NTAES

Offentlig versjon

Rapport

Registermanipulasjon

Foto: Shutterstock

Nasjonalt tverretatlig analyse- og etterretningssenter

Sammendrag

Registermanipulasjon har alvorlige konsekvenser for offentlig sektor, det private næringslivet og privatpersoner. Tilliten trues, og manipulasjon medfører både direkte og indirekte økonomiske konsekvenser.

Registermanipulasjon foregår både som del av reelle aktiviteter, og som ren fiksjon. Det avdekkes i alt fra enkeltsaker til kriminelle nettverk. Med digitalisering av offentlig forvaltning danner data fra ulike etater grunnlag for prosesser som er helt eller delvis automatiserte. Samtidig flyttes kriminell aktivitet over i det digitale rom. Manipulerte data i registre og rapporteringer gir grunnlag for feil vedtak og beslutninger som gir kriminelle aktører økonomisk vinning.

Rapporten bygger i stor grad på analyser av verdikjeder som omfatter identitetsforvaltning, foretaksforvaltning, Skatteetatens og Navs forvaltningsansvar, samt finansnæringens ansvarsområder. Resultatene vurderes å ha overføringsverdi til andre områder.

NTAES vurderer at det er flere sårbarheter som hindrer en effektiv forebygging og bekjempelse av manipulasjon og tilknyttet kriminalitet. I rapporten trekkes følgende sårbarheter frem:

Manglende samfunnsperspektiv i forvaltning av registre og data oppstår når risikovurderinger gjøres ut fra én etats behov. Risiko for manipulering er ikke tilstrekkelig vurdert.

Brukervennlighet går foran alt når digitale systemer og forvaltningsprosesser effektiviseres, uten å ha tilstrekkelige kontrollmekanismer. Forenklingene gjør det også lettere å begå kriminalitet.

Mangelfull deling av informasjon for å vurdere pålitelighet i dataene. Informasjon som kunne gitt en bedre risikobasert tilnærming benyttes ikke. Terskelen for deling av mistanker er høy og hemmet av manuelle prosesser og manglende juridiske avklaringer.

Manglende retting gjør at uriktige opplysninger blir lagt til grunn ved saksbehandling i egen etat eller av andre. Retting av feil er ofte begrenset til egne fagsystem og rettes ikke i registrene som brukes av øvrig forvaltning.

Rapporten viser en uønsket utvikling som kan få svært alvorlige konsekvenser.

Innhold

Innledning **4**
Metode **5**
Situasjonsbilde **6**
Verdier 6
Digitalisering og forenkling 7
Registrene og etatene 8
Personvern og samfunnsvern – en vurdering 12
Registermanipulasjon som fenomen 13
Sårbarheter **17**
Manglende samfunnsperspektiv i etatenes risikovurderinger 17
Brukervennlighet går foran alt 18
Mangelfull deling mellom etatene 19
Manglende retting av feil 20
Lånebedrageri og tilknyttet kriminalitet 22
Vurderinger 24
Hovedvurderinger **25**

Dato	25.11.2024
Infostopp	09.08.2024
Antall sider, inkludert omslag	26

Innledning

NTAES har fått i oppdrag av Styringsgruppen for NTAES og a-krimsamarbeidet å utarbeide en risikovurdering som viser muligheter for manipulering av relevante registre.[1] Hypotesen er at digitalisering og tilrettelegging for enklere rapportering av opplysninger gir sårbarheter som muliggjør lovbrudd. Rapporten skal belyse potensialet for manipulering blant annet ved å beskrive modus, vurdere sårbarheter og konsekvenser. Formålet er å gi etatene i a-krimsamarbeidet et strategisk bilde av den potensielle risikoen ved registermanipulasjon. Regjeringens digitaliseringsstrategi forutsetter god datakvalitet i registre som benyttes som felleskomponenter i det offentlige.

I denne rapporten er hovedvekten lagt på registermanipulasjon knyttet til virksomheters opplysninger. Innhenting av informasjon har i hovedsak knyttet seg til virksomheters registreringer i registre der Brønnøysundregistrene er registereier, og Skatteetatens og Navs bruk av opplysninger gjennom a-ordningen. Mange av funnene i rapporten har imidlertid overføringsverdi til andre forvaltningsområder og registre.

Rapporten beskriver hvorfor god registerkvalitet er viktig i det norske velferdssamfunnet, og gir en kort gjennomgang av dagens situasjonsbilde med oversikt over relevante registre. Registermanipulasjon som fenomen blir forklart og ulike former for manipulering er satt i en sammenheng.

Hovedfunnene fra analysen er fire sårbarheter knyttet til registermanipulasjon. De fire sårbarhetene er:

- manglende samfunnsperspektiv i etatenes risikovurderinger
- brukervennlighet går foran alt
- mangelfull deling mellom etatene
- manglende retting av feil.

For å illustrere sårbarhetene som er avdekket gjennomgås modus for lånebedrageri. Det viser hvordan kriminelle utnytter sårbarheter i systemene for å oppnå vinning.

1 Oppdrag gitt april 2023.

Metode

Rapporten er basert på informasjon hentet fra følgende etater:

- Brønnøysundregistrene
- Nav
- Politiet
- Skatteetaten

Innhentingen har foregått skriftlig og gjennom intervjuer.

Det er innhentet og sammenstilt informasjon om personer og virksomheter fra Navs, politiets og Skatteetatens registre. Opplysningene er brukt for å belyse utvalgte hypoteser. NTAES har foretatt stikkprøver for å verifisere eller falsifisere funn fra analyser.

I tillegg er det brukt informasjon fra offentlige kilder og fra flere av etatenes fagsystemer.

Innhentingsperioden har vært fra februar til august 2024.

Foto: Shutterstock

Situasjonsbilde

Verdier

Den norske velferdsstaten er bygget på tillit mellom statlige institusjoner og befolkningen i stort. I Norge er denne formen for tillit høy, og å opprettholde dette tillitsbåndet anses som avgjørende for utviklingen av velferdsstaten og offentlig forvaltning. Et viktig bidrag til å opprettholde en høy grad av tillit til statlige institusjoner er et velfungerende statsapparat og en forvaltning som imøtekommer befolkningens behov og forventninger. Det er derfor avgjørende at etatene forvalter registre med høy grad av åpenhet, presisjon og nøyaktighet. Dette sikrer både personvern, kontroll over eierskap og virksomhet, samt riktige trygdeutbetalinger og beregning av skatt. Samlet fremstår god forvaltning som et insentiv for befolkningen og virksomheter å oppgi riktige opplysninger.[2]

Registermanipulasjon utfordrer tillitsbåndet mellom velferdsstaten og befolkningen blant annet på grunn av de alvorlige konsekvensene skatteunndragelser, urettmessig utbetalte trygdeytelser og bedragerier knyttet til lån og kreditt har.[3] I dag er omfanget av registermanipulasjon uviss, inkludert hvilke og hvor store økonomiske konsekvenser den har for offentlig og privat sektor samt enkeltindivider. Slik speiler registermanipulasjon det bredere feltet for økonomisk kriminalitet hvor det eksisterer store mørketall, og hvor arbeidet med å forebygge, bekjempe, avdekke og etterforske krever store ressurser for politiet og kontrolletatene. Arbeidet mot registermanipulasjon må tas på alvor da det, gjennom sin utbredelse og virkning, i ytterste konsekvens må forstås som en trussel mot velferdsstaten og etatenes verdisett om høy politisk tillit og tillit til statlige institusjoner.[4]

Å avdekke sårbarheter og potensielle årsakssammenhenger og scenarioer kan bidra til en mer effektiv og presis forvaltning.

2 Meld. St. 15 (2023–2024) Felles verdier – felles ansvar. Styrket innsats for forebygging og bekjempelse av økonomisk kriminalitet. Justis- og beredskapsdepartementet. Kapittel 9

3 Meld. St. 15 (2023–2024) Felles verdier – felles ansvar. Styrket innsats for forebygging og bekjempelse av økonomisk kriminalitet. Justis- og beredskapsdepartementet. Kapittel 9

4 Meld. St. 15 (2023–2024) Felles verdier – felles ansvar. Styrket innsats for forebygging og bekjempelse av økonomisk kriminalitet. Justis- og beredskapsdepartementet. Kapittel 9

Mulighetene for feil og økonomiske tap kan reduseres, med det resultat at høy tillit til velferdsstaten og statlige institusjoner fortsatt sikres. Motsetningen til et slikt tillitsbasert samfunn er et kontrollsamfunn, der det er omfattende rapporteringskrav, overvåking og rigid regelstyring. Dersom samfunnet går i en slik retning kan man se for seg en negativ spiral med en økning i manuelle kontroller, og med det økte kostnader i offentlig sektor.

Digitalisering og forenkling

Digitalisering skal bidra til en mer effektiv offentlig sektor, mer verdiskaping i næringslivet og ikke minst en enklere hverdag for folk flest.[5]

Det er mange grunner til å ønske mer digitalisering i samfunnet vårt. Noen stikkord er økt brukervennlighet, raskere saksbehandling, mer tilgjengelige tjenester, effektivisering, riktig utbetaling til riktig tid, samt bedre utnyttelse av velferdsstatens penger. Fra regjeringshold ligger digitaliseringsstrategien til grunn for utviklingen som skjer i de fleste offentlige etater. Målsettingen som er uttrykt fra regjeringen er at flere oppgaver skal løses digitalt, og offentlig sektor skal utnytte det potensialet som ligger i «deling og bruk av data til å lage brukervennlige tjenester, og for å bidra til verdiskapning i næringslivet»[6]. I Norge er utgangspunktet godt for å få dette til, med gode grunndataregistre, godt utbygd digital infrastruktur og høy digital kompetanse.

Regjeringen har seks innsatsområder i sin strategi som alle skal legge til rette for hovedmålet om en «enklere hverdag for innbyggere og næringsliv». Dette innebærer blant annet at forvaltning av informasjon og data, og flyt av data mellom ulike aktører, skal være god. Ønskede konsekvenser er for eksempel at det skal gå raskere å få saken sin behandlet, at utbetaling av ytelser skjer raskt, og at det er enklere for brukerne av systemene å sende en søknad.

I strategier, instrukser og styringsdokumenter fra regjerings- og departementsnivå gis det ikke tydelige føringer og krav til at systemene skal forhindre og avdekke kriminalitet. Brukervennlighet og forenkling prioriteres dermed først i digitaliseringsprosessene.

For å nå målsettingene om en enklere hverdag gjør myndighetene endringer i regelverk og rutiner. Et eksempel på dette er at små aksjeselskap kan velge at årsregnskapet ikke skal revideres.[7] Gjennom slike forenklinger blir opplysninger i mindre grad kontrollert av tredjepart.

En av forutsetningene for å oppnå målsettingene i digitaliseringsstrategien er blant annet god datakvalitet og deling av data mellom aktører. Forvaltning av opplysninger er spredt på mange ulike aktører, som har ulike formål knyttet til ansvaret som registereier. Dette har innvirkning på hvordan opplysningene i registrene blir innhentet, kontrollert og forvaltet.

5 Digitaliserings- og forvaltningsdepartementet. (2019). Én digital offentlig sektor. Digitaliseringsstrategi for offentlig sektor 2019–2025. https://www.regjeringen.no/no/tema/statlig-forvaltning/it-politikk/digitaliseringsstrategi-for-offentlig-sektor/id2612415/

6 Digitaliserings- og forvaltningsdepartementet. (2019). Én digital offentlig sektor. Digitaliseringsstrategi for offentlig sektor 2019–2025. https://www.regjeringen.no/no/tema/statlig-forvaltning/it-politikk/digitaliseringsstrategi-for-offentlig-sektor/id2612415/

7 Altinn. (2024). Må jeg ha revisor? https://info.altinn.no/starte-og-drive/regnskap-og-revisjon/ma-jeg-ha-revisor/

Spørsmålet som politiet og kontrolletatene nå stiller seg, er hvordan utviklingen mot stadig mer digitaliserte, forenklede og automatiserte løsninger vil ha innvirkning på kriminalitetsbildet.

I denne rapporten vil NTAES se nærmere på om det er sånn at digitalisering og tilrettelegging for enklere rapportering av opplysninger gir et potensiale for manipulering av opplysninger som rapporteres til det offentlige. Vi søker å belyse flere hypoteser knyttet til dette:

- Digitalisering og tilrettelegging for enklere rapportering av opplysninger muliggjør raskere og mer omfattende lovbrudd.
- Opplysninger knyttet til virksomheter manipuleres for å oppnå vinning.
- Kriminelle[8] utnytter sårbarheter i offentlige registre.
- Etatene utnytter ikke potensialet digitalisering gir.
- Manglende informasjonsutveksling hindrer forebygging og avdekking av lovbrudd.

Forvaltning av informasjon og registre er kompleks og omfatter mange ulike aktører. I denne rapporten er hovedvekten lagt på enhetsregisteret og a-ordningen, sammenhengen mellom disse, forvaltningen og bruken av opplysningene.

Registrene og etatene

NTAES har ingen klar definisjon på hva et register er, men forholder oss til at det er opplysninger myndighetene samler inn og systematiserer om befolkningen på individnivå og virksomhetsnivå. Opplysningene kan være manipulert for å oppnå en fordel en ellers ikke har. Under kommer en introduksjon av viktige registre i offentlig forvaltning, registre som er med på å avgjøre om det foreligger rettigheter og plikter både hos Nav og Skatteetaten.

Folkeregisteret er Norges sentrale personregister og er en nasjonal felleskomponent.[9] Det er viktig at Folkeregisteret opprettholder god datakvalitet og distribuerer korrekte opplysninger for resten av samfunnet, slik at rettigheter og plikter blir ivaretatt. Det er Skatteetaten som har behandlingsansvar for registeret jf. folkeregisterloven.[10]

Brønnøysundregistrene er en statlig forvaltningsetat underlagt Nærings- og fiskeridepartementet. Brønnøysundregistrene forvalter og driver 17 registre[11] i Norge. Det er viktig å merke seg at Brønnøysundregistrene ikke er en kontrolletat, men de påser blant annet at innholdet i en registermelding ikke er i strid med et idømt rettighetstap[12] og/eller en konkurskarantene. Under følger fire av registrene Brønnøysundregistrene har ansvar for og som treffer oppdragets verdikjede.

8 Personer som begår straffbare handlinger/lovbrudd uavhengig av om de er dømt.
9 Felleskomponenter defineres som komponenter i IT-løsninger som kan sambrukes eller gjenbrukes flere steder i offentlig sektor.
10 Folkeregisterloven. (2016). Lov om folkeregistrering. (LOV-2016-12-09-88). Lovdata. https://lovdata.no/lov/2016-12-09-88
11 Register over reelle rettighetshavere kom 01.10.2024.
12 Straffeloven. (2005). Lov om straff, § 56. (LOV-2005-05-20-28). Lovdata. https://lovdata.no/lov/2005-05-20-28

Enhetsregisteret er en nasjonal felleskomponent og et grunndataregister som registrerer basisopplysninger om virksomheter. Dataene brukes på tvers i forvaltningen og blant private aktører. Alle som registreres får tildelt et organisasjonsnummer. Nummeret gir juridiske personer[13] m.m. en unik og entydig identifikator overfor offentlige myndigheter og andre. Registreringen i Enhetsregisteret er et vilkår for registrering i Merverdiavgiftsregisteret, Foretaksregisteret, Aa-registeret og Konkursregisteret med flere, og disse plikter også å benytte organisasjonsnummer og opplysninger fra Enhetsregisteret. Offentlige organer og registre som ikke er tilknyttede registre, plikter, der det er praktisk mulig, å benytte opplysninger fra Enhetsregisteret. Alle opplysningene i Enhetsregisteret er offentlige, med unntak av fødselsnummer og D-nummer.

Foretaksregistret registrerer alle norske og utenlandske foretak i Norge. Registrering i Foretaksregisteret gir vern for foretaksnavnet, firmaattest som legitimasjon overfor finansinstitusjoner og offentlige myndigheter m.fl., samt legitimasjon for personer med utøvende roller i foretaket. Alle næringsdrivende foretak plikter å registrere seg i Foretaksregisteret. Enkeltpersonforetak kan registrere seg på frivillig grunnlag. Tidligere plikt til registrering for visse typer enkeltpersonforetak ble opphevet 01.07.2024.[14]

Nå følger kun registreringsplikt for enkeltpersonforetak fra særlovgivningen, eksempelvis revisorloven.

En registrering i Foretaksregisteret gir blant annet legitimasjon overfor långivere og for utøvende personer i virksomheten. Foretaksregisteret skal sikre klare ansvarsforhold. Styremedlemmer og en eventuell revisor må selv skrive under på at de har påtatt seg ansvar. «Skrive under» gjøres oftest i dag med elektronisk signatur, som BankID, men kan også gjøres på papir.

Regnskapsregisteret registrerer årsregnskap fra regnskapspliktige virksomheter og kunngjør godkjenning av årsregnskap. Regnskapsregisteret[15] foretar kun en formalkontroll i sin saksbehandling av innsendte årsregnskap. Godkjenning av årsregnskap er det virksomhetene selv som har ansvar for etter gjeldene regelverk, eksempelvis vil årsregnskapet til et aksjeselskap godkjennes av selskapets generalforsamling[16] jf. aksjeloven. Plikten til å utarbeide årsregnskap og hva regnskapet skal inneholde følger av regnskapsloven med forskrifter. Revisjonsplikten kan unnlates når virksomheten har driftsinntekter under 7 millioner kroner, når balansen viser at bedriftens eiendeler og gjeld har verdi under 27 millioner kroner eller når gjennomsnittlig antall ansatte er under 10 årsverk.[17]

13 Et rettssubjekt som ikke er en fysisk person.

14 Foretaksregisterloven. (1985). Lov om registrering av foretak § 2-1, nr.7. (LOV-1985-06-21-78). Lovdata. https://lovdata.no/lov/1985-06-21-78

15 Regnskapsregisteret kommer til å gjøre en praksisendring når det kommer til mulighetene til å erstatte allerede innsendte årsregnskap. Dette skal ikke lenger være mulig etter praksisendringen.

16 En generalforsamling består av alle eierne i selskapet og har øverste myndighet. Dersom det er en aksjeeier, er generalforsamlingen denne ene aksjeeieren.

17 Revisorloven. (2020). Lov om revisjon og revisorer § 2-1. (LOV-2020-11.20.128). Lovdata. https://lovdata.no/lov/2020-11-20-128. Aksjeloven. (1997). Lov om aksjeselskaper § 7-6. (LOV-1997-06-13-44). Lovdata. https://lovdata.no/lov/1997-06-13-44.

Regnskapsregisteret brukes av svært mange, både offentlige og private, som et hjelpemiddel og en kilde til kunnskap om virksomhetene. Bankene vil alltid etterspørre årsregnskap ved låneopptak og kredittvurderinger.

Konkursregisteret inneholder blant annet opplysninger om konkursbo og tvangsavviklingsbo. Registeret inneholder sentrale opplysninger om hvert bo, blant annet hvem som er eller har vært daglig leder, styreleder og revisor i det registrerte foretaket, og om styreleder, daglig leder eller innehaver har roller i andre foretak på tidspunktet for åpningstidspunktet jf. forskrift om konkursregisteret.[18]

Konkursregisteret kan også gi opplysninger om noen har fått konkurskarantene. Konkurskarantene kan gis en person som ved uforsvarlig forretningsførsel er funnet uskikket til å stifte, være daglig leder, styremedlem eller varamedlem i et nytt selskap.

A-ordningen er en samordnet digital måte for arbeidsgivere å rapportere opplysninger om inntekt og ansatte til Nav, Skatteetaten og Statistisk sentralbyrå (SSB). Opplysningene sendes via arbeidsgivers lønnssystem eller via skatteetaten.no som a-meldinger. A-ordningen fungerer som en database[19] hvor Nav, SSB og Skatteetaten henter opplysninger til eget bruk, og distribuerer opplysninger videre til private og offentlige aktører etter samtykke eller hjemmel i lov. Skatteetaten forvalter ordningen på vegne av de andre etatene jf. a-opplysningsloven[20].

A-ordningen foretar en automatisk kontroll av a-meldingene etter gjeldene forretningsregler[21]. Oppstår det feilmeldinger, er det kun avvisningstilfellene som ikke registreres og distribueres videre.[22]

A-meldingen er en månedlig rapportering til a-ordningen. Arbeidsgiver/opplysningspliktige må ha organisasjonsnummer for hovedenhet (juridisk organisasjonsnummer) og underenhet (virksomhetsnummer) tildelt av Enhetsregisteret for å kunne sende a-melding. Arbeidsgiver må identifisere ansatte med fødselsnummer, D-nummer eller internasjonal identifikasjon for å få sendt inn opplysninger om blant annet inntekt og arbeidsforhold på den enkelte. Opplysningsplikten følger av a-opplysningsloven som viser til lovbestemmelser og forskrifter hvor omfanget av opplysningsplikten er spesifisert.

Det er kun opplysningspliktige selv som kan endre innhold i a-meldinger.

Aa-registeret er mottaker for rapporterte opplysninger om arbeidsforhold. For å bli registrert i Aa-registeret må virksomheten først registreres i Enhetsregisteret. Arbeidsforhold skal alltid registreres på virksomhetsnummer (underenhet). Meldepliktige opplysninger som startdato, lønnsendringsdato og permisjon med mer sendes

18 Forskrift om konkursregisteret mv. (1993). Forskrift om konkursregisteret og om kunngjøringer etter konkursloven. (FOR-1993-08-23-824). Lovdata. https://lovdata.no/forskrift/1993-08-23-824.

19 En samling av organiserte data.

20 A-opplysningsloven. (2012). Lov om arbeidsgivers innrapportering av ansettelses- og inntektsforhold m.m. (LOV-2012-06-22-43). Lovdata. https://lovdata.no/lov/2012-06-22-43.

21 Formaliteter som gjelder dataene.

22 Skatteetaten. (u.å.). Veiledning til a-melding. https://www.skatteetaten.no/bedrift-og-organisasjon/arbeidsgiver/a-meldingen/veiledning/.

via a-melding til Aa-registeret. Forskrift om Arbeidsgiver- og arbeidstakerregisteret[23] bestemmer hvilke opplysninger virksomheten skal rapportere og hvem som har tilgang til registeret. Det er Nav som eier og forvalter dataene i registeret.

Det er opplysningspliktige selv som må rette feil via a-meldinger.

Merverdiavgiftsregisteret (Mva-registeret/momsregisteret) er statens oversikt over merverdiavgiftspliktige foretak. En virksomhet er som hovedregel registreringspliktig når den har solgt varer eller tjenester for over 50 000 kroner i løpet av de siste 12 månedene jf. merverdiavgiftsloven.[24] Registreringen medfører at virksomhetene skal fakturere med merverdiavgift når en selger eller tar ut varer og tjenester. Når virksomhetene kjøper varer eller tjenester, kan de føre fradrag for merverdiavgiften. Virksomhetene rapporterer dette ved å sende en mva-melding[25] direkte via regnskapssystem eller på Skatteetaten.no en gang i året eller etter termin.[26] Når Skatteetaten har mottatt mva-meldingen blir denne beregnet automatisk[27] og virksomhetene får beskjed om hvor mye de skal betale i merverdiavgift eller hvor mye staten skal betale til virksomhetene.

Skatteetaten kan endre både registreringen og mva-meldingen.

Opplysninger om en virksomhet er registrert i Merverdiavgiftsregisteret er offentlige, og er synlige blant annet i Enhetsregisteret.

Aksjonærregisteret er Skatteetatens database over aksjeeiere i Norge. Registeret inneholder navn og informasjon om alle som eier aksjer, basert på opplysningene som er meldt inn av selskapene selv[28] i aksjonærregisteroppgaven. Aksjonærregisteroppgaven vil vise alle hendelser og transaksjoner i selskapet. Oppgaven må leveres hvert år innen 31. januar for å unngå tvangsmulkt. Opplysningene er tilgjengelig for alles innsyn i mai måned etter siste inntektsår.

Skatteetaten informerer om at det kan forekomme feil eller ufullstendige opplysninger i registeret. Nav bruker aksjonærregisteret både i utredningsfasen[29], før vedtak fattes, og i kontrollsaker for blant annet å sjekke en sykemeldts eierskap i bedriftene.[30]

23 Forskrift om AA-registeret. (2008). Forskrift om Arbeidsgiver- og arbeidstakerregisteret. (FOR-2008-08-18-942). Lovdata. https://lovdata.no/forskrift/2008-08-18-942.
24 Merverdiavgiftsloven. (2009). Lov om merverdiavgift. (LOV-2009-06-19-58). Lovdata. https://lovdata.no/lov/2009-06-19-58.
25 Skattemelding for merverdiavgift.
26 Årlig rapportering innen 10. mars, året etter inntektsåret. Første termin er januar/februar med rapporteringsfrist innen 10. april samme år osv.
27 Automatisk kontroll (risikobasert) og enkelte manuelle kontroller.
28 Euronext VPS kan også stå for innrapporteringen.
29 Automatisk riskindikator.
30 Informasjon fra Nav.

Stortinget fattet i 2014 vedtak om å utarbeide et oppdatert aksjonærregister i sanntid. Dette ble igjen vedtatt[31] i justiskomiteens innstilling[32] fra juni 2024.

Personvern og samfunnsvern – en vurdering

Personvern er en del av den digitale og teknologiske samfunnsutviklingen. Offentlige myndigheter må forholde seg til taushetsplikt og personvernlovgivningen[33] ved all behandling av personopplysninger. I tilfeller hvor det foreligger rettslig grunnlag[34] for å dele taushetsbelagte opplysninger, må opplysningene også kunne behandles etter personvernlovgivningen, både av avsender og mottaker.

For å avdekke feil og mulig manipulering av data i registrene, er det nødvendig å dele underliggende opplysninger som etatene sitter på, med andre brukere av registerdataene. Dette handler om informasjon som saksbehandlere normalt ikke ser i applikasjonene, samt data som ikke er en del av den automatiserte[35] saksbehandlingen. Feil i registrene, som etatene selv ikke kan rette opp eller som tar lang tid å korrigere, kan føre til at det blir fattet uriktige beslutninger både internt i egen etat og hos andre som benytter dataene.

Riksrevisjonen har belyst noe av problematikken med deling og gjenbruk av personopplysninger.[36] Undersøkelsen viser at etatene er usikre på hva de har lov til å dele og gjenbruke av opplysninger. Dette skyldes blant annet manglende og sene avklaringer av juridiske problemstillinger. Et eksempel som blir brukt er a-kriminformasjonsforskriften[37] hvor hver etat tolker regelverket selv før det skal harmoniseres. Arbeidet med tolking og harmonisering er per november 2024 ikke ferdig.

Nav uttaler til NTAES at anledningen til å dele personopplysninger utenom det tverretatlige

31 Vedtak nr. 521. (2023-2024). Justiskomiteen. https://www.stortinget.no/no/Saker-og-publikasjoner/Vedtak/Vedtak/Sak/?p=95752.

32 Innst. 412 S. (2023-2024). Innstilling fra justiskomiteen om Felles verdier – felles ansvar – Styrket innsats for forebygging og bekjempelse av økonomisk kriminalitet. Justiskomiteen. https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2023-2024/inns-202324-412s.

33 Grunnloven. (1814). Kongeriket Norges grunnlov, § 102. (LOV-1814-05-17). Lovdata. https://lovdata.no/lov/1814-05-17. Menneskerettsloven. (1999). Lov om styrking av menneskerettighetenes stilling i norsk rett, artikkel 8. (LOV-1999-05-21-30). Lovdata. https://lovdata.no/lov/1999-05-21-30. Personopplysningsloven. (2018). Lov om behandling av personopplysninger. (LOV-2018-06-15-38). Lovdata. https://lovdata.no/lov/2018-06-15-38.

34 For eksempel forvaltningsloven § 13 mfl., skatteforvaltningsloven kapittel 3, NAV-loven § 7.

35 Hel og delvis automatisering.

36 Dokument 3:8. (2023-2024). Riksrevisjonens undersøkelse av myndighetenes tilrettelegging for deling og gjenbruk av data i forvaltningen. https://www.riksrevisjonen.no/rapporter-mappe/no-2023-2024/myndighetenes-tilrettelegging-for-deling-og-gjenbruk-av-data-i-forvaltningen/.

37 A-kriminformasjonsforskriften. (2022). Forskrift om deling av taushetsbelagte opplysninger og behandling av personopplysninger m.m. i det tverretatlige samarbeidet mot arbeidslivskriminalitet. (FOR-2022-06-17-1045). Lovdata. https://lovdata.no/forskrift/2022-06-17-1045.

samarbeidet mot arbeidslivskriminalitet jf. a-kriminformasjonsforskriften, er snever.

I tillegg til krav om rettslig grunnlag for deling av opplysninger, er det et prinsipp i personvernforordningen at opplysningene skal brukes til det formålet de opprinnelig ble samlet inn for.[38] Viderebehandling av opplysninger kan være forenlig eller uforenlig med innsamlingsformålet jf. personvernforordningens artikkel 6 nr. 4. Hvis viderebehandlingen ikke er forenlig med innsamlingsformålet, må viderebehandlingen ha grunnlag i lov eller samtykke. A-kriminformasjonsforskriften jf. forvaltningsloven § 13 g vil kunne utgjøre rettslig grunnlag for viderebehandling ved deling og videre bruk av taushetsbelagte personopplysninger for nye og uforenlige formål.[39,40]

NTAES har selv bedt om personopplysninger til gjeldende oppdrag og erfarer at etatene tolker regelverket ulikt. Det skal også sies at taushetsplikten er hjemlet i forskjellige regelverk[41], men personvernlovgivningen er lik.

Med de rette forberedelsene har kriminelle aktører mulighet til å få utbetalinger de ikke har rett på både av Nav og Skatteetaten, forholdsvis raskt og enkelt. NTAES vurderer at for å verne om felleskapets verdier må etatene agere ved å samarbeide på tvers. Det vil være behov for å dele persondata, og etatene bør gjøre de nødvendige vurderinger som skal til, i takt med digitaliseringen. Personopplysninger kan bidra til analyser og etterretning som gjør at etatene kan avsløre og kjenne igjen modus, og dermed forvalte samfunnsverdiene mer riktig.

Registermanipulasjon som fenomen

Det finnes lite konkrete tall på hvor stort omfanget av økonomisk kriminalitet er. Beregninger av feilutbetalinger fra Nav, som inkluderer alt fra svindel til ubevisste feil, viser et forsiktig anslag på 5 milliarder kroner per år.[42]

Registermanipulering brukes som en forberedende handling for å kunne gjennomføre lovbrudd som gir vinning. De forberedende handlingene består blant annet av å skaffe seg eller få tilgang til en elektronisk ID, registrere eller overta en virksomhet, og rapportere grunnlagsopplysninger. I tillegg kan manipulering benyttes for å utløse vinningen og skjule spor.

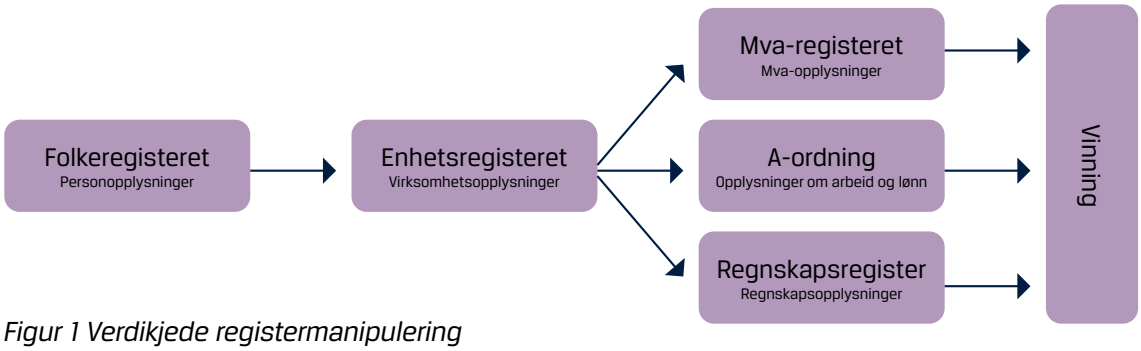
38 Personopplysningsloven. (2018). Lov om behandling av personopplysninger, generell personvernforordning, artikkel 5 nummer 1 bokstav b og artikkel 6 nummer 3 og 4. (LOV-2018-06-15-38). Lovdata. https://lovdata.no/lov/2018-06-15-38.

39 Prop.166 L (2020-2021). Endringer i forvaltningsloven m.m. (utvidet adgang til informasjonsdeling). Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-166-l-20202021/id2843338/.

40 Prop. 56 LS (2017–2018). Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen. Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-56-ls-20172018/id2594627/.

41 Som i skatteforvaltningsloven, NAV-loven og forvaltningsloven.

42 Haram, Ola (2024, 10. juni). Nav svindles for minst 5 milliarder i året: – Vi må sende anmeldelser i posten. VG. https://www.vg.no/nyheter/i/KMpGve/nav-svindles-for-minst-5-milliarder-i-aaret-maa-sende-politianmeldelser-i-posten



Figur 1 Verdikjede registermanipulering

Figur 1 viser hvordan manipulasjon av ulike registre flyter gjennom de offentlige registrene og medfører feil som gir mulighet for kriminell vinning.

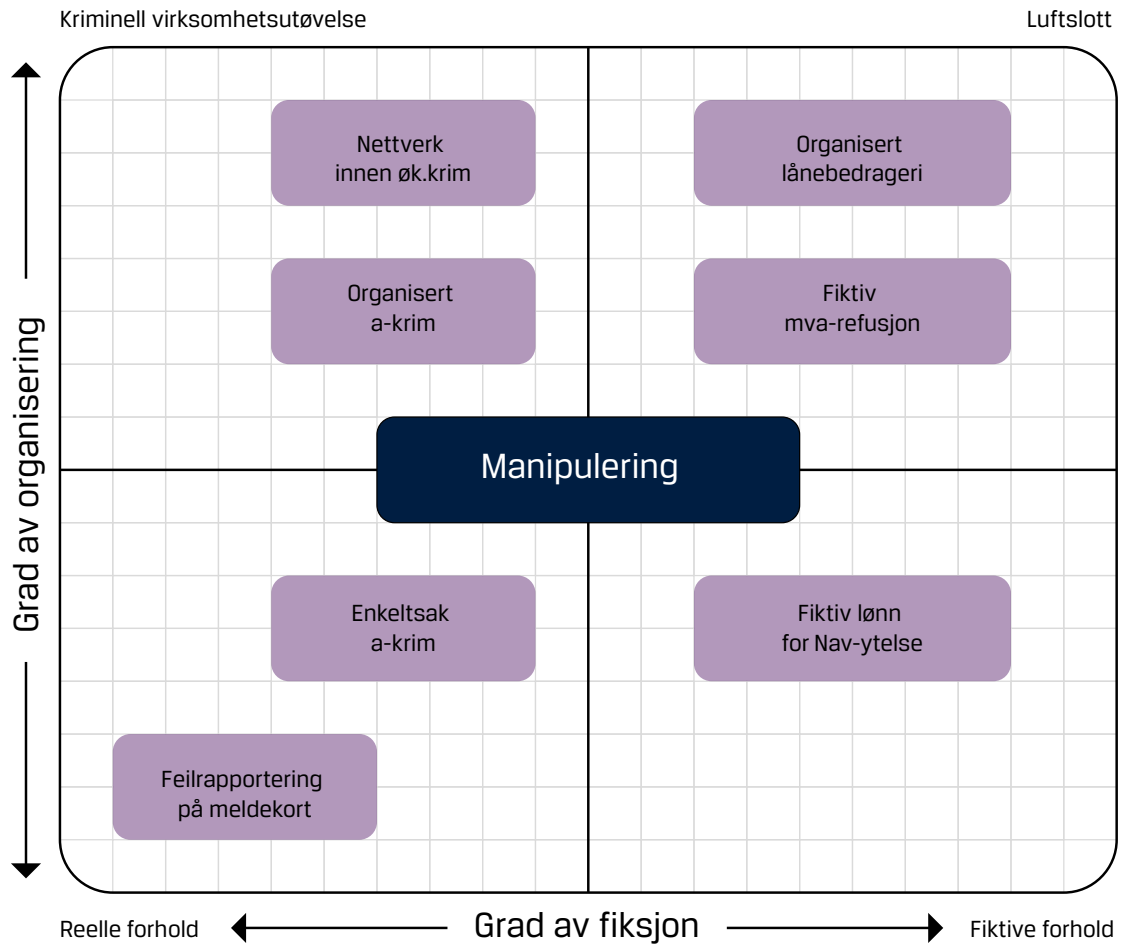
Identitetsmisbruk er én type registermanipulasjon. Å skaffe seg tilgang på andres identiteter er en forberedende handling for å blant annet kunne gjennomføre lovbrudd og kunne fordekke og forhindre avdekking. Virksomheter benyttes for å rapportere fiktive data til registrene som danner grunnlag for feil i aktuelle og senere saksbehandlingsprosesser.

Figur 2 illustrerer manipulasjon av opplysninger med varierende grad av organisering og fiksjon. Hvor stor trussel ulike aktører utgjør, og hvilke mottiltak som bør vurderes henger sammen med organiseringsgrad og grad av fiksjon. Avdekkede saker viser hvordan kriminelle på ulike måter manipulerer opplysninger for å kunne gjennomføre de kriminelle handlingene. Ved en enklere grad av organisering og lav grad av fiksjon utnyttes muligheter som allerede er etablerte, som for eksempel gjennom å ikke rapportere grunnlag for de faktiske forhold. Mer systematisk organisering og bruk av fiktive opplysninger kan danne grunnlag for større bedragerier.

Et tenkt eksempel på mulig omfang bygger på at 5 % (7 220) av foretak i Norge med mellom 1 til 9 ansatte,[43] melder et fiktivt ansettelsesforhold som over et år får 700 000 kroner utbetalt i sykepenger. Dette vil utgjøre 5 milliarder kroner i tapte velferdsmidler hos Nav.

For Skatteetaten vil mulig omfang ved at 7 220 foretak underrapporterer lønn på 700 000 kroner og omsetning med 1 million kroner medføre rundt 4 milliarder kroner i tapte skatteinntekter, basert på unndratt personskatt, arbeidsgiveravgift og merverdiavgift.

43 SSB, oppdatert 08.02.2024



Figur 2 Matrise som illustrerer ulik grad av organisering og fiksjon, med sakseksempler.

Grad av organisering omfatter hvor mange identiteter og foretak som inngår, kompleksitet i modus og om forholdene gjennomføres systematisk og over lengre tid.

Graden av fiksjon har betydning for hvordan kontrolletatene og politiet kan identifisere og motvirke trusselen. Dersom rapportering bygger på reelle legale forhold, er det vanskeligere å avdekke lovbrudd. På den andre siden vil rene «luftslott», uten rot i reelle forhold, være nærmest uten grenser for hva som kan fremstilles av opplysninger. Dermed kan slike bedrag få et enormt omfang.

I matrisen har vi trukket frem organiserte lånebedrageri som rene luftslott. Nav-bedrageri og mva-bedrageri kan være organisert med lignende modus og omfang. Lån og mva-refusjon gir store enkeltutbetalinger. Nav-ytelser utbetales som oftest over et lengre tidsrom, og Nav-bedrageri kan derfor gi høye samlede tap.

Tilretteleggere

Tilretteleggere og medvirkere er gjerne profesjonelle aktører som innehar roller[44] som innebærer høy grad av tillit i samfunnet, samtidig som de ofte har god oversikt over

44 Advokater, regnskapsførere, revisorer, leger, ansatte innen IT m.m.

regelverket, og dermed også hvordan det kan omgås.[45,46] Det kan også være andre som tilbyr tjenester som bidrar til å organisere og muliggjøre kriminalitet.

Tjenester som tilbys kan være stråpersoner, hylleselskap[47], formidling av arbeidskraft, salg av id, salg av fiktive sykmeldinger/legeerklæringer[48], dokumentforfalskning, fiktive og manipulerte regnskap, organisering og struktur m.m. Ikke alle av disse tjenestene er ulovlige, for eksempel er det lov å selge hylleselskaper.

Felles for etatene er at det er vanskelig å dokumentere hvem som gjør hva. Tilretteleggerne som muliggjør kriminalitet, er også flinke til å skjule aktivitetene.

Skatteetaten oppgir at det er en økning i antall tips som omtaler tilretteleggere og medvirkere til skattekriminalitet.[49] Økning i antall tips kan skyldes at temaet nylig har fått stor oppmerksomhet i medier og samfunnsdebatter,[50] og ikke nødvendigvis at bruken av tilretteleggere har økt i omfang.

Innsidere

En innsider er ifølge Nasjonal sikkerhetsmyndighet (NSM) en person som bevisst eller ubevisst tilrettelegger for trusselaktører eller på annen måte skader virksomheten gjennom tilganger og kunnskap personen har fått i kraft av å være på innsiden.[51,52]

For å gjennomføre manipulering, eller få informasjon som benyttes for å tilpasse informasjon som gis, kan kriminelle benytte seg av innsidere. I 2022 ble en ansatt i Nav og en tidligere ansatt i Nav, deretter ansatt i Skatteetaten, siktet for medvirkning til korrupsjon i forbindelse med utlån av 150 millioner kroner på falskt grunnlag, den såkalte Nordea-saken. I denne saken ble dokumentasjon fra Nav om låntakernes økonomiske situasjon manipulert og/eller forfalsket.

Hvor utbredt bruk av innsidere er, er ikke kjent, men både Skatteetaten og Nav omtaler dette som en trussel. Skatteetaten har i sin generelle sikkerhetsrutine innsidere som en trussel, og Nav har oppgitt at de vurderer innsidere å være en trussel mot kjennskap til sensitiv informasjon, kunnskap om sikkerhetssystemer og kontrollrutiner, databaser og IT-løsninger.

45 Økokrim. (2021). Temarapport om profesjonelle aktører. https://okokrim.custompublish.com/rapport-om-profesjonelle-aktoerer.6399017-411472.html.
46 Økokrim (2022). Trusselvurdering. https://www.okokrim.no/oekokrims-trusselvurdering-2022.6527255-549350.html.
47 Ferdig registrerte og ubrukte selskaper som selges.
48 Økokrim: Temarapport om Profesjonelle aktører 2021. Økokrim. (2021). Temarapport om profesjonelle aktører. https://okokrim.custompublish.com/rapport-om-profesjonelle-aktoerer.6399017-411472.html.
49 Skatteetaten. (2024). Trusselvurdering. Unntatt offentlighet etter offentlighetsloven offl. § 14, § 24.
50 Eksempel: Dokumentarserien «Den sorte svane» NRK.
51 Slagnes, B. (2023, 23.mai). Trusselen fra innsidere [audiopodcast]. Forsvarets forskningsinstitutt. https://www.ffi.no/aktuelt/podkaster/trusselen-fra-innsidere.
52 NSM. (2020). Temarapport om innsidetrusselen. https://nsm.no/regelverk-og-hjelp/rapporter/temarapport-om-innsidetrusselen..

Sårbarheter

I dette kapittelet vil de viktigste sårbarhetene som er avdekket i denne analysen bli gjennomgått. Sakseksempler er brukt for å illustrere hva konsekvensene kan være. I siste del av kapittelet gjennomgås lånebedrageri, som illustrerer konsekvensene av at kriminelle har avdekket sårbarheter som de utnytter for å oppnå vinning i stort omfang.

Manglende samfunnsperspektiv i etatenes risikovurderinger

Som vi har vist blir registrerte opplysninger gjenbrukt gjennom hele verdikjeden av informasjon og registre. Når opplysninger gjenbrukes slik, vil endringer i én registereiers prosesser og systemer kunne ha konsekvenser for andre etaters bruk av opplysningene til sine formål. Risiko knyttet til dette må vurderes av etatene.

Når det lages nye systemer, og når hele eller deler av prosesser digitaliseres, gjøres det risikovurderinger. I disse risikovurderingene gjøres det vurderinger knyttet til alt fra datasikkerhet til personvern som gjelder den enkelte etat.

Effektivitet og forenkling er i stor grad styrende for løsningene som velges i en digitaliseringsprosess. Da forenkler man for alle, også for den brukeren som vil manipulere og utnytte løsningen. For eksempel har det i Nav vært fokus primært på effektivisering av saksbehandlingsprosesser. I forlengelse av tillitsreformen[53] legges det også til grunn at etatene skal ha tillit til at innrapporterte data er av tilstrekkelig god nok kvalitet.

Flere av etatene melder at de ser at effekten av digitaliseringsprosesser kan påvirke potensialet for manipulering. Å implementere risikomoduler og regler i systemene som gjør at bedrageri kan forhindres eller bekjempes er måter etatene angriper denne problemstillingen.

Brønnøysundregistrene rapporterer at det bør sees på det store bildet når digitaliseringsprosesser settes i gang. Det er behov for mer kunnskap om hvordan Brønnøysundregistrenes opplysninger brukes, og hvordan det påvirker andre etaters bruk av opplysningene. Brønnøysundregistrene vurderer at en brukerreise bør sees på i et større perspektiv enn bare ett forvaltningsområde, og også ut fra en «kriminell» brukerreise.

Case: Manipulasjon av årsregnskap

Eldre selskap skifter eier og får ny daglig leder/styreleder. Gamle regnskap endres for flere år tilbake slik at selskapet på papiret oppnår en god kredittverdighet. Foretakenes regnskaper for aktuelle år er ikke underlagt revisjon.

Dagens Næringsliv har avslørt 6 selskaper som har levert identiske regnskap i modusen over.[54] Fem av selskapene har skaffet seg lån og varer på kreditt for titalls millioner,

53 Kommunal- og distriktsdepartementet. (2022). Om tillitsreformen. https://www.regjeringen.no/no/dokumenter/om-tillitsreformen/id2951643/.

54 Tallaksen, S. og Bakken, J. B. (2024, 19. januar). Ble offer for ny utspekulert svindel – her finner han igjen tyvegodset. Dagens Næringsliv. https://www.dn.no/magasinet/dokumentar/okonomisk-kriminalitet/cyberkriminalitet/byggebransjen/ble-offer-for-ny-utspekulert-svindel-her-finner-han-igjen-tyvegodset/2-1-1582125.

uten å gjøre opp for seg. Andre likheter mellom selskapene er at en person fyller rollen både som daglig leder og styreleder, og selskapene har benyttet postkasser/adresser på andres eiendom.

Politiet har mottatt flere anmeldelser i forskjellige politidistrikt. Disse sakene og anmeldelsene er ikke sett i sammenheng, og de er nå henlagt på grunn av manglende behandlingskapasitet.

NTAES´ vurdering er at tilfellene viser hvordan manipulerte data fra regnskapsregistret legges til grunn med stor samfunnsskade. Det senker tillit til offentlige registre, svekker verdien av å ha et register og gir økonomisk vinning for kriminelle.

Case: Manipulasjon skjules i mengden

Rapporteringer til Regnskapsregisteret (Brønnøysundregistrene) og Skatteetaten skal i utgangspunktet være lik. Det er ingen begrensinger i hvor mange ganger rapporteringer til Regnskapsregisteret og Skatteetaten kan endres. Analyser NTAES har gjort på avvik mellom opplysninger i Regnskapsregisteret og opplysninger gitt til Skatteetaten i skattemeldinger med næringsoppgave/næringsspesifikasjon, viser at det er mer enn 2000 aksjeselskap som har et avvik på over 50.000 kroner i rapportert resultat i 2022. Det store antallet avvik fører til at faktisk manipulasjon, det vil si der manipulerte data rapporteres for å kunne oppnå vinning, skjules i mengden av andre feil. Antallet medfører at en manuell oppfølgning er ressurskrevende. Samtidig er kontroll av innrapportering i stor grad redusert med bortfall av revisjonsplikt og redusert kontroll av registreringer og rapporteringer. Regelverk med unntak og særregler medfører økt kompleksitet og at ulogiske forhold kan ha sin forklaring.

Selv om enkeltsakene i media fremstår åpenbare og nærmest latterlige at ikke avdekkes, vil innrapporteringen i mange tilfeller kunne vært gjort uten at de fremstår mistenkelige. Dermed er sårbarheten for at data manipuleres fortsatt til stede.

Brukervennlighet går foran alt

I Navs virksomhetsstrategi er en av de fire ambisjonene: «Alle får pengene de har krav på, enkelt og forutsigbart».[55] I én av Skatteetatens fem ambisjoner er det lagt vekt på etaten skal møte næringsliv og innbyggere på en slik måte at det blir enklere å gjøre det rette og vanskeligere å gjøre feil.[56] Brønnøysundregistrene har blant annet som mål at «Brønnøysundregistrenes registerløsninger skal føre til en effektiv digital samhandling med næringslivet, frivillig sektor, offentlig sektor og privatpersoner».[57]

I utvikling av nye digitale løsninger er effektivitet og forenkling i stor grad styrende for de løsningene som velges. Dette innebærer at man forenkler for alle, også for de personene som ønsker å manipulere og utnytte løsningene.

Ved å ha tilgang til bank-ID kan kriminelle logge seg inn og manipulere informasjon fra hvor som helst. En betydelig sårbarhet er at kriminelle relativt enkelt og i stort omfang kan benytte andre personers elektroniske identifikasjon (eID), samt kjøpe, true eller bruke vold for at personer skal utføre handlinger med egen eID. I tillegg forsterkes den kriminelle kapasiteten av mulighetene

55 Nav. (2024). Navs Strategi. https://www.nav.no/strategi.
56 Skatteetaten. (u.å.). Skatteetatens strategi. https://www.skatteetaten.no/strategi/.
57 Brønnøysundregistrene. (2024). Oppdraget vårt. https://www.brreg.no/om-oss/oppdraget-vart/.

misbruk av foretak gir når de som faktisk står bak foretakene ikke er de som er registrerte rollehavere eller elektronisk signerer på vegne av foretaket.

«Mange av systemene baserer seg på egenfastsetting og «grønt løp». Det gjør oss avhengig av at det er effektive og treffsikre kontrollmekanismer som sikrer datakvaliteten.»[58]

Når nye digitale løsninger for søknad og innrapportering baserer seg på at brukere, skatteytere og virksomheter selv skal sende inn opplysninger, legge ved dokumentasjon og manøvrere seg gjennom en søknadsdialog, gir dette en ny type åpenhet om saksbehandlingsprosessene enn tidligere. Brukervennlighet innebærer enklere muligheter for å korrigere innsendte opplysninger, gjerne langt tilbake i tid. Kriminelle kan kartlegge hvordan de kan manipulere opplysninger og registreringer, og hvordan virksomheters fasader kan konstrueres, for å lykkes med registermanipulasjon.

Et viktig moment i å gjøre systemer og tjenester mer brukervennlige er at ting skal gå raskt. Saksbehandlingstiden skal reduseres til et minimum. Det er en bekymring hos etatene at den økte hastigheten i seg selv øker risikoen for at manipulasjon gir vinning for kriminelle.

Mangelfull deling mellom etatene

Opplysninger etatene og næringslivet bruker som grunnlag for å vurdere rettigheter og plikter ligger i noen få grunnlagsregistre.

I utgangspunktet er det en fornuftig tilnærming at opplysninger hentes inn én gang, og gjenbrukes flere ganger. Da kan etater, virksomheter og næringslivet hente de data de har behov for og rett til å bruke. Det gjør det også enklere for eksempelvis privatpersoner og virksomheter, som ikke må levere de samme opplysningene flere steder.

Ulike konsumenter av opplysninger og data har ulike behov. Registereierne har ikke nødvendigvis oversikt over hva andre konsumenter har behov for, og hvordan opplysningene skal brukes. Kartleggingen NTAES har gjort viser at det deles mye opplysninger og data mellom ulike aktører. Det som ikke deles er metadata om opplysningen. Det er flere slike type data som kan være relevant for ulike konsumenter, for eksempel: Når er opplysningen registrert, og av hvem? Har det skjedd endringer av opplysninger tilbake i tid? Dersom det er indikasjoner på at opplysninger er manipulerte kunne det også vært relevant for konsumentene å få informasjon om det, ved hjelp av en form for flagging.

Det er flere etater og deler av finansnæringen som har etablerte rutiner for deling av mistanker om manipulasjon og forsøk på bedrageri. Slik deling skjer i all hovedsak i prosaform, ikke som data. Måten informasjonen deles på er tidkrevende å behandle både for avsender og mottaker. Det mangler en mer systematisk form for deling mellom aktører som arbeider for å forebygge, bekjempe, avdekke og forhindre registermanipulering. De etablerte siloene mellom aktørene og internt i etatene hindrer effektiv deling av informasjon.

58 Skatteetaten. (2023). Forslag til nye tiltak knyttet til bevisste skatteunndragelser. Unntatt offentlighet etter offentlighetsloven §§ 14 og 24.

Manglende retting av feil

Opplysninger registreres i ett register, og opplysningene gjenbrukes inn i andre registre som grunnlag for vurdering av rettigheter og plikter. I forbindelse med en vurdering vil etatene kunne kontrollere om opplysningene er riktige. For eksempel kan Nav kontrollere om et arbeidsforhold er reelt eller fiktivt. Dersom Nav, ut fra sitt regelverk, finner at arbeidsforholdet er fiktivt, kan det bety at personen ikke har rett på arbeids- eller inntektsavhengige ytelser. Nav kan da vedta at ytelsen bortfaller. Det registrerte arbeidsforholdet og inntekt vil imidlertid kunne bli stående registrert i a-ordningen og Aa-registeret.

Det er opplysningspliktige som har ansvar for å gjøre endringer dersom noe er feil i opplysninger som er rapportert gjennom a-ordningen. Dersom Nav oppdager feil i for eksempel Aa-registeret vil opplysningspliktige bli bedt om rette feilen via a-ordningen. Blir ikke krav om retting fulgt opp, kan Nav ilegge arbeidsgiver overtredelsesgebyr eller tvangsmulkt, eller begge deler.

Brønnøysundregistrene foretar kun formalkontroll av meldingene som fører til registrering i deres registre. De kontrollerer om det er sammenheng mellom utfylte skjema og vedlagt dokumentasjon, men kan ikke kontrollere om den vedlagte dokumentasjonen er riktig. Dersom det er behov for at opplysningspliktige skal endre eller melde andre opplysninger til registrene, kan Brønnøysundregistrene ilegge tvangsmulkt, forsinkelsesgebyr eller iverksette tvangsoppløsning.[59]

Det at for eksempel et fiktivt arbeidsforhold blir stående registrert i Aa-registeret har konsekvenser for vurdering av rettigheter og plikter flere steder. For Navs del vil en registrert inntekt kunne bli tatt med som grunnlag for beregning av en fremtidig ytelse, for eksempel ved beregning av pensjonsgrunnlag. Utlendingsdirektoratet (UDI) forholder seg til den registrerte informasjon om arbeidsforhold og inntekt i a-ordningen i sin vurdering av søknader om familiegjenforening. De registrerte opplysningene inneholder ikke informasjon om at Nav har vurdert om arbeidsforholdet er fiktivt eller ikke. UDI må da vurdere dette ut fra sitt hjemmelsgrunnlag. For bankene vil en registrert inntekt danne grunnlag for vurderingen av om personen skal kunne ta opp lån eller ikke.

Regelverket står i noen tilfeller i veien for at korrekte opplysninger blir registrert. I Norge er det ikke ulovlig å bruke stråpersoner i roller i en virksomhet. Bruk av stråpersoner er generelt vanskelig å avdekke, og kan i mange tilfeller knyttes til identitetsmisbruk. I tillegg er det usikkert om Brønnøysundregistrene, som registereier, blir varslet dersom etatene avdekker bruk av stråpersoner. Brønnøysundregistrene får dermed ikke mulighet til å korrigere opplysningene i registrene.

Etatene kan altså sitte på tips og mistanker om at opplysninger i registeret er feil, eller de kan ha konkludert med at opplysningen er feil, og dermed ikke kan legges til grunn i vurdering av rettigheter og plikter. I mange tilfeller vil tvil rundt en opplysnings troverdighet ikke bli delt utenfor etaten eller det

59 Ileggelse av tvangsmulkt knytter seg i all hovedsak til pålegg om å endre eller melde opplysninger til registeret. Forsinkelsesgebyr kan ilegges når årsregnskapet ikke leveres til frist. Tvangsoppløsning skjer dersom en virksomhet ikke har lovpålagte roller registrert. Kilde: Brønnøysundregistrene


Foto: Shutterstock

enkelte fagsystemet. Det er dermed opp til hver enkelt etat eller instans å vurdere troverdighet og riktighet av en opplysning.

For å kunne avdekke kriminalitet er kontrolletatene og politiet avhengig av at registerkvaliteten er god. Kontroll på dataene i registrene er avgjørende for å hindre for eksempel identitetsmisbruk og bedragerier.

Case: Hvitvasking med mer

Høsten 2022 opprettes «Krim AS». Eier og styreleder er samme person. Formålet til aksjeselskapet er investeringer i verdipapirer og eiendom med mer. I 2023 rapporteres arbeidsforhold og inntekter via a-meldinger. Til sammen rapporteres det inntekter på ansatte for 5 000 000 kroner i løpet av noen måneder. Flesteparten av de ansatte mottar i tillegg stønader fra Nav, inkludert styreleder.

Skatteetaten finner at det ikke foreligger drift i selskapet. Skatteetaten tipser Nav kontroll om at de mistenker at de ansatte skal søke stønader hos Nav. Nav kontroll mistenker i tillegg id-tyveri og lånebedrageri. Styreleder søker om sykepenger. Søknaden blir avslått. To ansatte sender anmeldelse om id-tyveri og andre tar opp lån tilsvarende innrapportert inntekt. Enkelte ansatte korrigerer skattemeldingen. Det er kun innbetalt skatt på stønader fra Nav. Arbeidsgiver «Krim AS» har ikke betalt inn forskuddstrekk og arbeidsgiveravgift. Skatteetaten har saken til kontroll.

NTAES er blitt tipset om at hensikten med selskapet, og innrapporteringer av inntekter og arbeidsforhold, er å få «vasket» penger fra andre kriminelle aktiviteter. Politiet opplyser at flere av de ansatte i «Krim AS» er tilknyttet vinningskriminalitet og salg av narkotika.

Per august 2024 har alle arbeidsforholdene fått sluttdato satt av Nav registerforvaltning, men de er ikke fjernet eller markert som fiktive. Angående inntekter så vises disse som

reelle inntekter i saksbehandlingen hos Nav og kan fremdeles bli medberegnet i fremtidige stønader. Dette gjelder også for de som har korrigert egen skattemelding.

Lånebedrageri og tilknyttet kriminalitet

Registermanipulasjon, gjennom fiktive påstander og falsk dokumentasjon, er ikke nytt. Derimot har komplekse saker hos etatene vist at noe er i endring. Kriminelle aktører er involvert i mye annen kriminalitet og misbruker flere etater og privat næringsliv, samt viser en evne til å omstille tradisjonell kriminalitet til det digitale samfunn.

Måten lånebedrageri gjennomføres på illustrerer potensialet ved registermanipulasjon og et skifte i kriminalitetsutviklingen over til det digitale rom. I tillegg er utbyttet stort, og konsekvensene nærmest fraværende, for de som profittere på denne typen kriminalitet. Både privat og offentlig sektor blir rammet.

Lånebedrageri ved SBL

Samtykkebasert lånesøknad (SBL) muliggjør digital innhenting av skattegrunnlag og inntektsdata hos Skatteetaten med samtykkeløsning fra Altinn. SBL skal sikre en god kundeopplevelse ved at låneprosessen blir enklere og tryggere. I tillegg bidrar SBL til økt personvern, ved at lånesøker kun deler den informasjonen som er nødvendig for å behandle lånesøknaden.[60]

Låneprosessen med SBL har gitt økt sikkerhet og kvalitet i låneprosessen og muliggjør digitalisering som sparer långiver for store beløp.

Ved lånebedrageri gjennom SBL manipuleres lønnsinformasjon ved at foretak rapporterer lønn til a-ordningen for fiktive arbeidsforhold. Den fiktive lønnen ligger til grunn ved deling av informasjon med kredittinstitusjoner og danner grunnlag for tilsynelatende høy kredittverdighet slik at lån innvilges og øker størrelsen på mulig maksimalt lånebeløp.

Typer lånebedrageri

Det kan gjøres et skille mellom to ulike typer lånebedrageri:

1. Rene lånebedragerier (omfatter i stor grad forbrukslån og bilfinansiering)
2. Salg av kredittverdighet som en tjeneste (omfatter alle typer lån)

Rene lånebedragerier vil raskt kunne gi direkte økonomisk tap for långiver. Ved bilfinansiering fremgår ofte melding om at bilen er stjålet kort tid etter låneopptak. **«**Tyveriet**»** fremstår i flere tilfeller som rene bestillingsverk, særlig ved finansiering av dyrere biler.

Ved salg av kredittverdighet går bedraget i å fremstå kredittverdig og medfører ikke nødvendigvis et økonomisk tap for långiver. Imidlertid vil lånene ofte være langt over låntagers betalingsevne basert på hvite inntekter. I noen tilfeller er det mistanke om bruk av innsidere hos banker/låneagenter for å sikre at lånene blir innvilget.

Kjøp av slike tjenester kan være motivert av flere forhold. Det er indikasjoner på at tjenesten etterspørres for finansiering av eiendomskjøp hos personer som i hovedsak har illegale inntekter og dermed er ekskludert fra det ordinære lånemarkedet. Betjening av lånene med utbytte fra kriminalitet kan være del av hvitvasking. Det mistenkes også at lån går til oppgjør av narkotikagjeld, der pengeinnkrevere samarbeider med de som manipulerer. Trusler og vold anses vanlig i slike tilfeller og effekten er at gjeld til kriminelle byttes mot gjeld til banker.

60 BITS. (2024). Om tjenesten. https://dokumentasjon.dsop.no/dsop_sbl_om.html.

Modus rene lånebedrageri
Kort oppsummert omfatter lånebedrageri med SBL tre steg:

1. Kontroll over eID på mange personer og tilgang til foretak
2. Rapportere fiktiv lønn gjennom a-ordningen fra foretaket
3. Søke og få innvilget lån basert på et fiktivt grunnlag (den fiktive lønnen)

Modusen krever en del innsikt og kunnskap, men er ikke avansert. Fremgangsmåte ved manipulasjon er den samme som ved legal registrering og rapportering. Informasjon om fremgangsmåte finnes i offentlige brukerveiledninger, og dagens regnskapssystemer tilbyr stegvise veiledninger uten behov for økonomisk utdannelse. Kjernen i modusen er å sette de ellers legale aktivitetene sammen med den ulovlige aktiviteten, samt å ikke bli avslørt og sikre utbytte.

I modus for lånebedrageri blir den fiktive lønnen ofte slettet etter at lån er innvilget. Det vil dermed kunne fremstå som om at avviket er rettet opp. I a-ordningen er det brukere av informasjon sitt ansvar å vurdere den materielle kvaliteten og a-ordningen har ikke selv kontrolladgang eller ressurser til å kontrollere materielle forhold.

Modus i rene lånebedragerier er overførbart til offentlige etater. Ved Nav-bedrageri vil fremgangsmåten være lik, med eneste forskjell at det i steg tre sendes søknader om ytelser fra Nav istedenfor lånesøknader til bankene.

Personer og foretak

Omfanget av lånebedrageri er stort. For å få den kriminelle operasjonsplanen til å fungere kreves det tilgang på et stort antall foretak, og i tillegg mange personers IDer.

Foretakene som benyttes i lånebedrageri og rapportering av fiktiv lønn har i liten grad lagt ressurser i en fasade for å fremstå legitime. Bruk av foretak med tidligere drift gir imidlertid et skinn av reell drift. Foretakene er nesten alltid nyetablerte eller nylig registrert med ny rollehaver. En stor andel av foretakene er registret i en bransje som er mva-pliktig, uten at de er mva-registrert.

Bruk av ID
Bruken av personers ID varierer i fremgangsmåten, ut fra formålet.

- Én type rolle i lånebedrageri er personer som har kjøpt en fiktiv kredittverdighet og låneopptak. De blir registrert med fiktiv lønn. Basert på reell registrert inntekt og formue vil mange av personene ikke evne å betjene de store lånene, men lånene er likevel ofte betjent. Disse personene kan ha normale arbeidsforhold, være selvstendig næringsdrivende eller motta løpende trygdeytelser.
- En annen type rolle er personer som har gitt fra seg eID eller som utfører det de får beskjed om. En mulig årsak til at disse personene gjør dette er at de har gjeld til kriminelle eller blir utnyttet.
- En tredje type omfatter eID som kriminelle besitter på ulike grunnlag. Et typetilfelle er at personen har solgt eID eller er/har vært arbeidstaker innen arbeidslivskriminalitet der eID utnyttes.

I tillegg til disse tre typetilfellene av roller har NTAES i analysen funnet flere personer som fremstår som stråpersoner, ved at andre personer i realiteten disponerer foretakene.

Hva vet etatene om de kriminelle aktørene?
NTAES' analyse av et kjent miljø som har gjennomført en rekke lånebedrageri viser at etatenes informasjon og kunnskap om disse kriminelle aktørene er omfattende. En

stor andel av personene som er involvert har svært mange forhold som mistenkt, siktet eller dømt innen ulike kriminalitetsområder i politiets straffesaksregister. Informasjon fra andre myndigheter og etater viser at personene og foretakene er knyttet til flere alvorlige forhold:

- En rekke rapporter fra rapporteringspliktige etter hvitvaskingsloven til Financial Intelligence Unit (FIU) ved Økokrim
- Tips, feilutbetalingssaker, kontrollsaker og anmeldelser av mulig Nav-bedrageri
- Tips, kontrollsaker, forsøk på mva-svindel og anmeldelser fra Skatteetaten
- Meldinger om mulige feil fra a-ordningen, knyttet til at opplysningene er ulogiske opp mot registreringer i Brønnøysundregistrene

For de mer sentrale personene innen dette miljøet er det en dreining over til mer økonomisk kriminalitet. Bruk av foretak er gjennomgående en del av kriminalitetsbildet for personene. Knytningen til mer legal aktivitet omfatter både investeringer i næringslivet og drift, i begge tilfeller benyttes stråpersoner for å skjule knytningen.

Vurderinger

Lånebedrageri viser mange av de utfordringene samfunnet har med å sikre seg mot denne typen kriminalitet, både sårbarheter ved den overordnede risikohåndteringen og sårbarheter i digitale løsninger for å forebygge, bekjempe, avdekke og forhindre de konkrete forholdene.

Registrering av fiktiv lønn muliggjør ikke bare vinning gjennom lånebedrageri. Det åpner blant annet døren for trygdebedrageri og skattekriminalitet, samt legger til rette for feil beslutninger og vedtak både i offentlig og privat sektor, av stor verdi.

Flere deler av modus for lånebedrageri fremstår som systematisk gjennomført. Metoden krever at flere personer er aktive bidragsytere for å oppnå vinning. Imidlertid er aktivitetene lite avanserte sammenlignet med en del annen økonomisk kriminalitet, som gir grunn til bekymring for potensialet ved mer avanserte modus. Kriminelle aktører med større tekniske kapasiteter vil dermed kunne utgjøre en større trussel dersom sårbarhetene ikke lukkes.

Etatene har hver for seg informasjon om personene og virksomhetene som, dersom informasjonen samlet hadde vært inkludert i en risikobasert tilnærming, ville ført til at disse aktørene ikke hadde fått fornyet tillit. I tillegg observeres store forskjeller i risikotilnærming mellom finansnæringen og offentlig sektor. I finansnæringen benyttes elektroniske spor i identifisering av mulige bedragerier, mens i kontrolletatene og politiet benyttes slike spor kun når mistanken først er avdekket i enkelte mer alvorlige saker. I tillegg har personer i caset både konkurskarantener og næringsforbud, men slik informasjon er ikke innarbeidet hos etatene og for næringsforbud mangler en felles forvaltning.

Hovedvurderinger

Registermanipulasjon har alvorlige konsekvenser for offentlig sektor, det private næringslivet og privatpersoner. Det kan true grunnleggende verdier i velferdsstaten og medfører både direkte og indirekte økonomiske konsekvenser og tap. NTAES vurderer at det er flere sårbarheter som hindrer en effektiv og slagkraftig forebygging og bekjempelse av manipulasjon og kriminaliteten knyttet til denne.

Etatenes muligheter til å stanse registermanipulasjon avhenger av utvikling av regelverk, systemer, prosesser og samhandling. I tillegg er et viktig element hvordan personvernlovgivningen praktiseres.

Sårbarhetene som er avdekket i denne rapporten viser at det er store utfordringer som skal løses. De kriminelle utnytter og tilpasser seg muligheter som oppstår. Hvis ikke sårbarhetene lukkes, vil ikke etatene klare å stanse kriminaliteten ved registermanipulasjon og etterfølgende vinning.

Måten det arbeides med avdekking og bekjempelse av registermanipulasjon, fører til at etatene og politiet hver for seg må oppdage aktørene på nytt hver gang. Dette fordi avvik ikke avdekkes, mønstre ikke gjenkjennes og tidligere gjerninger ikke legges til grunn for å vurdere risiko.

- **Manglende samfunnsperspektiv i risikovurderingene**
  Digitalisering og forenkling et sted i verdikjeden kan påvirke andre etaters bruk av data og informasjon. Risikovurderingene mangler samfunnsperspektivet og tar ikke tilstrekkelig hensyn til mulighetene for manipulering og kriminalitet.
- **Brukervennlighet går foran alt**
  Når prosessene med rapportering og søknader digitaliseres og forenkles blir det enklere for alle, også for de som ønsker å manipulere og utnytte systemene. Forenklinger av regelverk og systemer kan også skape for stor åpenhet om prosesser og kontrollnivå.
- **Mangelfull deling mellom etatene**
  Data følger en enveiskjørt vei gjennom registrene, og det følger sjelden med bakgrunnsinformasjon og metadata som kan gi indikasjoner på manipulering. Det mangler en automatisk og strukturert deling av mistanker om manipulering.
- **Manglende retting av feil**
  Etatene legger data og informasjon fra registre til grunn for sin saksbehandling, uten at disse nødvendigvis kontrolleres mot en tredjepart. Feil i opplysninger i et register vil kunne bli stående og gjenbrukes i egen etat eller av andre etater. Ansvaret for å rette feil ligger i mange tilfeller hos den opplysningspliktige.

Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES)
c/o ØKOKRIM
Postboks 2093 Vika
N-0125 Oslo