene med å være fullverdig forsikringsselskaper. Rema 1000 Forsikring er et eksempel på en slik ny aktør i forsikringsmarkedet.

For forsikringsselskapene på sin side er det interessant å samarbeide med agenter fordi det gjør det mulig å nå ut til nye og flere brukergrupper. For å sikre seg distribusjon i Kina, har for eksempel Frankrikes største forsikringsselskap, AXA, inngått partnerskap med den kinesiske e-handelsplattformen Alibaba.[44] En fare ved å samarbeide med agenter er imidlertid at forsikringsselskapene på sikt kan miste den direkte kontakten med kundene, og dermed tilgang til verdifulle data.[45]

---

[43] World Economic Forum, «The Future of Financial Services How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed», 2015, http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf

[44] AXA, «AXA, Alibaba and Ant Financial Services announce global strategic partnership», 29.07.2016, https://www.axa.com/en/newsroom/press-releases/axa-alibaba-ant-financial-services-announce-global-strategic-partnership

[45] Financial Times, «Ten fintech start-ups that are causing a stir in insurance», 03.10.16, https://www.ft.com/content/db833e5a-6eb1-11e6-a0c9-1365ce54b926

Personvernutfordringer

De selskapene som sitter på mest forbrukerdata er vinnerne i dagens digitale økonomi. Forbrukeren nyter på sin side godt av personaliserte, nyttige og brukervennlige tjenester basert på analyse av disses opplysningene. Men utviklingen mot mer personaliserte tjenester kan også utfordre den enkeltes personvern.

I tiden fremover vil flere og flere avgjørelser som fattes om oss, gjøres av algoritmer istedenfor av et menneske. Automatiserte systemer basert på kunstig intelligens vil avgjøre om du får lån til å kjøpe nytt hus eller hvilke tilbud forsikringsselskapet vil gi akkurat deg. Det betyr i mange tilfeller mer effektive, presise og brukervennlige tjenester, men fra et personvernståsted er det også utfordringer knyttet til at algoritmene overtar.

Nye aktører og samarbeidskonstellasjoner i betalings- og forsikringsmarkedet vil innebære økt spredning av informasjon. Den økte kompleksitet i markedsstrukturen vil gjøre det mer utfordrende for forbrukeren å ha oversikt og kontroll over opplysningene sine. En endret markedsstruktur kan også medføre nye sårbarheter og risikoer knyttet til datasikkerhet.

Vi vil her se nærmere på noen av de viktigste personvernutfordringene som utviklingstrekkene beskrevet i forrige kapittel vil kunne medføre.

Nærgående kartlegging

For at persontilpassede tjenester skal fungere best mulig, kreves det mye data. Dette fører til en omfattende kartlegging av den enkelte. Det kan derfor bli utfordrende for oss forbrukere fremover å overskue totaliteten av hvilke opplysninger som samles inn om oss, samt hvilke slutninger selskapene kan trekke om oss på bakgrunn av disse opplysningene.

Personvernlovgivningen har bestemmelser som sier at det ikke skal samles inn mer data enn nødvendig for å oppnå formålet med behandlingen av opplysningene. Banker og forsikringsselskap vet mye om oss i dag, og med utviklingen av nye personaliserte løsninger, får de vite enda mer om oss. Selv om selskapene samler inn relevante opplysninger, krever loven at innsamlingen skal være rimelig og proporsjonal. I fremtiden blir det også viktig å vurdere om det er *rimelig* at selskapene skal vite så mye om oss.

I USA har Google inngått partnerskap med et selskap som kan spore 70 prosent av alle kjøp i «off line-butikker». Med tilgang til disse dataene kan Google sammenstille data om hvilke annonser folk ser, opp mot hva de faktisk kjøper. Google kan informere butikkjeder automatisk når deres digitale annonser gir konkrete kjøp.[46] I Europa vil et selskap som sitter på slike betalingsdata ikke kunne gi disse lovlig til andre aktører uten videre. Skulle Google derimot etablere en egen betalingstjeneste, vil selskapet få tilgang til nettopp slike data. Selskapet kan likevel ikke lovlig gjøre en kobling av betalingsdata opp mot søkehistorikk uten videre.

Ved å hente inn opplysninger om vår aktivitet gjennom sensorer, kan forsikringsselskapene kartlegge oss i detalj. Vi vil trolig se fremveksten av forretningsmodeller innen forsikring der selskapene ønsker å kartlegge vår *samlede* risiko på tvers av forsikringsområder, til forskjell fra i dag der vi har separate bil-, hus-, livs- og helseforsikringer. Slik deling av data på tvers av livsområder, kan skape en følelse av å bli overvåket.

Dataanalyse kan også avdekke opplysninger som den enkelte ikke har samtykket til å dele. Gjennom sammenstilling og analyse av innsamlede person-opplysninger, kan det genereres nye opplysninger, opplysninger som kan være sensitive. Ved innsamling av data fra kroppsnær teknologi for eksempel, er risikoen for å avsløre sensitive informasjon om brukeren ekstra høy. Forsikringsselskaper må derfor gjennomføre gode risikovurderinger før de tar i bruk slike produkter som aktivitetsarmbånd eller tilsvarende.

Mangel på valgmuligheter – bli sporet eller betal

Per i dag har vi bare sett starten på persontilpassede tjenester. Det betyr at de færreste nordmenn i dag har en forsikring basert på løpende innsamling av person-opplysninger eller en bankløsning som forteller dem at de bør skifte strømleverandør.

I fremtiden kan denne type persontilpassede tjenester bli mer utbredt. Vi kan da stå ovenfor en situasjon der vi blir «tvunget» inn i løsninger som overvåker livene våre i detalj. Enten fordi det ikke finnes alternativ, eller fordi alternativene er mye dyrere.

[46] Los Angeles Times, «Google starts tracking offline shopping — what you buy at stores in person», 23.05.2017, http://www.latimes.com/business/technology/la-fi-tn-google-ads-tracking-20170523-story.html

Vi kan komme i en situasjon der standarden er at alle som lar seg spore får den billige forsikringen, mens de som enten ikke vil eller ikke kan bli sporet, får dyrere forsikring. Individer med lav betalingsevne kan tvinges til å velge billigere produkter som krever sporing. I denne situasjonen taper personvernet, fordi det koster mer penger enn alternativet.

Persontilpasset forsikring kan også forsterke forskjellene mellom oss. Forsikringsselskaper vil konkurrere om de kundene som leverer data som viser at de lever sunne liv med lav risiko. De som faktisk har høyere risiko (for eksempel de som kjører uvørent, ikke trener eller har høy BMI) må betale dyrere forsikring. På sikt står hele forsikringsordningen med risikospredning som et kollektiv prosjekt, under press. Hvis utviklingen går i denne retningen, vil det kanskje være en bedre løsning for folk som må betale skyhøye forsikringspremier, å sette penger på sparekonto.

All informasjon er relevant

Intelligente datasystemer er avhengige av data. Jo mer data systemet har tilgang på, jo mer nøyaktig og presis hevdes det at analysen blir. Siden mye av livene våre er digitalisert, finnes det også store mengder data om oss.

Lovverket bygger på et prinsipp om dataminimalitet. Det er et prinsipp om at man skal bare behandle person-opplysninger som er adekvate og relevante, og ikke samle inn mer enn det som er nødvendig for formålet. Men hvis maskinen kan levere bedre analyser og resultater jo mer data de får tilgang til, hva blir da igjen av prinsippet om å begrense mengden opplysninger man behandler til et minimum?

Trenings- og helseapper kan si noe om risikoen ved å ha deg som forsikringstaker. Informasjon om hvor ofte telefonen din går tom for strøm brukes til å vurdere risikoen ved å ha deg som låntaker. Banker og forsikrings-selskaper har et legitimt behov for å kartlegge kundenes risikoprofil. I en stordata-kontekst kan i utgangspunktet *alle* data være relevante.

I stordatametoder er man på jakt etter å oppdage nye sammenhenger i et datamateriale. Ved å koordinere data fra ulike databaser, kanskje opprinnelig samlet inn for et annet formål, vil man kunne finne sammenhenger som ikke før var synlige.

Det vil være viktig for banker og forsikringsselskaper å gjøre gode risikovurderinger i forbindelse med stordata-analyser. Dette innebærer å gjøre vurderinger av hvilke data som er nødvendige å samle inn for å oppnå formålet med innsamlingen, hvilken risiko som er forbundet med å samle inn og behandle opplysningene, hvorvidt sammenstilling av opplysningene kan resultere i nye og sensitive opplysninger, og om det er mulig å benytte personvernfremmende tiltak som aggregering og pseudonymisering av de innsamlede dataene for å redusere personvernulempene.

Personvern i hjertet av virksomheten

AXA, Frankrikes største forsikringsselskap, har etablert et rådgivende panel på personvern (Data Privacy Advisory Panel). I dette panelet har de samlet de fremste ekspertene på personvern i Europa. Rådet treffes to ganger i året og diskuterer selskapets strategi og forretningsmodeller knyttet til innsamling og bruk av persondata.

Personvernekspertene gir blant annet råd om de regulatoriske og etiske rammene for bruk av personopplysninger og hvordan innebygd personvern og annen personvernfremmende teknologi kan brukes i utviklingen av nye tjenester. AXA ønsker å være en spydspiss i innovativ utnyttelse av data, men fremhever at dette må gjøres på en måte som bevarer tillitten hos kundene.

(Kilde: AXA, «AXA's Data Privacy Advisory Panel», https://www.axa.com/en/about-us/data-privacy)

Ugjennomsiktige algoritmer

Ved å bruke stordata og kunstig intelligens kan selskaper effektivisere mange av dagens løsninger og spare store summer. Når vi overlater stadig mer til maskinene, er det imidlertid viktig å spørre seg hvordan vi skal ivareta tilliten til de beslutningene som fattes. En utfordring ved mange av systemene som utvikles i dag, er at de er så komplekse at det nesten er umulig å forstå hvordan de fungerer. Automatiserte beslutningssystemer basert på kunstig intelligens blir derfor ofte omtalt som «svarte bokser». Hvis de som eier systemet ikke kan forklare hvordan det virker, hvordan skal vi da kunne ha tillit til at avgjørelsen er rettferdig?

Ettersom maskiner kan brukes til å trekke beslutninger av til dels stor betydning i den enkeltes liv, er det gitt særskilte regler for automatiserte beslutninger i den nye personvernforordningen. For at den automatiserte avgjørelsen skal omfattes av de særskilte reglene, må avgjørelsen ha en betydelig påvirkning for personen. Automatiserte beslutninger foretatt av banker og forsikringsselskaper vil ofte ha en slik betydelig påvirkning. Aktørene i finansnæringen må derfor trolig

forholde seg til de vilkårene i forordningen som er satt for å kunne benytte seg av automatiserte avgjørelser.

I det nye personvernregelverket finner vi bestemmelser som kan bidra til å øke bevisstheten rundt hvordan algoritmestyrte beslutningssystemer må lages for å fungere mest mulig etterrettelig og rettferdig. Det nye regelverket inneholder for eksempel en rett til forklaring på hvilke beslutningskriterier som ligger til grunn for beslutningen. I tiden fremover vil virksomheter som benytter komplekse datasystemer måtte finne brukervennlige måter å forklare hvordan algoritmen kom frem til beslutningen. Denne nye forpliktelsen i personvernforordningen inspirerer allerede forskningsmiljøer verden over til å utvikle mer åpen og gjennomsiktig kunstig intelligens. Dette er viktig arbeid.

Beslutninger basert på gale data

Det er et grunnkrav i personvernlovgivningen at virksomheter som behandler personopplysninger skal sørge for at opplysningene som behandles er korrekte. Hvis finansielle virksomheter benytter atferdsdata til å vurdere for eksempel kredittverdighet, er det en reel fare for at beslutningene fattes på grunnlag av uriktige data. Opplysninger hentet fra for eksempel sosiale medier gir ikke verifiserbar kunnskap om enkeltindivider. Hvis slike opplysninger brukes i byggingen av risikoprofiler, er det fare for at feil karaktertrekk blir tildelt individet. Når beslutninger fattes på grunnlag av feilaktige data, representerer det en trussel mot den enkeltes rett til rettferdig behandling.

Urettferdig eller urimelig behandling kan gjøre seg gjeldende på flere måter:

- En kunde kan bli avvist av finansielle institusjoner fordi feilaktige data kategoriserer vedkommende som en dårlig betaler.
- En kunde kan bli nektet å kjøpe et produkt eller en tjeneste fordi en analyse basert på feilaktige opplysninger hentet fra sosiale medier gir kunden dårlig kredittvurdering.
- En kunde får ikke mulighet til å inngå en kontrakt, for eksempel på et langsiktig lån, fordi noen har lagt ut feilaktige opplysninger på internett om at han lider av spillegalskap.

Diskriminering og økt sosial ulikhet

Økt bruk av personopplysninger for å personalisere tjenester, kan ha uheldige konsekvenser for marginaliserte og sårbare grupper. Hvis fysisk aktivitet skal bestemme om du får helseforsikring, og hvor mye du handler for på nett skal bestemme kredittvurderingen og avgjøre om du får ta opp lån, kan allerede marginaliserte individer eller grupper oppleve å måtte betale mer, eller ikke få tilgang til visse tjenester.

Profilering øker risikoen for uberettiget og usynlig diskriminering. Selv om dataene som legges til grunn for beslutningen er korrekte, kan de gi urettferdige og diskriminerende resultat for den enkelte.

En utfordring med automatiserte beslutningssystemer, er at de kan befeste og forsterke eksisterende fordommer og stereotypier. Algoritmer er ikke er mer objektive enn menneskene som lager dem. Våre fordommer kan overføres til maskinene. Intelligente systemer baserer seg på data man allerede har om enkeltpersoner eller grupper, og de kan i enkelte tilfeller være preget av fordommer og skjevheter.

Nylig avdekket en gruppe forskere ved Universitetet i Virginia at et bildegjenkjenningsprogram de var i ferd med å utvikle, automatisk koblet bilder av kjøkken med kvinner og ikke med menn. Dette hadde sammenheng med at bildedatabasen som algoritmen lærte fra, inneholdt bilder der kvinner i større grad enn menn var avbildet på kjøkken. Menn var i større grad enn kvinner avbildet med gevær og sportsutstyr. Denne skjevheten i datamaterialet fikk konsekvenser for læringen til algoritmen. Algoritmen for bildegjenkjenningen kjente ikke bare igjen mønsteret, den bidro til å *forsterke* skjevhetene som lå i databasen ved å automatisk å kategorisere alle personer som var avbildet på kjøkken som kvinner, selv når de var menn.

Slike skjevheter kan få alvorlige konsekvenser hvis de forekommer i automatiserte beslutningssystemer. Det kan føre til at sårbare grupper blir avskåret fra visse typer finansielle tjenester.

Tap av kontroll – hvem vet hva i plattformøkonomien?

Dagens forbrukere ferdes i et landskap der de ikke har full oversikt over hvilke spor de legger igjen, hvem som har tilgang til opplysningene deres og hva konsekvensene av at de legger igjen data kan være.

Et aktørbilde i endring bidrar til forvirringen. Hvis Google etter hvert leverer banktjenester, vil de potensielt kunne sammenstille bankopplysninger med opplysninger hentet inn om brukeren på YouTube, Gmail, Google Analytics og alle andre tjenester eid av Google.

Rema 1000 Forsikring tilbyr forsikringstjenester, og dagligvarekjeden Rema 1000 lanserte nylig en app som registrerer alle varene du kjøper hos dem. Det er ingenting som per i dag tyder på at Rema bruker handlevanene våre i forsikringsøyemed, men sammenblandingen av roller kan gjøre det uoversiktlig for forbrukeren.

I banksektoren vil det nye betalingstjenestedirektivet bidra ytterligere til et allerede uoversiktlig aktørbilde. Vi går fra en situasjon der ett selskap behandler alle våre bankopplysninger til en situasjon der vi kan dele de samme opplysningene med mange ulike selskaper, også amerikanske og kinesiske teknologigiganter.

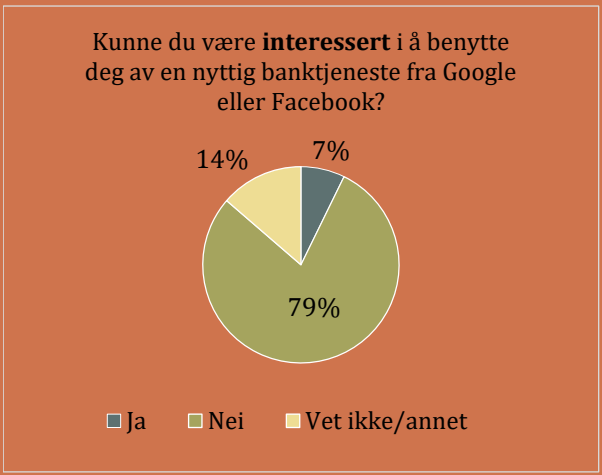
Mange tilbydere av betalingstjenester vil ofte samtidig tilby andre typer varer og tjenester, slik som for eksempel digitale handelsplattformer, sosiale nettverk, matvarer, elektronikk og nettbaserte spill. Betalingsdata vil være verdifulle for disse aktørene både til eget bruk og for salg til tredjeparter. Til tross for regler om behandling av personopplysninger i PSD2, samt de generelle personvernreglene, vil det være en risiko for at slike opplysninger behandles i strid med brukerens interesser.

Bankene har strenge krav om tilgangsstyring til konto-opplysninger for å hindre snoking fra ansatte. Kontoopplysninger kan inneholde sensitiv informasjon om helse, politisk tilknytning og seksuelle forhold. Hvordan vil dette bli håndtert av mindre oppstarts-bedrifter og selskap som Google og Facebook?

I forsikringsbransjen vil partnerskap mellom forsikrings-selskaper og tjenesteleverandører kunne gjøre det uklart for forbrukeren hvilke selskaper som samler inn hvilke data. Hvis et forsikringsselskap samarbeider med en leverandør av aktivitetsarmbånd, hvilke opplysninger får da sistnevnte selskap og til hvilke formål kan dette selskapet bruke opplysningene?

Et mer uoversiktlig aktørbilde og en mer uoversiktlig bruk og deling av data mellom selskaper, stiller store krav til åpenhet og gjennomsiktighet fra aktørene i bransjen. Dette må til for å sikre at kundene forstår hva de

Nei til banktjenester fra Google og Facebook



79 prosent av de spurte i personvernundersøkelsen 2017, oppgir at de ikke er interessert i å benytte en nyttig banktjeneste fra Google eller Facebook.

87 prosent av de spurte svarer ja på dette. Av de 87 prosentene som synes det er problematisk, svarer **fem prosent** at de likevel ville benyttet seg av tjenesten.

Svarene indikerer en tydelig skepsis blant folk om å blande sosial nettaktivitet med banktjenester. Kan dette tyde på at bankene ikke behøver å frykte konkurransen fra Facebook og Google med det aller første?

(Kilde: Datatilsynet, personvernundersøkelsen «Personvern - tilstand og trender 2017»)

samtykker til og har oversikt over hvilke selskaper som har hvilke opplysninger om dem. Det er spesielt viktig at virksomhetene er åpne om hvordan opplysningene brukes til kartlegging og profilering av kundene. Det er også viktig at forbrukerne har mulighet til å benytte en tjeneste uten samtidig å måtte akseptere at virksomheter som tjenesteleverandøren samarbeider med også kan samle inn og bruke opplysningene til andre formål.

Hvis det oppstår usikkerhet blant forbrukerne knyttet til hvordan selskaper samler inn og bruker deres opplysninger, kan dette i verste fall føre til svekket tillit til nye betalingstjenester og til personaliserte forsikringsprodukter.

Vanskelig å sammenligne tjenester

En følge av at aktørbildet blir mer uoversiktlig og komplekst, er at det blir vanskeligere å sammenligne pris og kvalitet på tjenestene[47]. Det vil komme flere aktører på markedet som tilbyr gratis tjenester, i bytte mot tilgang til personopplysninger. Mange nye fintech-tjenester vil hente inntjeningen fra verdiøkende tjenester. Det vil for eksempel innebære at tjenesten, i tillegg til å levere en betalingstjeneste, også samler inn opplysninger fra brukeren. Opplysningene vil benyttes til målrettet markedsføring og tilbud på produkter.

Betalingstjenester vil også kunne inngå samarbeid med aktører i handelsnæringen, og i bytte mot gratis betalingstjeneste få kundeopplysninger i retur. Andre aktører vil ta betalt i form av gebyr. Det blir utfordrende for forbrukeren å vurdere pris og kvalitet på tjenester. Personopplysninger vil for mange fremstå som et skjult betalingsmiddel.

Økt sårbarhet for cyberangrep

Med PSD2 blir banker pålagt å åpne opp sin infrastruktur for tredjeparter som ønsker å tilby betalings- og kontoinformasjonstjenester. I de fleste tilfellene vil bankene tilby API-er for tredjepartene slik at de kan utføre tjenester på vegne av kunden. Dette vil åpne opp en større angrepsflate for cyberkriminelle, ved at bankene ikke lenger kan skjule sine systemer bak brannmurer på samme måte som tidligere.

Tradisjonelt har API-er vært brukt til såkalt «trusted» virksomhet-til-virksomhet-kommunikasjon, og det har ikke vært etablert like sterke sikkerhetsmekanismer som for løsninger ut mot internett og forbruker. Ved utvikling av nye API-er blir det viktig at bankene bygger inn robuste sikkerhetsmekanismer, og at de baserer seg på at dette er en kommunikasjonskanal bankene i utgangspunktet ikke har tillitt til.[48]

Banker tilhører en bransje som har vært særlig opptatt av risikostyring og informasjonssikkerhet. Med PSD2 vil det komme mange flere aktører som skal behandle person-opplysninger, kontoinformasjon og transaksjonsdata. Dette vil ofte være nyetablerte og små selskaper som potensielt ikke setter de samme kravene til sikkerhet som de tradisjonelle aktørene. Informasjon som tidligere har vært håndtert av noen få, blir nå delt med mange. Det vil være er en risiko for at nye aktører kan bli et sårbart punkt og en vei inn for cyberkriminelle.

Håndtering av sikker identifisering

PSD2 skal legge til rette for innovasjon og konkurranse innen betalingstjenester gjennom regulert tilgang til betalingskontoer. Samtidig stilles det krav til aktørene slik at dette kan skje på en måte som ivaretar sikkerheten i betalingssystemet. Flere sentrale sikkerhetskrav er beskrevet i et utkast til regulatorisk teknisk standard fra European Banking Authority (EBA)[49].

I standarden står det blant annet at kunden må autentisere seg med minimum to uavhengige elementer. Disse kan være noe bare kunden vet (for eksempel en PIN-kode), noe bare kunden er i besittelse av (for eksempel en kodebrikke) og noe bare brukeren er (for eksempel et fingeravtrykk). Det stilles også krav til å sikre kundens personlige sikkerhetsinformasjon mot brudd på konfidensialitet og integritet.

Av praktiske hensyn er det er gjort enkelte unntak fra kravet om sterk autentisering, blant annet ved lave beløp og for transaksjoner med lav risiko. For å gjøre unntak må tilbydere av betalingstjenester gjennomføre en risiko-vurdering i sanntid, basert på en rekke faktorer slik at de evner å oppdage og forhindre forsøk på svindel.

Det kreves at tilbyderne av betalingstjenester må legitimere seg med kvalifiserte sertifikater overfor kontotilbyder før det gis tilgang til å utføre tjenester på vegne av kunden. All kommunikasjon mellom partene som går over internett må beskyttes med bruk av sterk kryptering. Implementerte sikkerhetstiltak skal periodisk

[47] Norges bank, «Finansiell infrastruktur», 2017, http://static.norges-bank.no/contentassets/0af5e6ca88d54c7ca6ab9cd8b44257c8/finansiell_infrastruktur_2017.pdf?v=05/18/2017145640&ft=.pdf

[48] Accenture, «PSD2 & Open Banking – Security and Fraud Impacts on Banks», 2017, https://www.accenture.com/t20170106T040658Z__w__/us-en/_acnmedia/PDF-40/Accenture-PSD2-Open-Banking-Security-Fraud-Impacts.pdf

[49] Ibid.

testes, evalueres og revideres av kompetente interne eller eksterne revisorer.

Forbud mot «screen scraping» i PSD2

Screen scraping er en metode som benyttes av tilbydere av betalingstjenester for å gjennomføre betalinger direkte fra kundens bankkonto. Dette skjer ved at kunden først gir sine passord og koder til tilbyderen av betalingstjenesten. Tilbyderen går deretter inn i kundens nettbank og initierer betalinger fra kundens konto.

I Norge ble det oppmerksomhet om screen scraping da enkelte norske banker sperret mot bruk av metoden for det svenske betalingsselskapet Trustly. Bankene, BankID Norge og Finans Norge, mente at sikkerheten i BankID undergraves når brukeren må oppgi sine hemmelige koder til en tredjepart. For å ivareta og opprettholde BankID som en sikker identifikasjon og for å forhindre ID-tyveri, bedrageri og annet misbruk, skal ikke kunden dele sine hemmeligheter med noen.

I tillegg til sikkerhetsutfordringene, påpekte de at en slik tilgang vil føre til at tredjeparten også får mulighet til å se hele kundeforholdet i nettbanken, ikke bare å gjennomføre betalinger. BankID brukes samtidig for tilgang til andre samfunnsviktige tjenester med sensitive personopplysninger.

Etter en klage fra Trustly har EFTA Surveillance Authority (ESA) åpnet undersøkelse mot Finans Norge, BankID Norge og enkelte norske banker for å avklare om konkurransereglene er brutt.[50]

EBAs utkast til regulatorisk teknisk standard, legger opp til bruk av dedikerte grensesnitt (API-er), samt at screen scraping blir forbudt under PSD2. Forbudet har møtt motstand fra fintech-bransjen som mener det vil medføre risiko for deres mulighet til å utføre tjenester dersom bankenes grensesnitt blir utilgjengelig.

EU-kommisjonen har kommet med et forslag om å utvide standarden, slik at den tillater screen scraping som en siste mulighet dersom bankens dedikerte grensesnitt er utilgjengelig. EBA er kritisk til EU-kommisjonens forslag, og har foreslått andre utvidelser som skal sikre tilgjengeligheten til bankenes dedikerte grensesnitt.[51] Det er fortsatt uavklart hva som blir den endelige reguleringen på dette området.

Svak sikkerhet i smarte ting

Forsikringsselskapene ser nye muligheter i å bruke personopplysninger til å levere personaliserte forsikringsprodukter. I stadig større grad tar vi i bruk armbånd, sensorer og andre enheter som samler og deler informasjon om alt fra helsen vår, til boligen vi bor i og bilen vi kjører. Mange av produktene har også smart-funksjonalitet som kan hjelpe oss til å styre deler av livet vårt og varsle om hendelser. Felles for de fleste er at de er tilkoblet et nettverk for styring og overføring av informasjon, såkalte Internet of Things (IoT). Denne tilkobling kan potensielt også være en vei inn for aktører med onde hensikter, enten de ønsker å hente ut opplysninger eller manipulere produktet til å gjøre spesifikke handlinger.

Det finnes mange eksempler på dårlig sikkerhet i IoT-produkter. I 2015 demonstrerte to forskere hvordan de klarte å ta full kontroll over en moderne bil ved å utnytte flere svakheter i bilens elektroniske systemer.[52] De kunne blant annet kontrollere rattet, skru av motoren og koble ut bilens bremsesystem - alt over en trådløs forbindelse og uten å være i nærheten av bilen.

I Norge fikk tilsvarende sikkerhetsutfordringer mye omtale når Forbrukerrådet testet GPS-klokker for barn.[53] GPS-klokkene fungerer i hovedsak som en smarttelefon som kommuniserer med foreldrene via en app. Foreldrene kan blant annet kommunisere med barnet og spore barnas lokasjon. Testen avdekket at det var mulig for uvedkommende å få tilgang til andre brukeres opplysninger. Med enkle grep kunne fremmede også ta kontroll over klokkene for å spore hvor barnet beveget seg, gi inntrykk av at barnet var et annet sted, eller kommunisere med barnet.

Det er en stor utfordring at sikkerhet ofte er en ettertanke ved utvikling av IoT-produkter. Usikre produkter kan medføre store konsekvenser for personvernet, og i verste fall være en fare for enkeltpersoners fysiske sikkerhet. Det er derfor viktig at forsikringsselskapene gjør nødvendige risikovurderinger før de innleder samarbeid med leverandører av IoT-produkter og at de setter strenge krav til samarbeidspartnerne sine om å levere trygge produkter.

---

50 Finans Norge, «ESA-sak angår sikkerheten i BankID», 26.10.2016, https://www.finansnorge.no/aktuelt/nyheter/2016/10/esa-sak-angar-sikkerheten-i-bankid/

51 EBA European Banking Authority, «EBA opinion on EC proposed amendments to RTS on SCA and CSC under PSD2», 29.06.2017, http://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf

52 Miller, Charlie og Chris Valasek, «Remote Exploitation of an Unaltered Passenger Vehicle», 2015, http://illmatics.com/Remote%20Car%20Hacking.pdf

53 Forbrukerrådet, «Elendig sikkerhet i GPS klokker for barn«, 18.10.2017, https://www.forbrukerradet.no/siste-nytt/elendig-sikkerhet-i-smartklokker-for-barn/

Endrer vi atferd når noen ser oss over skulderen?

Når alt vi gjør på nettet, i butikken, i bilen, i hjemmet eller når vi trener kan fanges opp, selges videre, analyseres og brukes til å levere persontilpassede tjenester, kan dette påvirke vår oppførsel. Det blir vanskelig å ha oversikt over hvem som ser deg over skuldra og som har tilgang til opplysninger om deg.

Når tjenester baseres på data om oss, kan det tenkes at mange vil endre atferd for å få en mer fordelaktig tjeneste. Man kan også tenke seg at noen unnlater å gjøre eller si ting som vil slå dårlig ut. Begrepet «nedkjølingseffekt» brukes vanligvis om former for selvsensur eller å legge bånd på seg. Eksempler på dette kan være at du lar være å ytre deg, ytrer deg mer konformt eller lar være å gjøre noe helt legitimt som du ellers ville gjort.

Begrepet brukes også når du lar være å si eller gjøre noe fordi du frykter at det du foretar deg kan spores og få konsekvenser for deg i fremtiden. Det kan for eksempel være at du unngår å bruke betalingsappen du vanligvis bruker når du kjøper medisin på apoteket, fordi du frykter for hvordan disse opplysningene kan brukes senere.

En livsforsikring som krever at forsikringstakeren går et visst antall skritt hver dag, kan oppleves som et press til å bevege seg mer. Dette vil kanskje av mange oppfattes som et dytt i riktig retning. Men hvis boksen i bilen registrerer hvor du kjører, og du ikke føler at du kan bevege deg fritt uten å bli overvåket, er det problematisk for din integritet og handlingsfrihet.

Nye regler for behandling av personopplysninger

I 2016 vedtok EU som tidligere nevnt en ny personvern-forordning som vil erstatte personverndirektivet (på engelsk General Data Protection Regulation – forkortet GDPR). Forordningen skal gjøres til norsk rett gjennom en ny personopplysningslov.

Forordningen bygger i stor grad på direktivet, men det både utvider og forsterker reguleringen. Den handler om personopplysningsvern (se faktaboks).

Regelverket er laget for å beskytte individets grunnleggende friheter og rettigheter ved behandling av personopplysninger om vedkommende. Samtidig er reglene også laget for å legge til rette for fri flyt av personopplysninger innenfor det indre markedet. Tanken er at lik standard for personopplysningsvern skal medvirke til at personopplysninger trygt kan overføres frem og tilbake over landegrensene, noe som vil bidra til utviklingen av det indre markedet.

Slik sett kan man si at forordningen vil skape et viktig rammeverk for konkurransen innenfor EØS-området. Alle virksomheter som driver innenfor finans- og forsikringsmarkedet i EØS, må behandle person-opplysninger i samsvar med de samme reglene, med de skrankene og mulighetene det gir. Reglene gjelder også for virksomheter som ikke er etablert i EØS-området, så lenge personopplysninger behandles i sammenheng med at man tilbyr varer eller tjenester til EØS-borgere.

Nedenfor gir vi en kort oversikt over noen av endringene forordningen fører med seg.

§ Personopplysningsvern

Personopplysningsvern kan brukes som det norske ordet på «data protection». Gjennom de senere årene har det, særlig innenfor EU, vokst frem et skille mellom retten til privatliv («right to privacy» eller «private life») og retten til personopplysningsvern («right to data protection»). Begge anses som grunnleggende rettigheter for individet.

Selv om disse rettighetene henger nært sammen, er de ikke identiske. I Norge er det tatt til orde for å begrepsmessig skille mellom personvern og personopplysningsvern for å holde tritt med den internasjonale utviklingen og for mer nyansert forståelse.

(Se «NOU 2009:1 Individ og integritet – Personvern i det digitale samfunnet», kapittel 4.1.5, https://www.regjeringen.no/no/dokumenter/nou-2009-1/id542049/)

Mer ansvar til virksomhetene

I forordningen går man i all hovedsak bort fra dagens melde- og konsesjonsplikt. Det vil ikke lenger være nødvendig å melde fra eller søke om konsesjon for å kunne behandle personopplysninger.

Forordningen legger opp til at den som behandler personopplysninger må vise ansvarlighet. Det er understreket i artikkel 5 nr. 2 at den behandlings-ansvarlige er ansvarlig for og skal kunne vise at han opptrer i samsvar med de grunnleggende prinsippene som styrer all behandling av personopplysninger.

Det er også lagt systematiske plikter på den behandlings-ansvarlige, slik som generell interkontroll og mer spesifikke plikter knyttet til vurdering av personvernkonsekvenser, forhåndsdrøfting med Datatilsynet og innebygd personvern. Det å opptre i samsvar med systempliktene skal bidra til at den behandlingsansvarlige overholder reglene for behandling av personopplysninger.

Forordningen legger også opp til at virksomheter kan utvikle bransjestandarder/atferdsnormer og sertifiserings-ordninger (artikkel 40-43). Disse mulighetene gir anledning til å vise ansvarlighet ved at man er med på sette standarder for et velutviklet og fungerende personopplysningsvern i praksis.

Det å være ansvarlig innebærer også at man kan bli holdt ansvarlig. Den som misligholder sitt ansvar kan for eksempel risikere store overtredelsesgebyr.

Skjerpet krav til samtykke

Samtykke fra den registrerte (den det behandles opplysninger om) gir rettslig grunnlag for å behandle personopplysninger. Slik er det i dag, og slik vil det være etter at forordningen trer i kraft. Grunnen til dette er ganske opplagt ettersom samtykke gjenspeiler den private autonomi – retten til å få bestemme selv over seg og sitt.

Samtykke er slik sett et uttrykk for respekt for den enkeltes frie vilje og selvbestemmelse. Det er respekten for denne som gir legitimitet til behandlingen – som gjør den lovlig.

I praksis har man sett en tendens til at samtykke er benyttet på måter som undergraver legitimiteten. Det kan for eksempel være at den registrerte ikke har noe annet valg enn å samtykke, eller at samtykke gis stilltiende eller passivt. Hva man samtykker til kan også være uklart.

Med forordningen kommer det noen viktige presiseringer:

Samtykke er i forordningen definert som en **«frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende»** (artikkel 4 nr. 11).

Her kommer det frem at samtykke må komme til uttrykk ved en erklæring eller annen tydelig bekreftelse. Et stilltiende samtykke eller passivitet kan ikke aksepteres som et uttrykk for samtykke. Dette kan ses i sammenheng med artikkel 7 nr.1 som krever at **den behandlingsansvarlige må kunne dokumentere at samtykke er gitt**.

Dersom samtykke gis i forbindelse med en skriftlig erklæring som også gjelder andre forhold, for eksempel i forbindelse med inngåelse av en avtale som regulerer et forsikringsavtaleforhold, må **samtykke til behandling av personopplysninger skilles klart og tydelig fra det øvrige innholdet i erklæringen** (artikkel 7 nr. 2). Enkelt sagt kan man ikke bake et samtykke inn i lang tekst som handler om en rekke forhold ved siden av det som gjelder samtykke til visse behandlinger. Spørsmålet om man kan få en tillatelse til å behandle ulike person-opplysninger til nærmere bestemte formål, må stilles særskilt og atskilt fra andre forhold.

Hvis det er snakk om gi samtykke til forskjellige typer behandlinger, for eksempel til forskjellige formål, må den registrerte få **anledning til å gi separate samtykker**. Man kan altså ikke gi valget mellom å samtykke til alt eller ingenting. Man må gi større grad av valgfrihet – man kan velge å si ja til noe og nei til andre ting.

Videre må **frivilligheten i et samtykke være reell**. I kommersielle sammenhenger vil det normalt ikke være anledning til å stille som betingelse for å kunne inngå en avtale eller bruke en tjeneste, at den registrerte må samtykke til behandling av personopplysninger som ikke er nødvendig for å gjennomføre avtalen/yte tjenesten (artikkel 7 nr. 4 og fortalen punkt 43).

Slike «take it or leave it-løsninger», hvor kunden må samtykke til behandlinger av opplysninger som ikke er nødvendige[54], fører med seg et press på å akseptere behandlinger man ellers ikke ville ha akseptert. Det undergraver den frie viljen og den personlige autonomien som er selve kjernen i samtykke.

§ Mer om samtykke

I forordningens fortale punkt 40 står det at en behandling av personopplysninger skal anses lovlig når den enten baserer seg på samtykke eller på annet legitimt grunnlag fastsatt i loven (enten forordningen selv eller nasjonal lov som forordningen viser til). Felles for disse andre legitime grunnlagene er at det da foreligger grunner til i større eller mindre grad å innskrenke selvbestemmelsesretten.

Fortalen punkt 43 sier at det er presumsjon for at samtykke ikke er frivillig dersom den registrerte ikke kan gi separate samtykker.

(Forordningens fortale er ikke juridisk bindende, men forklarer artiklenes innhold.)

Dataportabilitet

Med forordningen får vi en ny rettighet, nemlig retten til dataportabilitet (artikkel 20).[55]

Dette er en rettighet som gir den enkelte rett til å få sine personopplysninger utlevert på et strukturert, vanlig brukt og maskinlesbart format, og ta med seg disse dataene til en annen behandlingsansvarlig. Der det er teknisk mulig

[54] Begrepet 'nødvendig' skal tolkes strengt, se Article 29 Working Party, «Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC».

Article 29 Working Party (Art. 29 WP) er den øverste rådgivende forsamlingen for EU-kommisjonen i spørsmål om personvern og informasjons-sikkerhet. På deres nettside finnes alle deres veiledninger, opinions med mer: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[55] Art. 29 WP har laget en veileder om denne rettigheten, «Guidelines on the right to 'data portability'».

kan den registrerte kreve at opplysningene overføres direkte fra en behandlingsansvarlig til en annen.

Dataportabilitet er først og fremst begrunnet i hensynet til den registrertes kontroll med egne personopplysninger. Meningen er å styrke muligheten til å bestemme over sine egne data. For eksempel kan dataportabilitet bidra til at det blir lettere å skifte leverandør av tjenester ved at man kan ta med seg dataene sine. Dataportabilitet motvirker at man blir låst fast til én leverandør.

Dataportabilitet gir også muligheter for bruk av personopplysninger på tvers mellom selskaper, med den registrertes samtykke. Det kan bidra til innovasjon og utvikling av nye tjenester. Innenfor forsikring kan dataportabilitet for eksempel gjøre at kunden kan ta med sine personopplysninger over til et annet selskap for å høre om de kan gi et bedre tilbud.

Overfor banker vil for eksempel de nye konto-informasjonstjenestene som PSD2 direktivet legger til rette for, basere seg på en form for dataportabilitet. Med kundens samtykke må banken levere ut konto-opplysninger til en tredjepart, som igjen bruker disse for å gi en kontoinformasjonstjeneste til kunden. I motsetning til den generelle portabilitetsregelen i forordningen har banken etter PSD2 plikt til å legge til rette for overføring av data direkte til tredjepart.

Automatiserte avgjørelser

I forordningen finner vi også særskilte regler om automatiserte avgjørelser (artikkel 22).[56] Med automatisert avgjørelse menes en avgjørelse som utelukkende baserer seg på automatisert behandling av personopplysninger. Dette kan inkludere profilering.

§ Profilering

Med profilering menes at man behandler person-opplysninger for å vurdere, analysere eller forutsi visse personlige aspekter ved personer. Det kan særlig dreie seg om en persons arbeidsprestasjoner, økonomiske situasjon, helse, personlig preferanser, interesser, pålitelighet, atferd, lokasjon eller bevegelser.

(Se forordningen artikkel 4 nr. 4)

Avgjørelsen må ha rettslig virkning for personen, eller på tilsvarende vis være egnet til å ha betydelig påvirkning for å være omfattet av reglene om automatiserte avgjørelser.

I utgangspunktet har enhver person rett til å *ikke* bli gjenstand for en automatisert avgjørelse. Art. 29 WP har så langt lagt til grunn at dette i praksis er et uttrykk for et forbud. Det å bruke helautomatiserte avgjørelser er imidlertid lov i enkelte tilfeller. Dette gjelder der hvor:

- det er nødvendig for å inngå eller gjennomføre en avtale mellom den behandlingsansvarlige og den registrerte, eller
- det er tillatt i EU-lovgivningen eller nasjonal rett som sørger for at individenes grunnleggende interesser blir ivaretatt, eller
- den registrerte har gitt et eksplisitt samtykke

Fordi automatiserte avgjørelser kan ha stor betydning for den det gjelder, er det viktig å treffe tiltak for å sikre en rettferdig prosess.

Blant annet må avgjørelsen kunne forklares på en meningsfull måte – det må være gjennomsiktighet.[57] Den enkelte må settes i stand til å forstå **hvilke** opplysninger som er brukt og **hvorfor** avgjørelsen ble som den ble.

Det er også viktig at den enkelte får anledning til å protestere på avgjørelsen og si sin mening (artikkel 22 nr. 3). For eksempel kan det være at avgjørelsen er truffet på basis av opplysninger som ikke er helt korrekte eller de er ufullstendige, noe som kan gi grunnlag for en fornyet vurdering og et annet resultat. Man må også kunne tilby at et menneske ser på saken.

Rett til å protestere

Et viktig hensyn bak reglene om behandling av person-opplysninger er hver enkelt sin mulighet til å ha kontroll og innflytelse på om og hvordan opplysninger om en selv blir behandlet. Også der det behandles person-opplysninger uten samtykke, er det av sentral betydning at den enkelte, etter omstendighetene, har anledning til å komme til orde.

I forordningen er det gitt regler som sikrer en rett til å protestere på behandling av personopplysninger (artikkel 21).[58] For det første har man rett til å protestere der personopplysninger behandles fordi det er nødvendig

- for å ivareta en oppgave i samfunnets interesse
- for å utøve offentlig myndighet, eller

[56] Art. 29 WP har utarbeidet en veiledning om automatiserte avgjørelser, «Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, wp251»

[57] Se artikkel 13 nr. 2 (f), 14 nr. 2 (g), 15 nr. 1 (h) og fortalen punkt 71.

[58] Bestemmelsen bygger på personverndirektivet artikkel 14. Denne bestemmelsen ble ikke gjennomført eksplisitt i den norske personopplysningsloven.

- for å ivareta berettigede interesser som ikke overstyres av den registrertes interesser og grunnleggende rettigheter og friheter

Felles for disse tilfellene er at dette er **behandlinger som i utgangspunktet er lovlige å gjøre uten samtykke** (artikkel 6 bokstav e og f). Loven har her begrenset selvbestemmelsesretten ved å gjøre behandlingen tillatt uten samtykke.

Retten til å protestere kommer da inn som en garanti for at den enkelte, basert på grunner knyttet til hans eller hennes situasjon, likevel skal få en viss medbestemmelse.

Dersom den registrerte protesterer, må behandlingen av personopplysninger opphøre, med mindre den behandlingsansvarlige kan påvise at det faktisk er tungtveiende legitime interesser i favør av behandlingen. Det kan være interesser som må gå foran, eller at behandlingen er nødvendig for å kunne etablere, gjøre gjeldende eller forsvare et rettskrav.

For det andre har man rett til å protestere dersom personopplysninger behandles til **direkte markeds-føringsformål**. Denne retten er ubetinget (det er nok å komme med protesten) og behandlingen til dette formålet må stanse. Her er det viktig å ikke blande sammen retten til å protestere med kravet til rettslig grunnlag for i det hele tatt å kunne behandle personopplysninger til direkte markedsføringsformål. At man har en ubetinget rett til å protestere på denne behandlingen, betyr ikke at behandling av personopplysninger til dette formålet alltid kan skje uten forutgående samtykke. Hvorvidt behandlingen krever forutgående samtykke krever en konkret vurdering hvor blant annet art og omfang av personopplysningene man ønsker å behandle, har betydning.

For det tredje er det adgang til å protestere på **behandling av personopplysninger til vitenskapelige eller historiske forskningsformål eller statiske formål**. Dette gjelder med mindre behandlingen er nødvendig for å gjennomføre en oppgave i allmenhetens interesse.

Vurdering av personvernkonsekvenser

Forordningen stiller krav om at man gjennomfører vurdering av personvernkonsekvenser (Data Protection Impact Assesment – DPIA) *før* man går i gang med behandling av personopplysninger (artikkel 35).[59]

Det å foreta nøye overveielser og analyser før man behandler personopplysninger er viktig for å kunne ha kontroll over de utfordringene og problemstillingene som en behandling av personopplysninger kan føre med seg, og det er sentralt for å kunne vise at man som ansvarlig opptrer i samsvar med reglene. Særlig ved bruk av ny teknologi kan det være grunn til å gjennomføre en DPIA.

En DPIA er ikke nødvendig i alle sammenhenger hvor det skal behandles personopplysninger. Men, den skal gjennomføres i tilfeller hvor det er trolig at behandlingen «vil medføre en høy risiko for fysiske personers friheter og rettigheter». Hovedpoenget med dette er man særlig skal fremheve behandlinger som det er grunn til å tro at kan være problematiske. Dette betyr ikke at behandlinger av personopplysninger som *ikke* medfører høy risiko kan gjennomføres uten noen vurdering eller planlegging. Også slik behandling må skje under vanlige forpliktelser til internkontroll og så videre, og man må ha kontroll på at behandlingen skjer i samsvar med og innenfor lovens krav. Men for den type behandling som trolig vil medføre høy risiko for grunnleggende friheter og rettigheter, skal det foretas særskilte analyser og vurderinger før man går videre.

Hvis en virksomhet for eksempel planlegger å innføre automatiserte avgjørelser i forbindelse med lånesøknader eller forsikringsoppgjør, kan det være grunn til å tro at det kan føre til avslag eller forskjellsbehandling som den enkelte kan oppleve som urimelig og vanskelig å forstå. Eller hvis det for eksempel skal behandles personopplysninger for å lage personprofiler, vil det kunne medføre høy risiko for at analysen av dataene gir innsikt i forhold som er private – forhold som den enkelte kan oppleve som en invadering av privatlivet.

At det foreligger høy risiko er ikke det samme som at det er i strid med loven, eller at det er stor sannsynlighet for at man bryter loven. Poenget er at høy risiko betyr skjerpet krav til aktsomhet, og at situasjonen må analyseres og vurderes nøyere. Som ledd i dette må det da vurderes mulige tiltak som vil avhjelpe de utfordringene (risikofaktorene) som er identifisert. Utfallet av dette arbeidet – DPISA – kan være at det ikke (lenger) foreligger slik høy risiko som man innledningsvis la til grunn.

Dersom det etter nødvendige vurderinger og undersøkelse av mulige tiltak som kan avhjelpe risikoen, fremdeles er

[59] Art. 29 WP har laget en veileder om DPIA og gjennomføring av dette, «Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01 pdf»

grunn til å tro at det er høy risiko, skal saken legges frem for Datatilsynet til vurdering.

Innebygd personvern

Innebygd personvern, og personvern som standard-innstilling, bygger på tanken om at personopplysnings-vern i praksis kan implementeres og integreres gjennom tekniske og organisatoriske tiltak.[60]

Gjennom god design fra begynnelsen av i de løsningene som brukes for å behandle personopplysninger, vil reglene for behandling av personopplysninger lettere kunne etterleves.

Med forordningen gjelder det krav til å bygge personvern inn i de teknologiske hjelpemidlene som virksomhetene bruker for å behandle personopplysninger (artikkel 25). Dette innebærer blant annet at løsningene som standard bare skal samle inn opplysninger som er nødvendig for formålet, at opplysningene slettes automatisk når formålet med behandlingen av opplysningene er utført og at løsningen har tekniske tiltak som sikrer at tilgangen til opplysningene ikke er større enn nødvendig.

I personvernforordningen oppfordres det til å utvikle sertifiseringsmekanismer som påviser at virksomhetene overholder kravene som stilles til innebygd personvern.

Er PSD2 og forordningen godt harmonisert?

EUs reviderte betalingstjenestedirektiv PSD2 trer som nevnt kraft i januar 2018. Direktivet regulerer ulike former for betalingstjenester, men det er særlig to nye former for betalingstjenester som direktivet åpner for, og som er ventet å endre markedet. Det betalingsinitierings-tjenester og kontoinformasjonstjenester (se s. 4). Dette er tredjepartstjenester som en kunde kan bruke for å foreta betaling rett fra sin konto eller for å få tilgang til sin kontoinformasjon.

Bruken av tredjepartstjenester vil innebære behandling av personopplysninger, og det kan reises spørsmål om forholdet mellom reglene i PSD2 og reglene i personvernforordningen er godt harmonisert?[61]

I utgangspunktet synes begge regelverkene å bygge på samme grunntanke – kundens (den registrertes) selvbestemmelsesrett skal styrkes. Reglene i PSD2 har klare forgreininger til forordningens regler om dataportabilitet, samt at kunden gjennom å gi sitt samtykke får anledning til i større grad å bestemme hvordan hans eller hennes data skal behandles.

Samtidig synes det som at det lett kan oppstå uklarheter, for eksempel når det kommer til samtykke. PSD2 krever at betalingstjenestetilbyderne behandler personopplysninger på basis av kundens samtykke (PSD2 artikkel 94 nr. 2). Det er imidlertid ikke helt klart hvem skal være ansvarlig for å innhente kundens samtykke; tredjeparten, banken eller begge?

I henhold til personvernforordningen vil både banken og tredjeparten hver for seg være behandlingsansvarlige, og begge må forsikre seg om at de har kundens samtykke til behandling av personopplysninger. Det kan bety at det ikke er tilstrekkelig at bare tredjeparten får samtykke fra kunden, men at også banken må få tilstrekkelig bekreftelse fra kunden, inkludert hva kunden ønsker at banken skal gjøre[62].

[60] Datatilsynet har laget en veileder om innebygd personvern som er tilgjengelig på vår nettside: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/

[61] PSD2 artikkel 94 nr. 1 forutsetter at all behandling av personopplysninger for de formål PSD2 har, skal skje i samsvar med personverndirektivet. Det henvises her til et regelverk som er i ferd med å gå ut på dato, men fra mai 2018 må bestemmelsen leses som en henvisning til personvernforordningen, se forordningen artikkel 94 nr. 2.

[62] I Storbritannia er det utviklet en Open Banking API-standard som baserer seg på en prosess med innhenting og bekreftelse på samtykke: https://www.openbanking.org.uk/wpcore/wp-content/uploads/2017/10/Consent-Model-Guidelines-Part-1-Implementation.pdf

Oppsummering og anbefalinger

Banker og forsikringsselskaper har i dag høy tillitt. Forbrukerne forventer at finansielle tjenester er sikre og ivaretar personvernet på en god måte. I tiden fremover vil aktørbildet bli mer uoversiktlig. Flere aktører enn i dag vil behandle opplysninger om vår privatøkonomi. Det vil bli mer krevende for forbrukerne å holde oversikt over omfanget av personopplysninger de ulike aktørene samler inn og til hvilke formål de brukes. Folk anser opplysninger om sin privatøkonomi som svært beskyttelsesverdige. For aktører i finanssektoren vil derfor godt personvern kunne gjøres til et konkurransefortrinn.

Vi har her oppsummert noen punkter som leverandører av finansielle tjenester bør ta hensyn til for å ivareta kundenes personvern på en best mulig måte:

- **Personvern i hjertet av konsernet**

Personvern må forankres hos ledelsen. Det vil koste å lage tjenester med godt personvern, men det vil lønne seg i form av tillitt fra kundene. Virksomheter som ikke følger personvernregelverket risikerer betydelige kostnader, både ved gebyr for å ha brutt reglene og ved at de taper omdømme.

Etabler et etisk råd eller en komité hvor nye forretningsmodeller diskuteres før de sette ut i live. En slik komité kan også gi konsernledelsen innspill til hvordan personvernfremmende teknologi kan benyttes i nye forretningsmodeller og tjenester.

- **Åpenhet og gjennomsiktighet**

Lag løsninger som er åpne og gjennomsiktige. Fortell *hvilke* data som samles inn og *hvordan* de skal brukes, men prøv å gjør det enkelt og intuitivt. Lange personvernerklæringer er på ingen måte en garanti for god gjennomsiktighet. Bruk heller lagvis informasjon der kundene først blir presentert for en kortfattet oversikt, og så får mulighet til å gå inn i mer detaljerte forklaringer dersom de ønsker det.

Det er også lov å tenke kreativt. For eksempel kan forklaringer på hvordan personopplysninger behandles, presenteres ved hjelp av film eller animasjon istedenfor – eller i tillegg til – tekst.

Hvis dere benytter automatiserte avgjørelser, bruk løsninger som er åpne og transparente og som legger til rette for at beslutningene som systemet produserer kan forklares og overprøves. Foreta jevnlige revisjoner av algoritmene for å forsikre dere om at de automatiserte beslutningssystemene ikke produserer beslutninger som er urettferdige eller diskriminerende.

- **La kunden få velge**

Lag brukervennlige løsninger der kunden så langt som mulig kan velge hvilke opplysninger de vil dele og til hvilke formål de kan brukes. Lag gjerne valgpaneler for personvern (privacy dashboards) der det er hensiktsmessig.

- **Bruk personvernfremmende teknologi**

Profilering, automatisert behandling og persontilpassede tjenester medfører ofte behandling av personopplysninger i stor skala. Ledelsen må sikre at det settes av tilstrekkelige ressurser til innkjøp og programvareutvikling for å lage tjenester med innebygd personvern. Aktiv, god og innovativ bruk av innebygd personvern kan gi nye bank- og forsikringstjenester et konkurransemessig fortrinn, basert på den bærekraftige tilliten som godt personvern vil kunne skape, og ikke minst ivareta, i det lange løp.

- **Sertifisering og bransjenormer**

For å øke gjennomsiktigheten og overholdelsen av det nye personopplysningsregelverket, bør det oppmuntres til opprettelse av sertifiseringsmekanismer og personvernsegl og -merker, slik at de registrerte raskt kan vurdere nivået for vern av personopplysninger som relevante produkter og tjenester omfattes av.

Forsikringsselskaper, banker og fintech-selskaper bør også vurdere områder hvor det kan være formålstjenlig å utvikle bransjenormer (eksempelvis bransjenorm for betalingsinitieringstjenester og kontoinitieringstjenester, samt for personaliserte forsikringsprodukter).

- **Sårbarhet og risiko**

Ved utvikling av nye API-er blir det viktig at bankene gjør nødvendige risikovurderinger og bygger inn robuste sikkerhetsmekanismer. Nye aktører som skal behandle personopplysninger må gjøre egne vurderinger og har en selvstendig plikt til å ivareta personvernregelverkets krav til informasjonssikkerhet.

Det er viktig at forsikringsselskaper gjør nødvendige risikovurderinger før de innleder samarbeid med leverandører av Internet of Things-produkter, og at de stiller strenge krav til samarbeidspartnerne sine om å levere trygge produkter. For behandlinger som medfører høy risiko for personvernet, må aktørene også gjøre en vurdering av personvernkonsekvenser for å ivareta kravene i den nye personvernforordningen.

Referanseliste

Accenture, «Amplifyou. Technology for people. The Era of the Intelligent Insurer», 2017,
https://www.accenture.com/gb-en/_acnmedia/C6F35436B1B2461F84C6A766968B701C.pdf

Accenture, «PSD2 & Open Banking – Security and Fraud Impacts on Banks», 2017,
https://www.accenture.com/t20170106T040658Z__w__/us-en/_acnmedia/PDF-40/Accenture-PSD2-Open-Banking-Security-Fraud-Impacts.pdf

Aftenposten, «Alle bankene er snart med i Vipps», 11.10.2017,
https://www.aftenposten.no/okonomi/i/Pk2ko/Alle-bankene-er-snart-med-i-Vipps

Aftenposten, «Facebook har trolig milliardoverskudd i Norge - betalte under 500.000 kroner i skatt», 06.07.2017,
https://www.aftenposten.no/okonomi/i/jqOAA/Facebook-har-trolig-milliardoverskudd-i-Norge---betalte-under-500000-kroner-i-skatt

AXA, «AXA, Alibaba and Ant Financial Services announce global strategic partnership», 29.07.2016,
https://www.axa.com/en/newsroom/press-releases/axa-alibaba-ant-financial-services-announce-global-strategic-partnership

AXA, «AXA's Data Privacy Advisory Panel»,
https://www.axa.com/en/about-us/data-privacy

Blixrud, Katrine Berg og Ottesen, Christine Ask, «Personvern i finanssektoren», Gyldendal, Oslo, 2010

BigInsight, «Annual Report 2016», 2016

Capgemini, «Value-added services in insurance«, 2017,
https://www.capgemini.com/wp-content/uploads/2017/07/value_added_services_in_insurance_2017_2_web.pdf

Christl, Wolfie og Spiekermann, «Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy», Facultas, 2016

Christl, Wolfie, «Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions», Wien, 2017

CNNTech, «This startup uses battery life to determine credit scores», 24.08.2016
http://money.cnn.com/2016/08/24/technology/lenddo-smartphone-battery-loan/index.html

Dagens Næringsliv, «Gjensidige vil kaste ut konsulenter og hente inn «it-hoder», 21.04.2017,
https://www.dn.no/nyheter/2017/04/21/1152/Finans/gjensidige-vil-kaste-ut-konsulenter-og-hente-inn-it-hoder

Dagens Næringsliv, «Roboten gir lån hvis den får gode vibrasjoner fra kontoen din», 30.04.2017,
https://www.dn.no/nyheter/2017/04/30/1817/Privatokonomi/roboten-gir-lan-hvis-den-far-gode-vibrasjoner-fra-kontoen-din

Dagens Næringsliv, «Betaler regningen på syv sekunder med Facebook Messenger», 29.11.2017,
https://www.dn.no/nyheter/2017/11/29/0840/Finans/betaler-regningen-pa-syv-sekunder-med-facebook-messenger

Datatilsynet, «Big Data – personvernprinsipper under press», 2013,
https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/big-data_web.pdf

Datatilsynet, «Personvernundersøkelsen 2013/2014», 2014,
https://www.datatilsynet.no/globalassets/global/om-personvern/planer-strategier/personvernundersokelsen/samlerapport-personvernundersokelsen.pdf

Datatilsynet og Teknologirådet, «Tilstand og trender 2017», 2017,
https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/tilstand-og-trender-2017.pdf

EBA European Banking Authority, «EBA opinion on EC proposed amendments to RTS on SCA and CSC under PSD2», 29.06.2017,
http://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf

European Banking Authority, «Final report on draft RTS on SCA and CSC», 2017,
https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

E24, «Verdens største betalingsløsning lanseres i Norge – men ikke for nordmenn», 08.09.2017,
http://e24.no/naeringsliv/teknologi/verdens-stoerste-betalingsloesning-lanseres-i-norge-men-ikke-for-nordmenn/24133447

Finextra, «Starling releases Open API, talks up marketplace model», 2017,
https://www.finextra.com/newsarticle/30183/starling-releases-open-api-talks-up-marketplace-mode

Financial Times, «Insurance and the big data technology revolution», 24.02.2017,
https://www.ft.com/content/bb9f1ce8-f84b-11e6-bd4e-68d53499ed71

Financial Times, «Ten fintech start-ups that are causing a stir in insurance», 03.10.16,
https://www.ft.com/content/db833e5a-6eb1-11e6-a0c9-1365ce54b926

Financial Times, «Wearable technology: gathering data from tooth to toe», 21.11.2016,
https://www.ft.com/content/9b00b05c-70fe-11e6-a0c9-1365ce54b926

Finans Norge, «ESA-sak angår sikkerheten i BankID», 26.10.2016,
https://www.finansnorge.no/aktuelt/nyheter/2016/10/esa-sak-angar-sikkerheten-i-bankid/

Forbes, «Starbucks Holds More Cash Than Many Banks», 01.08.2016,
https://www.forbes.com/sites/niallmccarthy/2016/08/01/starbucks-holds-more-cash-than-many-banks-infographic/#5ca0d2ce231a

Forbrukerrådet, «Elendig sikkerhet i GPS klokker for barn», 18.10.2017,
https://www.forbrukerradet.no/siste-nytt/elendig-sikkerhet-i-smartklokker-for-barn/

GTNews, «False positives a growing headache», 08.10.15,
https://www.gtnews.com/articles/false-positives-a-growing-headache/

The Guardian, «Admiral to price car insurance based on Facebook posts», 02.11.2016,
https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts

The Guardian, «Facebook forces Admiral to pull plan to price car insurance based on posts», 02.11.2016,
https://www.theguardian.com/money/2016/nov/02/facebook-admiral-car-insurance-privacy-data

Kampanje, «Nordea og Vipps inngår samarbeid – konkurrent legger ned», 11.10.2017,
http://kampanje.com/tech/2017/10/nordea-og-vipps-inngar-samarbeid--konkurrent-legger-ned/

KPMG, «Meet EVA - the future face of the invisible bank», 2016,
https://home.kpmg.com/uk/en/home/insights/2016/10/meet-eva.html

Los Angeles Times, «Google starts tracking offline shopping — what you buy at stores in person», 23.05.2017,
http://www.latimes.com/business/technology/la-fi-tn-google-ads-tracking-20170523-story.html

Independent, «Swedish banks embrace artificial intelligence as a cure to closures», 31.07.17,
http://www.independent.co.uk/news/business/news/sweden-banks-robots-ai-artificial-intelligence-closures-financial-industry-online-digital-banking-a7868471.html

Information Commissioner's Office, «Big data, artificial intelligence, machine learning and data protection», 2017, https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/

McKinsey&Company, «The Age of Analytics: Competing in a Data-Driven World, desember», 2016, https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world

Miller, Charlie og Chris Valasek, «Remote Exploitation of an Unaltered Passenger Vehicle», 2015, http://illmatics.com/Remote%20Car%20Hacking.pdf

MIT Technology Review, «Why Insurance Companies Want to Subsidize Your Smart Home», 12.10.2016, https://www.technologyreview.com/s/602532/why-insurance-companies-want-to-subsidize-your-smart-home/

Mobgen/Accenture, «The Retail App: Ultimate Direct Link With The Customer», 2015, https://www.accenture.com/t20160708T043706__w__/us-en/_acnmedia/PDF-25/Accenture-Acquires-Mobgen-Expand-European-The-Retail-App.pdf

Norges Bank, Finansiell infrastruktur, 2017, http://static.norges-bank.no/contentassets/0af5e6ca88d54c7ca6ab9cd8b44257c8/finansiell_infrastruktur_2017.pdf?v=05/18/2017145640&ft=.pdf

Norges Bank, «Høringsuttalelse – utkast til regler tilsvarende det reviderte betalingstjenestedirektivet (PSD2) i norsk rett», 2017

PWC, «Customer centric banking. Aligning the GDPR and PSD II», 2017, https://www.pwc.co.uk/banking-capital-markets/assets/documents/customer-centric-banking-aligning-gdpr-psd-ii.pdf

Techcrunch, «Facebook Messenger now allows payments in its 30,000 chat bots», 12.09.2016, https://techcrunch.com/2016/09/12/messenger-bot-payments/

Techcrunch, «Facebook just secured an e-money license in Ireland, paving the way for Messenger payments in Europe», 07.12.2016, https://techcrunch.com/2016/12/07/facebook-just-secured-an-e-money-license-in-ireland-paving-way-for-messenger-payments-in-europe/

Techcrunch, «Watson Financial Services is born out of IBM's purchase of Promontory Financial Group», 29.09.2016, https://techcrunch.com/2016/09/29/watson-financial-services-is-born-out-of-ibms-purchase-of-promontory-financial-group/

TechinAsia, «Why Alipay is more than just the Chinese equivalent of PayPal», 03.08.2015, https://www.techinasia.com/talk/online-payment-provider-alipay-chinese-equivalent-paypal

Teknisk ukeblad, «Et halvt år med overvåking: Denne dingsen bekrefter mytene om unge sjåfører», 26.09.2017, https://www.tu.no/artikler/denne-dingsen-overvaker-bilisters-kjorestil-na-vil-de-bruke-kjoredataene-pa-helt-nye-omrader/408082

Universitetet i Tromsø, «UiT samarbeider med storbank om datanalyse», 10.06.2016, https://uit.no/om/enhet/aktuelt/nyhet?p_document_id=472218&p_dimension_id=88136

Wired, «Big data meets Big Brother as China moves to rate its citizens», 21.10.2017, http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

World Economic Forum, «The Future of Financial Services How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed», 2015, http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf

Besøksadresse:
Tollbugata 3, 0152 Oslo

Postadresse:
Postboks 8177 Dep.,
0034 Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no
twitter.com/datatilsynet