UNIVERSITETET I OSLO

Samfunnssikkerhet og digitale identiteter

Helhetlig, trygg og inkluderende digital identitetsforvaltning i Norge: Anbefalinger fra SODI-prosjektet

Marte Eidsand Kjørven (prosjektleder SODI, UiO)

Rolf Riisnæs (UiO), Tobias Mahler (UiO),
Kristian Gjøsteen (NTNU), Malcolm Langford (UiO),
Tone Linn Wærstad (UiO), Lars Petter Omland (UiO)

SODI-rapport 4/2025
Høringsutkast

Innholdsfortegnelse

1. Sammendrag[1]

"Du skal ikke tåle så inderlig vel, den urett som ikke rammer deg selv."

Den digitale identitetsforvaltningen i Norge er en suksess og en katastrofe på samme tid. God utbredelse av private, markedsbaserte løsninger for elektronisk identifisering (eID), særlig BankID, har lagt til rette for digitalisering av både privat og offentlig sektor. Det har gitt enklere tilgang til en rekke digitale tjenester for store deler av befolkningen og kostnadsbesparelser for mange offentlige og private aktører.

Universalnøkkelfunksjonen som gjør bruk av eID nyttig og kostnadsbesparende, fører imidlertid samtidig med seg alvorlige utfordringer og sårbarheter knyttet til utenforskap, ID-misbruk og sviktende rettssikkerhet. Når en eID kan brukes i tusenvis av ulike sammenhenger, er det også potensiale for identitetsmisbruk i alle disse sammenhengene. Kriminelle som tilegner seg andres eID kan manipulere informasjon i offentlige registre, overføre penger, søke om lån, opprette selskaper og få utbetalt offentlige stønader på feilaktig grunnlag. Dette fører til enorme tap for individer, selskaper og offentlige myndigheter. I verste fall kan mennesker bli utsatt for strafferettslig forfølgning, justismord og/eller økonomisk ruin som følge av handlinger begått av andre med deres digitale identitet.

Når en universalnøkkel i form av eID er nødvendig for tilgang til tjenester og deltakelse i samfunnet, blir konsekvensene også svært alvorlige for de som står uten nøkkel. Norske myndigheter har overlatt til private aktører, primært banker, å bestemme hvem som til enhver tid skal ha tilgang til digitale offentlige tjenester og hvem som for alle praktiske formål skal umyndiggjøres. Da Norsk Forbund for Utviklingshemmede klaget Digitaliserings- og forvaltningsdepartementet inn for Diskrimineringsnemnda, argumenterte departementet til overmål med at det ikke har «myndighet over» hvordan «bankene tolker og praktiserer gjeldende regelverk» om utstedelse av BankID. Dette til tross for at store deler av digitaliseringen av offentlig forvaltning altså baserer seg på nettopp BankID og andre privateide eID-systemer. Denne måten å organisere den digitale identitetsforvaltningen på reiser alvorlige utfordringer knyttet til rettssikkerhet, diskriminering og statens plikter knyttet til menneskerettighetene.

Den digitale identitetsforvaltningen i Norge preges av at noen aktører og deler av befolkningen høster gevinstene og fordelene, mens andre aktører, og særlig sårbare deler av befolkningen, bærer ulempene og kostnadene. Bendik, som ikke får BankID og derfor heller ikke tilgang til digitale offentlige tjenester fordi han har Downs syndrom,[2] og kreftsyke Magnhild som er utsatt for omfattende ID-misbruk med store konsekvenser,[3] er blant dem som betaler digitaliseringens pris. Og der noen offentlige aktører sparer penger på å digitalisere tjenestene sine, får andre offentlige aktører – bl.a. politi og påtalemyndighetene – økte kostnader som følge av den eksplosive veksten i digitale bedragerier.

---

[1] Prosjektet er finansiert av Norges Forskningsråd (prosjektnummer 320785). Prosjektets norske tittel er Samfunnssikkerhet og digitale identiteter. Rapportens hovedforfatter er Marte Eidsand Kjørven (prosjektleder i SODI, UiO). Medforfattere er Rolf Riisnæs (UiO), Tobias Mahler (UiO), Kristian Gjøsteen (NTNU), Malcolm Langford (UiO), Tone Linn Wærstad (UiO) og Lars Petter Halvorsen Omland (UiO).

[2] Bendik har downs – og en evig kamp mot BankID – Dagsavisen

[3] Kreftsyke Magnhild (71) utnyttes av kriminelle – NRK Norge – Oversikt over nyheter fra ulike deler av landet

Digitaliseringen har skjedd raskt og skapt nye muligheter, men den har også fått andre og videre konsekvenser enn hva det er tatt høyde for i de rettsreglene som hittil er blitt etablert for å sikre at digitaliseringen skjer på en forsvarlig måte.

Problemene knyttet til den digitale identitetsforvaltningen er nå blitt så omfattende og komplekse at det også kan komme til å utgjøre et samfunnssikkerhets- og beredskapsproblem. En alvorlig konsekvens av økt ID-misbruk og digitale bedragerier er at befolkningens tillit til digitale tjenester og offentlig kommunikasjon kan svekkes.

I kjernen av utfordringene ligger fraværet av en helhetlig strategi og styring av den digitale identitetsforvaltningen i Norge. Ansvarsforholdene er fragmenterte, samordning svikter og feltet preges av systematisk manglende demokratisk forankring. Viktige beslutningsprosesser er ugjennomsiktige og mangler involvering av berørte parter. Digital identitetsforvaltning er ikke bare et teknisk eller administrativt spørsmål – det er et grunnleggende demokratisk anliggende.

Problemene knyttet til fragmenterte ansvarsforhold og lav grad av strategisk styring ble påpekt allerede i 2019, i forbindelse med en områdegjennomgang av ID-forvaltningen.[4] I likelydende brev fra aktørene som utgjør Koordineringsgruppe for identitetsforvaltning (KoID) til sine respektive departementer høsten 2024 pekes det på disse utfordringene ennå ikke er løst.[5] En hovedanbefaling i områdegjennomgangen fra 2019 var å utarbeide en felles strategi for ID-forvaltningen. Seks år senere mangler det fremdeles en helhetlig strategi for identitetsforvaltningen som dekker både privat og offentlig sektor.

Det er nettopp dette tomrommet denne rapporten søker å fylle. I fravær av en offentlig utarbeidet strategi har vi i forskningsprosjektet SODI utviklet en helhetlig tilnærming til digital identitetsforvaltning i Norge, med konkrete forslag til tiltak. Rapporten har særlig fokus på tiltak som kan fremme inkludering, sikkerhet og bidra til økt rettssikkerhet. Vår analyse viser at utfordringene i dagens system ikke kan løses med enkle justeringer, men krever en helhetlig tilnærming som ivaretar både individuelle rettigheter og samfunnets behov for sikkerhet og effektivitet.

Rapporten introduserer ti overordnede styringsprinsipper for digital identitetsforvaltning:

1. Universell tilgang
2. Svindelforebygging og sikkerhetsløsninger
3. Gjenoppretting og reparasjon
4. Autonomi: Selvbestemmelse og personvern
5. Transparens: åpenhet og gjennomsiktighet
6. Ansvar: tilsyn, kontroll og sanksjoner
7. Innovasjon: interoperabilitet, valgfrihet og konkurranse
8. Samfunnssikkerhet og beredskap
9. Demokratisk forankring
10. Helhetlig styring: systemtenkning og samhandling

For hvert prinsipp drøfter vi dagens svakheter og presenterer forslag til tiltak.

[4] Rapporter – områdegjennomgang av ID-forvaltningen - regjeringen.no. Områdegjennomgangen består av en hovedrapport og en tilleggsrapport. Sistnevnte omhandler særskilt spørsmål om eID.
[5] Se bl.a. brev fra UDI til Justis- og beredskapsdepartementet, «Koordinering av identitetsforvaltningen» (27. september 2024), Ref. 24/32488-2.

Til sammen gir rapporten en oversikt over hvordan Norge kan bevege seg mot en digital identitetsforvaltning som er tryggere, mer inkluderende og demokratisk forankret. I lys av eIDAS 2.0 og planene om å innføre europeiske digitale identitetslommebøker (EUDI Wallets), står vi nå i en situasjon der valgene som tas, vil kunne forsterke dagens skjevheter – eller bli starten på en tryggere og mer inkluderende fremtid.

Nå gjelder det å benytte mulighetene som innføringen av den digitale lommeboken gir til å rette opp de skjevhetene som dagens løsninger har ført med seg. Det vil også gi muligheter for nye og bedre digitale tjenester til alle.

2. Innledning

2.1. Bakgrunn: Om SODI-prosjektet

Denne rapporten er utarbeidet av prosjektet 'Societal Security and Digital Identities' (SODI). SODI-prosjektet er finansiert av Norges Forskningsråd, og startet opp i 2021 som et tverrfaglig samarbeidsprosjekt. Det overordnede formålet med prosjektet er å undersøke hvordan juss og teknologi kan virke sammen for å avdekke og redusere sårbarheter og risiko knyttet til bruk og misbruk av systemer for elektronisk identifikasjon (eID). SODI-prosjektet har hatt et særlig fokus på sårbare grupper, og ivaretakelse av rettssikkerhet. Prosjektet er gjennomført av forskere fra fire forskningsinstitusjoner i Norge og Estland, i samarbeid med en rekke private og offentlige samarbeidspartnere.[6]

Som del av SODI-prosjektet har rettshjelpstilbudet ID-juristen i perioden 2021 til 2024 gitt gratis veiledning og juridisk bistand til personer som er utsatt for eID-svindel, eller som har problemer med å få tilgang til eID. Sakene som har kommet inn til ID-juristen gir et unikt innblikk i de problemene overgangen fra fysisk til elektronisk identifisering har skapt, hvem som er rammet og hvilke konsekvenser det har.[7]

Basert på erfaringer og saker fra ID-juristen, tverrfaglig forskning og dialog på tvers av offentlig og privat sektor, har SODI-prosjektet identifisert tekniske, juridiske, organisatoriske og institusjonelle svakheter i økosystemet som utgjør den digitale identitetsforvaltningen i Norge. Denne rapporten presenterer sårbarheter og risiko prosjektet har avdekket, og kommer med konkrete forslag til tiltak.

Både i lys av internasjonale rammeverk,[8] og basert på erfaringene her til lands bør Norge arbeide videre med å utvikle et mer robust, inkluderende og rettferdig økosystem for digital identitetsforvaltning. Innsiktene fra prosjektet er særlig relevante nå, i lys av Norges tilpasning til eIDAS 2.0 med tilhørende Europeiske Digitale Identitetslommebøker (EUDI Wallets). [9]

---

[6] Følgende aktører er partnere i SODI-prosjektet: UiO, NTNU, Universitetet i Tartu, JURK, Jussbuss, Kirkens Bymisjon Gatejuristen, Finans Norge, Bits, DNB, Forbrukerrådet, Forbrukertilsynet, Norsis, Tenerity, Skatteetaten, NAV, Digitaliseringsdirektoratet, Politidirektoratet, Utlendingsdirektoratet samt advokatfirmaene Haavind, Ræder, Brækhus, Bull, Langseth, CMS Kluge og Dalan.

[7] Sluttrapporten for prosjekt ID-juristen ble publisert høsten 2024, sluttrapport_id-juristen_endelig.pdf.

[8] FN's «DPI Safeguards Framework» Universal DPI Safeguards Framework og OECD Recommendation of the Council on OECD Legal Instruments the Governance of Digital Identity

[9] Forordning (EU) 2024/1183 (eIDAS2) endrer og utvider forordning (EU) 910/2014 (eIDAS) som er implementert i Norge gjennom lov om elektroniske tillitstjenester. Forordningene regulerer bl.a. eID,

2.2. Kort om rapporten og høring

Denne rapporten er et førsteutkast som sendes på høring våren 2025 til relevante aktører, interessenter og offentligheten med formål om å få tilbakemeldinger og innspill før en endelig versjon ferdigstilles. Rapporten bygger blant annet på forskning utført innen rammen av SODI-prosjektet og praktiske erfaringer fra rettshjelpstilbudet ID-juristen.[10] Deler av innholdet i rapporten overlapper med sluttrapporten fra ID-juristen, som ble ferdigstilt og publisert høsten 2024.[11] Den trekker også på erfaringer fra og dialog med private og offentlige aktører som er tilknyttet prosjektet. Det understrekes at samarbeidspartnerne som er med i SODI-prosjektet ikke har deltatt direkte i utformingen av rapporten, og at ulike samarbeidspartnere kan ha ulike meninger og interessekonflikter knyttet til rapportens anbefalinger.

Rapporten er dessuten basert på offentlige strategier, risiko- og sårbarhetsanalyser, og andre relevante rapporter fra norske og internasjonale aktører. Den presenterer avdekkede svakheter og risiko i dagens system for digital identitetsforvaltning i Norge, og fremmer konkrete tiltak for en mer robust, inkluderende og sikker forvaltning. En del tiltak er sammenfallende med tiltak som er anbefalt av andre aktører, for eksempel i Områdegjennomgangen av identitetsforvaltningen.

Den digitale identitetsforvaltningen er kompleks, og består av et stort økosystem av aktører, tekniske løsninger og rettslig regulering. Det er verken mulig å gi en uttømmende problembeskrivelse eller foreslå tiltak som løser alle problemer. Noen problemstillinger og forslag til tiltak er basert på et solid erfaringsgrunnlag. På andre områder er behandlingen mer overfladisk og tiltakene har mer preg av ideer.

Rapporten er strukturert slik at den først gir en oversikt over eksisterende mål, organisering og rettslig rammeverk for den digitale identitetsforvaltningen i Norge. Deretter presenteres 10 overordnede styringsprinsipper for den digitale identitetsforvaltningen, etterfulgt av en detaljert gjennomgang av dagens utfordringer knyttet til hvert styringsprinsipp med utkast til anbefalte tiltak for hver utfordring.

Avslutningsvis adresserer rapporten kort de strategiske veivalg Norge står overfor i lys av den kommende eIDAS 2.0-forordningen og innføringen av europeiske digitale identitetslommebøker (EUDI Wallet).

Den endelige rapporten vil bli lansert i forbindelse med avslutningen av SODI-prosjektet og sluttkonferansen som avholdes høsten 2025.

3. Digital identitetsforvaltning i Norge

3.1. Eksisterende mål og strategier

Identitetsforvaltning i en nasjonal kontekst handler om å ha systemer som sikrer at alle innbyggerne har en juridisk identitet som kan bevises og som gjør det mulig å knytte individene

elektronisk signatur og en rekke andre tillitstjenester. Forordning (EU) 2024/1183 er våren 2025 ennå ikke tatt inn i EØS-avtalen.

[10] En samlet oversikt over publikasjoner i SODI-prosjektet er tilgjengelig her: Publikasjoner - Institutt for privatrett.

[11] sluttrapport_id-juristen_endelig.pdf

til rettigheter og forpliktelser. Tilgang til en juridisk identitet som kan bevises fysisk og digitalt er en grunnforutsetning for deltakelse i samfunnet.

Koordineringsorganet for ID-forvaltning (KoID)[12] har definert hva som utgjør god identitetsforvaltning gjennom følgende visjon:

1. Én person, én identitet i Norge
2. Enhver som har fått tildelt et norsk identitetsnummer, i form av et d-nummer eller et fødselsnummer, skal gis mulighet til å dokumentere på en troverdig måte, at han er rette eier av identitetsnummeret fysisk og digitalt, for å ivareta grunnleggende behov.
3. Alle med et norsk identitetsnummer skal oppleve trygghet for at ingen andre skal kunne overta identiteten. Ingen med norsk identitetsnummer skal utsettes for ID-tyveri.
4. Ingen skal kunne operere med falske eller fiktive identiteter i Norge

Til tross for identitetsforvaltningens grunnleggende betydning for samfunnets funksjon, finnes det i dag ingen helhetlig strategi for identitetsforvaltning som omfatter både offentlig og privat sektor og som dekker alle sider av identitetsforvaltningen. To eksisterende strategier er likevel av sentral betydning:

Nasjonal strategi for eID i offentlig sektor[13] har som mål å «adressere svakheter ved eID-løsningene som er avgjørende for å nå ut til alle relevante brukergrupper, redusere digitalt utenforskap og understøtte bedre, mer robuste og helhetlige eID-løsninger for både brukere og sektorer». Strategien er en oppfølgning av en Områdegjennomgang av identitetsforvaltningen fra 2019.[14] Mer konkrete mål og tiltak inkluderer at alle skal kunne skaffe seg en eID på det sikkerhetsnivået de har behov for, at løsningene for innlogging til offentlige tjenester skal være sikre, kostnadseffektive og helhetlige, at det skal være sikre og effektive løsninger for eID til offentlige ansatte, at løsningene skal være tilpasset markeds- og teknologiutviklingen og at samordningen mellom sektorer og forvaltningsnivåer skal være kostnadseffektiv og god.[15]

Som tittelen tilsier, er strategien begrenset til nettopp bruk av eID i offentlig forvaltning, og tar ikke for seg andre deler av den digitale identitetsforvaltningen. Strategien dekker heller ikke alle deler av den digitale identitetsforvaltningen i offentlig sektor.

Den generelle **digitaliseringsstrategien** for 2024-2030 har et bredere nedslagsfelt, og en hovedmålsetting er at Norge skal være verdens mest digitaliserte land innen 2030.[16] Strategien løfter ikke identitetsforvaltning konkret, men peker på en del generelle mål og forutsetninger for digitalisering, som også er relevante for den digitale identitetsforvaltningen:

1. Forsterke styring og samordning i offentlig sektor
2. Sørge for en sikker og fremtidsrettet digital infrastruktur

[12] KoID består av Digdir, Skatteetaten, UDI og Politiet.
[13] Nasjonal strategi for eID i offentlig sektor
[14] Rapporter – områdegjennomgang av ID-forvaltningen - regjeringen.no. Områdegjennomgangen består av en hovedrapport og en tilleggsrapport. Sistnevnte omhandler særskilt spørsmål om eID.
[15] Strategien er supplert av en Handlingsplan for nasjonal strategi for eID i offentlig sektor: Handlingsplan for nasjonal strategi for eID i offentlig sektor | Digdir
[16] Digitaliserings- og forvaltningsdepartementet, Fremtidens digitale Norge Nasjonal digitaliseringsstrategi 2024-2030, Fremtidens digitale Norge – nasjonal digitaliseringsstrategi 2024–2030.

3. Styrke sikkerheten, beredskapen og kriminalitetsbekjempelsen
4. Sikre et godt og ivaretatt personvern for alle
5. Sikre en fremtidsrettet digital kompetanse

Strategien understreker også at regelverket som setter rammer for digitaliseringen «skal sikre grunnleggende rettigheter, blant annet retten til privatliv, ytringsfrihet og ikke-diskriminering».[17] Strategien inneholder imidlertid få konkrete tiltak og planer for hvordan de overordnede målsettingene skal oppnås. Etter vårt syn utgjør en helhetlig digital identitetsforvaltning, med de tiltakene som foreslås i denne rapporten, en grunnforutsetning for at målene i digitaliseringsstrategien skal kunne oppnås.

3.2. Et økosystem av aktører og løsninger

I den digitale identitetsforvaltningen spiller systemer for elektronisk identifikasjon (eID) en nøkkelrolle. Bruk av eID skal muliggjøre sikker identifisering og autentisering på nett, og dermed også sikker og rettmessig tilgang til både offentlige og private tjenester. I Norge står bruken av privateide markedsbaserte løsninger sentralt. BankID, Buypass og Comfides er markedsbaserte eID-systemer som tilbyr eID-er på sikkerhetsnivå «høyt» i henhold til det rettslige rammeverket.[18] I tillegg har vi den offentlige løsningen MinID, som er på det lavere sikkerhetsnivået «betydelig». eID-leverandørene har sentrale roller mht. sikkerhet, tildeling, bruk og tilbakekall/sperring av eID. En rekke private aktører tilbyr også såkalte tillitstjenester, som supplerer og støtter bruk av eID. eID-systemene, og særlig BankID – som er den mest brukte løsningen – har blitt så integrert i privat og offentlig sektor i Norge at det fungerer som en grunnleggende infrastruktur i identitetsforvaltningssystemet – et "underlag" som styrer "sosiale praksiser".[19]

Det finnes imidlertid også en rekke mer sektorspesifikke autentiserings- og eID-løsninger, som spiller sentrale roller på sine områder. I undervisningssektoren i Norge benyttes FEIDE som eID for elever på alle alderstrinn. Apple, Google og Facebook tilbyr såkalt føderert innlogging til andre tjenester. Vipps kan i en del sammenhenger brukes som innlogging. Også kredittkort har vært benyttet for identifiserings- og autentiseringsformål i enkelte sammenhenger. Banksektoren har dessuten i en viss utstrekning alternative løsninger for innlogging i nettbank for de som ikke har BankID.

Digital identitetsforvaltning handler imidlertid ikke bare om eID-systemer og tekniske autentiseringsløsninger som sådan, men involverer mange aktører med ulike roller og oppgaver, digitale infrastrukturer og løsninger og organisatoriske forhold. Vi skal i det følgende beskrive noen hovedelementer og sentrale aktører, uten at fremstillingen er ment å være uttømmende.

Offentlige myndigheter fastsetter en persons grunnidentitet i Folkeregisteret og har ansvar for utstedelse av fysiske ID-bevis, som danner grunnlaget for utstedelse av en eID. Folkeregisteret

[17] Ibid. s. 17.
[18] EUs forordning (EU) 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS), som er gjennomført i norsk rett i lov om elektroniske tillitstjenester (LOV-2018-06-15-44). eIDAS ble oppdatert i 2024, se senere i teksten. Se også Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften) (FOR-2019-11-21-1578).
[19] Benedict Kingsbury and Nahuel Maisley. "Infrastructures and laws: publics and publicness." *Annual Review of Law and Social Science* 17.1 (2021): 353-373.

administreres av Skatteetaten, som er underlagt Finansdepartementet. Politiet, som hører under Justis- og beredskapsdepartementet, har ansvar for utstedelse av ID-bevis (pass og nasjonalt ID-kort). Utlendingsdirektoratet, som er underlagt Justis- og beredskapsdepartementet, skal sette i verk flyktning- og innvandringspolitikken, og har interesser knyttet til i hvilken grad utlendinger skal inkluderes i den norske identitetsforvaltningen, herunder hvem som skal få norsk id-nummer og ID-bevis.

ID-porten er en offentlig autentiseringsløsning som gir innbyggerne tilgang til offentlige digitale tjenester. Gjennom ID-porten kan brukerne velge mellom BankID, Buypass, Commfides og MinID for å logge inn på offentlige tjenester som NAV, Skatteetaten og Helsenorge. I henhold til Digitaliseringsrundskrivet er det obligatorisk for statlige virksomheter å benytte ID-porten for innlogging.[20] Kommunene har fått en særlig oppfordring om å vurdere om kravene og anbefalingene i Digitaliseringsrundskrivet kan være relevante for deres digitaliseringsarbeid.[21] I praksis er dette oppfattet som en anbefaling bl.a. om bruk av offentlige felleskomponenter som ID-porten. ID-porten forvaltes av Digitaliseringsdirektoratet (Digdir). Digdir har også ansvar for drift og administrasjon av MinID. Digdir er underlagt Digitaliserings- og forvaltningsdepartementet (Dfd) som har det overordnede ansvaret for IKT- og forvaltningspolitikken.

Offentlige virksomheter som benytter ID-porten (gjerne omtalt som «tjenesteeiere»), bestemmer selv hvilke sikkerhetsnivåer som kreves for innlogging til deres tjenester. Noen tjenester krever eID på nivå "høyt", mens andre aksepterer nivå "betydelig". Dette betyr at kravet til eID varierer avhengig av tjenestens art og den risikovurderingen som er gjort av den enkelte etaten.

ID-porten kan kun brukes av offentlige virksomheter, og for tjenester utført for det offentlige eller i det offentliges interesse, og det finnes ingen tilsvarende felles portal for private tjenester. Det finnes imidlertid flere autentiseringsportaler for private virksomheter, som også bistår med integrasjon mot eID-leverandørene, men brukersteder som ønsker å tilby innlogging med f.eks. BankID må inngå en direkte avtale med eID-leverandøren.

Offentlige tjenesteeiere og private brukersteder har en viktig rolle i identitetsforvaltningen. Det er de som setter konkrete krav til sikkerhetsnivå for sine tjenester og meldinger, det er de som velger hvilke eID-tjenester de vil akseptere, det er de som tilrettelegger viktige deler av dialogen med brukerne, og derigjennom også kan påvirke holdninger og aktsomhet, og de har stor grad av kontroll på hvilken dokumentasjon som samles inn og lagres i forbindelse med transaksjoner på deres nettsteder o.l. Det er derfor sentralt at tjenesteeiere og brukersteder involveres i strategiene for identitetsforvaltningen slik at de kan bidra med synspunkter og løsninger og ansvarliggjøres for de valgene de tar.

---

[20] Rundskriv 9.2.2024 Nr. D-1/24, ref. 24/474-1, Digitaliseringsrundskrivet, Digitaliseringsrundskrivet - regjeringen.no, Punkt 1.7.

[21] Se brev fra kommunal- og distriktsdepartementet, datert 26. januar 2022, vedrørende "*Digitalisering i offentlig sektor - orientering til kommunesektoren*", der det bla fremgår at: *"Siden rundskrivet viser til regjeringsbeslutninger og en rekke krav som er hjemlet i lover som også gjelder for kommunal sektor, kan deler av rundskrivet være relevant for kommuner og fylkeskommuner. Rundskrivet er vedlagt. Departementet oppfordrer kommuner og fylkeskommuner til å gjøre seg kjent med kravene som stilles og anbefalingene som gis til statlige virksomheter på digitaliseringsområdet, og vurdere om noen av disse kan være relevante for digitaliseringsarbeidet i kommunal sektor."*

Systemer som bidrar til å håndtere og rette feil når identiteter og autentiseringsløsninger er misbrukt, i både privat og offentlig sektor, er også en del av identitetsforvaltningen. Når digitale identiteter er misbrukt som ledd i kriminell virksomhet, må feil rettes av involverte aktører. Politi- og påtalemyndigheter har ansvar for etterforskning og strafferettslig forfølgning. Privatrettslige tvister om konsekvenser av identitetsmisbruk avgjøres i siste instans av domstolene, som derfor også spiller en sentral rolle mht. å fordele risiko og ansvar for sårbarheter i den digitale identitetsforvaltningen.

3.3. Rettslig regulering av identitetsforvaltning

Fordi den digitale identitetsforvaltningen inkluderer en lang rekke aktører, organisatoriske forhold, tekniske løsninger og problemstillinger, er også den rettslige reguleringen av den digitale identitetsforvaltningen kompleks, og griper inn i mange ulike rettsområder.

eIDAS-forordningen fra 2014 (eIDAS 1.0) med tilhørende rettsakter, som regulerer eID og elektroniske signaturer, står sentralt. eIDAS-forordningen får i utgangspunktet kun anvendelse på de eID-ordningene «som er meldt av en medlemsstat» jf. artikkel 2 nr. 1. De eID-ordningene som blir meldt, er underlagt forordningens system for tilsyn og kontroll med at sikkerhetskravene som følger av forordningen med tilhørende rettsakter blir oppfylt.[22] I tillegg til eIDAS 1.0 finnes det en egen ordning i norsk rett, der tilbyderne selv kan deklarere hvilket sikkerhetsnivå de tilfredsstiller, såkalt selvdekarasjon av eID-systemer. Ordningen er regulert i selvdeklarasjonsforskriften.[23] I Norge er BankID og Buypass notifisert under eIDAS-regimet, mens Commfides og MinID er selvdeklarert.

I 2024 ble eIDAS 2.0 vedtatt. Den nye forordningen innebærer enkelte sentrale endringer i det rettslige rammeverket for eID. Den viktigste endringen er en plikt for medlemsstatene til å sikre at «alle» innbyggerne har tilgang til en såkalt Europeisk Digital Lommebok, som blant annet skal inneholde en eID på sikkerhetsnivå «høyt». Forordningen stiller tekniske krav til utforming og funksjonalitet i de digitale lommebøkene. Vi kommer nærmere tilbake til eIDAS 2.0 i punkt 6. Det er imidlertid viktig å ha klart for seg at både eIDAS 1.0 og eIDAS 2.0 kun regulerer enkelte sider av den digitale identitetsforvaltningen; primært i form av krav til eID-utstedere og tillitstjenestetilbydere, og tekniske krav til eID-systemer og etter hvert de digitale lommebøkene. Mange av utfordringene knyttet til den digitale identitetsforvaltningen gjelder forhold som ikke reguleres direkte av eIDAS – verken 1.0 eller 2.0. Dessuten gir eIDAS 2.0 medlemsstatene relativt stor valgfrihet mht. hvordan forordningen skal gjennomføres. Disse valgene kan ha stor betydning for hvorvidt vi forsterker eller avhjelper de utfordringene vi har i den digitale identitetsforvaltningen. Det er ytterst viktig at eIDAS 2.0 og implementering og bruk av de nye digitale lommebøkene ses i sammenheng med den digitale identitetsforvaltningen og reguleringen av denne i stort. Vi kommer som nevnt nærmere tilbake til eIDAS 2.0 i punkt 6. I det følgende skal vi kort beskrive andre sentrale regler og rettsområder som eIDAS 2.0 må ses i sammenheng med.

[22] Se særlig eIDAS artikkel 7, 9 og 12, Kommisjonens gjennomføringsbeslutning (EU) 2015/1502 om fastsettelse av tekniske minstespesifikasjoner og minstekrav til framgangsmåter for sikkerhetsnivåene for elektroniske identifikasjonsmidler og Kommisjonens gjennomføringsbeslutning (EU) 2015/296 om fastsettelse av saksbehandlingsregler for samarbeid mellom medlemsstatene om elektronisk identifikasjon.

[23] Se Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften) (FOR-2019-11-21-1578).

En trygg digital identitetsforvaltning har som tidligere nevnt tett sammenheng med fastsettelse av en persons grunnidentitet og tilgang til fysisk ID-bevis. Regler for dette finnes blant annet i folkeregisterloven, passloven og ID-kortloven.

Bruken av eID eller alternative autentiseringsløsninger kan dessuten være regulert i sektorspesifikk lovgivning. For eksempel brukes eID-løsninger for å fylle kravene til sterk kundeautentisering for betalingstjenester og for å identifisere og autentisere kunder i finansforetak som ledd i oppfyllelse av regler knyttet til forebygging av hvitvasking. Finansforetak og enkelte andre aktører, som for eksempel eiendomsmeglerforetak, er dessuten underlagt generelle krav til gjennomføring av risikovurderinger og sikkerhetstiltak i IKT-forskriften.

I offentlig sektor er elektronisk kommunikasjon særskilt regulert i forvaltningsloven § 15 a og i eForvaltningsforskriften. Offentlige myndigheter er også underlagt mer generelle plikter knyttet til blant annet ytelse av likeverdige tjenester til borgerne og oppfyllelse av menneskerettigheter.

Både offentlige og private tekniske løsninger må utformes i overensstemmelse med krav til universell utforming i likestillings- og diskrimineringsloven kapittel 3. Der personer for eksempel ikke får tilgang til private eller offentlige tjenester på grunn av forhold som utgjør et diskrimineringsgrunnlag, som alder, etnisitet eller funksjonsnedsettelser, blir også diskrimineringsregelverket relevant. Diskrimineringsforbudet gjelder for både private og offentlige aktører.

Identitetsforvaltning innebærer per definisjon innsamling og videre behandling av personopplysninger, og både utstedelse og bruk av eID skal skje i henhold til bestemmelsene i personvernforordningen (GDPR)[24] og personopplysningsloven[25].

Ettersom den digitale identitetsforvaltningen griper inn i mange ulike rettsområder, vil også flere tilsynsmyndigheter spille en rolle i dette økosystemet: Nkom skal føre tilsyn med eID-leverandører, Finanstilsynet har tilsynsansvar for finansforetak, Datatilsynet fører tilsyn med personvernregelverket, Uu-tilsynet fører tilsyn med regler om universell utforming, Sivilombudet fører kontroll med den offentlige forvaltningen for å hindre urett mot den enkelte – for å nevne noen.

Når digitale identiteter misbrukes i økonomisk kriminalitet, reguleres de straffbare forholdene av strafferetten, mens ulike privatrettslige regler gjerne vil være avgjørende for hvem som må bære det økonomiske tapet. Prosessretten, herunder regler om bevisbyrde, spiller også en sentral rolle.

3.4. Behov for systemtenkning og styringsprinsipper

I praksis har identitetsforvaltning alle kjennetegnene til et komplekst adaptivt system, der en rekke aktører har spesialiserte roller og oppgaver. [26] Det består av mange ulike elementer som er sammenkoblet og i kontinuerlig endring. Det betyr at systemet fort utvikler sin egen dynamikk og

[24] Forordning om vern av fysiske personer i forbindelse med behandling av personopplysninger (EU) 2016/769.
[25] Lov om behandling av personopplysninger (personopplysningsloven), LOV-2018-06-15-38.
[26] Scott Page, "What sociologists should know about complexity." *Annual Review of Sociology* 41.1 (2015): 21-41.

selvorganisering,[27] noe som igjen kan skape uforutsette konsekvenser for aktører og brukere – for eksempel omfattende svindel og ekskludering. Dessuten er det vanskelig å adressere disse konsekvenser enkeltvis eller stegvis. Det skyldes at systemet ikke er særlig transparent eller lett forklarbart, og at en endring på ett område kan ha utilsiktet effekter andre steder.[28] Resultatet er et system som kan forbli stabilt og motstandsdyktig mot endringsforsøk, men som også kan bli svært volatilt dersom det når et vippepunkt.[29] Et grunnleggende problem i den digitale identitetsforvaltningen er fravær av helhetlig styring og kontroll.

Disse problemene forsterkes ved at feltet er preget av en rekke *interessekonflikter* mellom ulike aktører og motstående hensyn som alle er en del av økosystemet. Dette omfatter interessekonflikter mellom private aktører og offentlig forvaltning, men også internt i offentlig forvaltning og mellom ulike private aktører. For eksempel kan innvandringspolitiske hensyn være i konflikt med hensyn til kontroll og sikker identifisering for spørsmål om hvilke utlendinger som skal tildeles norsk identifikasjonsnummer og ID-bevis. Økonomiske interesser hos privateide markedsaktører for eID kan tilsi en annen prioritering av inkludering og sikkerhet enn den som er foretrukket av offentlige myndighetsaktører. For å beskytte egne økonomiske interesser vil både private og offentlige brukersteder kanskje ønske at en stor del av risikoen for misbruk skal legges på sluttbrukerne. I noen sammenhenger vil hensyn til personvern, kriminalitetsbekjempelse og inkludering trekke i ulike retninger – og ulike aktører vil vekte de ulike hensynene forskjellig.

I denne rapporten vil vi, i form av en rekke problembeskrivelser, vise at en dypere forståelse av utfordringene forutsetter innsikt i systemets mange elementer, deres gjensidige koblinger og hvordan disse interaksjonene kan føre til utilsiktede konsekvenser. Dette krever en politikk som fokuserer på tiltak med gode systemiske virkninger, et styringsapparat som kan utføre kontroll og tilsyn, samt et sikkerhetsnett for alle som blir rammet.

4. Helhetlig strategi for digital identitetsforvaltning: Styringsprinsipper

Som nevnt, mangler det en helhetlig strategi for digital identitetsforvaltning i Norge. Gjeldende mål og strategier, slik disse er beskrevet i punkt 3.1, dekker bare enkelte sider ved identitetsforvaltningen. Etter vårt syn er det behov for å utvikle en helhetlig strategi, basert på følgende 10 styringsprinsipper:

1. **Universell tilgang**

Alle skal ha tilgang til en juridisk identitet som kan bevises fysisk og digitalt, og som gir likeverdig tilgang til grunnleggende offentlige og private tjenester. Digital identitet er en forutsetning for samfunnsdeltakelse, og det må sikres at ingen utelukkes på grunn av manglende tilgang til eller problemer med bruken av eID og andre tekniske løsninger. Myndighetene har en plikt til å jobbe aktivt for å sikre at digitale løsninger og infrastrukturer ikke fører til negativ forskjellsbehandling

[27] Van Assche, Kristof, et al. "The social, the ecological, and the adaptive. Von Bertalanffy's general systems theory and the adaptive governance of social-ecological systems." *Systems Research and Behavioral Science* 36.3 (2019): 308-321; Ruhl, J. B., Daniel Martin Katz, and Michael J. Bommarito. "Harnessing legal complexity." *Science* 355.6332 (2017): 1377-1378.
[28] Meadows, Donella. "Leverage points-places to intervene in a system." (2015).
[29] Anthea Roberts and Taylor St John. "Complex designers and emergent design: reforming the investment treaty system." *American Journal of International Law* 116.1 (2022): 96-149.

av utsatte grupper. Tekniske løsninger må utformes slik at de kan brukes av flest mulig, herunder av personer med funksjonsnedsettelser og lav digital kompetanse.

2. **Svindelforebygging og sikkerhetsløsninger**

Ingen individer skal oppleve uønsket bruk av sin egen digitale identitet. De tekniske og organisatoriske sikkerhetsløsningene må legge til rette for at brukerne og systemet som helhet kan hindre og oppdage uønsket bruk av digitale identiteter. Sikkerhetsløsningene må ta høyde for uønsket bruk fra både nærstående og fremmede. Opplæring og brukerstøtte må være tilgjengelig for brukerne, men de må kunne kontrollere bruken av sin digitale identitet uten omfattende opplæring eller kunnskap. Brukerstedene må ta høyde for at sikkerhetsløsningene kan svikte. Brukerstedene må også sørge for at brukerne forstår handlingen de gjennomfører.

3. **Rettssikkerhet: Gjenoppretting og reparasjon**

Den digitale identitetsforvaltningen må inkludere systemer for å gjenopprette kontroll over egen eID, rette feil og reparere problemer og skadevirkninger forårsaket av ID-misbruk. Fordi ingen systemer er feilfrie og det er umulig å forhindre all svindel og identitetsmisbruk, må det finnes effektive mekanismer for å rette feilene. Rettssikkerheten til ofrene må ivaretas og rettssystemet må sikre en rettferdig fordeling av tap og risiko.

4. **Autonomi: selvbestemmelse og personvern**

Alle individer skal ha kontroll over sin egen digitale identitet, hvem som har tilgang til den, og hvordan den brukes. Brukere skal ha rett til innsyn i egne identitetsdata og kunne begrense eller tilbakekalle samtykke til deling av opplysninger. Personvern er en grunnleggende menneskerettighet, og digital identitet må forvaltes i tråd med personvernlovgivning og prinsippene om dataminimalisering og brukerkontroll. Bruk av eID må være frivillig.

5. **Transparens: åpenhet og gjennomsiktighet**

Den digitale identitetsforvaltningen må være så åpen og gjennomsiktig som mulig. Dette gjelder både tekniske løsninger, organisatoriske forhold og sentrale beslutningsprosesser. Informasjon om tekniske løsninger og systemarkitektur bør være offentlig tilgjengelige med tilstrekkelig detaljeringsgrad. Selv om det i enkelte tilfeller kan være nødvendig å begrense innsyn i tekniske detaljer av hensyn til sikkerhet og personvern, må enhver slik begrensning bygge på en konkret risikovurdering. Eventuelt hemmelighold bør være snevert og ta hensyn til spesifikke innsynsbehov, som for eksempel oppklaring av svindelsaker.

6. **Ansvar: tilsyn, kontroll og sanksjoner**

Det må finnes en tydelig ansvarsfordeling mellom ulike aktører og tilsynsmyndigheter, og det må sikres at relevante aktører, herunder eID-leverandører, offentlige instanser og private brukersteder overholder regelverket. Regler og rettigheter har liten verdi dersom de ikke håndheves effektivt. Tilsynsmyndigheter må ha tilstrekkelige ressurser og myndighet til å gjennomføre revisjoner, pålegge sanksjoner og sørge for etterlevelse av krav til likebehandling, sikkerhet og personvern.

7. **Innovasjon: interoperabilitet, valgfrihet og konkurranse**

Digitale identitetsløsninger og tilhørende infrastruktur må være fleksible og legge til rette for teknologisk utvikling og innovasjon. Det bør arbeides for at ingen aktører får en monopollignende posisjon. eID-løsninger bør være interoperable og bygge på alminnelig

anerkjente og tilgjengelige standarder, slik at brukerne kan velge mellom ulike løsninger uten å miste tilgang til viktige tjenester. Offentlige og private aktører bør samarbeide for å utvikle nye, sikre og brukervennlige identitetsløsninger.

8. **Samfunnssikkerhet og beredskap**

Identitetsforvaltningen må være forberedt på cyberangrep, teknisk svikt og andre krisesituasjoner. eID-systemer og tilhørende infrastruktur må være robuste og sikre kontinuerlig tilgang til kritiske tjenester, selv i ekstraordinære situasjoner. Det må etableres beredskapsplaner som sikrer redundans og alternative løsninger dersom én identitetsleverandør skulle falle ut. Samtidig må tilliten til eID-systemene opprettholdes gjennom åpenhet, kontrollmekanismer og tydelig regulering.

9. **Demokratisk forankring**

Identitetsforvaltningen er en samfunnskritisk funksjon som må ha demokratisk forankring. Myndighetene må ha en tydelig rolle i styringen av digital identitet, og det må sikres at private aktører ikke får uforholdsmessig stor makt over hvem som får tilgang til samfunnet. Systemet må utformes slik at det sikrer reell deltakelse fra berørte interessenter, særlig sårbare og risikoutsatte personer, slik at deres behov ivaretas.

10. **Helhetlig styring: Systemtenkning og samhandling**

Identitetsforvaltningen er et komplekst system med mange elementer som er i stadig endring. Styringen må derfor være helhetlig slik at man unngår at tiltak som iverksettes på ett område får utilsiktede konsekvenser på et annet. Systemet omfatter en rekke ulike elementer, både tekniske, organisatoriske og rettslige – både privatrettslige og offentligrettslige. Alle disse elementene påvirker hverandre, og styringen må derfor identifisere hvilke konsekvenser endringer på ett område kan ha for helheten. For å sikre at ulike interessegrupper ivaretas når det gjelder konsekvenser av endringer, bør det legges til rette for gode arenaer for dialog om utfordringer og løsninger, og nye løsninger og tiltak bør testes på en måte som bekrefter at ønskede effekter oppnås. Ansvar og kontrollfunksjoner knyttet til løsninger og aktører i identitetsforvaltningen må være avklart og informasjon om dette må være lett tilgjengelig, bl.a. slik at det er mulig å diskutere om organiseringen er hensiktsmessig og fungerer som den skal.

5. Utfordringer og tiltak

I dette punktet skal vi beskrive utfordringene i den digitale identitetsforvaltningen i Norge. Vi tar utgangspunkt i de ti styringsprinsippene som er beskrevet ovenfor, og drøfter i hvilken grad dagens digitale identitetsforvaltning er i tråd med rettslige forpliktelser og overordnede mål. Drøftelsene bygger på erfaringer og forskning i SODI-prosjektet, samt ulike offentlig tilgjengelige rapporter og risiko- og sårbarhetsanalyser, erfaringer fra andre land og dialog med relevante private og offentlige aktører.

5.1. Universell tilgang

I dette punktet tar vi for oss utfordringer knyttet til styringsprinsipp nummer 1:

«Alle skal ha tilgang til en juridisk identitet som kan bevises fysisk og digitalt, og som gir likeverdig tilgang til grunnleggende offentlige og private tjenester. Digital identitet er en forutsetning for samfunnsdeltakelse, og det må sikres at ingen utelukkes på grunn av

manglende tilgang til eller problemer med bruken av eID og andre tekniske løsninger. Myndighetene har en plikt til å jobbe aktivt for å sikre at digitale løsninger og infrastrukturer ikke fører til negativ forskjellsbehandling av utsatte grupper. Tekniske løsninger må utformes slik at de kan brukes av flest mulig, herunder av personer med funksjonsnedsettelser og lav digital kompetanse.»

Digitaliseringen av samfunnet skaper store problemer med utenforskap som innebærer redusert eller manglende tilgang til offentlige og private tjenester og reduserte muligheter for likeverdig deltakelse i samfunnet. I eID-strategien oppgis det at ca. 14 % av befolkningen i Norge over 16 år (600.000 personer) regnes som ikke-digitale.[30] Utenforskapsproblemene skyldes et samvirke av flere forhold, som drøftes nærmere i det følgende:

- Flere grupper i befolkningen har ikke tilgang til eID på øverste sikkerhetsnivå (punkt 5.1.1)
- eID-løsningene og tilhørende infrastruktur er ikke tilstrekkelig universelt utformet og tilpasset ulike brukergruppers behov (punkt 5.1.2).
- Alternative analoge/fysiske og digitale løsninger er blitt dårligere eller helt borte (punkt 5.1.3).
- Fullmaktsløsninger eksisterer ikke eller er for dårlige (punkt 5.1.4).
- For mange tjenester krever eID på øverste sikkerhetsnivå (punkt 5.1.5).

Summen av disse forholdene fører til strukturell diskriminering og menneskerettsbrudd (punkt 5.1.6).

5.1.1. Flere grupper i befolkningen har ikke tilgang til eID på øverste sikkerhetsnivå

Manglende tilgang til BankID eller annen eID på øverste sikkerhetsnivå innebærer vanskeliggjort tilgang til både private og offentlige tjenester.[31] eIDAS og tilhørende regelverk oppstiller noen grunnvilkår for utstedelse av eID på nivå høyt. Innehaveren må være registrert i Folkeregisteret med et norsk identitetsnummer (d-nummer eller fødselsnummer) og ha et gyldig norsk eller utenlandsk identitetsbevis.[32] Det betyr at personer som ikke har et norsk identitetsnummer og/eller gyldig identitetsbevis heller ikke kan få eID i Norge. Tilgang til eID i Norge henger derfor sammen med reglene i passloven og ID-kortloven om hvem som har rett til norsk identitetsbevis og reglene i folkeregisterloven og folkeregisterforskriften om hvem som kan få norsk d-nummer

[30] Ibid. s. 20.

[31] Se Forbrukerrådet, Utanforskap i forbrukarmarknadene Digitale og andre hindringar som står i vegen for at forbrukarane kan kjøpe varer og tenester (2023), forbrukerradet-utanforskap-i-forbrukarmarknadene-no.pdf. Liodden m.fl., Flyktningers møte med NAV Kommunikasjon og tilgjengelighet i en digital kontekst, NIBR-Rapport 2023:1, Flyktningers møte med NAV, NIBR.pdf, s. 61-62, JOU Jusstudentenes offentlige utredninger 2020:4, Borgernes rettigheter i møte med det digitale samfunn og offentlig forvaltning, 2020-4-digital-ekskludering.pdf (uio.no), Midtgård m.fl., Rapport Digital ekskludering i NAV Hvem, når, hvorfor? (2022), Digital ekskludering i NAV — Hvem, når, hvorfor? - SINTEF, Hilde Mosve, Digital ekskludering (2021), Digital ekskludering – NTNU medisin og helse-

[32] Se nærmere om vilkårene i Erle Kathrine Sivertsen, «Kontraheringsplikt for tilbydere av eID – særlig om forholdet mellom kontraheringsplikt og diskrimineringsvernet», I: Kjørven, Hjort og Wærstad (red.), *Bruk og misbruk av elektronisk identifikasjon* (Karnov 2022).

eller fødselsnummer. Det betyr for eksempel at utenlandske studenter som studerer i Norge, ikke kan få en norsk eID fordi de ikke har rett til et norsk d-nummer.

Det er verdt å merke seg at vi ikke har klare regler om når en person har *rett* til å få utstedt eID. Reglene er utformet som krav til tilbyderne om hvilke vilkår som (minst) må være oppfylt for utstedelse. Som vi skal komme tilbake til, er det flere grupper som oppfyller vilkårene for eID på nivå høyt som likevel ikke får tilgang fordi utstederne opererer med flere og andre vilkår enn de som følger av eIDAS med tilhørende regelverk.

På grunn av BankID's dominerende posisjon i markedet for eID, og fordi BankID er den eneste eID'en som også gir tilgang til finansielle tjenester, fokuserer vi særlig på tilgang til BankID i fortsettelsen.

Innledningsvis vil vi påpeke at tilgang til BankID i praksis forutsetter at man har et kundeforhold i en bank. Det følger av standardavtale om BankID at «Banken din kan kreve at du har et kundeforhold i Banken for å utstede BankID til deg.»[33] En praktisk konsekvens av dette, er at forhold som er til hinder for opprettelse av et kundeforhold i en bank i praksis også er til hinder for tilgang til BankID. Dette får betydning for flere grupper på ulike måter.

For det første innebærer koplingen til finansielle tjenester at **hvitvaskingsregelverket** kan utgjøre et hinder for utstedelse og/eller føre til oppsigelse og sperring av BankID. Sakene kan deles i to kategorier: 1) tilfeller der hvitvaskingsreglene utgjør et reelt hinder og 2) tilfeller der bankene på grunn av «de-risking» ikke ønsker å opprette eller opprettholde et kundeforhold selv om hvitvaskingsreglene ikke utgjør et faktisk hinder (eller endog forbyr praksisen).[34]

Det europeiske banktilsynet (EBA) peker i en rapport fra 2022 på at de-risiking forekommer hos finansinstitusjoner over hele EU, og at dette kan føre til finansielt utenforskap og ekskludering av hele kundekategorier.[35] Asylsøkere fra høyrisikoland er særlig utsatt.

Å skille mellom tilfeller der hvitvaskingsreglene faktisk er til hinder for inngåelse av kundeforhold, og der bankene bedriver potensielt ulovlig «de-risking», kan være vanskelig eller umulig. Saken i FinKN-2020-627 er illustrerende: En kunde fikk avslag på søknad om opprettelse av kundeforhold under henvisning til hvitvaskingsreglene. Banken viste videre til at den ikke kunne gi noen nærmere begrunnelse under henvisning til avsløringsforbudet i hvitvaskingsloven § 28. Dermed kunne verken nemnda eller kunden vurdere om avslaget var saklig eller om det dreiet seg om usaklig «de-risking» eller eventuelt andre grunner som ikke utgjør saklig grunn for kontraheringsnektelse. Saken ble av den grunn avvist fra behandling i nemnda. I et rettssikkerhetsperspektiv er det åpenbart problematisk at personer kan bli nektet et kundeforhold, og dermed også BankID, uten en begrunnelse som gjør det mulig å overprøve om hvitvaskingsreglene utgjør et reelt hinder.

En annen sak fra Finansklagenemnda Bank er også illustrerende for hvitvaskingsreglene betydning for på feltet.[36] En bankkunde opplyste til banken at et større kontantinnskudd var lønn fra prostitusjon. Det er tillatt å selge (men ikke kjøpe) seksuelle tjenester i Norge. Penger tjent på prostitusjon er dermed lovlig ervervet. Finansklagenemnda tvilte ikke på bankkundens

[33] Bits, Avtale om BankID, 56bc0c8f6d2bc51d2392eabe053f83ec38a2d4dc.pdf
[34] «De-risking» eller risikoeliminering betyr at hele grupper nektes finansielle tjenester utelukkende på grunn av gruppens eller sektorens iboende hvitvaskingsrisiko. «De-risking» er ikke tillatt, men forekommer likevel.
[35] DIN-2019-439.
[36] FinKN-2022-234.

forklaring, men viste til at banken etter hvitvaskingsreglene ikke kan basere seg utelukkende på kundens forklaring. Siden dokumentasjon – naturlig nok – var umulig å oppdrive, var oppsigelse av kundens brukskonto, kort, nettbank og BankID saklig i følge Finansklagenemnda. Den praktiske konsekvensen er trolig at **prostituerte** som gruppe også vil ha problemer med tilgang til BankID.

For **barn og unge** er det flere barrierer for å få BankID. Utstedelse for mindreårige krever at barnet har fylt 12 år, at både barnet og foreldrene har et kundeforhold i banken, og at de med foreldreansvar gir sitt samtykke. Dersom foreldrene ikke oppfyller bankens krav til kundeforhold, for eksempel på grunn av hvitvaskingsregler eller manglende legitimasjon, påvirker dette også barnets mulighet til å få BankID. Foreldre med kundeforhold i ulike banker kan også oppleve utfordringer, da det kan kreve at én av dem bytter bank for å sikre at barnet får tilgang. Barn i fosterhjem eller barn med foreldre som ikke samarbeider, risikerer også å bli nektet BankID hvis en eller begge foreldre nekter å gi samtykke.[37]

Rapporten *Digitalt utenforskap blant barn og ungdom*, utarbeidet av Capgemini Invent for Redd Barna, dokumenterer hvordan manglende tilgang til BankID særlig rammer barn med begrensede oppholdstillatelser, barn med funksjonsnedsettelser og barn i kontakt med barnevernet. Ulik praksis blant eID-leverandørene bidrar til en uoversiktlig og uforutsigbar prosess for å skaffe eID.[38]

SODI-prosjektet har mottatt enkelthenvendelser om personer som får sperret BankID som følge av at det ikke er **regelmessig bevegelse på kontoen**: En kvinne fra Thailand med norsk ektefelle og 23 års botid i Norge, reiste til hjemlandet for en periode under pandemien. På grunn av krav til relegitimering, og at hun ikke kunne møte opp fysisk i banken med pass da hun befant seg i Thailand, ble konto og BankID sperret. Da hun returnerte til Norge og møtte opp i banken for å legitimere seg og få kontoen gjenåpnet, fikk hun ikke BankID med begrunnelse at det ikke hadde vært regelmessig bevegelse på kontoen. Hun ble fortalt at hun kunne søke igjen etter 3 måneder dersom hun kunne vise til at det i perioden regelmessig kom inntekt på kontoen.

Det er godt dokumentert at **utlendinger med d-nummer** har problemer med å få opprettet kundeforhold og BankID i norske banker.[39] Dette til tross for at verken hvitvaskingsregelverket, reglene for eID eller andre regler er til hinder for utstedelse av BankID på grunnlag av d-nummer, forutsatt at vedkommende har ID-bevis som oppfyller vilkårene.[40] I 2020 kom Diskrimineringsnemnda til at det utgjorde ulovlig diskriminering å nekte BankID til en svensk statsborger med norsk d-nummer. Avgjørelsen har imidlertid ikke ført til en endring i praksis hos mange banker. Fem år etter at Diskrimineringsnemnda kom til at det utgjorde diskriminering å ikke utstede BankID til utlendinger med d-nummer, står det fremdeles på DNB sin hjemmeside

---

[37] Katrine Kjærheim Fredwall og Tone Linn Wærstad, *Hvordan kan representasjonsreglene hindre digitalt utenforskap for barn i fosterhjem* Publisert i Fra barnerett til barns rettigheter Festskrift til Kirsten Sandberg 70 år.

[38] Capgemini-rapport-Digitalt-Utenforskap-Blant-Barn-og-Ungdom.pdf

[39] Se for eksempel Kirkens Bymisjon, I count Bostedsløse EU-migranter i Norge, Rapport_I-COUNT_2021.pdf; Lisa Dyrud, Lise Stefanussen og Sveinung Liland Hartveit, Utlendingers tilgang til banktjenester En undersøkelse av utlendingers tilgang til grunnleggende banktjenester og BankID, betydningen av reisedokumenter og Jussbuss sine erfaringer med reisedokumentsaker, SODI-rapport 2/2022, rapport-om-utlendingers-tilganger-banktjenester.pdf.

[40] Erle Katrine Sivertsen, Kontraheringsplikt for tilbydere av eID – særlig om forholdet mellom kontraheringsplikt og diskrimineringsvernet, I: Kjørven, Hjort og Wærstad (red.), Bruk og misbruk av elektronisk signatur (Karnov).

at de kun utsteder BankID til personer med norsk fødselsnummer.[41] Det er grunn til å tro at praksisen er en form for «de-risking». Det er vanskeligere og mer kostbart å gjennomføre løpende hvitvaskingstiltak på utlendinger med d-nummer, noe som kan gjøre det lite lønnsomt å ha denne gruppen som kunder.

Vanskeliggjort tilgang til eID for utlendinger har også en side til EØS-rettens grunnleggende fire friheter. Utlendinger som driver forretningsvirksomhet i Norge har store utfordringer med å håndtere virksomheten i Norge, herunder få signert avtaler, styremøteprotokoller osv. uten tilgang til BankID. Det er for øvrig verdt å merke seg at det tilsynelatende gjøres spesifikke unntak for visse grupper, herunder ansatte på ambassader og NATO-personell, som i følge DNB's nettsider likevel kan få opprettet kundeforhold med BankID basert på d-nummer, selv om det for alle andre utlendinger altså kreves norsk fødselsnummer.[42]

Det er i praksis svært vanskelig å få BankID for personer med utenlandsk **pass som ikke er maskinlesbart.**[43] FinKN har i sak FinKN-2023-868 uttalt at avslag på dette grunnlaget utgjør usaklig grunn for kontraheringsnektelse, men bankene har likevel ikke endret sin praksis. To år etter uttalelsen i FinKN, står det på DNB's hjemmeside at kun maskinlesbare pass godtas legitimasjonsdokumenter for å få utstedt BankID.[44]

Det er klart at BankID ikke skal eller bør utstedes til personer med falske ID-dokumenter. Spørsmålet er imidlertid om bankene er rigget med systemer som faktisk kan foreta gode vurderinger av ID-dokumentenes ekthet. Det er fare for at en slik retningslinje praktiseres på en måte som innebærer at det stilles spørsmål ved ektheten til ethvert pass som ikke er maskinlesbart. Det vil isåfall innebære en strategi for "de-risking" som er vanskelig både å oppdage og overprøve. Dette problemet gjør seg til en viss grad gjeldende også for Buypass og Commfides, som benytter Posten for gjennomføring av legitimasjonskontroll, se nærmere nedenfor. Problemet er imidlertid ikke bare knyttet til bankenes praksis, men er kanskje først og fremst et utslag av utfordringer knyttet til grunnidentifiseringen og utstedelse av fysiske id-bevis, som er myndighetenes ansvar.

Det er videre utfordrende for **bostedsløse** å få BankID. Finans Norge opplyser på sin hjemmeside at for å bli kunde i en bank i Norge må du «kunne oppgi bostedsadresse».[45] Kravet representerer et soleklart brudd på betalingskontodirektivet, som konkret oppstiller en rett til grunnleggende banktjenester også for bostedsløse. Når denne praksisen tillates av norske myndigheter, innebærer det et brudd på de EØS-rettslige forpliktelsene.[46]

Også Buypass opplyser om at du må oppgi bostedsadresse for å inngå avtale.[47] Vi antar at kravet til bostedsadresse i praksis henger sammen med fravær av fysiske skrankepunkter og behovet for å bruke «post i butikk» til legitimering osv. Problemet kan oppstå både i forbindelse med både utstedelse og i bruksfasen. Dersom en person har fått utstedt BankID på et tidspunkt vedkommende hadde adresse, men deretter blir bostedsløs og samtidig for eksempel glemmer

[41] BankID | Dagligbank fra A til Å - DNB.
[42] Ny i Norge | Slik blir du bankkunde - DNB
[43] Se nærmere om dette i Sluttrapport for ID-juristen.
[44] BankID | Dagligbank fra A til Å - DNB
[45] https://www.finansnorge.no/tema/ny-i-norge/artikkel-bli-bankkunde-i-norge/
[46] Se nærmere om dette i Sluttrapport for ID-juristen, særlig punkt 5.3.2, sluttrapport_id-juristen_endelig.pdf.
[47] Buypass ID i mobil - enkel og sikker innlogging | Buypass AS

passord eller mister kodebrikken, vil det oppstå problemer med å få gjenåpnet en sperret BankID.

SODI-prosjektet har mottatt enkelthenvendelser om at personer med **rusproblemer** har blitt nektet BankID på dette grunnlaget. Det er uvisst hva begrunnelsen for dette er, men det kan ha sammenheng med at banken vurderer det som sannsynlig at vedkommende ikke vil klare å ivareta sikkerheten og brukervilkårene.

Enkelte kan også få avslag på BankID på grunn av **språkvansker**. Det vises til sluttrapport for ID-juristen punkt 5.1:

> «En av ID-juristens klienter mistet tilgang til BankID på grunn av språkvansker. Klienten hadde BankID, men ble bedt om å legitimere seg på nytt. Klienten var EØS-borger og hadde pass. Den informasjonen vi fikk var at saksbehandler i banken syntes det var vanskelig å forstå vedkommende, og at hen derfor fikk avslag.»

Bankene opererer med vilkår om at BankID ikke kan utstedes til **personer som trenger hjelp** til bruken, herunder eldre og personer med fysiske og psykiske funksjonsnedsettelser. Praksisen bygger på en rettsforståelse om at EØS-rettslige krav til sikkerhet i eID-systemer, for elektroniske signaturer og betalingsinstrumenter, slik disse fremgår av eIDAS med tilhørende rettsakter og PSD 2, er til hinder for utstedelse av BankID til denne gruppen. Vi mener at denne rettsforståelsen er feil.[48] Tvert imot innebærer praksisen strukturell diskriminering og menneskerettsbrudd, se nærmere om dette nedenfor.

Et særskilt problem er at det er uklart hvilken rettslig forståelse staten legger til grunn til i denne sammenhengen. I mars 2024 gav Diskrimineringsnemnda sin uttalelse i en sak der Norsk Forbund for Utviklingshemmede (NFU) klaget inn Digitaliserings- og forvaltningsdepartementet (Dfd) for diskriminerende praksiser knyttet til eID.[49] NFU anførte at staten diskriminerer utviklingshemmede når svært mange digitale offentlige tjenester ikke er tilgjengelig for de som ikke får eID på øverste sikkerhetsnivå av de private tilbyderne.

For nemnda anførte Dfd at den ikke har «myndighet over» hvordan «bankene tolker og praktiserer gjeldende regelverk» om utstedelse av BankID. Samtidig avvises det at en alternativ, offentlig utstedt eID vil løse utfordringene, fordi departementet slutter seg til bankenes tolkning av EØS-retten slik at også en offentlig eID etter departementets syn må ekskludere personer som på grunn av fysiske eller psykiske funksjonsnedsettelser trenger hjelp til bruken. Diskrimineringsnemnda sa seg enig i staten på dette punktet. Avgjørelsen er klaget videre til Sivilombudet, som i skrivende stund ikke har tatt endelig stilling til klagen.

I eID-strategien er et av målene at eID på øverste sikkerhetsnivå skal tilgjengeliggjøres for «flere», men det er uklart om dette inkluderer gruppen av personer som trenger hjelp til bruken. På den annen side har digitaliseringsministeren uttalt i DN at Regjeringen jobber for «digital

[48] Se Marte Eidsand Kjørven og Tone Linn Wærstad, 'Digitalt utenforskap og diskriminering – I hvilken grad gir diskrimineringsregelverket og håndhevingen av dette et effektivt vern mot forskjellsbehandling på grunn av digitalt utenforskap som skyldes manglende tilgang til eID?', under publisering men tilgjengelig som pre-publication draft her: digitalt-utenforskap-og-diskrimineringsnemndas-praksis-etter-fagfelle-endelig---v110.12.24.pdf.
[49] Uttalelse avsagt 11. mars 2024, DIN-2022-355.

inkludering og eID til alle».[50] På denne bakgrunn er det høyst uklart om myndighetene overhodet har en plan om å sikre tilgang til eID på sikkerhetsnivå høyt for mennesker med fysiske eller psykiske funksjonsnedsettelser, eldre og andre som trenger hjelp til bruken.

Det er uten videre klart at også *håndhevingen* av den rettsforståelsen som er lagt til grunn foregår på måter som reiser alvorlige rettssikkerhetsproblemer. De aktuelle gruppene, særlig eldre og utviklingshemmede, rapporterer om at de må møte opp til «eksamen» i en fysisk bankfilial for å bevise at de er i stand til å håndtere BankID på egenhånd.[51] Der sitter det ansatte med kompetanse og utdanning innen finans og skal vurdere funksjonsnivået til mennesker med funksjonsnedsettelser.

I artikkelen «Digitalt utenforskap: Om tilgang til helse- og velferdsrettigheter etter soning»,[52] beskriver Mira Sofie Stokke digitalt utenforskap som oppstår **under soning og vedvarer etter løslatelse**. Funnene baserer seg på kvalitative intervjuer med seks tidligere innsatte i norske fengsler. Om tilgang til BankID skriver Stokke blant annet følgende:

> «Alle seks beskriver problemer med *tilgang* til BankID. Det er ulike årsaker. Når man ikke har bostedsadresse, eksempelvis etter løslatelse, kan ikke banken sende fra seg kodebrikken eller engangskoder. Et annet problem er episoder der politiet inndrar telefonen, slik at man ikke kan bruke BankID på mobil.
>
> Tilgangen til BankID avhenger også av muligheten til å legitimere seg. Det beskrives som «ikke kult» å ha med seg politi eller fengselsbetjenter i banken for å identifisere seg under soning. Det fremstår som noe tilfeldig hvem som opplever legitimasjonsproblemer.»

Når det konkret gjelder problemer som kan oppstå der politiet beslaglegger mobiltelefon med BankID, er også kjennelse fra Agder lagmannsrett (LA-2024-112736) illustrerende. Saken gjaldt en kvinne som var domfelt for forsøk på drap i tingretten og lagmannsretten. Etter at anke til Høyesterett var inngitt, men før Høyesterett hadde tatt stilling til anken, krevde hun utlevert PC og mobiltelefon som hadde blitt beslaglagt i forbindelse med at hun var pågrepet. Forsvareren hadde anført på vegne av sin klient at hun hadde behov for å få mobiltelefonen tilbake, fordi hun hadde BankID på denne. Det ble opplyst at hun hadde forsøkt å skaffe seg BankID-brikke, men «får avslag på både pass og ID-søknad fordi hun sitter i varetekt». Problemer med tilgang til BankID for tidligere innsatte er også trukket fram i Toreld og Innvær, Tilbakeføringsarbeid fra fengsel til samfunnet.[53]

Betraktninger knyttet til Buypass og Commfides

Også Buypass og Commfides tilbyr eID på sikkerhetsnivå høyt til innbyggere i Norge. Disse eID'ene er uavhengig av kundeforhold i bank. Det innebærer at man kan få eID fra Buypass eller Commfides uten kundeforhold i bank, og uten å måtte oppsøke en fysisk bankfilial som det blir stadig færre av. Legitimasjonskravene er imidlertid i stor grad de samme. Det kreves fremleggelse av pass, og at søker er registrert med fødselsnummer eller d-nummer i Folkeregisteret. Fordi identitetskontrollen typisk skjer i «post i butikk», må passet være

---

[50] Elektronisk ID skal være en selvfølge | DN, se også det opprinnelige innlegget fra Kjørven, Wærstad og Omland: Digitalisering av offentlige tjenester gir diskriminering | DN og tilsvaret til Tungs svar: Karianne Tung taler med to tunger | DN.

[51] Mamma føler seg umyndiggjort og hjelpeløs. Banken fratok henne BankID., Bendik har downs – og en evig kamp mot BankID – Dagsavisen

[52] Publisert i Kritisk Juss (2023).

[53] Tilbakeføringsarbeid fra fengsel til samfunnet | Fontene.no

maskinlesbart fordi de ansatte ikke har kompetanse til å gjennomføre en identitetskontroll med pass som ikke er maskinlesbare. Søkeren må dessuten ha en adresse, ref. ovenfor om dette.

Buypass' og Commfides' eID på sikkerhetsnivå høyt kan benyttes i ID-porten og gir derved tilgang til alle offentlige tjenester. Også Digipost tilbyr innlogging via ID-porten som håndterer begge eID'ene. Buypass eID kan også benyttes hos en del private tjenesteytere, men her er bildet mer sammensatt. Vi ser f.eks. at samhandlingsløsningen Pasientsky aksepterer både BankID og Buypass, mens Pasientpost, som bl.a. benyttes av enkelte private sykehus for innkallingsbrev mv, bare tilbyr BankID som løsning for innlogging. Tilsvarende ser vi at f.eks. Gjensidige aksepterer både BankID og Buypass i sin portal, mens Storebrand med underliggende selskaper bare aksepterer BankID. Dette er valg brukerstedene selv har tatt, og kan naturligvis endres, men det illustrerer at det per i dag ikke finnes noe fullgodt alternativ til BankID slik brukerstedene har innrettet seg i dagens norske marked.

Tilbaketrekking og klage

Prosessen knyttet til sperring av eID er ikke særskilt regulert. For BankID gjelder de generelle kravene i finansavtaleloven, men disse er ikke tilpasset eID og de store konsekvensene sperring av BankID medfører. Ved sperring av BankID er det i prinsippet mulig å klage til Finansklagenemnda, men prosessen her tar svært lang tid. eForvaltningsforskriften har bestemmelser om forvaltningsorganets mulighet til å reagere på misbruk av de digitale tjenestene, se nedenfor. Et liknende prinsipp burde (som minimum) gjelde for eID-utsteders mulighet til å suspendere eller på annen måte utestenge noen fra bruk av eID.

> "§ 14.Forvaltningsorganets adgang til å nekte bruk av elektronisk kommunikasjon
>
> Hvis det er grunn til å anta at noen misbruker adgangen til elektronisk kommunikasjon med forvaltningsorganet, kan vedkommende helt eller delvis nektes videre bruk av slik kommunikasjon med forvaltningsorganet.
>
> Før adgangen til å nekte bruk av elektronisk kommunikasjon med forvaltningsorganet iverksettes, skal forvaltningsorganet sende vedkommende varsel om at det vurderer å nekte videre bruk av slik kommunikasjon og begrunnelsen for dette. Vedkommende skal oppfordres til å uttale seg om grunnlaget for avgjørelsen. Forvaltningsorganet skal sette en frist for slik uttalelse. Hvis det finnes nødvendig av sikkerhetsmessige årsaker kan forvaltningsorganet iverksette avgjørelsen straks.
>
> Den som blir nektet bruk av elektronisk kommunikasjon etter første ledd kan påklage avgjørelsen. Reglene i forvaltningsloven kap. VI gjelder tilsvarende så langt de passer."

Det bør etableres tydelige varslings- og klageordninger for alle eIDer. I alle fall for en offentlig utstedt eID bør forvaltningsrettslige prinsipper gjelde ved tilbaketrekking og klage.

Oppsummerende betraktninger

Det er mange og ulikeartede årsaker til at personer ikke får tilgang til BankID (eller annen eID på øverste sikkerhetsnivå). Noen av årsakene handler om konkrete rettslige hindre, men i mange tilfeller handler det også om en rettslig insentivstruktur som ikke fremmer inkludering, jf. nærmere om tilsyn, kontroll og sanksjoner i punkt 5.6. For eksempel vil brudd på hvitvaskingsreglene kunne utløse store økonomiske sanksjoner fra tilsynsmyndighetene. Brudd på en lovfestet eller ulovfestet kontraheringsplikt får derimot ingen konsekvenser. Det er da rasjonelt og forutsigbart at bankene vil prioritere å være på «den sikre siden» mht.

hvitvaskingsregelverket fremfor å finne den samfunnsmessig beste balansen mellom hensynet til å motvirke økonomisk kriminalitet på den ene siden og utenforskap på den annen. De gruppene som faller utenfor er dessuten typisk grupper som det er liten økonomisk gevinst i å inkludere basert på bedriftsøkonomiske hensyn.

Disse forholdene understreker etter vårt syn behovet for at staten tar ansvar for utstedelse av eID. Det bør i den sammenheng sikres et særlig fokus på grupper som i dag opplever utfordringer med å få utstedt eID fra de private eID-utstederne.[54] Dersom myndighetene ikke ønsker eller vil gjøre dette, krever det som et minimum klar lovregulering og effektivt tilsyn og sanksjoner. Det vises i den forbindelse til sluttrapporten til ID-juristen punkt 5.3.3.[55]

Situasjonen for personer som trenger hjelp til bruken av eID, herunder eldre og personer med fysiske og psykiske funksjonsnedsettelser, er særlig akutt. Det er behov for strakstiltak da situasjonen for denne gruppen er prekær, og det ikke er tid til å vente på utvikling av nye tekniske løsninger, lovgivningsprosesser mv. To strakstiltak er aktuelle. For det første kan eID på sikkerhetsnivå høyt tillates brukt av verge på vegne av vergehaver – altså slik at eID utstedes i vergehavers navn og brukes av verge. Dette tillates allerede for MinID. For det andre bør eID på sikkerhetsnivå høyt tillates brukt med assistanse av en utvalgt person, selv om denne personen da får innsyn i sikkerhetsopplysninger. Finsk lovgiver har eksplisitt tillatt en slik løsning.[56] Vi mener en slik løsning ikke bare er tillatt under de aktuelle EØS-rettslige reglene, men at menneskerettighetene og diskrimineringsvernet – i dagens situasjon med de tekniske løsningene som finnes p.t. – også innebærer en plikt til å åpne for slik assistert bruk. Ved behov kan Lovavdelingen bes om å utrede spørsmålet.

Tiltak:

1. Alle må ha rett til en eID på øverste sikkerhetsnivå. Vi trenger en eID-lov tilsvarende passloven og ID-kortloven som oppstiller vilkår for utstedelse av eID og gir brukerne rett til eID når vilkårene er oppfylt. Loven må inneholde vilkår for utstedelse og sperring/oppsigelse, og må inkludere mekanismer for klage, tilsyn og kontroll og effektive sanksjoner. Det må særskilt oppstilles rett til assistert bruk.

2. Alle med rettigheter og plikter i Norge, som har behov for å kunne identifisere seg digitalt her, må ha rett til norsk identitetsnummer. Dette krever endringer i folkeregisterloven og folkeregisterforskriften.

3. Alle som har fått tildelt et fødsels eller d-nummer fra Norge, bør ha mulighet til å dokumentere det tildelte ID-nummeret fysisk og digitalt på en troverdig måte,[57] for eksempel ved å få tilgang til nasjonalt ID-kort.

---

[54] Se også KoIDs visjon punkt 2 (gjengitt i kapittel 1 ovenfor) der det fremgår at: "Enhver som har fått tildelt et norsk identitetsnummer, i form av et d-nummer eller et fødselsnummer, skal gis mulighet til å dokumentere på en troverdig måte, at han er rette eier av identitetsnummeret fysisk *og digitalt*, for å ivareta grunnleggende behov." [Uthevet her.]

[55] sluttrapport_id-juristen_endelig.pdf

[56] Se nærmere omtale av de finske reglene i Marte Eidsand Kjørven og Tone Linn Wærstad, 'Digitalt utenforskap og diskriminering – I hvilken grad gir diskrimineringsregelverket og håndhevingen av dette et effektivt vern mot forskjellsbehandling på grunn av digitalt utenforskap som skyldes manglende tilgang til eID?', under publisering men tilgjengelig som pre-publication draft her: digitalt-utenforskap-og-diskrimineringsnemndas-praksis-etter-fagfelle-endelig---v110.12.24.pdf.

[57] Dette er også foreslått i Områdegjennomgangen, Tilleggsrapporten, punkt 5.1.1.

4. Utstedelse av eID bør være basert på en sikker kopling til en grunnidentitet ved å ”låse” én person til én identitet i Norge ved kontrollen av biometriske data som skjer ved utstedelse av norske pass eller ID-kort.
5. Staten bør utvikle og tilby en eID på sikkerhetsnivå høyt som er tilgjengelig og tryggere å bruke for flere. En slik offentlig tilbudt eID kan og må tilfredsstille alle kravene ovenfor.
6. Ved bruk av markedsbaserte eID-løsninger i offentlig sektor må det i anskaffelsesprosessen stilles større krav til tilbyderne mht. praksisene rundt utstedelse og sperring. Det må stilles tydelige krav om ikke-diskriminering og ivaretakelse av rettssikkerhet i prosessen. Kravene må følges opp med tilsyn og kontroll.
7. BankID bør utstedes uavhengig av bankene, for eksempel slik at BankID selv tar ansvar for utstedelse slik at ikke hvitvaskingsreglene blir et hinder for utstedelse.
8. Myndighetene bør legge til rette for at private eID-leverandører kan benytte offentlige skrankepunkter for legitimasjonskontroll og innrullering ved utstedelse av eID.
9. Ved bruk av markedsbaserte eID-løsninger i offentlig sektor må det stilles større krav til tilbyderne mht. praksisene rundt utstedelse og sperring. Det må stilles tydelige krav om ikke-diskriminering og ivaretakelse av rettssikkerhet i prosessen. Kravene må følges opp med tilsyn og kontroll.
10. Som et strakstiltak bør det avklares og åpnes for at eID på sikkerhetsnivå høyt tillates brukt med assistanse fra en utvalgt person.

5.1.2. eID-løsningene og tilhørende infrastruktur er ikke tilstrekkelig universelt utformet og tilpasset ulike brukergruppers behov

Flere undersøkelser og brukererfaringer viser at både innrulleringsprosessen og bruken av BankID skaper betydelige utfordringer for mange.

Selve legitimasjonsprosessen for å få BankID er ikke tilrettelagt for alle. For å få utstedt en eID på høyt sikkerhetsnivå vil det som hovedregel være krav om legitimasjonskontroll basert på fysisk oppmøte hos en registreringsenhet. Dette kan utgjøre en hindring for enkelte, blant annet for personer med mobilitetsutfordringer.

Bankenes praksis med å nekte eller sperre BankID for personer som har behov for hjelp, forsterker denne problematikken. I en del tilfeller må disse brukerne møte opp fysisk i en bankfilial for å bevise at de kan bruke BankID på egenhånd. Det stiller store krav til tilgjengelighet og reiseavstand, samtidig som bankansatte ofte mangler kompetanse til å vurdere funksjonsevnen til kundene på en faglig forsvarlig måte.

For personer som ellers har rett til å få utstedt eID høy, mener vi registreringstjenesten må organiseres slik at legitimasjonskontroll kan foretas uten at personen må forflytte seg fysisk til en registreringsenhet hvis vedkommende har fysiske eller psykiske funksjonsnedsettelser som gjør dette umulig eller urimelig belastende eller vanskelig.

I den nylig vedtatte ETSI TS 119 461 (2025-02) *Identity proofing of trust service subjects*, fremgår det bl.a. at:

> "***INI-8.1-04:*** *The identity proofing process, or at least one process if alternative processes are available, shall be available to persons with disabilities in accordance with the applicable legislation.*"

Det bør legges til rette for at legitimasjonskontroll enten kan skje digitalt (f.eks. ved hjelp av samtidig video og presentering av pass e.l.) eller ved at registreringsenheten kan reise ut til denne gruppen med nødvendig utstyr. Dette gjøres bl.a. i forbindelse med valg, ved at valgmedarbeidere tilrettelegger for forhåndsstemming på institusjon. Det er også særregler om legitimering i forbindelse med valg på institusjon. Hvis en person som bor på institusjon mangler legitimasjon, kan en ansatt gå god for vedkommendes identitet. Den ansatte må vise legitimasjon.[58] Det finnes også mobile løsninger for biometriopptak (fingeravtrykk) for utstedelse av pass og ID-kort. Slike benyttes bl.a. ved enkelte norske utenriksstasjoner og som reserveløsninger. Tilsvarende prosedyrer og mekanismer bør kunne benyttes for å legge til rette for registrering og legitimering lokalt av personer med relevante funksjonsnedsettelser når det skal utstedes offentlig støttet eID på nivå høyt.

I bruksfasen opplever mange med funksjonsnedsettelser at BankID er vanskelig å bruke. Ifølge Forbrukerrådet oppgir 16 prosent av dem som ikke bruker BankID at funksjonsnedsettelser eller fysiske utfordringer er hovedårsaken.[59] En rapport fra Rambøll, utarbeidet for Nasjonal kommunikasjonsmyndighet (Nkom),[60] peker på at BankID er et komplekst system som krever mange operasjoner og dermed kan være vanskelig for personer med visse funksjonsnedsettelser, som for eksempel Parkinsons sykdom. Rapporten viser til at BankID krever flere steg og involverer ulike enheter gjennom totrinnsinnlogging med kodebrikke eller kodeapp, noe som skaper barrierer for mange brukere.

Blant eldre er også bruk av BankID en utfordring. Blindeforbundets rapport *Digital deltakelse* viser at 69 prosent av respondentene kan bruke BankID selv, mens 20 prosent er avhengige av assistanse.[61] Ni prosent av respondentene bruker ikke BankID i det hele tatt. E-komtilbydere rapporterer at kundeservice-medarbeidere ofte møter kunder som synes BankID er vanskelig å bruke,[62] og en rapport fra Redd Barna fremhever at signeringskravet for å få eID på høyt sikkerhetsnivå er en barriere, selv for personer med lettere funksjonsnedsettelser.[63]

Manglende tilrettelegging gjør at enkelte grupper ikke får tilgang til eID på øverste sikkerhetsnivå, og at mange som har fått det opplever den som vanskelig å bruke i praksis. Kravet om fysisk oppmøte, komplekse autentiseringsprosesser og mangel på alternative løsninger skaper hindringer for digital deltakelse, til tross for at universell utforming er et lovpålagt krav.

---

[58] Se Stemme på institusjon - Valgdirektoratet

[59] Forbrukerrådet, Utanforskap i forbrukarmarknadene Digitale og andre hindringar som står i vegen for at forbrukarane kan kjøpe varer og tenester, s. 14, forbrukerradet-utanforskap-i-forbrukarmarknadene-no.pdf.

[60] Nkom: «Sluttrapport Digital inkludering – ekomtjenester for alle» (2023), tilgjengelig: Ny innsikt rundt digitalt utenforskap - Nkom

[61] Respons Analyse, *Norges Blindeforbund: Digital deltakelse* (2023), Norges Blindeforbund | Synshemmedes organisasjon.

[62] Nkom: «Sluttrapport Digital inkludering – ekomtjenester for alle» (2023), tilgjengelig: Ny innsikt rundt digitalt utenforskap - Nkom

[63] https://www.reddbarna.no/content/uploads/2021/01/Capgemini-rapport-Digitalt-Utenforskap-Blant-Barn-og-Ungdom.pdf

Digitaliseringsdirektoratet har stilt krav om at eID'er som skal være tilgjengelig i ID-porten oppfyller krav i forskrift om universell utforming av IKT-løsninger § 4 med krav til beskrivelse av hvordan løsningene samsvarer med WCAG2.0 på nivå A og AA. Det er også Digitaliseringsdirektoratet som fører tilsyn med forskriften, se § 5. Situasjonsbeskrivelsen ovenfor gjør det naturlig å spørre om oppfølgingen av kravene er god nok, eller om det er kravene som ikke er tilstrekkelige.

Tiltak:

11. Registrering og legitimasjonskontroll for å få utstedt en offentlig støttet eID på nivå høyt bør kunne skje der eID-innehaveren oppholder seg hvis vedkommende er innlagt på institusjon, innsatt i fengsel, bevegelseshemmet eller på annen måte har vanskelig for å benytte ordinære skrankepunkter eller registreringssteder.
12. Tilbydere av eID-løsninger må sørge for at eID-løsningene er enkle og trygge å bruke for alle. Dette har også en side til utfordringene knyttet til hhv. svindelforebygging og sikkerhetsløsninger, jf. punkt 5.2 og innovasjon og konkurranse, jf. punkt 5.7. Mulige virkemidler er:
    - Bruksbegrenset eID for personer med begrenset rettslig handleevne.
    - Systematisk og integrert bruk av biometri
    - Dobbeltsigneringsfunksjoner for de som trenger assistanse
13. Myndighetene bør vurdere om det må stilles mer spesifiserte krav til universell utforming for eID'er som skal benyttes i ID-porten enn det som fremgår av loven og forskriften.

5.1.3. Alternative analoge/fysiske og digitale løsninger er blitt dårligere eller helt borte

Som en konsekvens av stor utbredelse av eID på øverste sikkerhetsnivå, med tilhørende stadig flere bruksområder, har alternative måter å få tilgang til private og offentlige tjenester blitt borte eller dårligere. Dette er kritisk både for de som ikke får tilgang til en slik eID, og de som i teorien har slik tilgang, men som likevel ikke får benyttet seg av den i praksis på grunn av for eksempel lav digital kompetanse, manglende tilgang til smarttelefon med mobildata, eller problemer med internettforbindelse.

Billettkontorer, bankfilialer og offentlige skranker legges ned og erstattes med digitale tjenester som ofte krever eID på øverste sikkerhetsnivå. Brukersteder som tidligere tok imot betaling i form av kontanter eller betalingskort, blir i økende grad erstattet med betalingslenker og Vipps, som krever BankID. For personer som ikke kan bruke disse løsningene, betyr dette i praksis at de utestenges fra viktige tjenester i hverdagen.

Når digitalisering skjer uten å sikre fungerende alternativer for de som ikke kan eller ønsker å bruke eID, skapes en situasjon der enkelte grupper faller helt utenfor samfunnet. Mangel på tilpassede løsninger rammer særlig eldre, personer med funksjonsnedsettelser og de med begrenset økonomisk eller teknologisk tilgang.

Problemet relaterer seg overgang til eID fra både fysiske og digitale alternativer. En sak fra Diskrimineringsnemnda kan tjene til illustrasjon: Et strømselskap erstattet innlogging på Min

Side med brukernavn og passord med innlogging med bruk av BankID, og dermed ble en svensk borger med eiendom og tilhørende strømavtale i Norge, stengt ute.[64]

Nedbyggingen av alternative måter å få tilgang til offentlige og private tjenester, innebærer samtidig at bruk av eID for alle praktiske formål blir obligatorisk. Dette er i strid med frivillighetsprinsippet som er lagt til grunn i FN's prinsipper om DPI og i eIDAS2 2.0 artikkel 5 a nr. som eksplisitt sier at

> *"The use of European Digital Identity Wallets shall be voluntary. Access to public and private services, access to the labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural or legal persons that do not use European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means."*

Når dette er en regel som gjelder for EUDIW, som skal være gratis tilgjengelig for alle, bør man ikke omgå det ved å kreve bruk av private eID-løsninger. Se også eForvaltningsforskriften § 4 siste ledd som pålegger forvaltningen å gjøre tilgjengelig eller anvise sikkerhetsmekanismer som kan benyttes. Det kan etter vår oppfatning ikke anses tilstrekkelig å henvise til private eID'er hvis disse løsningene i praksis ikke er tilgjengelig for den det gjelder, se også punkt 5.1.5 nedenfor.

Det er derfor viktig at offentlige myndigheter sørger for at både offentlige digitale tjenester, og grunnleggende private tjenester, er tilgjengelig uten at det forutsetter tilgang til og bruk av eID på øverste sikkerhetsnivå.

Inspirasjonen kunne tas fra erfaring med koronapandemien. Da koronasertifikatene ble etablert, var det i utgangspunktet en heldigital tjeneste, men det ble samtidig etablert alternative kanaler for å sikre at alle kunne skaffe seg et slikt sertifikat, bl.a. gjennom HELFO eller hos Dr Dropin. HELFO kunne skrive ut koronasertifikat og sende til folkeregistrert adresse basert på telefonhenvendelse. Hos Dr Dropin kunne man få skrevet ut koronasertifikat basert på vaksine. På tilsvarende måte bør man vurdere om digitale tjenester kan suppleres med bistand fra andre eksisterende publikumstjenester, f.eks. hos NAV eller Skatteetaten.

I denne sammenheng har det også betydning at virksomhetene ikke krever et høyere sikkerhetsnivå enn nødvendig for tilgang (se punkt 5.1.5), og man bør vurdere om også andre digitale autentiseringsmetoder kan være aktuelle, f.eks. brukernavn og passord, Feide, Vipps (for de som har det), eventuelt om Vipps i kombinasjon med annen tjeneste (engangskode eller kamera og fysisk legitimasjon e.l.) kan gi et tilfredsstillende sikkerhetsnivå.

Noen særlige problemstillinger reiser seg i relasjon til betalingstjenester, og særlig tilgang til onlinebetalinger. ektiv 2014/92/EU (Betalingskontodirektivet, PAD) har til formål å sikre grunnleggende betalingstjenester til alle borgere i EU/EØS. Det følger av artikkel 16 at medlemsstatene har en plikt til å sikre at grunnleggende betalingstjenester er tilgjengelig for alle. Det spesifiseres at dette inkluderer forbrukere uten en fast adresse, asylsøkere og forbrukere som ikke har fått oppholdstillatelse, men som ikke kan utvises av faktiske eller rettslige grunner. Grunnleggende betalingstjenester skal etter betalingskontodirektivet artikkel 17 bokstav d) inkludere muligheten for å betale for varer og tjenester på nett («onlinebetalinger»). Det norske systemet, der online-betalinger ofte forutsetter BankID, ivaretar ikke plikten etter betalingskontodirektivet til å sørge for at alle har mulighet til å gjennomføre

[64] Uttalelse avsagt 22. april 2024, DIN-2023-51.

betalinger på nett. Det finnes imidlertid andre måter å gjennomføre sterk kundeautentisering enn med BankID, og myndighetene må sørge for at slike alternative løsninger faktisk er tilgjengelig. Problemstillingene knyttet til tilgang til grunnleggende betalingstjenester og mangelfull gjennomføring av betalingskontodirektivet er nærmere beskrevet i ID-juristens sluttrapport og i SODI-prosjektets høringssvar til NOU 2024:21 Trygge og enkle betalinger for alle.[65]

Tiltak:

14. Gjennomgå lovverket for grunnleggende private og offentlige tjenester og stille krav om å tilby alternative digitale og/eller analoge løsninger. Dette kan for eksempel inkludere
    - Krav til aktører innen helse, herunder fastlegekontorer, om å ta imot betaling med betalingskort og/eller kontanter.
    - Krav til aktører som tilbyr kollektivtransport om tilgjengelige og alternative måter å kjøpe billetter.
    - Krav til tilgjengelighet og åpningstider for fysiske offentlige kontorer som NAV, Skatteetaten osv.
15. Alle betalingstjenestetilbydere pålegges å tilby alternative metoder for sterk kundeautentisering til kunder som ikke får BankID, samt sørge for at de alternative metodene godtas ifbm. betalinger på nett, ikke kun innlogging i nettbank.

5.1.4. Fullmaktsløsninger eksisterer ikke eller er for dårlige

Representasjons- og fullmaktsløsninger er enten fraværende eller dårlig tilpasset brukernes behov. Det finnes ingen sentral løsning for digitale fullmakter, og de få alternativene som eksisterer, er ofte utilstrekkelige. Ett eksempel gjelder digitale tjenester fra NAV, som ikke har løsninger for representasjon og fullmakt. Konsekvensene av dette er blant annet beskrevet i en sak i Amta, der en mor fortviler over at hun ikke får tilgang til sin 4 måneder gamle sønns «Min Side» hos NAV.[66] Sønnen har en kronisk lidelse, og moren har på den bakgrunn søkt om stønader hos NAV. Søknaden og informasjon knyttet til den er imidlertid kun tilgjengelig på sønnens egen «Min side», som moren ikke får tilgang til. Et betimelig spørsmål i den sammenheng er hva som er poenget med å ha digitale løsninger som innebærer at babyer har sin egen «min side» som ikke er tilgjengelig for foresatte.

Noen tjenester tilbyr isolerte fullmaktsløsninger, men disse har i en del tilfeller begrensninger som gjør dem lite anvendelige i praksis. Et eksempel er Digipost, hvor det kreves eID på øverste sikkerhetsnivå for å opprette en fullmakt. Dette skaper en betydelig utfordring for personer som har fått sin BankID sperret, for eksempel på grunn av mistanke om at de får hjelp av pårørende. Når BankID først er sperret, er det, slik vi forstår det, ikke lenger mulig å opprette fullmakt, selv i tilfeller hvor dette kunne vært en trygg og praktisk løsning for å ivareta personens interesser.

Bankenes fullmaktsløsninger er også mangelfulle.[67] I mange tilfeller tilbys kun en disponentordning, hvor en person får full tilgang til kontoen til fullmaktsgiveren. Dette

[65] Høring - NOU 2024: 21 Trygge og enkle betalinger for alle - regjeringen.no
[66] Horten, Nav | Vivi (29) får ikke elektronisk tilgang til sin 4 måneder gamle sønns «Min Side» hos Nav: – De sa jeg kunne skaffe ham en BankID.
[67] Kunne kapre bankkonto med papirskjema; BankID: Disposisjonsrett er ikke lett | Digi.no; Lurte banken trill rundt: Ved hjelp av enkle triks fikk de tilgang til Pers konto | Digi.no

innebærer at disponenten kan se hele kontohistorikken, inkludert tidligere transaksjoner, og har fri tilgang til alle kontoens midler. Det finnes ingen mulighet for mer begrensede fullmakter, for eksempel en løsning hvor fullmektigen kun kan betale regninger uten å ha innsyn i sensitive transaksjoner eller iverksette betalingstransaksjoner. Mange som har behov for assistanse i økonomiske spørsmål, trenger kun hjelp til spesifikke oppgaver, som å betale strømregningen eller kommunale avgifter. Med dagens løsninger tvinges de imidlertid til å gi full tilgang til hele økonomien, noe som både svekker personvernet og øker risikoen for misbruk.

Mangelen på muligheter for å sette beløpsgrenser på disponenters transaksjoner forsterker problemet. Disponenten har i praksis ubegrenset tilgang til midlene på kontoen, noe som kan føre til økonomisk usikkerhet og økt sårbarhet for misbruk. Dette rammer særlig personer med nedsatt dømmekraft eller periodiske helseutfordringer, som demens i tidlig fase, bipolar lidelse, depresjon eller alvorlig sykdom som påvirker kognitiv funksjon midlertidig. Mange i denne gruppen er fullt i stand til å håndtere sin egen økonomi store deler av tiden, men har i perioder behov for støtte.

Manglende mulighet for dobbeltsignering er også en vesentlig svakhet i dagens systemer. I situasjoner hvor to personer deler økonomi, er det ofte ønskelig med en løsning hvor større økonomiske disposisjoner må godkjennes av begge parter. Dette kan være spesielt viktig ved samlivsbrudd, i turbulente samliv, eller der en av partene er syk. Dobbeltsignering kunne også fungert som beslutningsstøtte for personer som i perioder har behov for hjelp, men fortsatt ønsker kontroll over sin egen økonomi. I dag er det få alternativer mellom full selvstendighet og vergeordning, som har høy terskel og innebærer omfattende administrasjon.

For personer med langvarige eller periodiske behov for økonomisk støtte, men som fortsatt er i stand til å ta selvstendige avgjørelser, finnes det i dag ingen gode løsninger. Mangel på fleksible fullmaktsløsninger gjør at mange enten må gi fra seg all kontroll eller stå uten nødvendig hjelp, noe som skaper utrygghet og svekker den økonomiske selvbestemmelsen for mange.

En særlig utfordring er digitale meldinger som kommer i ulike digitale kanaler og ikke blir lest fordi mottakeren ikke er digitalt aktiv eller ikke forstår varslene om nye meldinger, se nærmere om dette i punkt 5.4.3. Det burde være mulig å registrere en subsidiær varslingsadresse, slik at f.eks. en pårørende også fikk beskjed om at det var kommet en ny melding og kunne minne eller opplyse mottakeren om dette, og eventuelt bistå med å finne riktig kanal. Det kan minne om å bistå med å ta inn og legge frem posten fra postkassen slik at mottakeren selv kan åpne den. Det kan være nyttig bistand for personer som har egen eID, men synes det er vanskelig å orientere seg. Løsningen kan også kombineres med fullmakt til faktisk å åpne og lese meldingene, men behøver ikke nødvendigvis inneholde rett til å gjøre endringer eller foreta andre disposisjoner elektronisk på vegne av mottakeren. I denne sammenheng kan det være aktuelt å se på løsninger som gjør det mulig for fullmaktsgiver å få hjelp til å opprette fullmakter, f.eks. at en saksbehandler kan opprette fullmakt til en pårørende basert på muntlig fullmakt fra fullmaktsgiver som ikke selv er digitalt aktiv. Det bør vurderes om f.eks. saksbehandlere på lokale ligningskontorer eller NAV-kontorer kan bistå med dette. Det samme vil gjelde ekstern hjelp til etablering av attributtsertifikater (i denne sammenheng fullmaktssertifikater) til bruk i den digitale lommeboken (EUIDW) når den kommer. En stor gruppe personer med behov for å gi fullmakter til andre er ikke i stand til å registrere eller utstede digitale fullmakter selv. De bør ha mulighet til å få hjelp til å utstede, eller initiere utstedelse av, fullmakter, basert på muntlig eller papirbasert skriftlig fullmakt til noen som kan omsette fullmakten i utstedelse av et fullmaktssertifikat.

Regjeringen bevilget i 2024 2,6 millioner kroner til arbeid med en digital fullmaktsløsning for offentlige tjenester.[68] Ettersom løsningen kun er ment å gjelde for offentlige tjenester, vil det ikke løse problemene med manglende fullmaktsløsninger for private tjenester.

Avslutningsvis er det grunn til å understreke at selv om fullmaktsløsninger er svært viktig å få på plass, kan dette ikke komme istedenfor løsninger på problemene som er beskrevet ovenfor ang. tilgang til eID for alle og alternative fysiske og digitale løsninger for de som ikke ønsker å bruke digitale løsninger. Et grunnleggende utgangspunkt i relevante menneskerettigheter og i vergemålsretten er at alle skal kunne leve selvstendige liv, og ikke være avhengig av verge eller fullmektig. Dette har en side til det som beskrives i punkt 5.4.2 om at teknologien ikke må overstyre den juridiske privatautonomien.

Tiltak:

16. Offentlige myndigheter bør utvikle et sentralt fullmaktsregister på tvers av offentlig og privat sektor.
17. Private og offentlige aktører pålegges å ha fullmaktsløsninger knyttet til sine nettjenester, i alle fall når de representerer tilgang til innbyggernes lovbestemte rettigheter eller grunnleggende tjenester som bank, forsikring, lovbestemte registre, tilgang til egne helseopplysninger mv.
18. Stille krav til utforming av private fullmaktsløsninger, særlig i bankene, slik at disse dekker brukernes faktiske behov, herunder sikrer dataminimering og mulighet for begrensede fullmakter.
19. Offentlige servicekontorer bør kunne foreta disposisjoner på innbyggers vegne basert på ad hoc fullmakt når innbyggeren er fysisk til stede. Særlig gjelder dette reservasjoner og etablering av andre fullmakter.
20. Det bør utredes om fullmaktssertifikater som representerer en personlig fullmakt kan utstedes av andre enn fullmaktsgiver. Det kan være praktisk der bakgrunnen er at fullmaktsgiver ikke er digitalt aktiv, men må forholde seg til digitale tjenester (med bistand). Utrede en ordning der fullmaktsgiver møter opp et sted som kan utstede en (frasagns)fullmakt i form av et fullmaktssertifikat på fullmaktsgivers vegne basert på dennes muntlig uttrykte ønske.
21. Som et strakstiltak bør NKOM avklare at eID på sikkerhetsnivå høyt kan utstedes til bruk for verge på vegne av vergehaver og/eller at det åpnes for assistert bruk. Ved behov kan Lovavdelingen bes om å utrede dette på forhånd.
22. Som et strakstiltak bør Digitaliseringsdirektoratet etablere mer fleksible varslingsløsninger slik at en "hjelper" vedkommende velger, f.eks. en pårørende, får varsel og kan gjøre mottaker oppmerksom på at det venter en digital sending og hvilken kanal den er sendt i, f.eks. ved å åpne for subsidiære varslingsadresser i kontakt- og reservasjonsregisteret.

5.1.5. For mange tjenester krever eID på øverste sikkerhetsnivå

Det er brukerstedene/tjenesteeiere som vurderer hvilket sikkerhetsnivå som skal kreves for tilgang til deres tjenester. For offentlige tjenesteeiere følger dette av eForvaltningsforskriften § 4.

[68] Regjeringen vil ha en digital fullmaktsløsning for offentlige tjenester - regjeringen.no

Ifølge eID-strategien er det i dag 21 % av tjenestene som er tilgjengeliggjort via ID-porten som krever eID på nivå «høyt», mens resterende tjenester er tilgjengelig med MinID på nivå «betydelig». De 21 % av tjenestene som er på nivå "høyt" utgjør 66 % av de samlede årlige innloggingene med eID via ID-porten, og 94 % av brukerne velger uansett å benytte sin eID på nivå høyt, uavhengig av hvilket sikkerhetsnivå tjenesten krever.

I eID-strategien står det videre:

> Behovsanalysene viser imidlertid at enkelte virksomheter vurderer å innføre et gjennomgående krav om pålogging med en eID på sikkerhetsnivå høyt for tilgang til sine tjenester, for å forenkle sin infrastruktur og gjøre det mer sømløst for brukeren. Samtidig vil dette være en utfordring for tjenesteeierne dersom ikke alle brukerne har eID på høyt sikkerhetsnivå og tjenesteproduksjonen derfor må håndteres manuelt.[69]

Uttalelsen kan tyde på at hensyn til tilgjengelighet ikke tillegges den vekten det fortjener. Isteden vektlegges tjenesteeiernes eget behov for forenkling og sømløshet for de brukerne som har eID på øverste sikkerhetsnivå. Det er et tankekors at strategien viser at det på den annen side er en utfordring for «tjenesteeierne» å velge eID på sikkerhetsnivå høyt fordi det vil kreve manuell håndtering for de brukerne som da faller utenfor.

Det er verdt å peke på at Norge skiller seg ut i Norden når det gjelder bruk av eID på sikkerhetsnivå høyt. I Sverige er den dominerende løsningen BankID (et annet selskap og løsning enn den norske med samme navn) på sikkerhetsnivå betydelig, og denne gir tilgang til alt av offentlige og private digitale tjenester.

Vi vil også understreke at eForvaltningsforskriften § 4 siste ledd pålegger forvaltningen å gjøre tilgjengelig eller anvise sikkerhetsmekanismer som kan benyttes. eForvaltningsforskriften § 4 siste ledd lyder:

> "Forvaltningsorganet skal gjøre tilgjengelig sikkerhetstjenester og -produkter som oppfyller de krav forvaltningsorganet har stilt i henhold til annet og tredje ledd ovenfor eller anvise hvilke løsninger som ellers kan benyttes. Det samme gjelder for sikkerhetstjenester og -produkter som er nødvendig for å oppfylle kravene i § 5." [Forskriften § 5 gjelder sikring av konfidensialitet.]

Det er ikke tilstrekkelig å henvise til kommersielle løsninger dersom disse i praksis er utilgjengelige for mange innbyggere. Da er eID ikke “gjort tilgjengelig”, og man kan heller ikke si at det er anvist noen løsning "som ellers kan benyttes", hvis vedkommende som har behov for det ikke kan få tak i det. Når det offentlige krever eID på høyeste sikkerhetsnivå uten å tilby et reelt alternativ, forsterkes digitalt utenforskap unødvendig, og det er etter vår oppfatning i strid med de regler som gjelder og som ligger til grunn for prinsippet om digitalt førstevalg.

Tiltak:

23. Sette tydeligere krav og retningslinjer til private og offentlige brukersteder/tjenesteeiere ved valg av sikkerhetsnivå og sikre oppfølgning av at tjenesteeiere ikke stiller høyere sikkerhetskrav enn nødvendig.
24. Der brukerstedene tilbyr tjenester med forskjellige sikkerhetsbehov, må brukerstedet sømløst håndtere situasjoner der brukeren får behov for høyere sikkerhetsnivå.

[69] eID-strategien, s. 24.

25. Forsikre at offentlige virksomheter som krever bruk av sikkerhetsmekanismer for elektronisk kommunikasjon sikrer at det er egnede mekanismer (eID) tilgjengelig for innbyggerne for de tjenestene og på det sikkerhetsnivået den offentlige virksomheten har valgt å benytte. Hvis det er grupper som faller utenfor må det offentlige etablere et alternativ. Offentlige virksomheter må etablere alternativer for de av deres egne brukere som ikke kan få en eID på tilstrekkelig høyt nivå.

5.1.6. Dagens system fører til strukturell diskriminering og menneskerettsbrudd

De ulike utenforskapsproblemene som vi har behandlet over reiser mange aktuelle spørsmål om brudd på grunnleggende menneskerettigheter og diskrimineringsvernet for dem det gjelder.[70] Som vi har beskrevet over er det myndighetene som i stor grad tar i bruk ny teknologi knyttet til digitale løsninger for eID og samtidig bygges tilsvarende fysiske og analoge løsninger ned og nye alternative løsninger tilbys ikke. Når offentlige myndigheter anvender ny teknologi er det som Norges institusjon for menneskerettigheter har påpekt i en rapport nylig «myndighetenes ansvar at menneskerettighetene respekteres og vernes. Ansvaret gjelder både ved beslutninger om å innføre og modifisere digitale løsninger, og ved bruk av slik teknologi i statlig forvaltning.»[71]

Videre er det klart at menneskerettslige forpliktelser for myndighetene strekker seg utover den rene tilgangen til offentlige tjenester og offentlig saksbehandling. Det påligger også myndighetene å sikre universell og lik tilgang til grunnleggende private tjenester på en rekke områder ettersom disse i stor grad berører sentrale menneskerettigheter for dem det gjelder.

En grunnleggende utfordring knyttet til dette er at digitaliseringen av offentlig forvaltning baserer seg på markedsløsninger for eID. Det betyr i praksis at private markedsaktører bestemmer hvem som skal ha tilgang til offentlige digitale tjenester. Å frata mennesker rettslig handleevne er svært inngripende, og er derfor underlagt en lang rekke rettssikkerhetsgarantier i vergemålsretten. I praksis blir imidlertid disse rettssikkerhetsgarantiene tilsidesatt ved at markedsaktørene for eID på øverste sikkerhetsnivå etter eget forgodtbefinnende kan nekte folk tilgang, eller sperre tilgangen, til eID – som for alle praktiske formål har virkning som umyndiggjøring. Borgere som mister tilgang til sin eID, står ofte uten klagemuligheter eller rettssikkerhetsgarantier. Dette svekker deres mulighet til å delta i samfunnslivet og ivareta sine interesser.

Tiltak:

26. Myndighetene bør jevnlig gjennomføre menneskerettslige konsekvensanalyse av den digitale identitetsforvaltningen.
27. Tilsyns- og overvåkningsorganer som LDO og NIM bør fokusere på strukturelle diskrimineringsproblemer innen eID-området.

---

[70] For en grundigere drøftelse av diskrimineringsrettslige problemstillinger, se Marte Eidsand Kjørven og Tone Linn Wærstad, Digitalt utenforskap og diskrimineringer – I hvilken grad gir diskrimineringsregelverket og håndhevingen av dette et effektivt vern mot forskjellsbehandling på grunn av digitalt utenforskap som skyldes manglende tilgang til eID, under publisering, tilgjengelig som Pre publication draft, digitalt-utenforskap-og-diskrimineringsnemndas-praksis-etter-fagfelle-endelig---v110.12.24.pdf

[71] Ny teknologi og menneskerettigheter - Norges institusjon for menneskerettigheter. Pkt.7.

5.2. Svindelforebygging og sikkerhetsløsninger

I dette punktet tar vi for oss utfordringer knyttet til styringsprinsipp nummer 2:

«Ingen individer skal oppleve uønsket bruk av sin egen digitale identitet. De tekniske og organisatoriske sikkerhetsløsningene må legge til rette for at brukerne og systemet som helhet kan hindre og oppdage uønsket bruk av digitale identiteter. Sikkerhetsløsningene må ta høyde for uønsket bruk fra både nærstående og fremmede. Opplæring og brukerstøtte må være tilgjengelig for brukerne, men de må kunne kontrollere bruken av sin digitale identitet uten omfattende opplæring eller kunnskap. Brukerstedene må ta høyde for at sikkerhetsløsningene kan svikte. Brukerstedene må også sørge for at brukerne forstår handlingen de gjennomfører.»

Vi beskriver først ulike typer av ID-misbruk (punkt 5.2.1). Dette inkluderer blant annet misbruk av eID til å gjennomføre betalingstransaksjoner, inngå kredittavtaler, opprettelse av stråselskaper som brukes til å gjennomføre bedragerier mot offentlige og private aktører. Vi beskriver ulike metoder de kriminelle bruker for å gjennomføre ulike former bedragerier, herunder bruk av press, tvang og vold. Deretter går vi over til å beskrive noen mer konkrete sårbarheter som gjør identitetsmisbruk mulig.

- Sårbarheter i eID-systemene (punkt 5.2.2)
- Sårbarheter hos brukerstedene (punkt 5.2.3)
- Sårbarheter knyttet til bruk av eID i jobbsammenheng (punkt 5.2.4)
- Nye sikkerhetsutfordringer med KI-drevet ID-svindel (punkt 5.2.6)
- Sårbarheter knyttet til sluttbrukerne (punkt 5.2.7)
- Mangelfullt samarbeid og deling av data mellom aktører (punkt 5.2.8)

5.2.1. ID-misbruk som problem

Det har vært en eksplosiv vekst i digitale bedragerier de siste årene, og det er forventet at omfanget vil fortsette å øke.[72] Gjennom rettshjelpstiltaket ID-juristen har SODI-prosjektet hatt muligheten til å observere trender i svindelsaker gjennom prosjektets levetid. Svindlerne er tilpasningsdyktige, og svindelmetodene utvikles og innrettes slik at de til enhver tid rammer enkeltmennesker og systemer der de er svakest.

Ved identitetsmisbruk er risikoen stor for at myndigheter eller private aktører feilaktig holder en person ansvarlig – enten strafferettslig, forvaltningsrettslig eller økonomisk. I ytterste konsekvens kan dette føre til justismord og/eller økonomisk ruin for de som rammes. Det er derfor ekstremt viktig at en overordnet og helhetlig strategi for digital identitetsforvaltning også inkluderer tiltak for å sikre gjenoppretting og reparasjon for ofre for identitetsmisbruk, og tilstrekkelig ivaretakelse av ofrene i prosessen. Dette kommer vi nærmere tilbake til i punkt 5.3.

Digitalt identitetsmisbruk kan skje på mange ulike måter. Vi skal i det følgende ta for oss noen av de vanligste formene for ID-misbruk. Kategoriene er delvis overlappende.

Misbruk av BankID til å gjennomføre betalingstransaksjoner

Misbruk av BankID til å gjennomføre uautoriserte betalingstransaksjoner, er en av de vanligste formene for ID-misbruk. En mye anvendt svindelmetode er såkalt «phishing», hvor svindler via lenker i e-post, SMS, melding i sosiale medier e.l., leder svindelofferet til falske nettsider hvor

[72] Politiets trusselvurdering 2024 s. 11; Økokrim, *Bedrageri – et samfunnsproblem,* 2023 s. 18.

hen avkreves «innlogging» med BankID. Når svindelofferet taster inn brukernavn og passord videresendes informasjonen til svindler, og istandsetter denne til å tappe svindelofferets konto.

En liknende fremgangsmåte som phishing går ut på at offeret blir oppringt av svindler, og lurt til å gi fra seg sikkerhetsinformasjon muntlig. Denne metoden går gjerne under navnet «vishing» (voice phishing). Vishing er ofte kombinert med såkalt «spoofing» – manipulasjon av telefonnummer, slik at det på svindelofferets mobilskjerm ser ut som hen ringes av for eksempel banken eller politiet.

Denne typen klassiske tilfeller av BankID-misbruk har gått ned de siste årene, blant annet som følge av økte sikkerhetstiltak i bankene. Derimot har betalingssvindel der svindlerne gjennom profesjonell sosial manipulasjon lurer ofrene til å gjennomføre hele eller deler av prosessen for gjennomføring av betalinger økt. Denne typen svindel ligger på siden av hva man kan kalle «identitetsmisbruk». Også slik svindel er imidlertid muliggjort av digitalisering og overgang fra fysisk til digital autentisering mer generelt.[73]

Det er ikke bare enkeltpersoner som utsettes for betalingssvindel. Bedrifter og ideelle organisasjoner er også utsatt. Mange små bedrifter og ideelle organisasjoner har kontoer som disponeres av ansatte eller tillitsvalgte. Når disse bruker sin private BankID for tilgang, vil en kompromittert BankID gjerne føre til at både vedkommendes private konto og bedrifts-/organisasjonskontoen blir tømt av svindlere.

Lånesvindel

I perioden 2017-2020 var det en eksplosjon i lånesvindelsaker, som involverte misbruk av BankID. Etter at Høyesterett og lovgiver høsten 2020 la en større del av risikoen for tap etter slik svindel på bankene, satte bankene i verk tiltak og antall lånesvindelsaker gikk vesentlig ned i årene som fulgte.[74] Lånesvindelsakene som dominerte i perioden 2017-2020 var preget av lite profesjonell utførelse, og mange av sakene gjaldt misbruk av BankID i nære relasjoner. Antall lånesvindelsaker ser imidlertid ut til å være på vei opp igjen.[75] Sakene nå har et mer profesjonelt preg, og utføres trolig i større grad av organiserte kriminelle. Ofte skjer dette gjennom stråselskaper og i kombinasjon med andre bedragerier.

Avtaler om kjøp eller leie

ID-juristen har behandlet flere saker om misbruk av BankID til inngåelse av avtaler om mobilabonnement, kjøp av telefon eller annen småelektronikk, kjøp av klær og kjøp og leie av bil. Varekjøpene er ofte gjort via betalingshenstandsløsninger tilbudt av aktører som Klarna AB. Det inngås da en samtidig kjøps- og kredittavtale ved autorisering med BankID, hvoretter Klarna oppfyller betalingsforpliktelsen overfor selger og samtidig gir kjøper (svindler) betalingshenstand for kjøpesummen. Finans Norge trekker også frem kjøp og leasing av bil på kreditt, med tilhørende BankID-misbruk som en svindelvariant bankene ser i 2025.[76]

Identitetsmisbruk i selskapsforhold som ledd i bedragerier mot offentlige og private aktører

Et voksende problem er identitetsmisbruk i selskapsforhold. Personer får sin identitet misbrukt ved at de registreres som stråpersoner i sentrale roller i selskaper. Disse stråselskapene brukes

[73] Se sluttrapporten til ID-juristen, særlig punkt 4, for en grundigere redegjørelse for ulike svindeltyper og tilhørende rettssikkerhetsproblemer.
[74] Se sluttrapporten til ID-juristen, særlig punkt 4.2.4 for en nærmere beskrivelse av utviklingen.
[75] Finans Norge, Status og tiltak mot svindel for 2025
[76] Status og tiltak mot svindel for 2025

deretter til å gjennomføre en lang rekke bedragerier mot offentlige myndigheter, finansinstitusjoner og andre selskaper.

Fair Play Bygg, en organisasjon som jobber mot arbeidslivskriminalitet, erfarer at sårbare grupper som arbeidsinnvandrere og mennesker i rusmiljøet er særlig utsatt for denne typen omfattende ID-misbruk, som også kan inkludere bruk av press, tvang og vold.[77] De kriminelle som utfører dette hører gjerne til voldelige og organiserte kriminelle grupperinger. Ofrene ofte kan være redde for å anmelde bakmennene i frykt for represalier. Fair Play Bygg omtaler denne formen for identitetmisbruk som en «form for moderne slaveri» som er «muliggjort ved at det skal være enkelt å opprette bedrifter og få banklån».[78]

I sin ytterste konsekvens kan ofrene, som har sin identitet klistret til straffbare handlinger som for eksempel hvitvasking og bedragerier, blir strafferettslig forfulgt og dømt for handlinger utført av andre.

Denne typen systemmisbruk, som inkluderer misbruk av offentlige registre, særlig selskapsregistrene i Brønnøysund, er nærmere beskrevet i NTAES' rapport om Registermanipulasjon.[79]

Særlig om svindel og identitetsmisbruk som involverer fysisk tilstedeværelse, tvang, vold og/eller press

JURK og ID-juristen har de siste årene sett en økning i saker om økonomisk vold. Økonomisk vold innebærer at noen kontrollerer en annen persons økonomi uten deres samtykke, for eksempel ved å frata dem tilgang til egne midler eller tvinge dem til å ta opp lån. Et kjennetegn ved sakene, er at økonomisk vold er en del av et større voldsbilde, der utøveren er en nærstående.[80] Svenske forskere har beskrevet hvordan BankID og digitaliseringen av finansielle tjenester tilrettelegger for denne typen vold.[81]

En foruroligende utviklingstrend er at organiserte kriminelle nettverk oppsøker folk fysisk for å få tak i deres BankID. Dette rammer særlig enslige eldre kvinner.[82]

Som beskrevet ovenfor, er det dessuten et økende problem at sårbare grupper som kommer i kontakt med organiserte kriminelle får sine identiteter og eID misbrukt i omfattende bedragerier ved at de innsettes som stråpersoner i selskaper.

Annet identitetsmisbruk

I og med at BankID kan brukes i tusenvis av ulike sammenhenger, er det også potensiale for identitetsmisbruk i alle disse sammenhengene. En eID på sikkerhetsnivå høyt kan potensielt misbrukes til å overføre eiendom, registrere skilsmisse, få innsyn i sensitiv helseinformasjon og endring av kontonummer for utbetaling av Trumf-bonus, for å nevne noe.

---

[77] Fair Play Bygg Oslo, Årsrapport 2024, Arsmelding-Fair-Play-Bygg-2024-low_res.pdf, s. 26.
[78] Ny rapport: Slik tjener kriminelle enorme penger i norsk byggebransje – Dagsavisen
[79] NTAES, Registermanipulasjon, Rapport - Registermanipulasjon.
[80] Se også SODI-rapport 1/2022, side 25. Rapporten viser at ID-misbruk oftest utøves av en nærstående. Rundt 80 % av de som er utsatt for identitetskrenkelse av en nærstående, var kvinner.
[81] E-legitimation som verktyg för ekonomiskt våld | SvJT
[82] DNB og politiet roper varsku om farlig svindelmetode - DNB Nyheter

Høsten 2023 lyktes en svindler med å endre kontonummeret for utbetaling av offentlige stønader til en rekke NAV-brukere.[83]

Et annet eksempel gjelder en kvinne som ble utsatt for omfattende svindel av sin eks-samboer, som i tillegg til å ta opp 14 lån i hennes navn hadde tømt alle kontoene hennes, inkludert BSU-kontoen. Dette førte til at Skatteetaten fattet vedtak om straffeskatt fordi BSU-pengene ikke var blitt brukt til boligformål i tråd med reglene for BSU-konto.[84]

ID-juristen har også erfart at det å ta kontroll over innehaverens Digipost som ledd i en større svindeloperasjon mot vedkommende, er vanlig.

5.2.2. Sårbarheter i eID-systemene

BankID, Buypass og Commfides er alle definert til å være på øverste sikkerhetsnivå (nivå «høyt») ihht. det rettslige rammeverket for eID. Det er likevel flere utfordringer knyttet til sikkerheten i systemene. Disse relaterer seg til både utstedelsesfasen, bruksfasen og systemet for sperring når en eID er misbrukt.

Tidligere gjennomganger

I områdegjennomgangen av den digitale identitetsforvaltningen som ble gjennomført i 2019, ble det pekt på det som i rapporten omtales som to «grunnleggende sikkerhetshull»: For det første «begrensede kontrollmekanismer for å forhindre at en eID utstedes til feil person». Det stilles ikke krav om tilknytning og kontroll av identitetsbeviset som sådan og det norske fødsels- eller d-nummeret. eID-leverandørene skal ved førstegangs utstedelse kontrollere at innehaveren av identitetsbeviset er den samme personen som er registrert i Folkeregisteret, men det finnes ikke et system for å få til dette på en sikker måte. Identitetskontrollen som skjer ved utstedelse av eID er manuell, og det brukes ikke utstyr som kontrollerer og sammenligner biometriske trekk av den som møter opp til ID-kontroll og ID-beviset som fremvises. I praksis skjer ID-kontrollen ofte i «post i butikk», og gjennomføres da av medarbeidere uten tilstrekkelig kompetanse på ID-kontroll. Det utgjør en ytterligere sårbarhet at det kan utstedes flere eID'er, herunder flere BankID'er, til samme person, og i forbindelse med slike nye utstedelser kan søkeren benytte en allerede utstedt eID til identifisering og autentisering. En person som får tilgang til en annens eID, kan derfor bruke denne til å få utstedt en eller flere ny(e) eID ('er) i vedkommendes navn, men som er kontrollert av en annen. Finans Norge uttaler i en rapport fra 2025 at bankene «ser særlig en økning av svindlere som klarer å få tilgang til offerets konto og opprette en app i offerets navn, for eksempel BankID-appen eller mobilbankappen.»[85]

Dette har en side til det andre sikkerhetshullet områdegjennomgangen peker på: «begrensede kontrollmekanismer som kan kontrollere om brukeren av eID-en er den rettmessige eieren av eID-en påfølgende utstedelse».[86] Til det siste punktet peker rapporten særlig på at det ikke gjennom biometrisk kontroll eller på andre måter sikres ved autentiseringstilfelle at «brukeren av en eID er den rettmessige eieren» hver gang eID'en brukes. Det betyr at dersom «en person har fått tilgang til en annen brukers eID kan den utføre misbruk til evig tid».

Tre år etter områdegjennomgangen, i 2022, ble BankID og Buypass notifisert av Norge til Kommisjonen for godkjennelse som eID'er på sikkerhetsnivå «høyt» ihht. reglene i eIDAS-

[83] Tar grep etter Nav-svindel: – Et kappløp.
[84] Svindelofre må betale tilleggsskatt på stjålne BSU-penger | DN
[85] Status og tiltak mot svindel for 2025
[86] Capgemini Invent, Områdegjennomgang id-forvaltningen Tilleggsrapport (6. desemember 2019), 07-09-2021-tilleggsrapport.pdf.

forordningen. Når et eID-system som meldes til Kommisjonen undergis det en ekstern fagfellevurdering av om de tekniske og organisatoriske kravene for det angitte sikkerhetsnivået er oppfylt.[87] Kommisjonen fører en liste over notifiserte eID-systemer og tilhørende sikkerhetsnivå.[88]

Konklusjonene etter fagfellevurderingen av BankiD og Buypass er offentlig tilgjengelig på nett.[89] Den mer utfyllende rapporten er derimot ikke åpent tilgjengelig, men SODI-prosjektet er innvilget innsyn i en sladdet versjon.

Arbeidsgruppen som vurderte sikkerheten i systemene peker på og utdyper de sikkerhetshullene som ble påpekt i områdegjennomgangen. Det er kritiske merknader til sikkerheten i forbindelse med utstedelse og reaktivering av en sperret eID og til de løpende autentiseringsprosessene. Norge pålegges å sørge for at både BankID og Buypass gjennomfører en rekke forbedringer i sikkerheten. Arbeidsgruppen konkluderer med at BankID og Buypass kan godkjennes som eID-løsninger på sikkerhetsnivå «høyt», gitt at de påpekte sårbarhetene utbedres. BankID og Buypass skal ikke tillates brukt over landegrensene før dette er gjennomført. Vi er ikke kjent med om kravene stilt i forbindelse med fagfellevurderingen er fulgt opp og utbedret. I fagfellerapporten fremgår det også kritiske merknader til systemet for tilsyn og kontroll med eID-leverandørene. Vi kommer nærmere tilbake til dette nedenfor i punkt 5.6.

Kjente sårbarheter

Dagens eID-systemer har flere sårbarheter som øker risikoen for svindel, bedrageri og misbruk av digitale identiteter. I det følgende skal vi peke på noen konkrete sårbarheter knyttet til BankID.

BankID er svært sårbart overfor såkalte phishing-angrep, der brukeren manipuleres til å oppgi passord og engangskode på en svindelside (eventuelt godkjenne innloggingen i en app). Sikkerhetsmekanismene i BankID er til en viss grad ikke i stand til å oppdage slike svindelforsøk, og brukerne må derfor falle tilbake på allmenn sunn skepsis for å oppdage svindel. Erfaring[90] og laboratorieforsøk[91] antyder at brukere i liten grad vil være i stand til å benytte de nyere sikkerhetsmekanismene til å oppdage svindel. For eksempel er det lett for en bruker å overse at BankID-appen spør om en signatur for Lillevik Sparebank, i stedet for en *identifikasjon* (innlogging) over Lillevik Sparebank. Det er også lett for en bruker å la være å lese meldingene i BankID-appen (f.eks. hvis brukeren har vanskelig for å lese).

En annen svakhet i dagens system er at BankID-appen gir begrenset informasjon om hva brukeren faktisk godkjenner. Appen viser kun generelle meldinger som "Vil du identifisere deg overfor Lillevik Sparebank", uten å spesifisere hva handlingen innebærer. Dette gjør det vanskelig for brukerne å oppdage misbruk i sanntid og gir svindlere en større mulighet til å utnytte systemet. Dermed kan en svindler manipulere offeret til å tro at de bare logger inn på en

---

[87] Jf. Kommisjonens gjennomføringsbeslutning (EU) 2015/296 artikkel 7

[88] Listen er tilgjengelig her: Overview of pre-notified and notified eID schemes under eIDAS - eID User Community - (europa.eu)

[89] Opinion No. 3/2022 - eID User Community -

[90] A. Whitten and J. D. Tygar, “Why Johnny can’t encrypt: A usability evaluation of PGP 5.0,” in Proc. 1999 USENIX Security Symp., vol. 348, 1999, pp. 169–184; S. Ruoti and K. Seamons, "Johnny's Journey Toward Usable Secure Email," in IEEE Security & Privacy, vol. 17, no. 6, pp. 72-76, Nov.-Dec. 2019.

[91] K. Gjøsteen and A. S. Lund, “An experiment on the security of the Norwegian electronic voting protocol,” Annals of Telecommunications, vol. 71, no. 7-8, pp. 299–307, 2016; Melanie Volkamer, Oksana Kulyk, Jonas Ludwig, Niklas Fuhrberg: Increasing security without decreasing usability: A comparison of various verifiable voting systems. SOUPS @ USENIX Security Symposium 2022: 233-252.

kjent tjeneste (f.eks. ID-porten), mens de i realiteten signerer en låneavtale eller gir tilgang til sensitiv informasjon.

BankID-appen gjør heller ingen forskjell på trivielle og viktige transaksjoner som godkjennes. Det betyr at brukeren ikke får noe signal fra systemet som gir dem mulighet til å skjerpe oppmerksomheten når viktige transaksjoner skal gjennomføres. (I noen systemer, f.eks. noen nettbanker, utløses identifiseringsbehovet bare av visse transaksjoner.)

Det utgjør videre en sårbarhet at det er mulig å ha flere aktive OTP-er (One-Time Passwords) samtidig for ett BankID-sertifikat. Dersom en angriper kan manipulere brukeren til å godkjenne utstedelsen av en ny OTP (f.eks. via phishing), kan svindleren bruke denne nyutstedte OTP-en til å logge inn på vilkårlige tjenester, endre kontoinformasjon eller signere økonomiske forpliktelser, samtidig som brukeren bruker den opprinnelige OTP-en som før. Brukeren blir ikke nødvendigvis varslet om at flere autentiseringsprosesser skjer samtidig, noe som gir rom for avanserte svindelmetoder, herunder økonomisk tvang og misbruk i nære relasjoner.

Manglende systemer for proaktiv svindelovervåkning gjør at mange svindeltilfeller oppdages først etter at skaden har skjedd. Uten en helhetlig antisvindelløsning som kan overvåke mistenkelige transaksjoner i sanntid, varsle brukerne om uvanlig aktivitet og identifisere kjente svindelmønstre, forblir mange digitale angrep uoppdaget. Kriminelle kan operere med høy effektivitet uten risiko for rask inngripen fra bankene eller myndighetene.

I tillegg er sperringsmekanismene for BankID utilstrekkelige, noe som skaper problemer for svindelofre. Brukere som får sin BankID misbrukt, møter ofte en komplisert og tidkrevende prosess for å sperre sin digitale identitet og få utstedt en ny. Det finnes ingen enkle prosedyrer for raskt å gjenopprette kontroll over egen eID, noe som gir svindlere lengre tidsvindu til å utnytte identiteten før nødvendige tiltak kan iverksettes.

Begrenset transparens og brukerkontroll utgjør også en sikkerhetsrisiko. Det finnes ingen samlet løsning hvor en bruker enkelt kan se en oversikt over når og hvor deres BankID har blitt brukt. Dette betyr at brukerne har begrenset mulighet til å oppdage uautorisert bruk av sin eID og handle deretter. Uten en selvadministrert løsning der brukere kan overvåke sin aktivitetshistorikk, sperre eller begrense sin BankID ved behov, blir det vanskeligere å sikre autonomi og forebygge identitetsmisbruk. Se nærmere om dette nedenfor i punkt 5.4.1.

Tiltak:

28. Finans Norge sine anbefalinger fra svindelrapport fra 2025 gjennomføres:[92]
    - Begrense til én OTP per sertifikat.
    - Gi bedre kontekstinformasjon i BankID-appen.
    - Få i gang nytt antisvindelsystem.
    - Tilby en bedre løsning for sperring av BankID som har blitt brukt i svindel.
    - Innføre selvadministrert BankID og MinSide for kundehistorikk.
29. Forby utstedelse av mer enn én BankID med kodebrikke og én BankID-app per bruker. (Tilgang til kodebrikke som backup til appen.)

[92] Status og tiltak mot svindel for 2025

30. Bygge utstedelse av eID på offentlig utstedt digital ID ("PID" etter eIDAS 2.0 terminologi) som en offentlig utstedt grunnidentitet. Slik dagens infrastruktur er fremstår det mest naturlig at Folkeregisteret og Politiet sammen kan skape et slikt offentlig utstedt digitalt grunnidentitetsbevis.

31. eID-leverandørene bør implementere sterkere autentiseringsmekanismer for bruk av eID-ene, inkludert systematisk og integrert bruk av biometrisk verifisering.

5.2.3. Sårbarheter hos brukerstedene

Gitt de eksisterende eID-løsningene som finnes på markedet, med de sikkerhetshullene disse har, er det opp til hvert enkelt brukersted/tjenestetilbyder å vurdere om bruk av eID er «sikkert nok» eller om det er nødvendig med ytterligere sikkerhetstiltak. Det kan imidlertid virke som om mange – både offentlige og private – brukersteder, samt lovgiver, har tenkt at en eID på sikkerhetsnivå «høyt» nærmest automatisk betyr at det ikke er behov for ytterligere sikkerhetstiltak og kontrollmekanismer. En utviklingstrend ved digitaliseringen er at manuell identitetskontroll er erstattet av bruk av eID. I disse prosessene er brukervennlighet og forenkling prioritert, uten at det er tatt høyde for økt risiko og de sårbarheter som følger med bruk av eID. Som NTAES påpeker i sin rapport om registermanipulasjon:

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

Utviklingen knyttet til lånebedragerier gir et slående eksempel: I 2017 ble det vedtatt en lang rekke lovendringer som hadde til formål å legge til rette for digitalisering.[93] En av endringene var at krav om fysiske signaturer av både debitor og to vitner på gjeldsbrev som skulle brukes som tvangsgrunnlag ble erstattet av en elektronisk signert gjeldserklæring. Krav til vitnesignaturer ble fjernet. Samtidig ble såkalt «samtykkebasert» lånesøknad innført.[94] Systemet bygger på at kreditor henter inn inntektsopplysninger mv. direkte fra myndighetene via Altinn, slik at den som søker om lån ikke lenger trengte å sende inn skattemelding, lønnsslipper mv. Alt som behøves for å søke om lån er derfor tilgang til noens BankID. Dessuten innebærer systemet med samtykkebasert lånesøknad at det er mulig å manipulere kredittvurderingen fordi endringer i lønn og formue enkelt kan gjøres i offentlige registre uten å måtte fremlegge dokumentasjon. Svindlere med tilgang til noens BankID kan derfor først manipulere inntekts- og formuesinformasjonen og deretter søke lån i innehaverens navn. Da dette ble iverksatt hadde mange banker ingen sikkerhetstiltak utover å basere seg på BankID og informasjonen som ble hentet fra offentlige registre.

I årene 2017-2020 var det en eksplosjon i lånesvindelsaker. Først da Høyesterett og lovgiver slo fast at bankene ikke kunne velte denne risikoen over på BankID-innehaverne, ble det iverksatt ytterligere sikkerhetstiltak hos bankene i forbindelse med innvilgelse av lånesøknader. Som påpekt av Høyesterett:

> Jeg legger da vekt på at skadelidte, Easybank, er en profesjonell aktør som har valgt å inngå en avtale om lån med et beløp som for en enkeltperson er betydelig, utelukkende basert på identifikasjon og elektronisk signatur gjennom BankID. Som det er fremhevet i

[93] Prop. 6 L (2016-2017) Endringer i tinglysingsloven, inkassoloven og tvangsfullbyrdelsesloven mv. (teknologinøytralitet).
[94] Samtykkebasert lånesøknad - Bits AS.

> det jeg har sitert fra Prop.92 LS (2019–2020) side 183-184, ville det vært mulig for banken å foreta ytterligere kontrolltiltak før man u[t]betalte lånebeløpet. Dersom man hadde gjort dette, er det stor sannsynlighet for at misbruket ville vært unngått. Banken har dermed bevisst valgt en handlemåte som innebar en klar risiko for tap.

Finans Norge vedtok i etterkant av dette en bransjenorm som inneholdt tiltak for å avverge lånesvindel. Normen fastsatte for eksempel krav om at BankID-innehaveren skal varsles om kredittsøknader, at lån kun skal utbetales til et kontonummer som tilhører lånesøker og at kredittyter skal sjekke gjeldsregisteret både på søknadstidspunktet og på utbetalings-tidspunktet.[95]

Et annet eksempel er praksis hos NAV i forbindelse med at det høsten 2023 ble oppdaget at en rekke NAV-brukere hadde fått kontonummer for utbetaling av ytelser endret på grunn av BankID-misbruk gjennom et phising-angrep.[96] Allerede tre dager etter at svindelen ble oppdaget hadde NAV endret rutiner og tekniske løsninger slik at endring av kontonummer for utbetaling krever en ekstra bekreftelse, samt satt i verk utsendelse av sms til brukeren når kontonummer endres.

Selv om det finnes eksempler på det motsatte, er det imidlertid fremdeles (for) mange tjenester og brukersteder som baserer seg kun på innlogging med eID, uten å ha ytterligere sikkerhetsmekanismer.

Tiltak:

32. Brukerstedene må risikovurdere bruk av eID i de enkelte brukstilfellene.
33. eID-løsningene bør tilby varierte autentiseringsmekanismer tilpasset risikoen i transaksjonen, særlig ved høyrisiko-transaksjoner som signering av gjeldsbrev og endring av kontonummer. Brukerstedene bør spesifisere risikoen.
34. Brukerstedene bør varsle (utenom eID-systemet) til den transaksjonen gjelder ved transaksjoner (inkludert endringer) av høy verdi eller på annen måte av stor betydning for brukeren. Brukerstedene bør også benytte autentisering (f.eks. digital fremvisning av pass eller fysisk ID-kort med integrert biometrisk sjekk, eller fysisk oppmøte) utover eID der risikovurderingen tilsier det.
35. Brukerstedene må ha manuelle kontrollmekanismer for særlig risikofylte disposisjoner.
36. Det bør vurderes (gjen)innføring av vitnekrav for særlig risikofylte disposisjoner, som låneopptak.

5.2.4. Sårbarheter knyttet til bruk av privat eID i jobbsammenheng

I noen sektorer er det en utbredt praksis at ansatte bruker sin private eID/BankID i jobbsammenheng. Kommunesektorens interesseorganisasjon (KS) peker på at «normalen er at ansatte bruker sin alminnelige, private eID også ved behov for eID i arbeidsforhold».[97] Ett eksempel er løsningen for registrering av dødsfall og dødsårsak, hvor leger bruker sin private

[95] Finans Norge, *Bransjenorm – Hvordan forebygge, avdekke og følge opp tilfeller av misbruk av BankID til opptak av usikret kreditt til forbruker*, 2022.

[96] Tar grep etter Nav-svindel: – Et kappløp

[97] Høringssvar: Veileder for bruk av eID - Hjem

eID.[98] Et annet konkret eksempel gjelder saken der NSM-direktøren inngikk en ulovlig låneavtale på 200 millioner kroner.[99]

Dette skaper utfordringer fordi det blir en uheldig sammenblanding av privat og profesjonell identitet og kan reise spørsmål om både arbeidsgivers kontrollmuligheter og ansattes valgfrihet og rettigheter til å verne om sin personlige informasjon.

En sentral utfordring er at arbeidsgiver i mange tilfeller ikke tilbyr en tjeneste-eID, noe som gjør at ansatte må bruke sin private eID for å signere dokumenter, logge inn på offentlige registre eller bekrefte sin identitet i forbindelse med arbeidsoppgaver. Dette kan være problematisk både fordi det innebærer en uklar ansvarsdeling mellom den ansatte og arbeidsgiver, og fordi det kan gjøre det vanskelig å skille mellom private og arbeidsrelaterte handlinger. Dersom en ansatt utfører en handling med sin personlige eID i jobbsammenheng, kan det bli uklart hvem som faktisk er juridisk ansvarlig for handlingen – er det den ansatte personlig, eller er det virksomheten? Dette kan ha store konsekvenser i tilfeller hvor det oppstår feil eller misbruk.

Manglende skille mellom privat og profesjonell bruk av eID skaper flere tilleggsutfordringer når det gjelder sikkerhet. Dersom den ansattes private eID blir stjålet eller misbrukt, kan dette gi uautorisert tilgang til både sensitive data knyttet til arbeidsplassen i eksterne registre og mulighet for manipulering og uautoriserte disposisjoner på vegne av arbeidsgiver.

Når ansatte tvinges til å bruke sine private digitale identiteter for å utføre arbeidsoppgaver, kan det skape en uheldig maktubalanse mellom arbeidsgiver og arbeidstaker, og det kan også undergrave tilliten til eID-systemene. I en tid hvor digital autentisering blir stadig viktigere, er det behov for klare grenser mellom privat og profesjonell bruk av eID, samt løsninger som ivaretar ansattes rettigheter og personvern, jf. også punkt 5.4.

Tiltak:

37. Alle ansatte skal ha rett til å kreve at arbeidsgiver anskaffer en egen eID til den ansatte for bruk i arbeidsforholdet som alternativ til bruk av den ansattes egen private eID på vegne av arbeidsgiver.
38. Det må gjennomføres risikovurderinger der privat eID vurderes brukt i jobbsammenheng. Ved uakseptabel risiko bør privat eID ikke brukes i jobbsammenheng.
39. Der det der mulig bør ansatte utstyres med pseudonymt ansattsertifikat, f.eks. i bransjer som krever autorisasjon og har sentrale autorisasjonsregistre der f.eks. et profesjonsnummer kan verifiseres og valideres.

5.2.5. Systemmisbruk; særlig om registermanipulasjon

Risikoen i økosystemet den digitale identitetsforvaltningen utgjør, gjør at man ikke kan se på risikoen hos de enkelte brukerstedene isolert. Sikkerhetshull hos ett brukersted kan påvirke risikoen hos andre brukersteder. Dette er særlig tydelig for såkalt registermanipulasjon, der identitetsmisbruk til manipulasjon av informasjon i offentlige registre brukes til å gjennomføre bedragerier hos andre aktører.

Ett eksempel er lånebedragerier som utnytter systemet for såkalt samtykkebasert lånesøknad (SBL), jf. ovenfor om dette. SBL innebærer at långivere, med samtykke fra lånesøkeren, kan hente innteksgrunnlag for kredittvurderingen fra Skatteetaten via Altinn. Ved å manipulere

[98] Dødsfall og dødsårsak - Norsk helsenett
[99] Signerte ulovlig låneavtale med egen BankID | Digi.no

innteksopplysningene i Altinn, for eksempel ved å sende inn falske A-meldinger, kan svindlere øke offerets kredittverdighet og på den måten få ut store lån.

Et annet eksempel er det økende problemet med identitetsmisbruk i selskapsforhold, der stråpersoners identitet utnyttes for å opprette stråselskaper eller kapre reelle selskaper, ved manipulasjon av informasjonen i selskapsregistrene til Brønnøysund. De fiktive selskapene brukes deretter til å gjennomføre bedragerier i milliardklassen mot både offentlige myndigheter, finansinstitusjoner og andre selskaper. Denne formen for kriminalitet er nærmere beskrevet i Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) sin rapport *Registermanipulasjon* fra 2024. I rapporten pekes det på følgende:

> «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.»[100]

Fair Play Bygg Oslo, en organisasjon som jobber mot arbeidslivskriminalitet, har erfart at denne typen ID-misbruk er omfattende og økende, og at det typisk rammer personer i utsatte og sårbare posisjoner, som arbeidsinnvandrere og mennesker i rusmiljøet. Bakmennene er godt organisert og svært profesjonelle og drifter det FPBO beskriver som «ID-Tyverifabrikker» der menneskers identitet og eID blir utnyttet på det groveste.[101]

NTAES peker på følgende hovedårsaker som muliggjør registermanipulasjon:

- Manglende samfunnsperspektiv i risikovurderinger og forvaltningen av registre og data.
- Brukervennlighet har gått «foran alt når digitale systemer og forvaltningsprosesser effektiviseres, uten å ha tilstrekkelige kontrollmekanismer».
- Mangelfull deling av informasjon for å vurdere påliteligheten i dataene.
- Mangelfull retting gjør at uriktige opplysninger blir lagt til grunn ved saksbehandling i egen etat eller av andre.

Et grunnleggende problem knytter seg til Brønnøysundregistrenes mandat, ressurssituasjon og det rettslige rammeverket knyttet til registrering i registrene. Brønnøysundregistrene driver kun formalkontroll av dokumenter som sendes inn til registrering.

Sverige har erfart liknende problemer knyttet til (mis)bruk av stråpersoner i selskapsforhold. Det er i den forbindelse gjennomført en større utredning av hvordan man kan komme registermanipulasjon med selskaper til livs: SOU 2023:34 Bolag och brott og Prop. 2024/25:8 Bolag och brott. Tiltak og lovendringer som foreslått i proposisjonen ble vedtatt høsten 2024, og lovendringer trådte i kraft 1. januar 2025. Blant tiltakene som er vedtatt er strengere krav til registermyndigheten om å kontrollere riktigheten av opplysninger, ikke bare drive formalkontroll av innkomne dokumenter. Dette innebærer blant annet en mulighet og plikt til å kreve manuell kontakt med personer som skal registreres i sentrale posisjoner i selskaper i tilfeller der det er grunn til å mistenke at vedkommende er stråperson.

[100] NTAES, Registermanipulasjon (2024), Rapport - Registermanipulasjon, s. 18.
[101] Fair Play Bygg Oslo og omegn, Årsrapport 2024 (2025) Arsmelding-Fair-Play-Bygg-2024-low_res.pdf, s. 27.

Noen særlige problemstillinger reiser seg også for elektronisk tinglysing av disposisjoner vedrørende fast eiendom i Grunnboken.[102] SODI-prosjektet er ikke kjent med at ID-misbruk utgjør et stort praktisk problem på dette feltet i dag. *Risikoen* er imidlertid til stede også i forbindelse med eiendomsregistre. En viktig avklaring når det gjelder tinglysing er at misbruk av elektroniske identiteter skal regnes som falsk i forhold til tinglysingsloven § 27, slik at en ikke risikerer å miste sin faste eiendom til en godtroende kjøper ved såkalt ekstinksjon etter at eiendommen er overført til en annen ved slikt misbruk. Dette kunne med fordel være avklart i lovteksten.

Ved innføringen av elektronisk melding til tinglysing ble vitnekravene avskaffet på tross av faglige råd. Dette medfører at man ikke lenger sikrer noen bevismidler som kan klargjøre hvem som brukte den elektroniske identiteten i denne sammenhengen; var det gamle mor eller sønnen, som hjalp henne med å betale regninger? Dette bør snarest rettes opp. Det er også uheldig at om man vil disponere bankkontoen sin med elektronisk identitet, kan man ikke unngå at disposisjoner vedrørende fast eiendom kan gjennomføres på samme måte. Særlig i denne sammenhengen er det viktig at det innføres et skille mellom daglige transaksjoner og større transaksjoner når det gjelder bruk av elektroniske identiteter. Ved papirbasert tinglysing arkiveres bekreftede kopier av de tinglyste dokumentene.

Ved elektronisk innsendte dokumenter kreves det imidlertid ikke at den elektroniske identiteten er brukt slik at en kan se hva det er underskrevet på; det holder at vedkommende har identifisert seg. Dette er uheldig, siden tinglysingskopiene etter noen år kanskje er det eneste beviset for hva som faktisk ble avtalt vedørende en fast eiendom. Også dette bør rettes opp.

Tiltak:

40. Det gjennomføres en tilsvarende utredning som i Sverige om registermanipulasjon i selskapsforhold, med vurdering av om tiltak og lovendringer som er iverksatt der også bør innføres i Norge.
41. Brønnøysundregistrene bør ha ansvar for å sikre at opplysninger som registreres er riktige, ikke kun formalkontroll av opplysninger. Dette krever flere ressurser og endret mandat.
42. Det bør lovfestes at misbruk av elektronisk signatur regnes som falsk i forhold til tinglysingsloven § 27.
43. Det bør gjeninnføres vitnekrav ved tinglysing.
44. Ved tinglysing bør det kreves ikke bare en elektronisk identifikasjon, men også en elektronisk sammenheng mellom identifiseringen og den teksten som signeres.

[102] For en nærmere beskrivelse av problemstillingene som reiser seg i tilknytning til tinglysing i fast eiendom, se Erik Røsæg, Elektroniske signaturer og tinglysing, i: Kjørven, Hjort og Wærstad (red.) Bruk og misbruk av elektronisk identifikasjon (Karnov).

5.2.6. Nye sikkerhetsutfordringer med KI-drevet ID-svindel

Kunstig intelligens (KI) representerer allerede en betydelig sikkerhetsutfordring innen ID-svindel, og det er rimelig å forvente at denne trusselen vil øke.[103] En rapport fra Signicat estimerer at 38% av tapene knyttet til ID-bedrageri involverer KI.[104] Generativ KI kan både forbedre eksisterende svindelmetoder og introdusere nye angrepsformer. Typisk vil dette ofte innebære etterligning av mennesker (i lyd og bilde) og mer effektiv dokumentforfalskning.

Svindelmetodene bruker gjerne «deepfake» KI for å skape falske bilder, videoer og stemmer. For å klone en stemme eller utseendet til en person, behøver KI-en opplæringsdata fra denne personen, slik at maskinen danner seg et bilde av personen eller dens stemme. Utenfor Norge har det vært eksempler der skadevare skal ha bedt brukere om å skanne ansiktet og ID-dokumenter, for å generere deepfakes brukt overfor banker.[105]

KI-drevet ID-svindel er økende internasjonalt, men det er foreløpig uklart hvordan den vil påvirke norske eID-systemer direkte. Bilder, stemmer eller video kan brukes for å lure enkelte ID-verifikasjonsmetoder som antagelig er mer utbredt utenfor Norge. Dette gjelder spesielt der brukeren blir bedt om å laste opp et bilde av et ID-kort, en selfie eller video, for eksempel i forbindelse med innrullering eller ved senere verifikasjon. Bruk av deep fake-materiale er lite aktuelt der det kreves et fysisk møte i skranken, slik det kreves ved første gangs innrullering i Norge.

Kloning av stemmer eller utseendet til en person offeret kjenner har blitt brukt for å lure personer til å overføre penger. Stemmen eller videoen kan for eksempel vise eller høres ut som en bedriftsleder eller et nært familiemedlem i en krisesituasjon, og dette har blitt brukt både via telefon eller i et videomøte.[106] Dessuten kan falske videoer på nett som viser kjente personer som anbefaler visse investeringer brukes til å utføre et phishing-angrep, for eksempel der en milliardær tilsynelatende anbefaler å klikke på en lenke. Videre kan KI bli brukt i alle faser av en ordinær eID-svindel, for å forbedre svindlerens metoder, lage mer overbevisende eposter brukt i phishing-angrep, eller bistå med å programmere skadevare.

Kunstig intelligens kan også brukes for å skape «syntetiske identiteter», dvs. falske identiteter som kombinerer ekte personopplysninger (for eksempel et fødselsnummer) med mange falske opplysninger, som samlet sett fremstår som autentiske. KI kan bidra til å skape et overbevisende helhetsinntrykk av en ekte person, selv om mange av opplysningene er oppspinn.

KI-verktøy som eksisterer på markedet tillater i varierende grad at brukeren skaper et bilde eller en video av en ekte person. EUs KI-forordning, vedtatt i 2024, innfører en plikt til å merke video,

---

[103] US Department of Homeland Security ,"Increasing Threat of Deepfake Identities," 13. November 2024, link; FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, FIN-2024-Alert004 November 13, 2024, https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

[104] Signicat og Consult Hyperion, "The Battle Against AI-driven Identity Fraud", 2024, The-Battle-Against-AI-driven-Identity-Fraud-2024-Signicat.pdf, s. 12.

[105] Bill Toulas, New 'Gold Pickaxe' Android, iOS malware steals your face for fraud, Bleeping Computer Blog, 15. Februar 2024, New 'Gold Pickaxe' Android, iOS malware steals your face for fraud.

[106] Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company | Trend Micro (US); Top 5 Cases of AI Deepfake Fraud From 2024 Exposed | Blog | Incode

audio og bilder som er deep fake, men det vil sannsynligvis likevel finnes programvare som ikke merker audiovisuelle produkter, og kriminelle vil kunne bruke denne programvaren til ID-svindel.[107] Samtidig er utfordringen dynamisk, noe som gjør tiltak vanskeligere. I teorien kan myndighetene tilby rådgivning om hvordan deep fake kan gjenkjennes, for eksempel ved å publisere en liste av deep fake indikatorer, slik amerikanske myndigheter har gjort.[108] I praksis er det imidlertid en fare for at slike lister blir utdaterte og da virker mot sin hensikt.

Tiltak:

45. Ta i bruk KI systemer som kan avsløre ID-svindel, for eksempel gjenkjenne avvik i måten bilder eller video vises på, analysere metadata, simulere angrep eller søke etter tilsvarende bilder på nett (reverse image search).
46. Utstedere og brukersteder bør vise varsomhet med å tillate ad hoc verifikasjonsmetoder der brukeren ikke er fysisk til stede i skranken, for eksempel videomøter.
47. Verifikasjonsmetoder der brukeren ikke er fysisk til stede i skranken (f.eks. digital fremvisning av pass eller ID-kort med integrert biometrisk sjekk) må jevnlig reevalueres med tanke på nye KI-drevne angrep (i tillegg til andre angrep).
48. Forsikre at alle relevante aktører i systemet får opplæring om hva KI kan få til (AI literacy).

5.2.7. Sårbarheter knyttet til sluttbrukerne

I praksis blir sluttbrukerne sittende med restrisikoen for å passe på sin egen digitale identitet, gitt sikkerhetshullene og risikoene som er beskrevet ovenfor.

Det utgjør en særlig sårbarhet at sikkerheten i systemet forutsetter at brukerne ikke deler sikkerhetsinformasjon og eID med tredjepersoner. Norsis har gjennomført en undersøkelse som viser at ca. 10 % av befolkningen enten deler egen eID eller bruker andres eID.[109] I de fleste tilfeller skjer dette frivillig og er et utslag av tillit og behov for praktisk hjelp. Det er imidlertid et voksende problem at kriminelle bruker press, tvang og vold for å tilegne seg andres eID, jf. nærmere om dette ovenfor i punkt 5.2.1.[110] I fravær av kontrollmekanismer som sjekker at brukeren av eID'en er den rettmessige innehaveren ved hvert enkelt brukstilfelle, utgjør dette en svært alvorlig sårbarhet.

Bruk av press, trusler og vold for å få tilgang til andres eID eller for å få vedkommende til å bruke egen eID er også et utbredt problem i nære relasjoner. Svenske forskere beskriver hvordan BankID og digitaliseringen av finansielle tjenester tilrettelegger for økonomisk vold mot kvinner som lever i voldelige forhold.[111] Juridisk Rådgivning for Kvinner (JURK) har lenge advart mot det samme.[112] I SODI-prosjektet ble det gjennomført en analyse av 292 svindelsaker behandlet hos

[107] KI-forordningen Art. 40: Europa-Parlamentets og Rådets Forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens, OJ *L, 2024/1689, 12.7.2024,* ELI: http://data.europa.eu/eli/reg/2024/1689/oj

[108] inCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, FIN-2024-Alert004 November 13, 2024, https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

[109] Norsis, Nordmenn og digital sikkerhetskultur 2024, Nordmenn og digital sikkerhetskultur 2024 - NorSIS
[110] Fair Play Bygg, Årsrapport 2024, Arsmelding-Fair-Play-Bygg-2024-low_res.pdf.
[111] E-legitimation som verktyg för ekonomiskt våld | SvJT.
[112] Advarer mot økonomisk vold mot kvinner.

rettshjelpstiltakene JURK, Jussbuss og Gatejuristen mellom 2015 og 2021.[113] To tredjedeler av ofrene hadde et nært forhold til lovbryteren: et familiemedlem, en nær venn eller en partner. Analyser av datamaterialet viste imidlertid en kjønnsdeling mht. relasjonen til svindler. For kvinnene hadde så mye som 80 % et nært forhold til lovbryteren, mens tilsvarende tall for de mannlige ofrene bare var 36 %. Dette viser viktigheten av å integrere kjønnsperspektiver for å forstå digitalt identitetstyveri, inkludert bruk av vold.

Tiltakene som er beskrevet ovenfor vil være viktige tiltak for å begrense sluttbrukers risiko. I tillegg bør følgende tiltak særskilt rettet mot sluttbrukerne gjennomføres:

Tiltak:

49. eID-leverandørene må sørge for at brukeren, i forbindelse med utstedelse av eID, får tilbud om god opplæring i trygg bruk av eID-en.
50. Myndighetene og eID-leverandørene må sammen øke bevisstheten om risikoene ved deling av eID, f.eks. gjennom informasjonskampanjer.
51. eID-leverandørene og brukerstedene må innføre bedre brukervarsling ved forsøk på uvanlig innlogging eller transaksjoner.
52. eID-leverandørene må gi brukerne mulighet til å sette begrensninger på egen eID-bruk, for eksempel geografisk eller etter type transaksjon.
53. eID-leverandørene må utvikle enklere sperremekanismer for raskt å kunne stoppe misbruk av eID.
54. eID-leverandørene må bedre brukeres mulighet til innsyn i og kontroll over egen eID, se punkt 5.4.1.

5.2.8. Mangelfullt samarbeid og deling av data mellom aktører

Som nevnt over i punkt 5.2.5 om systemmisbruk og registermanipulasjon utgjør manglende samarbeid og begrenset deling av data mellom aktører en vesentlig utfordring i forebygging av svindel og identitetsmisbruk. Problemet er imidlertid ikke begrenset til å gjelde registermanipulasjon.

I dagens situasjon opererer mange aktører, både offentlige og private, med egne systemer og prosesser uten tilstrekkelig utveksling av relevant informasjon. Dette fører til at faresignaler og mønstre knyttet til potensielt identitetsmisbruk eller svindel ikke oppdages og håndteres tidsnok. Finans Norge peker på behovet for mer deling av data mellom bankene, og mellom bankene, politiet, offentlige etater og ekomtilbyderne, og opplyser at finansnæringen vurderer

> «å utvikle et felles system for transaksjonsovervåkning og analyse, og/eller et datadelingssystem mellom bankene. Et slikt felles system kan bidra til å oppdage pågående svindel raskere, og bidra til å forebygge lignende svindel hos andre banker.»[114]

Begrensninger knyttet til personvernregelverk, ulik tolkning av taushetsplikt og manglende felles plattformer for sikker deling av sensitive data er en utfordring i dagens situasjon. Konsekvensen er at kriminelle lettere kan utnytte fragmenterte løsninger, og at effektiviteten av forebyggende tiltak blir svekket.

---

[113] Ellen Bennin Brataas, Mira Sofie Stokke og Amelia Svensson, Rapport om misbruk av eID Empirisk studie av kjennetegn ved svindelsaker behandlet hos rettshjelpstiltakene Jussbuss, JURK og Gatejuristen, for å avdekke digitale sårbarheter ved bruk av eID, SODI-rapport 1/2022, Rapport om misbruk av eID.
[114] Status og tiltak mot svindel for 2025

Det er åpenbart et behov for mer deling av data for å bekjempe økonomisk kriminalitet og identitetsmisbruk. Det er positivt i så måte at Finanstilsynet og Datatilsynet i 2025 har satt i gang et sandkasseprosjekt om datadeling.[115] Formålet med prosjektet er å utforske muligheter for datadeling som ligger i dagens regelverk, samt vurdere eventuelle behov for regelverksutvikling.

I arbeidet knyttet til deling av data, er det imidlertid viktig at det skjer på måter som ikke forsterker problemer vi allerede har med finansielt utenforskap og de-risking hos finansforetakene. I praksis ser vi ofte at personer som utsettes for bedragerier i tillegg fungerer som muldyr for hvitvasking, og i flere tilfeller blir disse strafferettslig forfulgt for uaktsom hvitvasking.[116] I tilfeller av identitetsmisbruk er det dessuten en risiko for at uskyldige personer blir flagget som kriminelle i datadelingssystemene. Dette kan få store konsekvenser for tilgangen til finansielle tjenester idet finansforetakene typisk vil si opp kundeforholdet når kriminell aktivitet oppdages. Slik dagens situasjon er, vil dette også innebære oppsigelse av BankID. Dersom bankene har et felles system for deling av data knyttet til hvem som har brukt betalingstjenester og andre finansielle tjenester i kriminell aktivitet, kan dette føre til at vedkommende ikke får opprettet kundeforhold noe sted.

I utkast til ny betalingstjenesteforordning, PSR, forsterkes plikten til transaksjonsovervåkning og det åpnes eksplisitt for mer deling av data.[117] Dette er imidlertid kombinert med et forbud mot oppsigelse av kundeforhold på dette grunnlag, se samme artikkel nr. 6:

> The processing of personal data in accordance with paragraph 4 shall not lead to termination of the contractual relationship with the customer by the payment service provider or affect their future on-boarding by another payment service provider ***unless a thorough fraud investigation conducted by the relevant authorities has concluded that the customer participated in the fraudulent activity***.

Det er litt uklart hva det betyr at kunden har «participated» i bedragerivirksomheten, særlig i lys av særnorske regler som – i motsetning til mange andre land – har straffebud som rammer ikke bare forsettlig, men også uaktsom, hvitvasking. Dessuten er det et spørsmål om det er en god ide at f.eks. unge mennesker som har kommet på skråplanet, og opptrådt som muldyr, for all fremtid skal være utestengt fra tilgang til betalingstjenester. Her må det i hvert fall sikres tilgang til grunnleggende betalingstjenester for alle – også de som er mistenkt eller straffedømt for økonomisk kriminalitet. En slik rett til grunnleggende betalingstjenester for alle følger av betalingskontodirektivet, men som beskrevet i punkt 5.1.3 er disse reglene ikke tilstrekkelig gjennomført og fulgt opp i Norge.

En annen problemstilling gjelder forholdet til eIDAS 2.0, og hvorvidt denne er til hinder for deling av data når transaksjoner og handler foretas via den nye Europeiske digitale lommeboken. eIDAS 2.0 artikkel 5a (18) oppstiller et utgangspunkt om at brukerne skal ha full kontroll over egne data og oppstiller følgende forbud:

> The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital

[115] Alle som søkte får bli med | Datatilsynet
[116] To eksempler er beskrevet her: Ble ofre for Tinder-svindel – dømt for uaktsom hvitvasking | DN
[117] Se artikkel 83: Texts adopted - Payment services in the internal market and amending Regulation (EU) No 1093/2010 - Tuesday, 23 April 2024.

Identity Wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise.

Det bør utredes hvilken betydning dette eventuelt har for igangsatte og planlagte prosjekter om datadeling.

Tiltak:

55. Myndighetene bør sørge for bedre samhandling og deling av informasjon mellom private og offentlige aktører, mellom ulike private aktører og mellom ulike offentlige aktører. Dette må skje på måter som ivaretar personvernet og rettssikkerheten og ikke fører til en forsterkning av problemer med finansiell ekskludering.
56. Det gjennomføres en utredning av mulighetsrommet etter eIDAS 2.0 for igangsatte og planlagte prosjekter om datadeling.

5.3. Gjenoppretting og reparasjon

I dette punktet beskriver vi utfordringer knyttet til styringsprinsippet nummer 3:

«Den digitale identitetsforvaltningen må inkludere systemer for å gjenopprette kontroll over egen eID, rette feil og reparere problemer og skadevirkninger forårsaket av ID-misbruk. Fordi Ingen systemer er feilfrie og det er umulig å forhindre all svindel og identitetsmisbruk, må det finnes effektive mekanismer for å rette feilene. Rettssikkerheten til ofrene må ivaretas og rettssystemet må sikre en rettferdig fordeling av tap og risiko.»

Drøftelsene tar utgangspunkt i følgende utfordringer:

- Reglene om tapsfordeling etter ID-misbruk gir ikke et sterkt nok vern (punkt 5.3.1)
- Utfordringer i kommunikasjon med og klagebehandling hos finansinstitusjoner (punkt 5.3.2)
- Offentlige myndigheter mangler retningslinjer og systemer for å rette opp feil etter identitetsmisbruk (punkt 5.3.3)
- Manglende rettshjelp og praktisk hjelp (punkt 5.3.4)
- Begrenset tilgang til og kompetanse til å forstå bevis kan føre til feilaktige avgjørelser (punkt 5.3.5)
- Utfordringer knyttet til strafferettslig forfølgning og forholdet til sivilrettslige krav (punkt 5.3.6)
- Mangler ved systemer for å rette feil opplysninger i registre (punkt 5.3.7)

5.3.1. Reglene om tapsfordeling etter ID-misbruk gir ikke et sterkt nok vern

Finansavtaleloven har siden 1999 hatt regler om tapsfordeling etter *betalingssvindel*. I 2020 ble det vedtatt regler i ny finansavtaleloven som utvidet forbrukervernet til også å gjelde *lånesvindel*. Kort og upresist må banken som hovedregel bære forbrukerkunders tap ved misbruk av BankID til å gjennomføre uautoriserte betalingstransaksjoner eller ved signering av lån eller andre avtaler om finansielle tjenester, med fradrag med fradrag på inntil NOK 12 000 ved grov uaktsom atferd fra svindelofferet og bortfall av ansvar ved forsett.

Ikke minst som følge av arbeidet i SODI-prosjektet og ID-juristens innsats, har det vært en utvikling i retts- og nemndspraksis i mer forbrukervennlig retning mot større vern for

svindelofre.[118] Domstolene var imidlertid svært strenge i mange år, som vi viser i en kvantitativ analyses av sivile svindelsaker om erstatningsrett og avtalerett i perioden 2017-2020.[119] Dessuten er det fremdeles slik at de privatrettslige reglene om tapsfordeling etter ID-misbruk etter vårt syn ikke beskytter ofrene tilstrekkelig.

For det første **er bedrifter og ideelle organisasjoner ikke omfattet** av finansavtalelovens vern. PSD 2 åpner for å gi små og mellomstore bedrifter samme vern som forbrukere på dette området, men norsk lovgiver har ikke benyttet seg av denne muligheten.

For det andre utgjør **finansavtalelovens varslingsregler en betydelig utfordring**.[120] Det er to frister som må overholdes. Den relative reklamasjonsfristen pålegger kunden å varsle «uten ugrunnet opphold» etter at hen fikk *faktisk* kjennskap til misbruket, og den absolutte reklamasjonsfristen innebærer at varselet ikke kan inngis senere enn 13 måneder etter at misbruket fant sted (belastningstidspunktet).[121] Konsekvensen av fristoversittelse er at svindelofferet ikke kan påberope seg tapsfordelingsreglene i finansavtaleloven, og kan derfor føre til store tap.

ID-juristen har erfart at reklamasjonsfristene innebærer en høyst reell trussel mot svindelofre, som kan lede til alvorlige rettstap. De gir et uforholdsmessig vern til finansinstitusjonene på bekostning av svindelofre – særlig personer utsatt for lånesvindel i nære relasjoner. Vi mener at bankenes behov for innrettelse ikke bør veie tyngre enn svindelofrenes rettssikkerhet, og at svindelofre som er utsatt for svindlere som har skjult sine spor ikke bør ha dårligere rettsvern enn andre svindelofre. Særlig den absolutte fristen på 13 måneder er problematisk. I tilfeller der en ektefelle har tatt kontroll over den andres BankID og bankkonto, vil svindelofferet for eksempel ikke bli oppmerksom på svindelen før en separasjonsprosess som innledes lenge etter utløpet av fristen.

For det tredje er **tapsfordeling etter svindel som ikke knytter seg til finansielle tjenester**, og som derfor faller utenfor finansavtaleloven, ikke særskilt regulert. Tapsfordelingen vil derfor måtte basere seg på alminnelige avtale- og erstatningsrettslige regler. Disse reglene gir ofte ikke klare svar på hvem som må bære tapet, og en slik rettslig uklarhet vil alltid være til ulempe for den minst ressurssterke parten, som ikke har råd til rettshjelp og kostbare rettslige prosesser.

Problemet omfatter ulike typer krav, og omfatter alt fra ID-misbruk ved inngåelse av avtaler om kjøp eller leie til offentligrettslige krav som skattekrav, bøter og tilbakebetalingskrav fra ulike offentlige kreditorer i forbindelse med stråselskaper. Særlig alvorlige konsekvenser får dette for personer som opplever å få sin identitet misbrukt til opprettelse av selskaper med personlig ansvar, herunder enkeltpersonforetak. Offentlige myndigheter har ingen retningslinjer eller systemer for håndtering av denne type krav, hvor klagefrister på vedtak osv. typisk har løpt ut for lengst innen offeret får kunnskap om kravene.

For det fjerde gir rettsreglene svakt vern i tilfeller som involverer **tvang, press og vold**. Finansavtalelovens særregler om tapsfordeling får ikke anvendelse når noen er presset eller tvunget til å bruke egen BankID til for eksempel å signere låneavtaler. Avtaleloven fra 1918 favoriserer gjennomgående den godtroende medkontrahenten (banken).

---

[118] Utviklingen er nærmere beskrevet i ID-juristens sluttrapport.
[119] Omland, Nilsen og Langford, Dommeradferd i digitale svindelsaker, SODI Working Paper #/2025, UiO.
[120] Se ID-juristens sluttrapport punkt 4.4.6.
[121] Finansavtaleloven § 4-24 annet ledd

Når det særskilt gjelder tilfeller av vold i nære relasjoner, har dette en side til FNs kvinnediskrimineringskonvensjon og Europarådets konvensjon om forebygging og bekjempelse av vold mot kvinner og familievold (Istanbulkonvensjonen), som forplikter Norge til å gjøre lovgivningstiltak for å forebygge og bekjempe økonomisk vold og vold utført med digitale midler.[122] JURK og ID-juristen har erfart at personer som er påført gjeld som følge av økonomisk vold mangler rettslig beskyttelse. Avtaleloven § 28 beskytter de som signerer en avtale under frykt for eget eller andres liv mot forpliktelsene avtalen stifter. Lovens utforming tar imidlertid ikke høyde for digitalisering eller den økte forståelsen av dynamikken i voldelige relasjoner, og gir derfor ikke tilstrekkelig beskyttelse til voldsutsatte.[123]

Avtalelovens voldsbegrep dekker i utgangspunktet kun fysisk maktanvendelse, og i tillegg må volden og tvangen være grov.[124] For at en trussel kan omfattes av bestemmelsen, må den fremkalle begrunnet frykt for noens liv eller helbred.[125] Så lenge medkontrahenten (f.eks. utlånsbanken) var i aktsom god tro, stilles det dessuten et krav om at den utsatte må varsle «uten ugrundet ophold» etter at tvangen har opphørt. I en digital kontekst hevder bankene som regel at de var i god tro om forholdene rundt låneopptaket – hvordan skulle de kunne avdekke hva som lå bak den digitale lånesøknaden? Videre er reklamasjonsfristen ukjent og lite tilgjengelig for svindelofre, og det tar som regel uansett lang tid før de klarer å orientere seg etter å ha brutt ut av en voldelig relasjon. Dette fører til at mange blir sittende med gjeldsforpliktelser de ikke selv har stiftet fordi de ikke reklamerer tidsnok – i henhold til en arkaisk avtalelovgivning.

I Sverige har Riksrevisionen nylig gjennomført en granskning av statens innsats mot økonomisk vold i nære relasjoner.[126] Rapporten inkluderer betraktninger knyttet til bruk av eID og konkluderer med at Regjeringen ikke har oppfylt sine plikter slik disse følger blant annet av menneskerettighetene nevnt over. Det pekes blant annet på at utredninger knyttet til eID gjennomgående ikke drøfter risiko og håndtering av økonomisk vold som disse systemene legger til rette for. Dersom tilsvarende granskning hadde blitt gjennomført i Norge ville resultatene trolig blitt det samme. Ett eksempel er at eID-strategien peker på at dagens eID-systemer «kan være utsatt for misbruk i nære relasjoner», men uten at strategien har ett eneste tiltak knyttet til denne risikoen.

Rettferdighetsbetraktninger tilsier at det ikke bør være sluttbrukerne, som for alle praktiske formål er tvunget til å benytte eID og digitale løsninger for å kunne fungere i samfunnet, som må bære tapene når gevinstene ved digitaliseringen tas inn av andre aktører (både offentlige og private). Dessuten har tapsfordelingsregler som legger en større andel av tapsrisikoen på

---

[122] Istanbulkonvensjonens artikkel 2 nr. 1 jf. artikkel 3 bokstav b og artikkel 12. GREVIO, *General Recommendation No. 1 on the digital dimension of violence against women,* 2021. FNs konvensjon om avskaffelse av alle former for diskriminering av kvinner (KDK), vernet mot vold er behandlet av FNs kvinnediskrimineringskomité i *General recommendation No. 35* (2017).

[123] Se Foss, Amanda Marie og Tone Linn Wærstad «Avtaleloven § 28 i lys av et moderne voldsbegrep» (under publisering i festskrift til Juridisk rådgivning for kvinner, 2025) og Kari Kiperberg Werenskjolds masteravhandling «BankID-svindel i nære relasjonar: Spørsmålet om avtalebinding i lys av det menneskerettslege vernet mot økonomisk vald», 2020.

[124] Karnov kommentar nr. 4 og nr. 1 til avtaleloven § 28.

[125] Karnov kommentar nr. 5 til avtaleloven § 28.

[126] Riksrevisionen, 'Statens insatser mot ekonomiskt våld i nära reationer', RiR 2025:6, Statens insatser mot ekonomiskt våld i nära relationer (RiR 2025:6).

profesjonelle parter vist seg å være svært effektive verktøy for å *forhindre* svindel og ID-misbruk fordi det gir insentiver til den profesjonelle parten om å iverksette ytterligere sikkerhetstiltak.

Vi har sett dette i Norge etter at Høyesterett og lovgiver plasserte ansvaret for tap ved lånesvindel på bankene. Etter at bankene måtte bære tapene, viser tall fra ID-juristen og domstolene at denne typen svindel markant.

Tilsvarende effekt så vi etter at Høyesterett i 2022 avklarte at bankene må bære tapet etter telefonsvindel der kunden ble lurt til å oppgi BankID-informasjon. Året etter pekte Finanstilsynet i sin årlige risiko- og sårbarhetsanalyse på at høyesterettsdommen «ser ut til å ha medført et økt fokus på området fra foretakenes side».[127] Finanstilsynets nyeste svindelstatistikk viser at svindeltyper der banken typisk må bære tapet, har gått ned, mens svindeltyper der kunden typisk må bære tapet, har gått opp.[128] Fintech-selskaper SODI-prosjektet har vært i kontakt med erfarer at endringer i den rettslige tapsfordelingen var direkte utløsende årsak til at de fikk solgt sine tjenester som øker sikkerheten.

Også internasjonalt er effekten av tapsfordelingsregler tydelig. I Storbritannia har myndighetene innført regler som pålegger bankene å dekke tapene etter svindel som i Norge fortsatt faller utenfor dagens lovverk («godkjente» svindeltransaksjoner).[129] Resultatet har vært en nedgang i denne typen svindel.[130]

Det er derfor viktig å få på plass en helhetlig regulering av tapsfordeling som gir insentiver til de aktørene som er best rustet til å forhindre ID-misbruk før det skjer. Finans Norge har foreslått at teleskaper og digitale plattformer også må ta deler av regningen når svindel blir muliggjort gjennom deres tjenester. Dette er et veldig godt forslag. Det samme gjelder offentlige aktører. I den grad svindelen relaterer seg til finansielle tjenester bør et slikt system legge opp til at den svindelutsatte kunden får sitt tap dekket av banken, som deretter kan kreve regress for hele eller deler av beløpet hos de aktørene som har bidratt til å muliggjøre svindelen. Dette for å unngå at bankkunder blir kasteballer mellom ulike aktører.

En helhetlig regulering av økonomisk ansvar etter svindel, med de rette insentivene, vil trolig gi flere positive effekter:

- Den vil redusere de totale tapene ved å stimulere til bedre svindelbekjempelse.
- Den vil pulverisere tapene og gi bedre beskyttelse til forbrukere, bedrifter og ideelle organisasjoner.
- Den vil stimulere til innovasjon og støtte til norske gründerselskaper innen Fintech, som utvikler nye løsninger for effektiv svindelbekjempelse.
- Den vil være en langt mer kostnadseffektiv strategi enn å øke bevilgningene til politiet i samme tempo som økningen av svindel i samfunnet.

Tiltak:

[127] årlige risiko- og sårbarhetsanalyse
[128] svindelstatistikk
[129] Payment Systems Regulator (PSR), Authorised push payment (APP) scams performance report (Juli 2024), APP fraud performance data | Payment Systems Regulator.
[130] Iflg. Ibid., falt tapene etter APP-transaksjoner med 12 % fra 2022 til 2023, se s. 7. Dette til tross for at antall forsøk på APP-svindel økte med 12 % i samme periode.

57. Utrede og foreslå en helhetlig regulering av tapsfordeling etter ID-misbruk. En slik regulering bør inkludere alle tiltakene i 58-63.
58. Gi små og mellomstore bedrifter og ideelle organisasjoner samme vern som forbrukere i finansavtaleloven.
59. Fordele ansvaret for tap på flere aktører enn finansinstitusjoner og på flere finansinstitusjoner (ikke kun den svindelutsatte kundens betalingstjenestetilbyder).
60. Regulere tapsfordeling i situasjoner som faller utenfor finansavtalelovens anvendelsesområde.
61. Oppdatere avtalelovens ugyldighetsregler ved digitale avtaleinngåelser med en moderne forståelse av vold og tilpasset et digitalt samfunn der bedrifter og kunder, særlig forbrukere, inngår avtaler i en digital setting der vold, press og utnytting ikke er synlig. En slik revisjon må inkludere både vilkårene for og konsekvensene av ugyldighet slik at den ivaretar offeret i situasjoner der vedkommende ikke har fått nyttiggjort seg verdiene det er snakk om og ikke kan klandres, jf. tilsvarende regulering i vergemålsloven § 15 første ledd tredje punktum. Revisjonen må ta hensyn til et moderne voldsbegrep slik det er regulert i internasjonale konvensjoner.
62. Varslingsregler i både avtaleloven og finansavtaleloven bør revideres.
63. Tapsfordeling for offentligrettslige krav som springer ut av ID-misbruk eller press, tvang og vold må særskilt reguleres.

5.3.2. Utfordringer i kommunikasjon med og klagebehandling hos finansinstitusjoner

Erfaring hos ID-juristen viser at det er store utfordringer knyttet til kommunikasjon med og klagebehandling hos finansinstitusjonene når kunder er utsatt for svindel og ID-misbruk.[131]

En stor del av ID-juristens arbeid på vegne av klientene har vært av praktisk art. I svindelsaker skal banker og kreditorpretendenter kontaktes og varsles om svindelen, holdes løpende underrettet om utvikling i eventuell straffesak mot svindler og det må kommuniseres om krav, motkrav, påstander og tilsvar. De fleste norske banker har bygget ned sine telefoniske kundebehandlingstilbud, og søker i stedet å basere seg på kommunikasjon via chatbotter eller andre meldingstjenester som kan kreve innlogging i nettbanken. Disse tjenestene er uegnet for å motta og håndtere varsler om svindel. En person som har sperret sin BankID som følge av svindel, kan ikke logge inn i nettbanken for å benytte meldingstjenester der.

Ved henvendelse over telefon er man som regel henvist til lange ventetider. Når man endelig når frem til en kundemedarbeider har vedkommende sjelden tilstrekkelig kunnskap om svindelbekjempelse eller digital utestengelse, eller juridisk kompetanse. I de bankene som har egne medarbeidere som arbeider med svindel, er slike avdelinger ofte ikke helgebemannet, slik at et fredagssvindeloffer må vente hele helgen på å få bistand og tilgang på informasjon som kan være svært tidssensitiv. Tilsvarende mangel på mulighet til å kommunisere med kvalifiserte medarbeidere eksisterer der inndrivelse er overtatt av, eller kravet er overdratt til, inkassoforetak.

Det er også utfordringer knyttet til behandlingen av klager og krav fra kundene som bygger på finansavtalelovens forbrukervernregler. Systemene for å fremme krav er i en del tilfeller kompliserte og lite tilgjengelige for kundene. I tillegg er tilbakemeldingene fra bankene ofte

[131] Dette punktet bygger på ID-juristens sluttrapport, særlig punkt 4.4.5.

skrevet på måter som er vanskelig for kunden å forstå, og med et språk og formuleringer som er avskrekkene og legger skyld på kundene.

Finansavtaleloven har regler om behandling av klager i § 3-53, som innebærer plikter for foretakene til å ha «passende og effektive rutiner for behandling av klager og krav fra kundene». Det er også krav til skriftlig svar som skal komme senest 15 virkedager etter at klagen er sendt inn. I tillegg har Finans Norge utarbeidet en bransjenorm om hvordan bankene skal forebygge, avdekke og følge opp tilfeller av misbruk av BankID til usikret kreditt.[132] Denne har et eget punkt om «Kundeoppfølgning» i punkt 9.2:

> BankID-innehavere som tar kontakt med Banken og uttrykker at de kan være utsatt for misbruk skal få informasjon om klagebehandling, herunder saksbehandlingstid, BankID-innehavers rettigheter og videre klagemuligheter. BankID-innehaver bør få tildelt en kontaktperson eller et eget kontaktpunkt som har ansvar for videre bistand

ID-juristens erfaring er imidlertid at verken reglene i finansavtaleloven eller bransjenormen følges i praksis. I lånesvindelsakene ID-juristen har behandlet, har bankene ofte brukt svært lang tid på å avgjøre om offeret holdes ansvarlig, og flere purringer har vært nødvendig underveis i prosessen. Ofte har det tatt opptil et halvt år å få svar fra banken. Dersom saken etterforskes av politiet, settes den typisk i bero hos foretaket i påvente av straffesak, og i disse tilfellene kan det ta flere år før en endelig avgjørelse foreligger. I denne perioden lider svindelofferet under usikkerhet, betalingsanmerkninger og renter som kan øke gjelden betydelig. Manglende økonomisk avklaring kan også gjøre det umulig å leie bolig eller inngå andre enkle avtaler.

I transaksjonssvindelsaker har ID-juristen erfart at det ofte tar over ett år før banken avgjør om de vil bringe saken inn for Finansklagenemnda etter tilbakeføring av beløpet, noe som skaper unødig usikkerhet.

ID-juristens erfaringer samsvarer med hva tilsynsmyndighetene i Storbritannia avdekket da de i et tematilsyn i 2023 undersøkte bankenes håndtering av svindelsaker.[133] Tilsynet konkluderte blant annet med at flere finansinstitusjoner hadde

- poor complaint handling including firms often taking too long to respond to customer complaints
- customers provided with decision letters that were sometimes unclear, confusing, or included unhelpful and, on occasion, accusatory language
- limited evidence that firms are appropriately taking account of characteristics of customer vulnerability when making decisions about fraud claims and complaints

Den store forskjellen mellom Norge og Storbritannia på dette feltet er imidlertid at norske tilsynsmyndigheter er totalt fraværende.

En særskilt problemstilling gjelder tilbakeføringsplikten med omvendt prosessbyrde etter finansavtaleloven § 4-32. ID-juristen erfarte at bankene ikke fulgte disse reglene, og varslet i

---

[132] Se til inspirasjon Finans Norge, *Bransjenorm om hvordan forebygge, avdekke og følge opp tilfeller av misbruk av BankID til opptak av usikret kreditt til forbrukere*, punkt 9.2. ID-juristens inntrykk er at bransjenormen ikke har ledet til nødvendig atferdsendring hos bankene.

[133] Anti-fraud controls and complaint handling in firms (with a focus on APP Fraud) | FCA

april 2022 Forbrukertilsynet og Finanstilsynet om dette.[134] Varselet resulterte i at Forbrukertilsynet opprettet tilsynssak. Tilsynet avdekket systematiske brudd på finansavtalelovens regler, og Forbrukertilsynet sendte i desember 2022 et orienteringsbrev til *samtlige* norske banker, hvor det redegjorde for riktig regelforståelse og fremsatte krav om en omgående overhaling av bankenes håndtering av svindelsaker.[135] ID-juristen erfarte at dette umiddelbart førte til forbedring i bankenes praksiser. Nå, i 2025 – og etter at ID-juristen er lagt ned – erfarer imidlertid Jussbuss at bankene i mange saker ikke oppfyller finansavtalelovens tilbakeføringsplikt.[136] Help Forsikring, som tilbyr svindelforsikring med bistand til svindelofre, meldte om det samme i 2024.[137]

Tiltak:

64. Banker og inkassoforetak bør ha dedikerte svindelmedarbeidere tilgjengelig hele uken. Svindelofre må få rask bistand fra kompetente ansatte og tildeles en fast kontaktperson.
65. Tilsynsmyndigheter bør pålegge banker å sikre tilstrekkelig kompetanse og organisering, forankret i finansavtaleloven § 3-1.
66. Svindelofre bør ikke bli økonomisk skadelidende som følge av lang saksbehandlingstid hos foretakene. En særskilt regel om at kredittrenter og forsinkelsesrenter ikke løper under klagebehandling og/eller berostillelse i påvente av straffesak, bør innføres.

5.3.3. Offentlige myndigheter mangler retningslinjer og systemer for å rette opp feil etter identitetsmisbruk

Det er ikke bare finansinstitusjoner og bedrifter som kan komme til å holde ofre for identitetsmisbruk ansvarlig for økonomiske konsekvenser av ID-misbruk. Offentlige myndigheter mangler retningslinjer og systemer for å rette opp i feil etter identitetsmisbruk. Vi vil trekke frem tre eksempler som illustrerer problemene:

Fair Play Bygg, en organisasjon som jobber mot arbeidslivskriminalitet, har fortalt historien til Hamid som kom til Norge som flyktning i 2013 da han var 16 år gammel.[138] Hamid startet på videregående opplæring innen tømrerfaget, og en «arbeidsgiver» tilbød han lærlingplass. «Arbeidsgiveren» var imidlertid kriminell og utnyttet både arbeidskraften og identiteten til Hamid. Arbeidsgiveren opprettet et enkeltpersonforetak i Hamids navn, og gjennom dette foretaket drev arbeidsgiveren kriminell byggevirksomhet. Krav og bøter fra offentlige myndigheter kommer i Hamids Digipost, som han ikke vet at eksisterer. Etter flere års kamp, med bistand fra ulike ideelle organisasjoner og offentlig omtale av saken i mediene og andre steder, frafalt de offentlige kreditorene kravene i begynnelsen av 2025.[139] Det er imidlertid grunn til å tro at den offentlige omtalen spilte inn,[140] og at andre ofre i samme situasjon ikke er i stand til å oppnå et slikt resultat. ID-juristen beskriver at det har vært «vanskelig – tilnærmet umulig» å bistå personer som er utsatt for identitetsmisbruk i selskapsforhold.[141]

---

[134] ID-juristen, *Finansforetaks brudd på tilbakeføringsplikt etter finansavtaleloven § 37*, 2022.

[135] Forbrukertilsynet, *Orientering til bankene - krav til bankenes tilbakeføring av forbrukers tap ved uautoriserte transaksjoner*, 2022.

[136] Bankenes sviktende ansvar i praksis

[137] Banker svikter svindelofre | DN

[138] Arsmelding-Fair-Play-Bygg-2023_TIL_NETT_lavopplost.pdf

[139] Arsmelding-Fair-Play-Bygg-2024-low_res.pdf

[140] Se blant annet Staten ofrer enkeltmennesker på digitaliseringens alter | DN

[141] Se ID-juristens sluttrapport punkt 4.2.6 og 4.4.10.

Et annet eksempel gjelder en kvinne som ble utsatt for omfattende BankID-misbruk av sin daværende samboer. Samboeren tok opp lån hos 14 ulike kredittinstitusjoner med en samlet sum på 2,5 millioner og tømte alle kvinnens kontoer, inkludert BSU-kontoen for til sammen 500.000 kroner. Samboeren ble strafferettslig dømt for forholdet, inkludert underslag av penger på BSU-kontoen. Likevel mente Skatteetaten at kvinnen hadde brutt vilkårene for BSU-kontoen slik at hun etter skatteloven § 16-10 måtte tilbakebetale skattefradraget hun hadde fått tidligere knyttet til BSU-sparingen. Kvinnen anmodet om omgjøring av vedtaket, men Skatteetaten svarte:

> «Regelverket åpner altså ikke for unntak for tilfelle der årsaken til at midlene ikke er brukt til boligformål er at skattepliktige er utsatt for underslag. Vi forstår at det oppfattes som urimelig at underslaget skal få ytterligere økonomiske belastninger i form av tillegg i skatt, men dette er et forhold mellom henne og gjerningspersonen (må eventuelt søke erstatning av vedkommende).»

Etter medieomtale av også denne saken,[142] ombestemte skattemyndighetene seg to år senere. Etter det SODI-prosjektet vet, har imidlertid ikke saken ført til mer strukturelle endringer mht. hvordan offentlige myndigheter håndterer saker og krav som involverer ID-misbruk.

Det siste eksempelet gjelder en større svindeloperasjon rettet mot NAV-brukere høsten 2023. Et phishing-angrep førte til at en svindler lyktes med å logge inn og endre kontonummer for utbetaling av offentlige ytelser for ca. 40 NAV-brukere.[143] Da NAV forstod at det dreide seg om et større angrep, var de svært raske i håndtering av saken. Som nevnte ovenfor allerede etter tre dager var både rutiner og tekniske løsninger knyttet til endring av kontonummer endret. Sikkerhetstiltakene inkluderte at endring av kontonummer krever en ekstra bekreftelse samt utsendelse av varsel på sms til brukeren når kontonummer endres. NAV sørget dessuten for rask reparasjon og gjenoppretting ved å sørge for utbetaling av ytelsene som de rammede brukerne ikke hadde mottatt som følge av svindelen. Saken er et eksempel til etterfølgelse både hva gjelder sikkerhetstiltak og evnen til rask reparasjon og gjenoppretting. Det er likevel et tankekors at de første brukerne som henvendte seg til NAV med spørsmål om manglende utbetaling av ytelsene ble avvist under henvisning til at brukernes BankID var blitt brukt i forbindelse med kontoendringen og at det derfor ikke var NAV sitt problem. Problemet ble først tatt tak i da det kom *mange* henvendelser om dette til NAV.

Tiltak:

67. Det utarbeides sentrale retningslinjer/rundskriv for offentlige aktørers håndtering av henvendelser med påstand om ID-misbruk.

5.3.4. Manglende rettshjelp og praktisk hjelp

Saker om ID-misbruk er ofte komplekse og krevende, både juridisk og praktisk.[144] Uten kvalifisert bistand har svindelofre liten mulighet til å ivareta sine rettigheter. Selv om politiet etterforsker og tar ut tiltale, gjenstår ofte krevende oppgaver for offeret – som å systematisere krav og holde oversikt i en kaotisk inndrivelsesprosess. Mange opplever inkassopågang fra nye kreditorer, selv

[142] Svindelofre må betale tilleggsskatt på stjålne BSU-penger | DN
[143] Tar grep etter Nav-svindel: – Et kappløp
[144] Teksten I dette punktet er en forkortet versjon av det som fremgår av Sluttrapporten til ID-juristen punkt 4.4.2.

etter avtale om at kravet skal stilles i bero. Å håndtere slike saker alene er ofte urealistisk – både på grunn av kompleksiteten og den emosjonelle belastningen.

Det finnes ingen offentlig ordning som gir rettshjelp i saker om ID-svindel. Forsikringer dekker noe, men langt fra alle er omfattet. For mange er ideelle tiltak eller studentrettshjelp eneste alternativ. Kompleks lånesvindel og bruk av stråpersoner i selskaper krever særlig kompetanse og kapasitet. Uten bistand risikerer ofrene fraværsdommer, tvangssalg og økonomisk ruin – selv når kravene mangler rettslig grunnlag.

Da det ble vedtatt regler med et forsterket forbrukervern mot lånesvindel, antok man at rettshjelpsbehovet ville bli mindre. Dette var en del av begrunnelsen for at rettshjelpsutvalget i sin utredning fra 2020 ikke gikk inn for å prioritere saker om ID-misbruk i fremtidens rettshjelpslov.[145] Erfaringene til ID-juristen tilsier imidlertid at finansavtaleloven 2020 og nyere avklaringer i rettspraksis dessverre ikke har løst alle problemer. Det reises stadig nye og kompliserte faktiske og rettslige problemstillinger. Svindlerne er fleksible og tilpasningsdyktige, tar raskt i bruk ny teknologi og utnytter stadig nye sårbarheter.

Erfaringene fra ID-juristen viser dessuten betydningen av spesialisert og samordnet bistand for å sikre en rettsutvikling som i tilstrekkelig grad ivaretar ofrenes behov.

For saker som gjelder vold i nære relasjoner, reiser dette også menneskerettslige spørsmål. I generell anbefaling nr. 33 fremhever Kvinnediskrimineringskomitéen, som er FNs kvinnekonvensjons overvåkningskomite, at staten plikter å lage et system for rettshjelp som er tilgjengelig og svarer til kvinnenes behov.[146] GREVIO, som er overvåkningskomiteen til Istanbulkonvensjonen[147], understreker at staten skal sikre ressurser til rettshjelp for å effektivt forhindre og forfølge vold som utføres gjennom digitale midler.[148] Vernet mot vold beskyttes ikke på en tilstrekkelig måte dersom bare enkelte sider av volden dekkes av fri rettshjelp.[149]

ID-juristen har avdekket betydelig rettshjelpsbehov og bidratt til viktige rettsavklaringer. Etter at ID-juristen avsluttet sin virksomhet, er det imidlertid fare for tilbakegang hvis ikke offentlige tiltak kommer på plass. Her kan Norge med fordel se hen til Danmark og det statlige hjelpetilbudet "Cyberhotline for digital sikkerhet". Dette er en statlig finansiert hjelpetjeneste hvor både borgere og virksomheter kan få råd og veiledning. Telefonen er åpen fra kl. 8 til 20 hverdager og 10 til 16 i helger og på helligdager - året rundt. Telefonen er også åpen utenfor disse tidene, for akutthjelp til å sperre eID, samt hjelp til virksomheter som er midt i et cyberangrep.

Tiltak:

68. Bistand i forbindelse med ID-misbruk av et visst omfang bør omfattes av den offentlige rettshjelpsordningen og må utløse rett til fritt rettsråd og fri sakførsel.

---

[145] Se NOU 2020:5, s. 163.

[146] General recommendation No. 33 on women's access to justice, CEDAW/C/GC/33, 2015 avsnitt 37.

[147] Europarådets konvensjon om forebygging og bekjempelse av vold mot kvinner og familievold (Istanbulkonvensjonen)

[148] GREVIO, *General Recommendation No. 1 on the digital dimension of violence against women,* GREVIO (2021), avsnitt 57 c

[149] Se nærmere Kari Kipperberg Werenskjolds masteravhandling «BankID-svindel i nære relasjonar: Spørsmålet om avtalebinding i lys av det menneskerettslege vernet mot økonomisk vald», 2020 s. 13-15 og s. 45.

69. Det offentlige bør tilby tilpasset førstelinjehjelp til dem som opplever ID-misbruk, jf. det statlige hjelpetilbudet i Danmark.
70. Utvide Gjeldsregisteret til å inkludere opplysninger om saker som er stilt i bero, og liknende avtaler knyttet til gjeld som inngår i innkassobyårenes porteføljer, og kreve at kjøper av porteføljen må respektere disse.

5.3.5. Begrenset tilgang til og kompetanse til å forstå bevis kan føre til feilaktige avgjørelser

Saker om ID-misbruk reiser særlige bevismessige utfordringer. Det er utfordrende for innehaveren av en eID å bevise at vedkommende ikke foretok disposisjonene selv, eller at disposisjonene ble utført under press, tvang eller vold. I praksis snus bevisbyrden, uten at innehaveren har tilgang til nødvendige tekniske bevis ettersom disse er kontrollert i sin helhet av andre aktører.

En sak fra Borgarting lagmannsrett fra 2019 er illustrerende.[150] Den handler om en mann som benektet å ha signert en låneavtale, men som i Oslo tingrett ikke ble trodd på dette. Han ble derfor dømt til å oppfylle forpliktelsene etter låneavtalen. Først da han hyret inn en privatetterforsker som oppdaget spionprogramvare på PC'en hans, ble han trodd på at avtalen ikke var signert av han selv. Kravet ble deretter frafalt før saken skulle opp for lagmannsretten.

Også i HR-2020-2021-A (BankID-misbruk I) stod uenighet om tekniske forhold sentralt. En mann ble i både tingretten og lagmannsretten funnet erstatningsansvarlig for lån opptatt med hans BankID. I avsnitt 84 til 87 beskriver Høyesterett hvordan en «fremlagt logg» over når den aktuelle BankID-kodebrikken var blitt brukt, hadde stått sentralt i lagmannsrettens bevisvurdering. Da saken stod for Høyesterett viste det seg imidlertid at loggen var feiltolket. Dette ble avgjørende for bevisvurderingen i Høyesterett. At feilen ikke ble oppdaget før i aller siste instans viser imidlertid sårbarheten som ligger i bevissituasjonen i disse sakene. Dette har en side til problemet som beskrives i punkt 5.4.1 om brukernes manglende innsyn i og kontroll over egen eID og personopplysninger. Brukerne har ikke tilgang til loggen som viser når, hvor og til hva deres BankID er brukt.

Svindelofferet har ofte ikke tilgang til andre bevis enn sin egen forklaring om at hen ikke har gjennomført disposisjonen eller signert selv. Dette har også sammenheng med hvordan personvernreglene er forstått. Personvernnemndas sak PVN-2019-08 omhandler et tilfelle der en person var utsatt for misbruk av identitet og personnummer til inngåelse av et mobilabonnement. Offeret ønsket innsyn i samtalelogg for å sjekke om mobilnummeret hadde hatt kontakt med finansinstitusjoner. Personvernnemnda avviste innsynsbegjæringen fordi opplysningene:

> «... ikke er personopplysninger om A, men personopplysninger om den som har opprettet mobilabonnementet. GDPR artikkel 15 gir da heller ikke A rett til innsyn. Det er politiet som i et slikt tilfelle vil kunne be om utlevering av opplysninger. Når politiet ikke har funnet grunn til å etterforske ytterligere, kan ikke A velge å tre inn i den rollen.»

Som følge av nemndas avgjørelse vil svindelofre være avhengige av politiets etterforskning for å bringe relevante bevis på bordet, se nærmere om dette i neste punkt. Vi vil i denne forbindelse kort bemerke at European Data Protection Board (EDPB) i januar 2022 ga klart uttrykk for at svindelofre har rett til innsyn i tilfeller som over nevnt, slik at personvernnemndas avgjørelse

[150] LB-2019-192625.

ikke kan anses å gi uttrykk for gjeldende rett.[151] Fordi norske aktører har en tendens til ikke å tolke EØS-retten på selvstendig grunnlag, men forholde seg til det norske avgjørelsesorganer har bestemt, hjelper imidlertid ikke nødvendigvis dette.

Finansavtaleloven har særskilte bevisregler i §§ 3-6 og 3-7 som skal ivareta hensynet til svindelofre og den asymmetriske tilgangen til tekniske bevis. Reglene trådte i kraft 1. januar 2023, og det er foreløpig uklart hvordan reglene vil bli tolket og hvilken effekt de vil ha. Utenfor finansavtalelovens anvendelsesområde er det imidlertid de alminnelige bevisreglene som gjelder.

Tiltak:

71. Datatilsynet bør følge EDPBs anbefalinger i tilfeller av ID-misbruk.
72. Det bør utredes om særskilte bevisregler bør innføres også på andre områder enn det som er dekket av finansavtaleloven.

5.3.6. Utfordringer knyttet til strafferettslig forfølgning og forholdet til sivilrettslige krav

Det er flere utfordringer knyttet til strafferettslig forfølgning av bedragerier og identitetskrenkelser.[152] Disse relaterer seg til de strafferettslige reglene som sådan, til oppfølgning av anmeldelser og til forholdet til sivilrettslige krav.

Identitetskrenkelser er straffbart etter straffeloven § 202, med en strafferamme på inntil 2 års fengsel. Bestemmelsen rammer tilfeller der noen uberettiget setter seg i besittelse av en annens identitetsbevis eller opptrer med en annens identitet med formål om å oppnå en uberettiget vinning eller påføre andre tap eller ulempe. Det er særlig tre problemer med bestemmelsen:

For det første rammer den ikke tilfeller der noens identitet misbrukes ved at de registreres som ansatte i stråselskaper som ledd i den type systemmisbruk som er beskrevet ovenfor under punkt 5.2.5. Alt som trengs for å registrere noen som ansatt er tilgang til personopplysninger som navn og fødselsnummer. I et slikt tilfelle har ikke den kriminelle nødvendigvis tilgang til vedkommendes identitetsbevis og den kriminelle utgir seg heller ikke for å være den fiktive ansatte. Bedragerier gjennomført via stråselskapet med de fiktive ansatte kan naturligvis likevel forfølges strafferettslig, men den som er utsatt for misbruk av sin identitet vil da ikke få status som fornærmet. Dette til tross for at det kan ha store konsekvenser å feilaktig bli registrert som ansatt i et stråselskap, blant annet fordi det kan føre til at andre offentlige ytelser stanses.

For det andre er den lave strafferammen et problem både fordi den i en del situasjoner ikke står i forhold til den faktiske forbrytelsen og fordi den kan påvirke prioriteringene til påtalemyndigheten. Personer som får sin identitet totalt overtatt av kriminelle, som bruker deres eID og identitet til å begå en lang rekke kriminelle handlinger, utsettes for et svært alvorlig

[151] EDPB (European Data Protection Board). Guidelines 01/2022 on data subject rights - Right of access. (18. januar 2022).

[152] For en komparativ analyse av norsk og estisk rett av utvalgte problemstillinger om forholdet mellom strafferettslig forfølgning og sivile krav i ID-svindelsaker, se Maria Astrup Hjort, Piia Kalamees og Laura Kask, Misuse of Electronic Signatures and eID Owner Liability: A Comparative Analysis of Estonian and Norwegian Legislative Frameworks and Practice, European Business Law Review, volume 36, issue 2 (2025), pp 287-312, httpss://doi.org/10.54648/eulr2025012.

inngrep i sin personlige integritet og frihet.[153] For disse tilfellene burde straffeloven hatt et alternativ om «grov» identitetskrenkelse, med en høyere strafferamme. Dette har også en side til prioriteringer i politi- og påtalemyndighetene, som gjerne er instruert til å prioritere mer alvorlig kriminalitet.

For det tredje kan det være uklart når bruk av en annens identitet er «uberettiget». Når mennesker i sårbare posisjoner får sin identitet misbrukt som ledd i kriminell aktivitet kan dette skje i en gråsone av press, trusler og «frivillighet». Dette gjelder for eksempel der en person med rusavhengighet blir presset til å gjøre opp narkotikagjeld ved å overgi sin eID. Et konkret eksempel er gjengitt i en dom fra Oslo tingrett hvor retten uttaler at en av de fornærmede forklarte at «han ble truet med å bli knivstukket hvis han ikke ga fra seg sin bank kodebrikke, og at han ble lovet penger dersom han ga fra seg brikken».[154] Også i nære relasjoner som preges av psykisk og fysisk vold kan det være gråsoner av «frivillighet» ifht. de disposisjonene som blir gjennomført. Dersom disse personene anmelder forholdet kan de bli møtt med at de selv har vært delaktige og derfor ikke er offer for noen straffbar handling (men tvert imot har medvirket til straffbare handlinger overfor andre).

Det er grunn til å tro at mange som utsettes for ID-misbruk ikke anmelder forholdet til politiet. Dette gjelder særlig de som står i et avhengighetsforhold til bakmannen, som for eksempel fremmedarbeidere eller personer som utsettes for økonomisk (og annen) vold i nære relasjoner. Fair Play bygg skriver følgende i sin årsrapport for 2024:

> Bak usynliggjøringen av fornærmede i ID-misbruksaker, står det hele mennesker som fortjener å ikke bli reduserte til tall, men også vitner med verdifull informasjon. Vi møter fortvilte mennesker som i tillegg til styreverv i byggeselskaper også er registrert som eiere av kjøretøy, kontoer eller narkotikadepotleiligheter disponert av kriminelle med stor voldskapital. Andre er kommet til Norge for å jobbe for å forsørge familien sin i hjemlandet, men endte opp med stor gjeld og straffeansvar for kriminelle handlinger de ikke ante var begått i deres navn.[155]

FPBO peker her på den mest alvorlige utfordringen: Faren for justismord ved at ofre for ID-misbruk blir strafferettslig forfulgt og dømt for straffbare forhold begått av andre i deres navn. Frykt for represalier kan gjøre at enkelte velger å ta en slik straff fremfor å fortelle hva som faktisk har skjedd. Dersom dette skal unngås må mennesker i disse situasjonene tilbys praktisk støtte og hjelp om de velger å anmelde forholdet. Dette vil ikke bare være til fordel for personen som er rammet, men kan også føre til at politiet kan få verdifull informasjon om bakmenn og dermed bedre muligheter for å oppklare sakene.

I de tilfellene der ID-svindel anmeldes, blir imidlertid flertallet av sakene henlagt, også der gjerningspersonen er kjent. De siste fem årene har politiet i snitt henlagt 62 prosent av saker om økonomisk kriminalitet.[156] Flere av ID-juristens klienter har oppgitt at politiet allerede ved

---

[153] Fair Play Bygg Oslo og omegn, Årsrapport 2024 (2025) Arsmelding-Fair-Play-Bygg-2024-low_res.pdf, s. 27.
[154] TOSL-2021-83084.
[155] Ibid. s. 26.
[156] Økokrim, *Trusselvurdering for 2024*, s. 8. Av de ferdig etterforskedede lovbruddene i 2023, ble 7.2% (21 500 lovbrudd) henlagt på grunn av manglende saksbehandlingskapasitet alene. Av disse var godt over halvparten tyverier eller bedragerier, se Statistisk Sentralbyrå, *Høyeste antallet henleggelser på ti år*, 2024.

levering av anmeldelse informerer om at forholdet ikke vil bli fulgt opp. Det er viktig at denne utviklingen snus. I den forbindelse er det gledelig at Bedragerienheten på Gjøvik nå er operasjonell. For at dette tilskuddet til politiets svindelbekjempelse skal bidra til en reversering av henleggelsesutviklingen, er det viktig at senteret bidrar til effektiv kriminalitetsbekjempelse på tvers av politidistriktene. Det som ser ut som ett tilfelle av digitalt bedrageri og identitetskrenkelse, inngår ofte som en del av organisert ID-kriminalitet. Det er derfor avgjørende at enkelttilfeller av digitalt bedrageri sees i sammenheng, og ikke henlegges hver for seg som individuelle tilfeller av mindre alvorlig økonomisk kriminalitet. I Meld. St. 15 (2023 – 2024) fremheves det at senteret skal bidra til å «forebygge» bedrageri gjennom samhandling med forvaltningsorganer, bedrageriutsatte næringer og andre interessenter, samt å bistå departementet i regelverksarbeid.[157] Dette er viktige oppgaver som det er prisverdig at politiet nå prioriterer. Det er likevel viktig at enheten bidrar til effektiv *bekjempelse* av økonomisk kriminalitet, og ikke bare fokuserer på forebygging. Erfaring fra svindelfeltet viser at opplæring og informasjonskampanjer har begrenset innvirkning på vår evne til å motstå svindelangrep. Det er derfor særlig viktig at politiet har en avskrekkende effekt på motivasjonen til potensielle digitale bedragere.

For et svindeloffer vil det kunne ha stor betydning om og hvordan politiet følger opp en anmeldelse om digitalt bedrageri og identitetskrenkelse. Politiets etterforskning vil for det første kunne belyse saken. Hvis etterforskning avdekker forhold som taler for at svindelofferet er utsatt for bedrageri og identitetskrenkelse, vil vedkommende få en bedre bevismessig stilling. Motsetningsvis har ID-juristen erfart at når straffesaken henlegges, vil kreditorpretendent ofte betvile offerets historie. I slike tilfeller vil offeret også ha vansker med å selv innhente relevante bevis, delvis som følge av manglende kompetanse og delvis som følge av utbredt feiltolkning av personvernreglene (se foregående punkt om sistnevnte).

For det andre vil en fellende dom mot svindler kunne lede til at kreditorpretendenter frafaller krav mot svindelofferet.[158] I slike tilfeller vil det være bevist utover enhver rimelig tvil at den gjeldsstiftende disposisjonen er utført av enn annen, hvilket har vist seg å motivere kreditorpretendenter til å frafalle krav mot svindelofferet og heller vende seg mot svindler. Enkelte motparter har sågar vist seg villige til å frafalle kravet allerede idet etterforskning igangsettes, ettersom også et slikt påtaleskritt underbygger svindelofferets forklaring om at den aktuelle disposisjonen er gjennomført av en annen. Motsetningsvis viser erfaringer fra ID-juristen at frifinnelse av svindler er til særlig ugunst for svindelofre. Dette skyldes at mange kreditorpretendenter opptrer som om det ikke er et skille mellom strafferettslig og privatrettslig beviskrav. At det i straffesaken ikke er bevist *utover enhver rimelig tvil* at svindler har inngått kredittavtalen, er ikke det samme som at det mangler *sannsynlighetsovervekt* for at gjelden har et svindelopphav. Men når svindler frikjennes for et bestemt krav, eller påtalemyndighet av ulike årsaker ikke inkluderer kravet i tiltalebeslutningen, behandles dette likevel av en rekke kreditorpretendenter som ensbetydende med at kravet må være stiftet av svindelofferet. En slik feilaktig tilnærming til beviskravet leder til gjenopptakelse av pågang overfor svindelofferet.

---

[157] I Meld. St. 15 (2023 –2024) *Melding til Stortinget Felles verdier – felles ansvar Styrket innsats for forebygging og bekjempelse av økonomisk kriminalitet* s. 55.

[158] Finansbransjens hovedorganisasjon, Finans Norge, har utarbeidet en bransjenorm hvor det fremgår at der rettskraftig dom mot gjerningspersonen foreligger, skal banken «som hovedregel» ikke forfølge kravet overfor BankID-innehaver, se Finans Norge, *Bransjenorm – Hvordan forebygge, avdekke og følge opp tilfeller av misbruk av BankID til opptak av usikret kreditt til forbruker*, punkt 10.2. ID-juristen har blandet erfaring med hvordan normen er fulgt opp av banker i praksis.

Erfaringsmessig får paradoksalt nok svindelofferet i slike tilfeller en enda vanskeligere oppgave, idet hun nå både må bevise egen uskyld og overbevise kreditorpretendent, inkassoforetak og namsmyndigheter om at svindlers frifinnelse ikke automatisk innebærer at disposisjonen er stiftet av svindelofferet.

Utformingen av påstandsgrunnlaget vil også kunne ha betydning for svindelofferets privatrettslige stilling. ID-juristen har opplevd at motparter (særlig banker) har brukt svindelofferets regressadgang der svindler dømmes til å svare erstatning til *svindelofferet*, som argument for fortsatt pågang mot offeret. En dom som fastsetter svindlers erstatningsansvar overfor *kredittgiver* (eller annen motpart), gir svindelofferet et håndfast motargument mot en slik begrunnelse fra bank/inkassoforetak.

Lang saksbehandlingstid knyttet til etterforskning og forfølgning utgjør videre et selvstendig problem. ID-juristen erfarer at en del finansinstitusjoner godtar å sette krav i forbindelse med omtvistet gjeld i «bero» mens politiet etterforsker saken. Som ID-juristen påpeker, har imidlertid slik «berostillelse» også store negative konsekvenser for ofrene i form av både psykisk påkjenning å leve med en uavklart rettslig posisjon, at gjeldsordning blir utelukket i denne perioden og at høye rentesatser på omtvistede lån likevel løper slik at kravet vokser raskt og betydelig.[159]

I tillegg til å ha ansvar for etterforskning og påtale av digitale bedragerier og identitetskrenkelse, har politiet en viktig rolle som informasjonsgiver til svindelofre. Politiet er ofte en av de første aktørene ofre vender seg til etter å ha oppdaget digital svindel. Politiets møte med svindelofferet i førstelinje kan ha stor innvirkning på hvordan vedkommende håndterer den privatrettslige siden av svindelen. ID-juristen har erfart at politiet har formidlet til en rekke svindelofre at når anmeldelsen først er levert, er det meste av jobben gjort. Enkelte svindelofre er eksplisitt rådgitt om å unnlate å besvare henvendelser fra kreditorpretendenter, inkassoforetak mv. Det medfører ikke riktighet at politiets oppfølging av forholdet setter de privatrettslige konsekvensene «på pause». Slike misvisende uttalelser fra politiet kan tvert om gjøre at svindelofferet lider alvorlig rettstap. Erfaringer fra ID-juristens klientgruppe antyder at det er behov for opplæring av politiets førstelinje om privatrettslige konsekvenser av eID-svindel, slik at svindelofre kan gis kortfattet og riktig informasjon om strakstiltak, samt bli henvist til relevante aktører som kan gi mer inngående juridisk bistand (Jussbuss, JURK, Kontoret for fri rettshjelp mv.).

Tiltak:

73. Revisjon av straffeloven § 202 slik at den rammer flere former for identitetsmisbruk. Innføring av en ny bestemmelse om grovt identitetsmisbruk med en høyere strafferamme.
74. Mennesker i sårbare posisjoner som velger å anmelde, må tilbys praktisk hjelp og bistand.
75. Det gjennomføres en utredning med sikte på å foreslå tiltak som reduserer de negative konsekvensene av at svindelofre står i en uavklart økonomisk posisjon mens de strafferettslige forholdene er under etterforskning og evt. påtale. Svindelofre bør kunne kreve berostillelse av omstridt gjeld uten at verken avtalte renter eller forsinkelsesrenter løper i denne perioden.

[159] Se Sluttrapport for ID-juristen, punkt 4.4.5, s. 34, sluttrapport_id-juristen_endelig.pdf.

76. Bedragerienheten på Gjøvik bør utarbeide retningslinjer for effektiv etterforskning og påtale av digitale bedragerier og identitetskrenkelser på tvers av politidistrikt, og innta en koordinerende rolle for nasjonal bekjempelse av kriminalitetsformen.
77. Politidirektoratet bør utarbeide rundskriv og sørge for opplæring som sikrer tilstrekkelig kunnskap i politiets førstelinje om privatrettslige konsekvenser av digitalt bedrageri og identitetskrenkelse, slik at svindelofre kan veiledes og henvises til relevante ressurser.

5.3.7. Mangler ved systemer for å rette feil opplysninger i registre

Når noen er utsatt for ID-misbruk vil det føre til registrering av informasjon som er feil. Gjeld tatt opp av en svindler blir registrert på eID-innehaveren, manglende betaling av gjelden fører til betalingsanmerkninger for eID-innehaveren, konkurs i et selskap der en person er innsatt som styreleder, daglig leder e.l. mot vedkommendes vilje vil fremgå av selskapsregisteret og etter hvert i konkursregisteret osv. osv.

Det har vist seg utfordrende å få rettet opplysninger i Brønnøysundregistrene, når en person feilaktig er registrert som stråperson i et selskap. Også i tilfeller der svindlere har klart å «kapre» et selskap ved å misbruke identiteten til en faktisk rolleinnehaver, har det vært vanskelig å få rettet feilen.

Utover faren for å materielt sett bli holdt ansvarlig for disposisjoner man ikke har gjort frivillig, har det i seg selv negative konsekvenser å stå registrert i ulike registre. Når gjeld feilaktig er registrert i gjeldsregisteret påvirker det kredittvurderinger og dermed mulighet for å få lån til for eksempel å kjøpe eller bytte bolig. Betalingsanmerkninger som skyldes svindel og eID-misbruket man er utsatt for, påvirker også kredittvurderinger og muligheten til for eksempel å kunne inngå avtaler om mobilabonnement, strøm, handle på nett med betalingsutsettelse/faktura osv.

Det finnes regler for enkelte registre som har til formål å sikre at registrerte opplysninger er riktige og som skal gi mulighet for å få rettet opplysninger som er feil. Eksempelvis følger det av kredittopplysningsloven § 11 at inkassoopplysninger som stammer fra en omtvistet fordring ikke skal brukes i kredittopplysningsvirksomhet. Videre følger det av § 19 at det skal sendes forhåndsvarsel før betalingsanmerkninger og andre kredittopplysninger registreres, og at den registrerte innen 14 dager fra mottak av slikt forhåndsvarsel oppfordres til å melde fra om feil. Det er imidlertid ikke gitt at slike meldinger kommer fram til mottakeren, se nærmere om dette i punkt 5.4.3.

Tilsvarende regler finnes imidlertid ikke for omtvistet gjeld som er registrert i Gjeldsregisteret. Gjeldsregisteret inneholder til enhver tid de gjeldsopplysninger som finansforetakene har rapportert inn, og på registerets hjemmeside henvises man til å ta kontakt med det enkelte finansforetak dersom man mener det er registrert feil opplysninger.[160] Det er da opp til det aktuelle finansforetaket å vurdere innsigelsen. ID-juristen har erfart er at det er svært krevende å få gehør for sletting av omtvistet gjeld, og at slik gjeld typisk blir stående registrert i lang tid i påvente av en eventuell avklaring knyttet til strafferettslig etterforskning og forfølgning.[161] Dermed vil slik gjeld bli stående i registeret og kunne være til hinder for refinansiering, boligbytte mv. Rettshjelpstiltakene erfarer også at retting av opplysninger i Brønnøysundregistrene, for eksempel der noen feilaktig er registrert som innehaver, styreleder e.l. i et foretak, er krevende.

[160] Gjeldsregisteret.
[161] Se Sluttrapport for ID-juristen, s. 34, sluttrapport_id-juristen_endelig.pdf.

Tiltak:

78. Det gjennomføres en utredning av reglene for alle relevante registre, herunder Gjeldsregistreret og Brønnøysundregistrene, for å sikre at mekanismer er på plass for retting av feil opplysninger.

5.4. Autonomi: selvbestemmelse og personvern

I dette punktet beskrives utfordringer knyttet til styringsprinsipp nummer 4:

«Alle individer skal ha kontroll over sin egen digitale identitet, hvem som har tilgang til den, og hvordan den brukes. Brukere skal ha rett til innsyn i egne identitetsdata og kunne begrense eller tilbakekalle samtykke til deling av opplysninger. Personvern er en grunnleggende menneskerettighet, og digital identitet må forvaltes i tråd med personvernlovgivning og prinsippene om dataminimalisering og brukerkontroll. Bruk av eID må være frivillig.»

Flere av utfordringene som er beskrevet ovenfor, har også en side til dette prinsippet. Noen av de viktigste koblingene er:

Problemet som er beskrevet i punkt 5.1.3 om at alternative analoge/fysiske og digitale løsninger er blitt dårligere eller helt borte, har også en side til autonomi og selvbestemmelse. Når eID på høyeste sikkerhetsnivå blir en forutsetning for tilgang til både offentlige og private tjenester, tvinges individet inn i en digital infrastruktur uten reelle alternativer. Personer som ikke får eller ønsker å bruke eID, mister i praksis muligheten til å delta på lik linje i samfunnet. Når eID blir eneste mulighet, overstyres individets rett til selv å bestemme hvordan man vil interagere med samfunnet.

I punkt 5.2.4 har vi beskrevet hvordan bruk av privat eID i jobbsammenheng skaper sikkerhetsmessige sårbarheter for både arbeidstakeren og arbeidsgiveren. Dette har imidlertid også en side til autonomi, selvbestemmelse og personvern. Datatilsynet har pekt på at bruk av privat eID i jobbsammenheng er utilfredsstillende blant annet fordi det medfører en sammenblanding mellom rollen som privatperson og rollen som ansatt og fordi det innebærer at den ansatte pålegges å medbringe kodebrikke eller privat mobil hver dag til arbeidsplassen.[162] Krav om bruk av privat eID i jobbsammenheng medfører også at den ansatte tvinges til å inngå en avtale med en privat eID-utsteder. Inngåelse av slik avtale bør i prinsippet være frivillig.

I punkt 5.2.8 beskriver vi mangelfullt samarbeid og deling av data mellom aktører. Behov for deling av data mellom aktører for å forebygge svindel har en klar motsats i personvernhensyn. Det sentrale er å finne en hensiktsmessig balanse mellom sikkerhet på den ene side og personvern på den annen.

I punkt 5.3 har vi drøftet ulike problemer knyttet til gjenoppretting og reparasjon ved ID-misbruk. Grunnleggende sett er dette også utfordringer knyttet til autonomi og selvbestemmelse. Når det offentlige mangler retningslinjer og systemer for rette opp feil etter identitetsmisbruk (punkt 5.3.3), og det er mangler ved systemer for å rette feil i opplysninger i offentlige registre (punkt 5.3.7), innebærer dette samtidig inngrep i den enkeltes autonomi og kontroll over egne

[162] Brev fra Datatilsynet til Kommunal- og Distriktsdepartementet, Uttalelse – Utkast til ny strategi for eID i offentlig sektor, referanse 22/02003-2 (25.4.2022). Merk at dette brevet ikke er publisert som et høringssvar til utkastet til eID-strategi.

personopplysninger, samt brudd på kravet om at personopplysninger som behandles skal være korrekte og oppdaterte og den registrerte har krav på å få rettet opplysninger som er feil.

I det følgende vil vi særskilt drøfte følgende utfordringer:

- Manglende innsyn i og kontroll over egen eID og personopplysninger (punkt 5.4.1)
- Teknologien overstyrer den juridiske privatautonomien (punkt 5.4.2)
- Digitalisering og bruk av eID kan føre til rettstap fordi informasjon ikke kommer frem til brukeren (punkt 5.4.3)

5.4.1. Manglende innsyn i og kontroll over egen eID og personopplysninger

Brukere av eID i Norge har i praksis begrensede muligheter til å få innsyn i hvordan deres digitale identitet brukes. Den enkelte eID-innehaver har riktignok – i teorien – rett til innsyn i hvilke personopplysninger som behandles om vedkommende, både hos eID-utstederen og hos det enkelte brukersted, se personvernforordningen artikkel 13-15.[163] Det er ingen tvil om at bruk av en personlig eID innebærer behandling av personopplysninger. Brukerens problem er imidlertid at det ikke finnes noen samlet logg der man kan se når, hvor og til hvilket formål ens eID har vært benyttet, og det er heller ingen enkel funksjon for å få en oversikt over hvor mange eID-er som er utstedt i ens eget navn. Mangelen på innsyn og kontroll over egen digital identitet svekker både individets personvern og rettssikkerhet, jf. også ovenfor om tilgang til bevis.

Datatilsynet har tidligere uttrykt bekymring for hvordan eID-forvaltningen balanserer personvern og sikkerhet. I et innspill til regjeringens arbeid med eID-strategi peker tilsynet på at bruk av eID på unødvendig høyt sikkerhetsnivå kan være problematisk i lys av personvernprinsippet om dataminimering.[164] Innspillet synes først og fremst å gjelde det Datatilsynet mener er unødig bruk av fødselsnummer, både generelt og når ansatte bruker eID i situasjoner der de representerer sin arbeidsgiver. Videre har tilsynet understreket at det er viktig at løsninger for digital identitet utvikles med innebygd personvern. Bruk av fødselsnummer er imidlertid ikke spesielt for eID på høyt sikkerhetsnivå. Fødselsnummer behandles også ved bruk av MinID når det er nødvendig for tjenesten det logges inn på. Og bruksvilkårene i ID-porten påpeker at tjenesteeierne som benytter ID-porten må oppfylle de særlige kravene til bruk av fødselsnummer i personopplysningsloven § 12.

Det kan være gode grunner til å etablere en samlet oversikt over hvem som har fått utstedt eID på nivå høy, og om vedkommende har en eller flere slike eID'er, se bl.a. det som er skrevet i punkt 5.4.3 om en eventuell plikt for avsender til å sjekke om mottaker har slik eID og dermed kan få tilgang til en melding på nivå høy før en slik melding sendes elektronisk.

Derimot er det flere motforestillinger mot å etablere samlede oversikter over hva den enkelte har brukt sin eID til (den enkeltes *transaksjoner)*. En slik oversikt kan være egnet til å fortelle mye om den enkelte eID-bruker og dennes atferd, og et sentralt register vil kunne bli et attraktivt angrepsmål. Et slikt tiltak bør derfor i høyden gjelde for den enkelte eID, og være begrenset til f.eks. oversikt over hvilke brukersteder som har etterspurt status for eID'en hos eID-utstederen

[163] Personvernforordningen gjelder også for eID'er som faller inn under eIDAS' virkeområde, se artikkel 2 nr. 4 (ny i eIDAS v2, forordning (EU) 2024/1183, og erstatter tidligere artikkel 5 i forordning (EU) 910/2014).
[164] Brev fra Datatilsynet til Kommunal- og Distriktsdepartementet, Uttalelse – Utkast til ny strategi for eID i offentlig sektor, referanse 22/02003-2 (25.4.2022). Merk at dette brevet ikke er publisert som et høringssvar til utkastet til eID-strategi.

og tidspunktet for dette, men ikke opplysninger om hva den er brukt til (dataminimering). Hva eID'en er brukt til må det enkelte brukersted holde oversikt over.

For den kommende EUDI Wallet, vil en slik oversikt finnes i lommeboken, slik at brukeren selv kan holde oversikt, men samtidig er det krav om at ikke utstedere eller andre aktører skal kunne etablere koplinger mellom bruk og bruker.

Hensynene bak den avgrensningen som er gjort for EUDI Wallet når det gjelder kopling mellom bruk og bruker, er relevante også for andre løsninger enn lommeboken, og fordeler og ulemper med eventuelle nye registre bør vurderes nøye. Brukeren bør også ha anledning til å reservere seg for slig lagring som ellers gjøres fordi man antar at det er i brukerens interesse. Den lagring utsteder selv må foreta for å kunne dokumentere sin praksis, tjenestekvalitet og sikkerhet, kan imidlertid ikke omfattes av reservasjonsretten.

Under enhver omstendighet bør eID-utstederne vurdere sin egen praksis når det gjelder å håndtere begjæringer om innsyn i behandlingen av personopplysninger om en selv fra den enkelte eID-innehaver, og gjøre dette mer tilgjengelig og brukervennlig der det er mulig.

I forlengelsen av dette bør det også være mulig for den enkelte eID-innehaver å styre egen risiko ved å selv kunne bestemme hva slags disposisjoner som skal kunne gjennomføres med eID'en. Slik systemet er i dag, utvides i praksis den enkelte brukers risiko hver gang nye brukersteder og tjenesteeiere inkluderes. Dette skjer uten at innehaverne blir informert eller har noen mulighet for å reservere seg. For eksempel bør det være mulig å sperre for bruk av egen eID til inngåelse av avtaler om forbrukslån og registrering i selskapsregistrene.

Tiltak:

79. Alle bør ha rett til en brukerstyrt eID med mulighet for bruksbegrensninger og tilgang til logg som viser når, hvor og til hva eID'en er brukt, se også 5.2.6.[165] Loggen bør bare være tilgjengelig for brukeren selv og gjelde for den enkelte eID. Brukeren bør kunne reservere seg mot registrering av opplysninger som ellers skjer av hensyn til brukeren.
80. Kontakt- og reservasjonsregisteret bør utvides med opplysninger om hvorvidt brukeren har fått utstedt en eID på nivå høy (og som ikke er trukket tilbake) og hvem som har utstedt eID'en eller eID'ene. Oversikten må være tilgjengelig for brukeren selv og for avsendere som har rett (og plikt) til å benytte kontakt- og reservasjonsregisteret for å sende elektroniske meldinger slik at de (f.eks. forvaltningen, et legekontor eller inkassoselskap) ikke sender en melding på sikkerhetsnivå høyt til en person som ikke kan få tak i meldingen fordi vedkommende ikke har eID på riktig sikkerhetsnivå. Se også om meldinger som ikke kommer frem i punkt 5.4.3.

5.4.2. Teknologien overstyrer den juridiske privatautonomien

Teknologiske løsninger for digital identitet er i økende grad en forutsetning for å utøve rettigheter og inngå rettslige disposisjoner, men systemene er ofte ikke tilpasset den juridiske handleevnen ulike grupper har i ulike sammenhenger. De tekniske løsningene setter i praksis begrensninger for hvem som kan handle på egne vegne og hvem som kan bistås av andre, på måter som ikke er samordnet med rettstilstanden for øvrig.

Et eksempel er tilgang til digital helsetjenester for ungdom. Ungdom er helserettslig myndige fra fylte 16 år og kan selv bestemme over egen helsehjelp. I praksis kan imidlertid 16- og 17-åringer

[165] Dette er også foreslått av Finans Norge, Status og tiltak mot svindel for 2025

ikke benytte seg av digitale helsetjenester dersom foresatte ikke samtykker til at ungdommen får BankID eller annen eID på øverste sikkerhetsnivå.

Personer med funksjonsnedsettelser møter lignende problemer. Selv om retten til å inngå avtaler og utføre rettslige handlinger i utgangspunktet ikke er avhengig av at en person kan gjennomføre handlingen helt uten bistand, er dette ofte et krav for å få utstedt eID. Flere banker praktiserer regler som sier at BankID kun kan utstedes til personer som kan bruke løsningen selvstendig, uten hjelp fra pårørende eller andre. Dette er i strid med prinsippene i FN-konvensjonen om rettighetene til personer med nedsatt funksjonsevne (CRPD), som fastslår at funksjonshemmede har rett til å ta beslutninger på egne vegne med nødvendig støtte. Også i norsk vergemålsrett ligger det til grunn at personer som har verge, som hovedregel har rettslig handleevne og kan inngå avtaler selv. Likevel får mange personer med funksjonsnedsettelser ikke tilgang til eID, noe som i praksis innebærer en digital umyndiggjøring.

Mangelen på fleksible fullmaktsløsninger forsterker dette problemet. En person som ligger på sykehus og ikke selv kan betale regningene sine, har ingen mulighet til å gi en tredjepart begrenset fullmakt til å utføre denne handlingen, jf. ovenfor i punkt 5.1.4. Bankenes disponentløsninger tar tid å få på plass og gir full tilgang til hele kontoen og alle transaksjoner, noe som ofte er en uakseptabel løsning. Det finnes heller ingen mekanismer som tillater dobbeltsignering eller andre former for beslutningsstøtte, noe som kunne ha hjulpet personer som i perioder har redusert kapasitet til å håndtere egen økonomi og andre disposisjoner.

I praksis betyr dette at teknologien innfører begrensninger på den juridiske handleevnen, selv der loven ikke gjør det. Digitale løsninger overstyrer retten til å ta beslutninger på egne vegne eller få bistand i tråd med etablerte juridiske prinsipper. De rettslige utgangspunktene for menneskerettigheter, vergemål og privatautonomi blir i realiteten satt til side fordi teknologien ikke gir rom for nyanserte løsninger. Dette utfordrer grunnleggende rettigheter og skaper store praktiske problemer for dem som rammes.

Verger kan i dag bruke MinID på vegne av vergehaver som ikke er i stand til å håndtere en eID på egenhånd, men dette tillates i dag ikke av markedsaktørene som utsteder eID på øverste sikkerhetsnivå, jf. ovenfor. Det beste er at det finnes gode sentrale fullmaktsløsninger på tvers av privat og offentlig sektor slik at verger og andre som bistår personer som har problemer med digitale løsninger kan bruke egen eID når de representerer vergehaver eller fullmektig. Dette vil imidlertid ta noe tid å få på plass. På grunn av den svært prekære situasjonen for personer som bistås av verge, bør det som et strakstiltak åpnes for at verger tillates å bruke vergehavers eID på øverste sikkerhetsnivå på dennes vegne, se også punkt 5.1. Denne muligheten kan fjernes når eID er tilgjengelig for flere og sentrale fullmaktsløsninger er på plass.

Den som får et papirbrev hjem til seg eller til institusjonen, kan selv bestemme hvem som skal tømme postkassen og åpne brevet. På samme måte burde det være mulig å la andre lese digital post på vegne av en selv. En eID som kan benyttes for å få tilgang til informasjon om en selv, men som har begrensninger med hensyn til økonomiske transaksjoner, kan være en løsning på dette. Spørsmålet er om dagens eID-er kan tilrettelegges for slik bruk, uten samtidig å skape usikkerhet for eID-er generelt. Det kan tenkes i alle fall to veier til en slik løsning.

For det første kan man knytte tilleggsinformasjon til eID-en i forbindelse med selve autentiseringen. Når noen benytter en eID på høyt sikkerhetsnivå til autentisering, vil det alltid bli gjort en kontroll av at eID-en fortsatt er gyldig. Da kan man samtidig sjekke om det er (andre) begrensninger knyttet til eID-en. Man kan f.eks. tenke seg at handlingsbegrensninger er

registrert i en tilhørende katalog (slik tilfellet er for fødselsnummer hos eID-leverandørene i dag) og at opplysninger om eventuelle handlingsbegrensninger utleveres sammen med statusinformasjon om eID-en som hentes når autentiseringen gjennomføres. Den som mottar statusinformasjonen (om eID-en er gyldig eller ikke) mottar da også handlingsbegrensningen (fra eID-leverandørens katalog).

Den andre muligheten er å legge begrensningen direkte i sertifikatet for de sertifikatbaserte eID-løsningene som benytter såkalte kvalifiserte sertifikater. Sertifikatformatet som benyttes for kvalifiserte sertifikater har en utvidelse (QCStatement) som er obligatorisk for kvalifiserte sertifikater. Det er definert flere QCStatements med spesifikk betydning. Blant disse er et valgfritt statement som gjør det mulig å sette en begrensning på bruken av sertifikatet til et visst pengebeløp. Utvidelsen er lite brukt. Den har sitt opphav i e-signaturdirektivet (1999/93/EF) og var da knyttet til direktivets bestemmelse om sertifikatutstederens erstatningsansvar. Denne koplingen til sertifikatutsteders ansvar er ikke videreført i eIDAS, men utvidelsen finnes fortsatt i spesifikasjonene for kvalifiserte sertifikater, se ETSI EN 319 412-5 V2.4.1 (2023-09) punkt 4.3.2. Man kan tenke seg at det å sette verdien til 0 i sertifikatet kan tolkes (i Norge) slik at det er et rent legitimasjonsdokument, og at rettslig handleevne må vurderes separat, slik at også personer med begrenset rettslig handleevne kan disponere egen eID bl.a. for å få tilgang til offentlige tjenester (hvis de ikke får egen eID i dag). Utvidelsen er strengt tatt knyttet til signeringssertifikater, men i dag benyttes vel fortsatt i stor grad det samme sertifikatformatet for eID hos de norske tilbyderne (selv om nøkkelbruken er satt til autentisering). Det burde ikke være umulig å få en slik tolkning av utvidelsen inn i bl.a. ID-porten. Vi har allerede en norsk profil for de kvalifiserte sertifikatene (SEID) som tar stilling til nasjonale valg og utvidelser. Den kan oppdateres slik at muligheten for å sette beløpsbegrensning tas inn. For den gruppen som i dag ikke får eID på nivå høyt, og dermed ikke får tilgang til en del digital post til seg selv, ville et slikt tiltak kunne ha effekt selv om det bare er nasjonalt. Det kan om nødvendig også knyttes til mer presis informasjon i eID-leverandørens katalog som nyanserer handlingsbegrensningen og som utleveres sammen med statusinformasjon for sertifikatet (se tilsvarende ovenfor).

Tiltak:

81. Alle må ha rett til eID på samme måte som alle har rett til fysisk ID-bevis, uavhengig av funksjonsnedsettelser og digitale og fysiske ferdigheter. Dette kan om nødvendig gjøres ved å utstede eID-er med begrenset bruksområde eller rettigheter, eller ved å kunne registrere bruksbegrensninger i sertifikat-/eID-katalogen og utlevere bruksbegrensningene sammen med status for eID-en når den benyttes.

5.4.3. Digitalisering og bruk av eID kan føre til rettstap fordi informasjon ikke kommer frem til mottakeren

Da eForvaltningsforskriften[166] ble vedtatt første gang i 2002, og videreført i 2004, var det klart at innbyggerne hadde rett til å kommunisere elektronisk med forvaltningen, men at forhåndsvarsler, enkeltvedtak, og andre meldinger av betydning for den enkelte, *fra* forvaltningen, krevde uttrykkelig samtykke fra den enkelte mottaker. Videre skulle det sendes varsel til den adressen innbyggeren hadde oppgitt for slikt varsel om at en melding var tilgjengelig. Hvis meldingen ikke ble lest i løpet av en uke, skulle meldingen sendes ut på

[166] Forskrift 25. Juni 2004 nr 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).

papir.[167] Dette ble endret med innføringen av såkalt "digitalt førstevalg". Fra 1. januar 2014 fremgår det av eForvaltningsforskriften § 8 at: "Et forvaltningsorgan kan benytte elektronisk kommunikasjon når det henvender seg til andre". Meldingen skal gjøres tilgjengelige fra "egnet informasjonssystem". Dette kan være virksomhetens "Min side" eller en sikker digital postkasse, og det skal sendes varsel om at meldingen finnes der basert på opplysninger fra kontakt- og reservasjonsregisteret. Hvis meldingen ikke blir lest innen en uke, skal det sendes nytt varsel. Hvis meldingen fortsatt ikke blir lest selv om nytt varsel er sendt, har avsender ingen flere forpliktelser til oppfølging etter forskriften. Liknende regler har kommet til på andre områder, men med varierende grad av klarhet og det virker å være noe ulik praksis på tvers av bransjer.

Slike regler om såkalt «digitalt førstevalg» i kombinasjon med bruk av Digipost og andre digitale postkasser og portaler, samt manglende kontroll over og innsikt i om borgerne har tilgang til en aktiv eID, skaper betydelige utfordringer når det gjelder autonomi og tilgang til og kontroll over egne opplysninger.

Bruk av Digipost og andre digitale postkasser skaper utfordringer knyttet til informasjonstilgang og oppfølging av rettslige frister. Reglene om digitalt førstevalg, kombinert med et fravær av sammenheng mellom tilgang til/sperring av eID/BankID, fører til at viktig informasjon, herunder innkalling til legetimer, helseinformasjon, vedtak, pengekrav, innkassovarsler mv., kan havne i en digital postkasse som brukeren ikke har tilgang til uten at avsenderen er klar over det. Også i et beredskapsperspektiv er det viktig at offentlige myndigheter til enhver tid har oversikt over hvilke borgere som rent faktisk har – og ikke har - tilgang til en aktiv eID på øverste sikkerhetsnivå. Dette for å sikre at viktig informasjon når ut til dem det gjelder.

Konkret utgjør det et potensielt alvorlig rettssikkerhetsproblem at slik informasjon gjøres tilgjengelig via virksomhetens "Min side", sendes til eBoks, Digipost e.l. uten at avsender vet om mottaker har en aktiv eID som gjør det mulig å få tilgang til meldingen, og heller ikke iverksetter andre tiltak hvis meldingene ikke blir lest.

Løsningene med varsling fungerer ikke godt nok og ikke slik de var tenkt. Da regelen var at det måtte innhentes samtykke, var det også større sannsynlighet for at den som samtykket faktisk fulgte opp varsler til den adressen de selv hadde oppgitt, og at de var mer forberedt på at meldinger kunne komme og bedre rustet til å forstå hva det innebar. Nå skal det ikke mer til enn at en personer er registrert med en elektronisk adresse i kontakt- og reservasjonsregisteret, og ikke aktivt har reservert seg, så kan alle forvaltningsorganer gjøre meldinger tilgjengelig elektronisk uten nærmere undersøkelser. Varsling er alt som skal til. Gjentatt varsling, i de tilfellene en melding ikke blir lest, har vist seg ikke å være tilstrekkelig. For det første har det ingen effekt hvis varselet aldri har kommet frem, f.eks. fordi varslingsadressen ikke er oppdatert. For det andre vil det ikke hjelpe dersom mottakeren ikke forstår hva varselet gjelder, eller hvor vedkommende skal logge seg inn for å få tilgang til meldingen. Det er nå et stort antall digitale postkasser i bruk (bl.a. innenfor helseområdet) og store forvaltningsorganer og virksomheter har hver sin egen "Min side" for innbyggere og kunder. Varslene skal av sikkerhetshensyn ikke inneholde direkte lenke, og innbyggere frarådes, korrekt nok, å trykke på slike lenker (fare for

[167] § 8 om underretning om enkeltvedtak mv fra forvaltningen lød opprinnelig slik:
"1) Underretning om enkeltvedtak kan skje ved bruk av elektronisk kommunikasjon dersom parten uttrykkelig har godtatt dette og oppgitt den elektroniske adresse forvaltningsorganet skal benytte for å sende varsel etter nr. (2) nedenfor. ...
7) Har parten ikke skaffet seg tilgang til enkeltvedtaket innen én uke fra det tidspunkt det ble sendt varsel om det, eller vedtaket ble gjort tilgjengelig, skal underretning skje i henhold til de reglene som gjelder når det ikke er gitt samtykke til elektronisk kommunikasjon, jf. forvaltningslovens § 27 [dvs. på papir]."

phishing). For mange er dette komplisert og ikke til å forstå. På toppen av det hele, har prinsippet om digitalt førstevalg ikke noe krav om at avsender må forsikre seg om at mottaker har en eID på det sikkerhetsnivået som er nødvendig for å få tilgang til meldingen.

Prinsippet om digitalt førstevalg er antakelig kommet for å bli, men det må iverksettes tiltak som avbøter de uheldige konsekvensene av hvordan dette nå gjøres i praksis. For det første må det mer aktivt opplyses om muligheten for å reservere seg, hvordan det kan skje, og konsekvensene av det. Det må også være mulig å reservere seg mot elektronisk kommunikasjon med private aktører. For det andre bør kravene til varsling og oppfølging av uleste meldinger, gjelde flere enn de som omfattes av eForvaltningsforskriften i dag, slik at ikke pengekrav, prøvesvar, innkalling til konsultasjon på sykehus mv blir liggende ulest. For det tredje må det legges til rette for at den som gjør meldinger tilgjengelig elektronisk forsikrer seg om at mottakeren enten har en eID som gjør det mulig å skaffe seg tilgang til meldingen, slik det er foreslått i punkt 5.4.1 ovenfor, eller tilbyr en alternativ måte for å få tilgang til den. Og endelig må uleste meldinger følges opp mer aktivt enn det som skjer i dag med gjentatt varsling til samme adresse. Disse tiltakene kan med fordel kombineres med det som er skrevet om bedre fullmaktsløsninger og subsidiære varslingsadresser som gjør det lettere for pårørende eller andre nærstående å bistå dem som sliter med å forstå kompleksiteten i systemene.

Tiltak:

82. Det må aktivt informeres om muligheten for å reservere seg mot digital post fra forvaltningen, hvordan det gjøres og konsekvensene av det.
83. Reservasjonsretten bør utvides til å kunne gjøres gjeldende for flere typer meldinger og tjenester enn i dag, og overfor både offentlige og private virksomheter. Det bør være mulig å reservere seg bare mot noen tjenester, eller å oppheve reservasjon bare for enkelte tjenester.
84. Alle typer meldinger som må antas å ha stor betydning for den enkelte bør omfattes av kravene til varsling og oppfølging hvis de ikke leses, ikke bare de meldingene som omfattes av eForvaltningsforskriftens § 8. Dette kan muligens baseres på den kategorisering som avsender uansett må gjøre i forbindelse med valg av varslingsmetode og sikkerhetsnivå mv, f.eks. at alle meldinger på sikkerhetsnivå høyt må følges opp av avsender.
85. Det bør vurderes å gjeninnføre ettersending av meldinger i fysisk post, dersom digital post ikke åpnes, slik løsningen var i henhold til eforvaltningsforskriften § 8 frem til 2014 (fra 2004, og tilsvarende i § 7 i 2002-forskriften frem til 2004). Det bør også vurderes andre former for oppfølging hvis digital post ikke leses, f.eks. per telefon når forholdene gjør det hensiktsmessig og trygt.
86. Det bør utredes om kontakt- og reservasjonsregisteret kan inneholde opplysninger om den enkelte har eID på nivå høy og om denne er i aktiv bruk slik at avsender kan sjekke dette før melding sendes digitalt på sikkerhetsnivå høyt, slik det er foreslått under punkt 5.4.1.

5.5. Transparens: åpenhet og gjennomsiktighet

I dette punktet beskrives utfordringer knyttet til styringsprinsipp nummer 5:

«Den digitale identitetsforvaltningen må være så åpen og gjennomsiktig som mulig. Dette gjelder både tekniske løsninger, organisatoriske forhold og sentrale beslutningsprosesser.

Informasjon om tekniske løsninger og systemarkitektur bør være offentlig tilgjengelige med tilstrekkelig detaljeringsgrad. Selv om det i enkelte tilfeller kan være nødvendig å begrense innsyn i tekniske detaljer av hensyn til sikkerhet og personvern, må enhver slik begrensning bygge på en konkret risikovurdering. Eventuelt hemmelighold bør være snevert og ta hensyn til spesifikke innsynsbehov, som for eksempel oppklaring av svindelsaker.»

Transparens er et grunnleggende prinsipp for digital ID-forvaltning.[168] Åpenhet bidrar til at brukere, tilsynsmyndigheter, og andre interessenter kan forstå hvordan systemet faktisk fungerer, både rettslig og teknisk. Vi gir først en kort oversikt over hvordan manglende åpenhet om ulike sider av ID-forvaltning påvirker flere av problemene påpekt i denne rapporten. Deretter konsentrerer vi oss om åpenhet rundt tekniske aspekter av eIDer, samt et eventuelt behov for begrenset hemmelighold.

Manglende åpenhet påvirker flere aktører i ID-forvaltningen, og transparens er avgjørende både for helhetlig styring og for å ivareta brukernes rettigheter. Sluttbrukere kan ha behov for opplysninger om egne disposisjoner (punkt 5.4.1 ovenfor) foretatt i sammenheng med egen eID. Personer som ikke har tilgang til eID kan møte utfordringer knyttet til kriterier for å kvalifisere for eID, samt manglende begrunnelser om avslag (punkt 5.1.1 ovenfor). For at beslutningstakere og tilsynsorganer skal kunne gjøre jobben sin effektivt, må de ha god innsikt i hvordan systemet fungerer. I dag er dette ofte ikke tilfelle. Brukersteder kan ha behov for opplysninger, inkludert sikkerhetsrelevante aspekter, for å vurdere hvilke kompenserende tiltak de bør gjennomføre. Og tilsynsmyndigheter behøver tilgang til informasjon for å vurdere hvilke tiltak de bør pålegge.

Ett av problemene er at det er svært krevende å forstå på et tilstrekkelig detaljert nivå hvordan den digitale identitetsforvaltningen faktisk fungerer. Det finnes ingen samlet og oppdatert beskrivelse av hvordan den norske digitale ID forvaltningen faktisk er bygd opp –teknisk, organisatorisk og rettslig. For eksempel er det ikke tydelig forklart hvilke aktører som godtar innlogging med ulike eID-er.[169] Dermed er viktige deler av systemets arkitektur utilgjengelig.

Mangel på åpenhet om tekniske løsninger i eID-systemer har flere negative konsekvenser. Det er anerkjent at åpenhet bedrer den tekniske kvaliteten på sikkerhetssystemer.[170] Det finnes flere eldre studier av norske eID-systemer som har funnet tekniske feil i løsningene[171] (vi kjenner ikke til at disse feilene har blitt utnyttet til svindel; vi kjenner ikke til noen som har lett etter feil i nyere tid). Manglende transparens kan bidra til sårbarhet. For eksempel er brukerdialogene ofte uforutsigbare, og det finnes ingen mulighet for å vite om meldingen brukeren ser avviker fra det som bør kunne forventes.

Dessuten vil manglende kunnskap om de tekniske løsningene by på utfordringer for brukeren når det oppstår en uenighet om ansvar. Punkt 5.2.2 viser at sikkerheten i eID-systemer ikke er spesielt høy, men en eID-tilbyder vil kunne hevde at "eID-systemet vårt er på høyeste sikkerhetsnivå" og "forfatterne av Punkt 5.2.2 kjenner ikke til alle våre sikkerhetsmekanismer". Uten åpenhet er det vanskelig å konkret imøtegå påstander om effektive hemmelige

[168] OECD Recommendation of the Council on the Governance of Digital Identity av 08/06/2023 (vår utheving): «3.Facilitate inclusive and collaborative stakeholder engagement throughout the design, development, and implementation of digital identity systems, to promote *transparency*, accountability, and alignment with user needs and expectations».
[169] Et slikt register vil også få betydning for implementering av eIDAS 2.0, se epicenter1.
[170] https://www.schneier.com/crypto-gram/archives/2002/0515.html#1
[171] Yngve Espelid, Lars-Helge Netland, André N. Klingsheim, Kjell Jørgen Hole: Robbing Banks with Their Own Software-an Exploit Against Norwegian Online Banks. SEC 2008: 63-77; Kristian Gjøsteen: Weaknesses in BankID, a PKI-Substitute Deployed by Norwegian Banks. EuroPKI 2008: 196-206.

sikkerhetsmekanismer. Manglende åpenhet om tekniske løsninger gjør det også vanskeligere for svindelofre å finne ut av og forstå hvordan de har blitt svindlet, jf. blant annet HR-2020-2021-A der logger ble feiltolket i lavere rettsinstanser. Se nærmere ovenfor i punkt 5.3.5 om konsekvensene for rettssikkerheten og dermed mulighetene for gjenoppretting og reparasjon når det gjelder tilgang til bevis.

Selv om det i enkelte tilfeller kan være nødvendig å begrense innsyn i tekniske detaljer av hensyn til sikkerhet, må enhver slik begrensning bygge på en konkret risikovurdering. Eventuelt hemmelighold bør være snevert og ta hensyn til spesifikke innsynsbehov, som for eksempel oppklaring av svindelsaker.

Det finnes sikkerhetsmekanismer som mister noe av effekten, eller endog all effekten, om de blir offentlig kjent. Et eksempel er overvåkningssystemer som leter etter mistenkelig oppførsel. Dersom man kjenner overvåkningssystemet i detalj kan man ofte tilpasse svindelen slik at den ikke oppdages, for eksempel ved å dele opp transaksjoner for å komme under beløpsgrenser eller øke tidsrommet mellom to transaksjoner. Men dette gjelder bare noen få sikkerhetsmekanismer.

Det er dermed ikke fornuftig med full åpenhet om alle de tekniske delene av systemet, men de bitene som må holdes hemmelig bør heller ikke nødvendigvis godtas som argumenter i en rettstvist der den andre parten ikke har ressurser til å ettergå påstandene.

Brukere må dessuten ha tilgang til informasjon som setter dem i stand til å utøve informerte valg og utøve forbrukermakt, eksempelvis ved å velge tilbydere som behandler svindelsaker bedre eller har mer brukervennlige løsninger. Bankenes håndtering av svindel varierer, men det finnes ingen offentlig tilgjengelig statistikk som lar forbrukere sammenligne praksis. I henhold til forskrift om systemer for betalingstjenester § 2(4) rapporteres slike tall til Finanstilsynet, men de offentliggjøres ikke. I Storbritannia publiseres tilsvarende tall og viser store forskjeller mellom banker. Mangelen på transparens i Norge gjør at forbrukere ikke vet hvilken bank som beskytter dem best, og hvordan de blir behandlet ved tap. Synspunktene er nærmere utdypet i ID-juristens sluttrapport, punkt 4.4.4.

Manglende tilgang til upubliserte avgjørelser i forliksråd og tingretter, svekker også muligheten til å ettergå rettspraksis i detalj og finne relevante beslutningsmønstre. Dette har også vist seg å være viktig for rettssikkerhet i domstolene.

Tiltak:

87. Finanstilsynet bør offentliggjøre detaljert statistikk for svindelhåndtering, inkludert hvordan det svindelforebyggende arbeidet virker, hvor mange svindler som gjennomføres og hvem som tar tapet i svindlene
88. Myndighetene bør pålegge eID-leverandørene å være transparente om den tekniske funksjonaliteten til eID-ene, herunder arkitektur og tekniske detaljer. Det kan gis snevre unntak for detaljer om sikkerhetsmekanismer som slutter å fungere hvis angriperne kjenner disse detaljene.

5.6. Ansvar: tilsyn, kontroll og sanksjoner

I dette punktet beskrives utfordringer knyttet til styringsprinsipp nummer 6:

«Det må finnes en tydelig ansvarsfordeling mellom ulike aktører og tilsynsmyndigheter, og det må sikres at relevante aktører, herunder eID-leverandører, offentlige instanser og private

brukersteder overholder regelverket. Regler og rettigheter har liten verdi dersom de ikke håndheves effektivt. Tilsynsmyndigheter må ha tilstrekkelige ressurser og myndighet til å gjennomføre revisjoner, pålegge sanksjoner og sørge for etterlevelse av krav til likebehandling, sikkerhet og personvern.»

Effektive regler og rettigheter for digital identitet forutsetter at det finnes tydelige ansvarsforhold, robuste tilsynsordninger og reelle sanksjonsmuligheter. Dersom håndhevelsen av regelverket er mangelfull, svekkes både sikkerheten, brukernes rettigheter og tilliten til systemet. Dagens tilsyns- og kontrollregime for eID-løsninger i Norge preges imidlertid av uklare ansvarsforhold, manglende koordinering mellom tilsynsmyndigheter, svak oppfølging av kritiske inkluderings- og sikkerhetsutfordringer og lite effektive sanksjoner.

Flere offentlige aktører har et tilsynsansvar for ulike aspekter av digital identitet:

- **Nasjonal kommunikasjonsmyndighet (Nkom)** har ansvar for tilsyn med eID-løsninger og tillitstjenester.
- **Datatilsynet** fører tilsyn med behandling av personopplysninger knyttet til eID og vurderer ivaretakelse av personvernhensyn.
- **Finanstilsynet** har ansvar for sikkerheten ved bruk av eID i finanssektoren.
- **Forbrukertilsynet** overvåker forbrukernes rettigheter ved bruk av eID, inkludert beskyttelse mot svindel og misbruk.
- **Uu-tilsynet**, underlagt Digitaliseringsdirektoratet, fører tilsyn med reglene om universell utforming.
- **Diskrimineringsnemnda** behandler saker om diskriminering, inkludert tilfeller der manglende tilgang til eID fører til forskjellsbehandling.

Til tross for at flere myndigheter har ansvar på ulike områder, er det flere svakheter hvordan systemet for tilsyn og kontroll fungerer. Vi har allerede vært inne på noen av disse svakhetene. For eksempel kan ulik tilgang til sanksjoner hos forskjellige tilsynsmyndigheter gi uheldige insentivstrukturer. Der Diskrimineringsnemnda ikke har tilgang til noen økonomiske sanksjoner for brudd på diskrimineringsregelverket, kan Finanstilsynet ilegge store bøter for brudd på hvitvaskingsregelverket. Det er grunn til å tro at dette gir finansinstitusjonene insentiver til å overoppfylle hvitvaskingsregelverket på bekostning av forbud mot diskriminering, jf. ovenfor i punkt 5.1.1. I punkt 5.3.5 har vi beskrevet hvordan Datatilsynet sin tolkning av personvernregelverket utgjør et hinder for tilgang til bevis for ofre for identitetsmisbruk. I punkt 5.3.2 har vi vist til fravær av tilsyn knyttet til overholdelse av finansavtalelovens regler om finansinstitusjoners klagebehandling.

Verken Finanstilsynet eller Forbrukertilsynet har etter det SODI-prosjektet kjenner til gjennomført tilsyn når det kommer til bankenes vilkårlige praksiser med nektelse og inndragning av BankID. Flere saker har imidlertid blitt behandlet av Diskrimineringsnemnda og Finansklagenemnda. Et grunnleggende problem når det gjelder Diskrimineringsnemnda sin praksis er feiltolkning av relevante EØS-rettslige regler og fravær av drøftelser opp mot relevante menneskerettigheter.[172] I enkelte tilfeller har imidlertid nemnda kommet til at nektelse av

[172] Marte Eidsand Kjørven og Tone Linn Wærstad, Digitalt utenforskap og diskriminering – I hvilken grad gir diskrimineringsregelverket og håndhevingen av dette et effektivt vern mot forskjellsbehandling på grunn

BankID innebærer et brudd på diskrimineringsforbudet. Også Finansklagenemnda har i noen tilfeller konkludert med brudd på kontraheringsplikten ved utstedelse av BankID. Et alvorlig problem er at disse avgjørelsene tilsynelatende ikke har avstedkommet endringer i bankenes utstedelsespraksis. Det kan i den forbindelse vises til det som er beskrevet ovenfor i punkt 5.1.1 om blant annet praksis knyttet til nektelse av BankID for personer med d-nummer eller utenlandsk pass som ikke er maskinlesbart.

Som beskrevet ovenfor under punkt 5.2.2, ble BankID og Buypass i 2022 notifisert til EU-kommisjonen for godkjennelse på sikkerhetsnivå "høyt" under eIDAS-forordningen. I denne prosessen ble det gjennomført en fagfellevurdering som påpekte flere alvorlige sikkerhetshull. Arbeidsgruppen uttrykte også bekymring over kvaliteten på internkontroller og effektiviteten av tilsynsregimet:

> "The number of critical concerns raised during the peer review process, … , inevitably raises concerns on the accuracy of the internal audits and the effectiveness of supervisory regime. Because of this, the peer reviewers would like to recommend Norway to conduct a review of the audit requirements and the criteria to be applied in the audit and the mechanisms for supervision."

Poenget synes å være at BankID og Buypass har vært *selvdeklarert* på sikkerhetsnivå "høy" i en årrekke, uten at de forhold som er avdekket av arbeidsgruppen i fagfellevurderingen er fanget opp av verken Nkom som tilsynsmyndighet eller av markedsaktørene selv i sine internkontroller.

SODI-prosjektet har heller ikke kjennskap til at myndighetene har stilt krav om utbedring av sikkerhetshull i forbindelse med offentlige anskaffelser av eID-tjenester. Offentlige digitale tjenester krever bruk av eID, men brukerne har ingen valgfrihet – de må inngå avtale med de aktørene som finnes, selv om dette innebærer risiko knyttet til de påpekte sikkerhetsmanglene.

Tiltak:

89. Etter selvdeklarasjonsforskriften § 10 annet ledd, kan NKOM pålegge tilbyder av eID-løsning å gjennomføre revisjon for å dokumentere oppfyllelse av kravene til nivå høyt. Denne muligheten til å kreve revisjon bør benyttes i større grad enn i dag for å sikre at kravene faktisk blir, og holdes, oppfylt.
90. Finanstilsynet og/eller Forbrukertilsynet gjennomfører tilsyn med bankenes praksiser knyttet til nektelse og inndragning av BankID.
91. Det gjennomføres en utredning av totaliteten i tilsyns- og sanksjonssystemet med en vurdering og avklaring av ulike tilsynsmyndigheters rolle og ansvar.

5.7. Innovasjon: interoperabilitet, valgfrihet og konkurranse

I dette punktet drøftes utfordringer knyttet til styringsprinsipp nummer 7:

«Digitale identitetsløsninger og tilhørende infrastruktur må være fleksible og legge til rette for teknologisk utvikling og innovasjon. Det bør arbeides for at ingen aktører får en monopollignende posisjon. eID-løsninger bør være interoperable og bygge på alminnelig anerkjente og tilgjengelige standarder, slik at brukerne kan velge mellom ulike løsninger uten å

---

av digitalt utenforskap som skyldes manglende tilgang til eID?, (under publisering, tilgjengelig som pre publication draft) https://www.jus.uio.no/ifp/forskning/prosjekter/sodi/publikasjoner/vitenskapelige-publikasjoner/digitalt-utenforskap-og-diskrimineringsnemndas-praksis-etter-fagfelle-endelig---v110.12.24.pdf

miste tilgang til viktige tjenester. Offentlige og private aktører bør samarbeide for å utvikle nye, sikre og brukervennlige identitetsløsninger.»

Det er tre privateide eID-løsninger på øverste sikkerhetsnivå som er tilgjengelig i Norge er BankID, Buypass og Commfides. Den offentlige eID'en MinID er tilgjengelig på nivå betydelig. Av ca. 300 millioner innlogginger til offentlige digitale tjenester i 2021, ble BankID benyttet i 93,44 % av innloggingene mens MinID stod for 5,5 % av innloggingene. Buypass stod for 1,02 % av innloggingene, mens Commfides ble benyttet i 0.01 % av tilfellene.[173] BankID er også eneste løsning for å logge inn på nettbanker og lignende tjenester. Buypass og Commfides benyttes på sin side i flere bransjeløsninger som ikke inngår i tallene til ID-porten, men utbredelsen er likevel mindre enn for BankID.

Siden nesten alle trenger tilgang til banktjenester, vil nesten alle ha BankID. Det er dermed få umiddelbare og allmenne insentiver til å anskaffe seg andre eID-er. Når én markedsaktør har en så dominerende posisjon, hemmer det konkurranse. I områdegjennomgangen pekes det på at «BankIDs dominerende markedsposisjon [utgjør] en prisrisiko for det offentlige».

Manglende konkurranse kan også hemme innovasjon. Også i Sverige har finansnæringens eID-løsning (som også heter BankID) en dominerende posisjon. Likevel har særlig Freja eID lykkes med å etablere seg, blant annet ved å konkurrere på å tilby mer tilgjengelige løsninger. Deres eID-løsning inkluderer blant annet en funksjon med «delt kontroll» for personer som trenger hjelp og støtte i bruken av digitale tjenester.[174] Utvikling av denne funksjonen ble delvis finansiert av midler utdelt av Post- och telestyrelsen (tilsvarende Nkom i Norge) som del av en innovasjonskonkurranse der det ble tildelt midler til utvikling av mer inkluderende teknologi.[175] Når konkurransen i markedet er svak krever det at myndighetene arbeider aktivt for å få frem sikre og inkluderende løsninger.

En mulighet for å bedre konkurransen er å stimulere bruken av en felles "mellommann" mellom eID-leverandøren og brukerstedene, slik at brukerstedene slipper å forholde seg til mange eID-leverandører. Det finnes flere private autentiseringsportaler i det norske markedet. En annen mulighet er å åpne ID-porten for alle eID-leverandører som tilfredsstiller kravene til ett av de to sikkerhetsnivåene som ID-porten tilbyr. Det er ikke opplagt hvordan dette kan la seg gjøre, men det bør utredes om ID-porten kan åpne for tilknytning for alle eID-leverandører som tilfredsstiller en felles kravspesifikasjon og et sett med standard forretningsvilkår (altså at alle som er kvalifisert får tilgang på like vilkår).

Særlig i forbindelse med innføring av eIDAS 2.0, bør det tas grep som kan legge til rette for bedre konkurranse i markedet i fremtiden. Offentlige myndigheter bør tilby en digital grunninfrastruktur, som private aktører kan bygge på med like vilkår.

Tiltak:

92. Det bør settes av midler til å gjennomføre en innovasjonskonkurranse for inkluderende eID-løsninger.
93. Det bør utredes om ID-porten kan legge til rette for at alle eID-er som oppfyller en felles kravspesifikasjon og forretningsmessige standardvilkår kan knyttes til ID-porten uten å måtte gå veien om nye offentlige anskaffelser.

[173] eID-strategien s. 9.
[174] Delad Kontroll - Freja
[175] PTS beviljar innovationsbidrag till Verisec och Freja eID - Freja

94. Det må bli en rettslig plikt til at banker og andre finansvirksomheter må godta eID-løsninger på tilstrekkelig sikkerhetsnivå, eventuelt basert på felles godkjenning i finanssektoren.
95. Tydeligere reguleringer av dominerende markedsaktører når det gjelder sikkerhet og tilgjengelighet for alle grupper.

5.8. Samfunnssikkerhet og beredskap

I dette punktet drøftes utfordringer knyttet til styringsprinsipp nummer 8:

«Identitetsforvaltningen må være forberedt på cyberangrep, teknisk svikt og andre krisesituasjoner. eID-systemer og tilhørende infrastruktur må være robuste og sikre kontinuerlig tilgang til kritiske tjenester, selv i ekstraordinære situasjoner. Det må etableres beredskapsplaner som sikrer redundans og alternative løsninger dersom én identitetsleverandør skulle falle ut. Samtidig må tilliten til eID-systemene opprettholdes gjennom åpenhet, kontrollmekanismer og tydelig regulering.»

Systemer for eID utgjør en del av samfunnets kritiske infrastruktur og må vurderes i et bredere perspektiv som omfatter beredskap, samfunnssikkerhet og tillit. Risikoen for alvorlige konsekvenser øker i takt med eID-systemenes utbredelse og bruksområder. Når én digital identitet gir tilgang til både offentlige og private tjenester, skaper dette både effektivitet og risiko. En mer omfattende bruk av eID gjør systemene til attraktive mål for svindel, cyberangrep og driftsforstyrrelser.

Den norske digitale identitetsforvaltningen er i stor grad avhengig av få leverandører, hvor særlig BankID har en dominerende posisjon. Områdegjennomgangen av identitetsforvaltningen peker på at avhengigheten av BankID utgjør en digital sårbarhet for både finansnæringen og offentlig sektor og at systemet medfører at offentlige myndigheter har «manglende strategisk kontroll over infrastrukturen».[176] Ved større tekniske feil eller cyberangrep kan hele systemet for digital autentisering settes ut av spill, med alvorlige konsekvenser for enkeltindivider, virksomheter og offentlige myndigheter.

Nedetid på eID-systemer kan lamme viktige samfunnsfunksjoner som tilgang til helsejournaler, utbetaling av offentlige ytelser eller gjennomføring av økonomiske transaksjoner. Et eksempel på dette var driftsbruddene hos BankID vinteren 2021, hvor brukere i perioder mistet tilgang til sine digitale tjenester. Finanstilsynet påpekte i etterkant at driftsavbruddene var alvorlige og kunne ha fått større konsekvenser for samfunnssikkerheten.[177]

I Sverige ble deres versjon av Bankid utsatt for et overbelastningsangrep i april 2025 som førte til at tjenesten var nede i ca. tre timer.[178] I etterkant av hendelsen uttalte Civilminister Erik Slottner at den viser et behov for at staten tar et større ansvar for borgernes digitale identitet, og at det må finnes flere alternative eID- og signeringsløsninger.[179]

For en enkeltperson kan manglende tilgang til eID på et kritisk tidspunkt bety at vedkommende mister en søknadsfrist, ikke får hentet ut nødvendige medisiner eller ikke får tilgang til midler for

[176] Områdegjennomgang ID-forvaltningen – tilleggsrapport, s. 74.
[177] Finanstilsynet ser alvorlig på BankID-trøbbel – E24
[178] Driftsinformation
[179] Attacken mot Bank-id: "Kommer hända igen" - Dagens PS

å betale regninger. For myndighetene kan det bety at offentlige tjenester ikke fungerer som de skal, og at viktige samfunnsfunksjoner stopper opp.

Avhengigheten av få aktører innebærer også en systemisk risiko ved at en feil, en svindelbølge eller en sikkerhetsbrist kan få konsekvenser på tvers av sektorer. Dersom en svindler får tilgang til en persons eID, kan den samme eID-en brukes til en rekke ulike formål, fra økonomiske bedragerier til opprettelse av falske selskaper.

Når én eID fungerer som en universalnøkkel for både banktjenester, offentlige tjenester, eiendomstransaksjoner og bedriftsregistrering, øker den potensielle gevinsten ved misbruk. Funksjonaliteten som gjør eID nyttig og fleksibel, kan dermed også gjøre systemet mer sårbart for organiserte kriminelle miljøer, se nærmere om systemmisbruk og registermanipulasjon i punkt 5.2.5. Denne utviklingen av profesjonelle svindeloperasjoner innebærer en økende samfunnsrisiko.[180]

En alvorlig konsekvens av økt eID-misbruk er at befolkningens tillit til digitale tjenester og offentlig kommunikasjon kan svekkes. Økokrim har pekt på at omfanget av bedragerier er så stort at det utgjør et samfunnsproblem som «utfordrer tilliten til teknologiske løsninger, i mellommenneskelige relasjoner, til myndighetene og til viktige samfunnsinstitusjoner».[181] Dette kan igjen føre til at viktig informasjon fra det offentlige ikke blir lest eller tatt på alvor, noe som svekker effektiviteten i myndighetenes kommunikasjon med befolkningen.

Det finnes ikke ett eller noen få tiltak som løser utfordringene knyttet til samfunnssikkerhet og beredskap. En helhetlig identitetsforvaltning med gjennomføring av tiltak knyttet til alle utfordringene som er beskrevet i denne rapporten, er nødvendig for å opprettholde tillit og dermed også samfunnssikkerheten på lengre sikt. Vi vil likevel særskilt fremheve betydningen av å gjøre seg mindre avhengig av én eID (BankID) som et svært viktig tiltak knyttet til beredskap.

Mange av tiltakene som allerede er foreslått tidligere i rapporten vil også kunne bidra til å bedre samfunnssikkerheten. Dette gjelder for eksempel utvikling av en offentlig kontrollert eID og tiltak som skal sikre at det finnes alternative måter å få tilgang til grunnleggende tjenester. Tiltak for å tette sikkerhetshull og forhindre svindel og ID-misbruk er viktig for den generelle tilliten og dermed også for samfunnssikkerheten. Tiltak for helhetlig styring, jf. punkt 5.10 nedenfor, er også svært viktig for samfunnssikkerheten.

Tiltak:

96. Det må etableres beredskapsplaner som sikrer redundans og alternative løsninger dersom én identitetsleverandør skulle falle ut.

5.9. Demokratisk forankring

I dette punktet drøftes utfordringer knyttet til styringsprinsipp nummer 9:

«Identitetsforvaltningen er en samfunnskritisk funksjon som må ha demokratisk forankring. Myndighetene må ha en tydelig rolle i styringen av digital identitet, og det må sikres at private aktører ikke får uforholdsmessig stor makt over hvem som får tilgang til samfunnet. Systemet

[180] Beredskapsrisikoen i en svensk kontekst er nærmere beskrevet i SOU 2023:61, s. 96 flg. Tilsvarende betraktninger gjør seg gjeldende også i Norge.
[181] Økokrim, Årsrapport 2023, Økokrim - Årsrapport 2023, s. 18.

må utformes slik at det sikrer reell deltakelse fra berørte interessenter, særlig sårbare og risikoutsatte personer, slik at deres behov ivaretas.»

Digital identitetsforvaltning er ikke bare et teknisk eller administrativt spørsmål – det er et grunnleggende demokratisk anliggende. Retten til å kunne bevise hvem man er, og å få tilgang til samfunnets tjenester på like vilkår, utgjør en forutsetning for reell deltakelse i samfunnet. Når den digitale identitetsforvaltningen svikter, påvirker det den generelle samfunnssikkerheten og tilliten i samfunnet, jf. ovenfor om dette.

Den digitale identitetsforvaltningen med tilhørende beslutninger er imidlertid preget av interne prosesser i offentlig forvaltning, som er lite gjennomsiktige og har svak demokratisk forankring. Et svært viktig spørsmål i denne sammenhengen er hvilken rolle staten og andre interessenter skal ha når det gjelder eID. I en norsk kontekst har dette særlig blitt diskutert i relasjon til de nasjonale ID-kortene, og om disse skulle inkludere en statlig eID.

Den første strategien for eID i offentlig sektor er angivelig fra 2008. I forordet til den nye eID-strategien fra 2023 står det at «mye fungerer godt med dagens markedsbaserte strategi for eID fra 2008». Noen strategi fra 2008 finnes imidlertid ikke offentlig tilgjengelig på nett. SODI-prosjektet har bedt om innsyn i strategien fra 2008, men ingen aktører som er forespurt har klart å oppdrive den. Isteden er det vist til et dokument fra 2007 som har tittelen «Høringsversjon Strategi for eID og e-signatur i offentlig sektor».[182] Dette dokumentet bygger imidlertid *ikke* på en «markedsbasert strategi». Tvert imot er den primære anbefalingen i dette dokumentet at det etableres og distribueres en offentlig eID på øverste sikkerhetsnivå tilknyttet nasjonale ID-kort. Denne løsningen, der offentlige myndigheter tar ansvar for å tilby eID til borgerne ble vurdert som den beste, «særlig sett fra et samfunnsøkonomisk perspektiv».[183] Den samme anbefalingen er gitt i en rapport fra daværende Justis- og politidepartementet om Nasjonalt ID-kort, også fra 2007.[184]

Spørsmålet om eID på de nasjonale ID-kortene er videre behandlet i forbindelse med lovforberedelsen til ID-kortloven. I proposisjonen fra 2015 uttales det blant annet at

> Det er lang tradisjon i Norge for at det offentlige har tatt ansvar for borgernes fysiske legitimasjon gjennom utstedelse av pass og førerkort. Lovforslaget legger til rette for at alle som fyller vilkårene for å få et nasjonalt ID-kort også skal kunne få et offentlig utstedt elektronisk identitetsbevis (eID).[185]

Det tas likevel forbehold om at det «gjenstår noe utredning for å sikre at planlagt løsning blir brukervennlig og kostnadseffektiv før det tas endelig beslutning om å realisere eID». Beslutningen ble tilsynelatende tatt året etter, da Regjeringen i pressemelding fra 2016, med tittel «Elektronisk ID på nasjonalt ID-kort» uttalte at «Regjeringen har besluttet at politiet skal utstede elektronisk ID (eID) når det nasjonale ID-kortet kommer i 2017.»[186] eID på nasjonalt ID-

---

[182] Arbeidsgruppe nedsatt av Fornyings- og administrasjonsdepartementet, Høringsversjon Strategi for eID og e-signatur i offentlig sektor Versjon 1.0, Microsoft Word - Strategi for eID i offentlig sektor v1-1_13.03.07.doc. SODI-prosjektet har etterspurt den endelige versjonen av strategien, blant annet ved en innsynsbegjæring. Vi har da kun blitt henvist til dette dokumentet som altså har tittel «Høringsversjon». Det er uklart for oss om det finnes andre versjoner.
[183] Ibid. s. 16.
[184] Justis- og politidepartementet, Sluttrapport februar 2007 Nasjonalt ID-kort.
[185] Prop 66 L (2014-15) Lov om nasjonalt identitetskort.
[186] Pressemelding nr. 48-2016, 3. mai 2016. Pressemeldingen er ikke lenger offentlig tilgjengelig på Regjeringen.no.

kort ble også forutsatt så sent som i 2019, i tiltaksoversikten til nasjonal strategi for digital sikkerhet.[187]

Noen år senere ble det imidlertid besluttet å skrinlegge prosjektet med nasjonal eID på ID-kortene. Det har ikke lykkes SODI-prosjektet å finne ut konkret hvordan denne beslutningen ble truffet og hvem som ble involvert, men det er sannsynlig at den ble fattet på bakgrunn av Områdegjennomgangen av identitetsforvaltningen som ble gjennomført i 2018-2019, og som er nevnt flere ganger tidligere i rapporten. Områdegjennomganger er et instrument som brukes som en del av «regjeringens budsjettprosess for å utrede og foreslå endringer som kan gi bedre måloppnåelse og økt handlingsrom i budsjettene».[188] Den aktuelle områdegjennomgangen av identitetsforvaltningen består av en hovedrapport og en tilleggsrapport, hvorav sistnevnte særskilt behandlet spørsmål om eID. Dokumentene er utarbeidet av konsulentselskapet Capgemini på oppdrag fra Finansdepartementet (FIN), Justis- og beredskapsdepartementet (JD), Samferdselsdepartementet (SD) og Kommunal- og moderniseringsdepartementet (KMD). Områdegjennomgangen konkluderte med at «samlet nytte av nasjonal eID [er] begrenset» og anbefalte at prosjektet med utvikling av slik statlig eID ble avviklet. Dette til tross for at områdegjennomgangen for øvrig hadde påvist en rekke utfordringer med dagens modell. Områdegjennomgangen var ikke gjenstand for offentlig høring, og den ble heller ikke publisert på nett før flere år senere.

Et betimelig spørsmål er om vurderingen mht. nytteverdien av en nasjonal eID ville sett annerledes ut dersom spørsmålet hadde blitt behandlet gjennom en åpen og demokratisk prosess med offentlig høring, fremfor som et internt og lukket budsjettspørsmål. Da utkast til ny strategi for eID i offentlig forvaltning ble sendt på offentlig høring i 2022,[189] var det tydelig at svært mange høringsinstanser var uenig i konsulentselskapets og Regjeringens vurdering av nytteverdien av en nasjonal eID i offentlig regi. I utkastet som ble sendt på høring var et av tiltakene som ble foreslått «Realisering av en offentlig utstedt eID på sikkerhetsnivå høyt skal vurderes».[190] Forslaget ble begrunnet med utfordringer knyttet til inkludering, sårbarhet/beredskap og konkurranse.

Høringsinstanser som uttalte seg *negativt* til dette forslaget var: DNB, Bankenes ID-tjeneste, BankID, Abelia (NHOs landsforening for kunnskaps- og teknologibedrifter), Buypass, Commfides, Eika gruppen (lokalbanker), Finans Norge, IKT Norge og Posten Norge.[191]

Høringsinstanser som var *positive* til forslaget var: Forbrukerrådet, Hovedorganisasjonen Virke, Aera Payment & Identification AS, Eldreombudet, Datatilsynet, Apotekforeningen, Barne-, ungdoms- og familiedirektoratet (Bufdir), Bergen kommune, Direktoratet for e-helse, Skate, Helse Nord, KS, Kommunesektorens organisasjon, Likestillings- og diskrimineringsombudet, Nasjonalforeningen for folkehelsen, Norsk forbund for utviklingshemmede, NOAS, Norsk organisasjon for asylsøkere, Oslo kommune, Politidirektoratet, Signicat, UngMeistring, Forskningssenter for digitale psykiske helsetjenester, Haukeland Universitetssykehus og Utlendingsdirektoratet. Skillelinjene er tydelige mellom aktører som har økonomiske interesser i

[187] Tiltaksoversikt til nasjonal strategi for digital sikkerhet, se tiltak nr. 49 på s. 30.
[188] Områdegjennomganger - regjeringen.no.
[189] Høring - utkast til ny strategi for eID i offentlig sektor - regjeringen.no.
[190] Se utkast til strategi, tiltak nr. 2 under overskriften «Ambisjon og tiltak» (dokumentet mangler sidetall), utkast-til-ny-strategi-for-eid-i-offentlig-sektor-hor-l84994.pdf.
[191] Alle høringssvarene er tilgjengelig her: Høring - utkast til ny strategi for eID i offentlig sektor - regjeringen.no.

at dagens modell med kun markedsbaserte løsninger er tilgjengelige og på den andre siden de fleste andre aktører.

Selve den demokratiske forankringen av den digitale identitetsforvaltningen bemerkes også særskilt av flere høringsinstanser. Hovedorganisasjonen Virke skriver i sitt høringssvar at eID-strategien «er for lite ambisiøs, har et for snevert nedslagsfelt og mangler politisk forankring» og peker på at uten en slik politisk forankring «bidrar eID-strategien … til at Norge blir enda mer avhengig av monopolistiske, private identitetsløsninger» og at dette er «i strid med borgernes rettigheter».[192] Signicat mener en «bør være forbi vurderingsstadiet når det gjelder offentlig eID på nivå høyt» og viser til at der «andre land tar steg for å opprette en nasjonal, digital identitet, står Norge fast ved gamle løsninger».[193]

Forbrukerrådet peker på at det bør «utvikles en eID-løsning med høyeste sikkerhetsnivå og under demokratisk kontroll, som sikrer forbrukerne tilgang til offentlige tjenester».[194] Samtidig pekes det på at siden dette vil «utfordre BankIDs enerådende stilling i markedet», må det forventes «at regjeringens foreslåtte strategi vil utløse ulike former for motstand fra næringslivsaktører». En slik motstand er da også tydelig fra de aktuelle aktørenes høringssvar. DNB skriver eksempelvis at gevinstene ved den markedsbaserte modellen «er betydelige» og at de vil «advare mot å bruke offentlige penger som kunne gitt velferd for innbyggerne, på å utvikle egne alternative løsninger».[195]

Den endelig vedtatte strategien er tilnærmet identisk med utkastet som ble sendt på høring. Ingen av høringsinstansenes synspunkter er gjengitt eller kommentert. De svært få endringene som er gjort, viser imidlertid hvilke instanser som i en viss utstrekning er hørt. Det ovenfor nevnte foreslåtte tiltaket «Realisering av en offentlig utstedt eID på sikkerhetsnivå høyt skal vurderes» og den tilhørende setningen om det «videre arbeidet med en offentlig eID på sikkerhetsnivå høyt som er omtalt under mål 1» er fjernet i den endelige versjonen av strategien. Dette er isteden erstattet med følgende i den tilhørende handlingsplanen: «Regjeringen vil vurdere utbredelse av en offentlig utstedt eID på sikkerhetsnivå høyt blant brukergruppene som ikke har en eID på sikkerhetsnivå høyt i dag.» Det skal altså tilsynelatende ikke lenger vurderes en offentlig eID som er tilgjengelig for *alle*. I tillegg har den endelig vedtatte strategien fått én ny setning som ikke var der i utkastet: «Flere av tiltakene vil også kunne ha virkning for privat sektor, og departementet vil derfor inkludere markedsaktørene i arbeidet med en handlingsplan.» Øvrige aktører og høringsinstanser får derimot ingen lovnader om deltakelse og innvirkning i videre beslutningsprosesser.

Tre prioriterte tiltak i eID-strategien er fulgt opp ved at Digitaliserings- og forvaltningsdepartementet har gitt et felles oppdrag til Digitaliseringsdirektoratet, Politidirektoratet, Skattedirektoratet og Utlendingsdirektoratet om gjennomføring av en såkalt konseptvalgutredning (KVU).[196] De tre aktuelle tiltakene som skal utredes i KVU'en er 1) «grunnlaget for et markedsbasert samarbeid om kjerneinfrastruktur for utstedelse av eID til brukere … og økosystem for den digitale lommeboken» som kommer med eIDAS 2.0, 2) «hvordan eID på høyt sikkerhetsnivå kan gjøres tilgjengelig for flere», og 3) hvordan offentlig sektor kan legge til rette for å «gjennomføre ID-kontroll digitalt og gjennom personlig oppmøte

[192] Høring - utkast til ny strategi for eID i offentlig sektor - regjeringen.no
[193] Høring - utkast til ny strategi for eID i offentlig sektor - regjeringen.no
[194] Høring - utkast til ny strategi for eID i offentlig sektor - regjeringen.no
[195] Høring - utkast til ny strategi for eID i offentlig sektor - regjeringen.no
[196] Brev fra Digitaliserings- og forvaltningsdepartementet 20. januar 2025, ref. 24/204-27.

som oppfyller kravene til sikkerhetsnivå høyt for eID». eIDAS 2.0 krever at «alle» skal ha tilgang til en digital lommebok med eID. Det følger av oppdragsbrevet at «hvem «alle» er vil skje som en del av utredningsarbeidets første steg». Videre fremgår det at «Skatteetaten, Politidirektoratet, utlendingsdirektoratet, eID-utstedere og andre markedsaktører er blitt utpekt som relevante samarbeidspartnere for Digitaliseringsdirektoratet i utredningsarbeidet». Mens markedsaktørene ifølge oppdragsbrevet «**skal** involveres i gjennomføringen av KVU'en», er «andre offentlige, private og ideelle virksomheter» henvist til at de «**kan** involveres etter behov». Det er altså tilsynelatende primært markedsaktørene for eID som skal være med å bestemme behov, løsninger og ikke minst hvem «alle» egentlig er – herunder om mennesker med psykiske og fysiske funksjonsnedsettelser er inkludert i «alle».

I forlengelsen av dette er det også verdt å nevne at Digdir i begynnelsen av 2025 nedsatte en såkalt «ekspertgruppe for implementering av eIDAS 2.0».[197] Ifølge invitasjonen skal ekspertgruppa «bidra med råd og utveksling av beste praksis for å sikre at krav, standarder og rettsakter for den digitale lommeboka varetar norske interesser».[198] I tillegg til representanter fra offentlige aktører, ble følgende invitert inn for å sikre ivaretakelse av «norske interesser»: BankID, Buypass, Commfides, Bits, Finans Norge og Virke.

Fraværet av åpne og demokratiske utredninger og høringsprosesser preger feltet. Den eneste NOU'en de senere år som berører spørsmål om eID er NOU 2024:21 Trygge og enkle betalinger for alle.[199] Betalingsutvalget legger imidlertid feilaktig til grunn at det eksisterer et arbeid «med å etablere en offentlig eID på sikkerhetsnivå «høyt»» og ber om at «dette arbeidet gis høy prioritet».[200] Dette altså til tross for at det *ikke* pågår et arbeid for å etablere en slik offentlig eID.

At det hersker forvirring mht. hva som egentlig er myndighetenes standpunkt, kan ha sammenheng med at kommunikasjonen rundt dette er sprikende. Illustrerende i så måte er en sak for Diskrimineringsnemnda der Norsk Forbund for Utviklingshemmede (NFU) klaget inn Digitaliserings- og forvaltningsdepartementet (Dfd) for diskriminerende praksiser knyttet til eID.[201] NFU anførte at staten diskriminerer utviklingshemmede når svært mange digitale offentlige tjenester ikke er tilgjengelig for de som ikke får eID på øverste sikkerhetsnivå av de private tilbyderne. For nemnda anførte Dfd at departementet ikke har «myndighet over» hvordan «bankene tolker og praktiserer gjeldende regelverk» om utstedelse av BankID. Samtidig avvises det at en alternativ, offentlig utstedt eID vil løse utfordringene, fordi EØS-retten etter departementets syn oppstiller et forbud mot å utstede eID på øverste sikkerhetsnivå til utviklingshemmede og andre som trenger hjelp til bruken. Samtidig har digitaliseringsministeren uttalt i DN at Regjeringen jobber for «digital inkludering og eID til alle».[202] De to synspunktene som er fremført i hhv. klagesaken for Diskrimineringsnmenda og i DN, lar seg imidlertid ikke forene.

---

[197] eInnsyn - Ekspertgruppe eIDAS 2.0. – 2024/2082 – Norwegian Digitalisation Agency

[198] Digdir, «Invitasjon til ekspertgruppe for implementering av eIDAS 2.0», Ref. 24/2082-1, 10.12.2024.

[199] NOU 2024: 21 - regjeringen.no. Se også SODI-prosjektets høringssvar v/Marte Eidsand Kjørven: Høring - NOU 2024: 21 Trygge og enkle betalinger for alle - regjeringen.no

[200] NOU 2024:21 Trygge og enkle betalinger for alle, punkt 6.4.3.

[201] Diskrimineringsnemnda, sak 2022/818, avgjørelse datert 11. mars 2024, se 22-355-offentlig-versjon-av-uttalelse.pdf

[202] Elektronisk ID skal være en selvfølge | DN, se også det opprinnelige innlegget fra Kjørven, Wærstad og Omland: Digitalisering av offentlige tjenester gir diskriminering | DN og tilsvaret til Tungs svar: Karianne Tung taler med to tunger | DN.

Samlet fremstår prosessene rundt viktige beslutninger i den digitale identitetsforvaltningen som ugjennomsiktige med svært svak demokratisk forankring og involvering av berørte parter. Til sammenlikning er det i Sverige gjennomførte en lang rekke SOU'er på dette feltet de senere år:

- SOU 2017:114 reboot – omstart för den digitala förvaltningen, kapittel 10: Förvaltningsgemensamma digitala funktioner och elektronisk identifiering
- SOU 2019:14 Ett säkert statligt ID-kort – med e-legitimation
- SOU 2021:62 Användning av e-legitimation i tjänsten i den offentliga förvaltningen
- SOU 2023:16: Tillit och integritet på den digitala betalningsmarkaden m.m., se særlig kap. 8
- SOU 2023:61: En säker och tilgänglig statlig e-legitimation
- SOU 2024:45 Kompletterandre bestämmelser til EUs reviderade förordning om elektronisk identifiering.

Det er behov for å gjenreise og styrke det demokratiske grunnlaget for identitetsforvaltningen. Det bør etableres mekanismer for å sikre deltakelse fra sivilsamfunnet, brukerorganisasjoner og særlig berørte grupper i utformingen og evalueringen av systemene. Særlig viktig er det å inkludere stemmer fra grupper som i dag opplever utenforskap og ekskludering. Demokratisk forankring handler ikke bare om representasjon, men også om innsyn, ansvarliggjøring og mulighet for å påvirke – både gjennom politiske prosesser og individuelle rettighetsmekanismer.

Tiltak:

97. Nedsett et offentlig utvalg med mandat å gjennomgå den digitale identitetsforvaltningen
98. Etabler et nasjonalt råd eller forum for digital identitet med bredt sammensatt deltakelse, inkludert sivilsamfunn og sårbare grupper.

5.10. Helhetlig styring: Systemtenkning og samhandling

I dette punktet drøftes utfordringer knyttet til styringsprinsipp nummer 10:

«Identitetsforvaltningen er et komplekst system med mange elementer som er i stadig endring. Styringen må derfor være helhetlig slik at man unngår at tiltak som iverksettes på ett område får utilsiktede konsekvenser på et annet. Systemet omfatter en rekke ulike elementer, både tekniske, organisatoriske og rettslige – både privatrettslige og offentligrettslige. Alle disse elementene påvirker hverandre, og styringen må derfor identifisere hvilke konsekvenser endringer på ett område kan ha for helheten. For å sikre at ulike interessegrupper ivaretas når det gjelder konsekvenser av endringer, bør det legges til rette for gode arenaer for dialog om utfordringer og løsninger, og nye løsninger og tiltak bør testes på en måte som bekrefter at ønskede effekter oppnås. Ansvar og kontrollfunksjoner knyttet til løsninger og aktører i identitetsforvaltningen må være avklart og informasjon om dette må være lett tilgjengelig, bl.a. slik at det er mulig å diskutere om organiseringen er hensiktsmessig og fungerer som den skal.»

ID forvaltningen er preget av manglende helhetlig styring og kontroll. ID-forvaltningen kjennetegnes ved tverrsektorielle problemstillinger i et komplekst adaptivt system, noe som utfordrer sektorprinsippet.[203] Som følge av utfordringene knyttet til de ni foregående styringsprinsippene har systemet utviklet sine egne og ofte utilsiktede og uønskede egenskaper.

[203] Områdegjennomgangen, s. 214

For eksempel fører økonomiske *insentiver* til å kategorisere eID som høy-sikkerhet til sterk ekskludering av mange borgere og innvandrere, og begrenser innsikten i systemet for tilsyn. Det er manglende *feedback*-systemer som varsler myndighetene om cybersikkerhets- og rettssikkerhetsutfordringer, samt *kontroll*mekanismer med sanksjoner som gjør det kostbart å ignorere avgjørelser av andre organer (f.eks. Diskrimineringsnemnda) eller byrder fra sikkerhetssvakheter som faller på brukere og ikke bankene. Dessuten ser det ut som systemet ikke er rigget for *nye utviklinger*, som KI-drevet svindel.

Allerede i områdegjennomgangen av 2019, s. 9 ble ID-forvaltningen beskrevet som preget av fragmenterte ansvarsforhold:

> «Dagens ID-forvaltning har ikke én eier eller én aktør som arbeider som premissgiver. Konsekvensen av fragmentering og lav grad av strategisk styring er at ingen i tilstrekkelig grad har tatt ansvar for å gi helhetlige føringer eller ta helhetlige prinsipielle beslutninger. Helhetlige vurderinger med tanke på brukervennlighet, kvalitet og sikkerhet og ressursbruk blir i mindre grad ivaretatt i dagens styringsmodell.»

Bildet synes å være delvis uendret i 2025, noe som fremkommer tydelig i likelydende brev fra KoID-aktørene til sine respektive departementer høsten 2024:

> «Områdegjennomgangen av ID-forvaltningen fra 2019 tydeliggjorde at identitetsforvaltningen var fragmentert. Det ble pekt på utfordringer knyttet til lav grad av strategisk styring, fragmentert regelverk, utfordringer ved brukervennligheten i identitetsforvaltningen, sikkerhetsutfordringer og lav bevissthet rundt samlet ressursbruk. Etatene er av den oppfatning at flere av disse utfordringene ennå ikke er løst.»[204]

En av hovedanbefalingene fra områdegjennomgangen var å utarbeide en felles strategi for ID-forvaltningen, selv om dette alene ble vurdert «å ha liten positiv konsekvens».[205] Våren 2023 la regjeringen fram Nasjonal strategi for eID i offentlig forvaltning. Som tittelen tilsier, er strategien begrenset til bruk av eID nettopp i offentlig forvaltning. I og med at myndighetene baserer seg på markedsbaserte eID-løsninger, som kan brukes på tvers av både privat og offentlig sektor, er det imidlertid behov for en helhetlig strategi og helhetlig styring. Digitaliserings- og forvaltningsdepartementet har i samarbeid med Digitaliseringsdirektoratet utarbeidet en handlingsplan for den nasjonale strategien, men også denne planen følger sektorprinsippet og konsentrerer seg om offentlig sektor.[206]

Etter samtaler med ulike offentlige aktører med berøringspunkter til eID-problemene, er vårt inntrykk at det mangler en felles bevissthet på tvers av ulike offentlige instanser om slike berøringspunkter. ID-forvaltningen preges fortsatt av manglende overordnet styring av helheten, og ingen aktør har dette som kjerneoppgave (med unntak av NID og KoID). NID har en meget begrenset rolle og det gjenstår å se hva KoIDs egenevaluering viser, når den foreligger.

For å forbedre et komplekst adaptivt system som eID, kreves det minst fire typer tiltak. Uten disse tiltakene risikerer man at enkelttiltak bare flytter problemene til et nytt område (som å presse en ballong på ett punkt og få luften til å forflytte seg til et annet). Det første tiltaket er å tildele ansvar til en aktør som har et overordnet ansvar for å sikre at systemet fungerer som ønsket. Det andre tiltaket er å forbedre informasjonsstrømmene slik at utfordringer og

[204] Se bl.a. brev fra UDI til Justis- og beredskapsdepartementet, «Koordinering av identitetsforvaltningen» (27. september 2024), Ref. 24/32488-2.
[205] Områdegjennomgangen, s. 248
[206] Handlingsplan for nasjonal strategi for eID i offentlig sektor | Digdir

manglende ansvar blir avdekket av de rette aktørene tidlig, slik at aktørene kan diskutere nye og innovative løsninger (og ikke fem år for sent i saker som kommer til Høyesterett). Det tredje tiltaket er å se på insentiver og regler som påvirker systemene, samt kontinuerlig justere dem etter innhenting av kunnskap slik at de har ønsket effekt. Det fjerde tiltaket er å vurdere om paradigmet som styrer hele eID-systemet er preget av en unødvendig vekting av effektivisering for enkelte sterke aktører, fremfor rettssikkerhet og effektivisering for svakere aktører.

I forlengelsen av dette vil vi påpeke at et særskilt problem synes å være fravær av vilje til å bruke ressurser på å sikre helhetlige og gode tiltak. Det virker som om offentlige myndigheter tror at det er mulig å oppnå store effektivitets- og kostnadsbesparelser uten å gjøre investeringer av betydning. Et helt sentralt overordnet mål med eID-strategien er å spare penger: gjennom hele strategien fremheves det at løsningene skal være «kostnadseffektive». Samtidig er strategien begrenset til å tiltak som kan «finansieres innenfor gjeldende budsjettrammer». Dette ble eksplisitt understreket av Finansdepartementet i deres høringssvar til strategien: «Finansdepartementet vil bemerke at konkrete tiltak som varsles i strategien må begrenses til tiltak som kan gjennomføres innenfor gjeldende budsjettrammer.»[207]

Ordtaket «å spare seg til fant» har sjelden vært mer treffende. Konsekvensene av de alvorlige utfordringene med den digitale identitetsforvaltningen som er beskrevet i denne rapporten er svært kostbare på et samfunnsnivå. I den sammenhengen vil vi også fremheve betydningen av bredere kost-nytte vurderinger i forbindelse med digitaliseringsprosjekter.

Ett konkret eksempel er såkalt «samtykkebasert lånesøknad», som er en del av DSOP-samarbeidet (Digital Samhandling Offentlig Privat). Løsningen går ut på at banker ifbm. lånesøknader kan hente inn inntektsinformasjon direkte fra Altinn. På den måten forenkles lånesøknadsprosessen, og det eneste lånesøkeren trenger er BankID. I prosjektets aktivitetsrapport for 2022 er gevinsten anslått å være 13 milliarder kroner over 10 år, basert på at lånesøknadsprosessen hos bankene krever vesentlig mindre jobb.[208] Tre år senere fremhever imidlertid Finans Norge i sin svindelrapport at «svindel med samtykkebasert lånesøknad (SBL) er en type lånebedrageri som ofte er en del av en større svindel, og kan være knyttet til svindel i Skatteetaten, NAV og forsikring.»[209] Problemet er at løsningen legger til rette for den type systemmisbruk og registermanipulasjon som er beskrevet ovenfor i punkt 5.2.5. Med tilgang til noens BankID kan kriminelle først manipulere inntektsopplysninger slik at kredittverdigheten øker, og deretter gjennomføre lånesvindel. Denne typen svindel har eksplodert de siste årene, og spørsmålet er om ikke vinningen har gått opp i spinningen – og vel så det.

Trolig er det på et samfunnsnivå vesentlig billigere og mer kostnadseffektivt å investere i en helhetlig, trygg og inkluderende digital identitetsforvaltning enn å ta utgiftene som følger med å ikke gjøre det.

Tiltak:

99. Gi én statsråd, ett departement og én etat (eventuelt direktorat) et helhetlig ansvar for ID-forvaltningen. Forslaget er nærmere beskrevet i områdegjennomgangen fra 2019, pkt. 16.1.7. Vi slutter oss til anbefalingen.
100. Det må bevilges tilstrekkelige midler til en forsvarlig, helhetlig digital identitetsforvaltning.

[207] Høring - utkast til ny strategi for eID i offentlig sektor, se Finansdepartementet 2022.pdf
[208] dsop-aktivitetsrapport-2022.pdf
[209] Status og tiltak mot svindel for 2025

101. Et statlig organ bør jevnlig gjennomføre en helhetlig risikovurdering av eID forvaltningen i Norge, der blant annet systemisk risiko vurderes og risikoreduserende tiltak drøftes i dialog med representanter for relevante brukergrupper.
102. Midler til evaluering, forskning og innovasjon innen cybersikkerhet og rettshjelp bør fordeles av regjeringen for å styrke kunnskap, cybersikkerhet, transparens og rettssikkerhet i systemet.

6. Særlig om betydningen av eIDAS 2.0 og innføring av EDIW

Som drøftelsene i punkt 5 har vist, er det store utfordringer knyttet til den digitale identitetsforvaltningen i Norge. Et sentralt spørsmål er i hvilken grad gjennomføring av eIDAS 2.0 med tilhørende lansering av den europeiske digitale identitetslommeboken (EDIW) vil avhjelpe disse utfordringene.

Det kan umiddelbart slås fast at mange av utfordringene og tiltakene beskrevet i denne rapporten ikke reguleres direkte av eIDAS 2.0. Forordningen regulerer eksempelvis ikke nasjonale regler om gjenoppretting og reparasjon (tapsfordeling), den stiller ikke krav til helhetlig styring av identitetsforvaltningen og den berører ikke spørsmål i nasjonal rett om eventuelle ekstra sikkerhetstiltak hos brukerstedene for spesifikke disposisjoner – for å nevne noe.

I hvilken grad de tekniske kravene til sikkerhet vil avhjelpe de utfordringene vi har i dag med digitalt identitetsmisbruk, kommer til en viss grad an på hvordan gjennomføringsrettsaktene til syvende og sist blir seende ut – forhold som i skrivende stund ikke er avklart. I august 2024 sendte en lang rekke organisasjoner og individuelle eksperter et åpent brev til Europakommisjonen og representanter for medlemsstatene, der de uttrykker dyp bekymring for at gjennomføringsrettsaktene til eIDAS 2.0 ikke gir tilstrekkelig sikkerhet.[210] Også Eurosmart, en interesseorganisasjon for IT-sikkerhetsindustrien har ropt varsku om uakseptabel risiko knyttet til de digitale identitetslommebøkene.[211] Eurosmart sin gjennomgang av både samfunnsrisikoen og risikoen knyttet til svindel og identitetsmisbruk som rammer enkeltpersoner og bedrifter, med potensielt store økonomiske konsekvenser, er som en blåkopi av flere av de sentrale risikoene som er beskrevet i denne rapporten, og som allerede har materialisert seg i Norge som følge av universalnøkkelfunksjonen BankID har i det norske samfunnet. Det er i alle tilfelle utfordrende å forhindre misbruk i form av tvang, vold og press gjennom tekniske løsninger.

Når det gjelder utfordringene knyttet til universell tilgang, er det derimot klart at eIDAS 2.0 stiller vesentlig strengere krav til medlemslandene enn det som følger av eIDAS 1.0. Det følger av artikkel 5a nr. 1 at statene er forpliktet til å sikre at «all natural and legal persons in the Union» skal ha tilgang til en EDIW med en integrert eID. Forordningen er klar på at «alle» skal ha tilgang til EDIW, og det er etter vårt syn ikke anledning til å utestenge personer på grunnlag av funksjonsnedsettelser, lave digitale ferdigheter, språkproblemer e.l. Når det konkret gjelder utlendinger, er imidlertid forordningen mindre klar på hvilke utlendinger som i denne sammenhengen omfattes. Det samme gjelder barn og unge, der forordningen ikke berører spørsmål om aldersgrense.

[210] eIDAS_-_European_eID_Implementation_Open_Letter.pdf
[211] 2024_09_10_Low-Security-in-the-EUDI-WalletV1.2_FINAL.pdf

I en norsk kontekst har flere av utfordringene sammenheng med BankID-systemet og den dominerende markedsposisjonen BankID har. eIDAS 2.0 artikkel 5a nr. 2 åpner for at medlemsstatene kan velge mellom å tilby EDIW selv, gjennom et offentlig-privat samarbeid, eller ved å anerkjenne én eller flere private tilbydere. Det som er klart, er at statene har en mer fremtredende rolle og ansvar i eIDAS 2.0.

For å sikre nasjonal sikkerhet, digital suverenitet, og inkludering, anbefaler vi at Norge velger en statlig styrt tilnærming til EUDI-lommeboken, der en offentlig kontrollert eID spiller en sentral rolle. Som beskrevet i punkt 5.9, viste høringen til strategien for eID i offentlig forvaltning at et overveldende flertall av høringsinstansene ønsket seg en offentlig eID. Det var stort sett bare markedsaktørene for eID og finansnæringen som eier BankID som ikke ønsket seg dette. Også i høringssvarene til digitaliseringsstrategien forutsetter enkelte høringsinstanser at det kommer en offentlig kontrollert eID.[212] En slik løsning utelukker imidlertid ikke et samarbeid med private aktører, og man kan tenke seg mange ulike varianter av et privat-offentlig samarbeid.

Norge står nå ved et veiskille der resultatet av de strategiske valgene som tas i forbindelse med gjennomføring av eIDAS og innføring av de digitale identitetslommebøkene vil ha avgjørende betydning for hvorvidt vi forsterker eller avhjelper utfordringene vi har i den digitale identitetsforvaltningen. Det er foreløpig lagt opp til at en del av disse viktige beslutningene skal tas basert på en såkalt KVU-prosess. Etter vårt syn bør disse spørsmålene drøftes helhetlig av et offentlig utvalg (NOU), der man ser eIDAS 2.0 i sammenheng med øvrige spørsmål i den digitale identitetsforvaltningen. Det vises særskilt til punkt 5.9 ovenfor, om behovet for åpne og demokratisk forankrede prosesser.

Oversikt over anbefalte tiltak

Styringsprinsipp 1: Universell tilgang

Flere grupper i befolkningen har ikke tilgang til eID på øverste sikkerhetsnivå.

1. Alle må ha rett til en eID på øverste sikkerhetsnivå. Vi trenger en eID-lov tilsvarende passloven og ID-kortloven som oppstiller vilkår for utstedelse av eID og gir brukerne rett til eID når vilkårene er oppfylt. Loven må inneholde vilkår for utstedelse og sperring/oppsigelse, og må inkludere mekanismer for klage, tilsyn og kontroll og effektive sanksjoner. Det må særskilt oppstilles rett til assistert bruk.
2. Alle med rettigheter og plikter i Norge, som har behov for å kunne identifisere seg digitalt her, må ha rett til norsk identitetsnummer. Dette krever endringer i folkeregisterloven og folkeregisterforskriften.
3. Alle som har fått tildelt et fødsels eller d-nummer fra Norge, bør ha mulighet til å dokumentere det tildelte ID-nummeret fysisk og digitalt på en troverdig måte,[213] for eksempel ved å få tilgang til nasjonalt ID-kort.

[212] Likestillings- og diskrimineringsombudet skriver i sitt høringssvar at ombudet «er kjent med at Regjeringen jobber med å utvikle eID som skal være tilgjengelig for alle. Ombudet mener at dette arbeidet må intensiveres for å hindre utenforskap». ldos-innspill-til-ny-digitaliseringsstrategi.pdf

[213] Dette er også foreslått i Områdegjennomgangen, Tilleggsrapporten, punkt 5.1.1.

4. Utstedelse av eID bør være basert på en sikker kopling til en grunnidentitet ved å ”låse” én person til én identitet i Norge ved kontrollen av biometriske data som skjer ved utstedelse av norske pass eller ID-kort.
5. Staten bør utvikle og tilby en eID på sikkerhetsnivå høyt som er tilgjengelig og tryggere å bruke for flere. En slik offentlig tilbudt eID kan og må tilfredsstille alle kravene ovenfor.
6. Ved bruk av markedsbaserte eID-løsninger i offentlig sektor må det i anskaffelsesprosessen stilles større krav til tilbyderne mht. praksisene rundt utstedelse og sperring. Det må stilles tydelige krav om ikke-diskriminering og ivaretakelse av rettssikkerhet i prosessen. Kravene må følges opp med tilsyn og kontroll.
7. BankID bør utstedes uavhengig av bankene, for eksempel slik at BankID selv tar ansvar for utstedelse slik at ikke hvitvaskingsreglene blir et hinder for utstedelse.
8. Myndighetene bør legge til rette for at private eID-leverandører kan benytte offentlige skrankepunkter for legitimasjonskontroll og innrullering ved utstedelse av eID.
9. Ved bruk av markedsbaserte eID-løsninger i offentlig sektor må det stilles større krav til tilbyderne mht. praksisene rundt utstedelse og sperring. Det må stilles tydelige krav om ikke-diskriminering og ivaretakelse av rettssikkerhet i prosessen. Kravene må følges opp med tilsyn og kontroll.
10. Som et strakstiltak bør det avklares og åpnes for at eID på sikkerhetsnivå høyt tillates brukt med assistanse fra en utvalgt person.

eID-løsningene og tilhørende infrastruktur er ikke tilstrekkelig universelt utformet og tilpasset

11. Registrering og legitimasjonskontroll for å få utstedt en offentlig støttet eID på nivå høyt bør kunne skje der eID-innehaveren oppholder seg hvis vedkommende er innlagt på institusjon, innsatt i fengsel, bevegelseshemmet eller på annen måte har vanskelig for å benytte ordinære skrankepunkter eller registreringssteder.
12. Tilbydere av eID-løsninger må sørge for at eID-løsningene er enkle og trygge å bruke for alle. Dette har også en side til utfordringene knyttet til hhv. svindelforebygging og sikkerhetsløsninger, jf. punkt 5.2 og innovasjon og konkurranse, jf. punkt 5.7. Mulige virkemidler er:
    - Bruksbegrenset eID for personer med begrenset rettslig handleevne.
    - Systematisk og integrert bruk av biometri
    - Dobbeltsigneringsfunksjoner for de som trenger assistanse
13. Myndighetene bør vurdere om det må stilles mer spesifiserte krav til universell utforming for eID'er som skal benyttes i ID-porten enn det som fremgår av loven og forskriften.

Alternative analoge/fysiske og digitale løsninger er blitt dårligere eller helt borte

14. Gjennomgå lovverket for grunnleggende private og offentlige tjenester og stille krav om å tilby alternative digitale og/eller analoge løsninger. Dette kan for eksempel inkludere
    - Krav til aktører innen helse, herunder fastlegekontorer, om å ta imot betaling med betalingskort og/eller kontanter.
    - Krav til aktører som tilbyr kollektivtransport om tilgjengelige og alternative måter å kjøpe billetter.
    - Krav til tilgjengelighet og åpningstider for fysiske offentlige kontorer som NAV, Skatteetaten osv.

15. Alle betalingstjenestetilbydere pålegges å tilby alternative metoder for sterk kundeautentisering til kunder som ikke får BankID, samt sørge for at de alternative metodene godtas ifbm. betalinger på nett, ikke kun innlogging i nettbank.

Fullmaktsløsninger eksisterer ikke eller er for dårlige

16. Offentlige myndigheter bør utvikle et sentralt fullmaktsregister på tvers av offentlig og privat sektor.
17. Private og offentlige aktører pålegges å ha fullmaktsløsninger knyttet til sine nettjenester, i alle fall når de representerer tilgang til innbyggernes lovbestemte rettigheter eller grunnleggende tjenester som bank, forsikring, lovbestemte registre, tilgang til egne helseopplysninger mv.
18. Stille krav til utforming av private fullmaktsløsninger, særlig i bankene, slik at disse dekker brukernes faktiske behov, herunder sikrer dataminimering og mulighet for begrensede fullmakter.
19. Offentlige servicekontorer bør kunne foreta disposisjoner på innbyggers vegne basert på ad hoc fullmakt når innbyggeren er fysisk til stede. Særlig gjelder dette reservasjoner og etablering av andre fullmakter.
20. Det bør utredes om fullmaktssertifikater som representerer en personlig fullmakt kan utstedes av andre enn fullmaktsgiver. Det kan være praktisk der bakgrunnen er at fullmaktsgiver ikke er digitalt aktiv, men må forholde seg til digitale tjenester (med bistand). Utrede en ordning der fullmaktsgiver møter opp et sted som kan utstede en (frasagns)fullmakt i form av et fullmaktssertifikat på fullmaktsgivers vegne basert på dennes muntlig uttrykte ønske.
21. Som et strakstiltak bør NKOM avklare at eID på sikkerhetsnivå høyt kan utstedes til bruk for verge på vegne av vergehaver og/eller at det åpnes for assistert bruk. Ved behov kan Lovavdelingen bes om å utrede dette på forhånd.
22. Som et strakstiltak bør Digitaliseringsdirektoratet etablere mer fleksible varslingsløsninger slik at en "hjelper" vedkommende velger, f.eks. en pårørende, får varsel og kan gjøre mottaker oppmerksom på at det venter en digital sending og hvilken kanal den er sendt i, f.eks. ved å åpne for subsidiære varslingsadresser i kontakt- og reservasjonsregisteret.

For mange tjenester krever eID på øverste sikkerhetsnivå

23. Sette tydeligere krav og retningslinjer til private og offentlige brukersteder/tjenesteeiere ved valg av sikkerhetsnivå og sikre oppfølgning av at tjenesteeiere ikke stiller høyere sikkerhetskrav enn nødvendig.
24. Der brukerstedene tilbyr tjenester med forskjellige sikkerhetsbehov, må brukerstedet sømløst håndtere situasjoner der brukeren får behov for høyere sikkerhetsnivå.
25. Forsikre at offentlige virksomheter som krever bruk av sikkerhetsmekanismer for elektronisk kommunikasjon sikrer at det er egnede mekanismer (eID) tilgjengelig for innbyggerne for de tjenestene og på det sikkerhetsnivået den offentlige virksomheten har valgt å benytte. Hvis det er grupper som faller utenfor må det offentlige etablere et alternativ. Offentlige virksomheter må etablere alternativer for de av deres egne brukere som ikke kan få en eID på tilstrekkelig høyt nivå.

Dagens system fører til strukturell diskriminering og menneskerettsbrudd

26. Myndighetene bør jevnlig gjennomføre menneskerettslige konsekvensanalyse av den digitale identitetsforvaltningen.
27. Tilsyns- og overvåkningsorganer som LDO og NIM bør fokusere på strukturelle diskrimineringsproblemer innen eID-området.

Styringsprinsipp 2: Svindelforebygging og sikkerhetsløsninger

Sårbarheter i eID-systemene

28. Finans Norge sine anbefalinger fra svindelrapport fra 2025 gjennomføres:[214]
    - Begrense til én OTP per sertifikat.
    - Gi bedre kontekstinformasjon i BankID-appen.
    - Få i gang nytt antisvindelsystem.
    - Tilby en bedre løsning for sperring av BankID som har blitt brukt i svindel.
    - Innføre selvadministrert BankID og MinSide for kundehistorikk.
29. Forby utstedelse av mer enn én BankID med kodebrikke og én BankID-app per bruker. (Tilgang til kodebrikke som backup til appen.)
30. Bygge utstedelse av eID på offentlig utstedt digital ID ("PID" etter eIDAS 2.0 terminologi) som en offentlig utstedt grunnidentitet. Slik dagens infrastruktur er fremstår det mest naturlig at Folkeregisteret og Politiet sammen kan skape et slikt offentlig utstedt digitalt grunnidentitetsbevis.
31. eID-leverandørene bør implementere sterkere autentiseringsmekanismer for bruk av eID-ene, inkludert systematisk og integrert bruk av biometrisk verifisering.

Sårbarheter hos brukerstedene

32. Brukerstedene må risikovurdere bruk av eID i de enkelte brukstilfellene.
33. eID-løsningene bør tilby varierte autentiseringsmekanismer tilpasset risikoen i transaksjonen, særlig ved høyrisiko-transaksjoner som signering av gjeldsbrev og endring av kontonummer. Brukerstedene bør spesifisere risikoen.
34. Brukerstedene bør varsle (utenom eID-systemet) til den transaksjonen gjelder ved transaksjoner (inkludert endringer) av høy verdi eller på annen måte av stor betydning for brukeren. Brukerstedene bør også benytte autentisering (f.eks. digital fremvisning av pass eller fysisk ID-kort med integrert biometrisk sjekk, eller fysisk oppmøte) utover eID der risikovurderingen tilsier det.
35. Brukerstedene må ha manuelle kontrollmekanismer for særlig risikofylte disposisjoner.
36. Det bør vurderes (gjen)innføring av vitnekrav for særlig risikofylte disposisjoner, som låneopptak.

Sårbarheter knyttet til bruk av privat eID i jobbsammenheng

[214] Status og tiltak mot svindel for 2025

37. Alle ansatte skal ha rett til å kreve at arbeidsgiver anskaffer en egen eID til den ansatte for bruk i arbeidsforholdet som alternativ til bruk av den ansattes egen private eID på vegne av arbeidsgiver.
38. Det må gjennomføres risikovurderinger der privat eID vurderes brukt i jobbsammenheng. Ved uakseptabel risiko bør privat eID ikke brukes i jobbsammenheng.
39. Der det der mulig bør ansatte utstyres med pseudonymt ansattsertifikat, f.eks. i bransjer som krever autorisasjon og har sentrale autorisasjonsregistre der f.eks. et profesjonsnummer kan verifiseres og valideres.

Systemmisbruk; særlig om registermanipulasjon

40. Det gjennomføres en tilsvarende utredning som i Sverige om registermanipulasjon i selskapsforhold, med vurdering av om tiltak og lovendringer som er iverksatt der også bør innføres i Norge.
41. Brønnøysundregistrene bør ha ansvar for å sikre at opplysninger som registreres er riktige, ikke kun formalkontroll av opplysninger. Dette krever flere ressurser og endret mandat.
42. Det bør lovfestes at misbruk av elektronisk signatur regnes som falsk i forhold til tinglysingsloven § 27.
43. Det bør gjeninnføres vitnekrav ved tinglysing.
44. Ved tinglysing bør det kreves ikke bare en elektronisk identifikasjon, men også en elektronisk sammenheng mellom identifiseringen og den teksten som signeres.

Nye sikkerhetsutfordringer med KI-drevet ID-svindel

45. Ta i bruk KI systemer som kan avsløre ID-svindel, for eksempel gjenkjenne avvik i måten bilder eller video vises på, analysere metadata, simulere angrep eller søke etter tilsvarende bilder på nett (reverse image search).
46. Utstedere og brukersteder bør vise varsomhet med å tillate ad hoc verifikasjonsmetoder der brukeren ikke er fysisk til stede i skranken, for eksempel videomøter.
47. Verifikasjonsmetoder der brukeren ikke er fysisk til stede i skranken (f.eks. digital fremvisning av pass eller ID-kort med integrert biometrisk sjekk) må jevnlig reevalueres med tanke på nye KI-drevne angrep (i tillegg til andre angrep).
48. Forsikre at alle relevante aktører i systemet får opplæring om hva KI kan få til (AI literacy)

Sårbarheter knyttet til sluttbrukerne

49. eID-leverandørene må sørge for at brukeren, i forbindelse med utstedelse av eID, får tilbud om god opplæring i trygg bruk av eID-en.
50. Myndighetene og eID-leverandørene må sammen øke bevisstheten om risikoene ved deling av eID, f.eks. gjennom informasjonskampanjer.
51. eID-leverandørene og brukerstedene må innføre bedre brukervarsling ved forsøk på uvanlig innlogging eller transaksjoner.
52. eID-leverandørene må gi brukerne mulighet til å sette begrensninger på egen eID-bruk, for eksempel geografisk eller etter type transaksjon.
53. eID-leverandørene må utvikle enklere sperremekanismer for raskt å kunne stoppe misbruk av eID.
54. eID-leverandørene må bedre brukeres mulighet til innsyn i og kontroll over egen eID, se punkt 5.4.1.

Mangelfullt samarbeid og deling av data mellom aktører

55. Myndighetene bør sørge for bedre samhandling og deling av informasjon mellom private og offentlige aktører, mellom ulike private aktører og mellom ulike offentlige aktører. Dette må skje på måter som ivaretar personvernet og rettssikkerheten og ikke fører til en forsterkning av problemer med finansiell ekskludering.
56. Det gjennomføres en utredning av mulighetsrommet etter eIDAS 2.0 for igangsatte og planlagte prosjekter om datadeling.

Styringsprinsipp 3: Gjenoppretting og reparasjon

Reglene om tapsfordeling etter ID-misbruk gir ikke et sterkt nok vern

57. Utrede og foreslå en helhetlig regulering av tapsfordeling etter ID-misbruk. En slik regulering bør inkludere alle tiltakene i 58-63.
58. Gi små og mellomstore bedrifter og ideelle organisasjoner samme vern som forbrukere i finansavtaleloven.
59. Fordele ansvaret for tap på flere aktører enn finansinstitusjoner og på flere finansinstitusjoner (ikke kun den svindelutsatte kundens betalingstjenestetilbyder).
60. Regulere tapsfordeling i situasjoner som faller utenfor finansavtalelovens anvendelsesområde.
61. Oppdatere avtalelovens ugyldighetsregler ved digitale avtaleinngåelser med en moderne forståelse av vold og tilpasset et digitalt samfunn der bedrifter og kunder, særlig forbrukere, inngår avtaler i en digital setting der vold, press og utnytting ikke er synlig. En slik revisjon må inkludere både vilkårene for og konsekvensene av ugyldighet slik at den ivaretar offeret i situasjoner der vedkommende ikke har fått nyttiggjort seg verdiene det er snakk om og ikke kan klandres, jf. tilsvarende regulering i vergemålsloven § 15 første ledd tredje punktum. Revisjonen må ta hensyn til et moderne voldsbegrep slik det er regulert i internasjonale konvensjoner.
62. Varslingsregler i både avtaleloven og finansavtaleloven bør revideres.
63. Tapsfordeling for offentligrettslige krav som springer ut av ID-misbruk eller press, tvang og vold må særskilt reguleres.

Utfordringer i kommunikasjonen med og klagebehandlingen hos finansinstitusjoner

64. Bistand i forbindelse med ID-misbruk av et visst omfang bør omfattes av den offentlige rettshjelpsordningen og må utløse rett til fritt rettsråd og fri sakførsel.
65. Det offentlige bør tilby tilpasset førstelinjehjelp til dem som opplever ID-misbruk, jf. det statlige hjelpetilbudet i Danmark.
66. Utvide Gjeldsregisteret til å inkludere opplysninger om saker som er stilt i bero, og liknende avtaler knyttet til gjeld som inngår i innkassobyårenes porteføljer, og kreve at kjøper av porteføljen må respektere disse.

Offentlige myndigheter mangler retningslinjer og systemer for å rette opp feil etter identitetsmisbruk

67. Det utarbeides sentrale retningslinjer/rundskriv for offentlige aktørers håndtering av henvendelser med påstand om id-misbruk.

Manglende rettshjelp og praktisk hjelp

68. Bistand i forbindelse med ID-misbruk av et visst omfang bør omfattes av den offentlige rettshjelpsordningen og må utløse rett til fritt rettsråd og fri sakførsel.
69. Det offentlige bør tilby tilpasset førstelinjehjelp til dem som opplever ID-misbruk, jf. det statlige hjelpetilbudet i Danmark.
70. Utvide Gjeldsregisteret til å inkludere opplysninger om saker som er stilt i bero, og liknende avtaler knyttet til gjeld som inngår i innkassobyårenes porteføljer, og kreve at kjøper av porteføljen må respektere disse.

Begrenset tilgang til sentrale bevis og kompetanse til å forstå hva digitale bevismidler betyr

71. Datatilsynet bør følge EDPBs anbefalinger i tilfeller av ID-misbruk.
72. Det bør utredes om særskilte bevisregler bør innføres også på andre områder enn det som er dekket av finansavtaleloven.

Utfordringer knyttet til sammenhengen mellom strafferettslig forfølgning og sivilrettslige krav

73. Revisjon av straffeloven § 202 slik at den rammer flere former for identitetsmisbruk. Innføring av en ny bestemmelse om grovt identitetsmisbruk med en høyere strafferamme.
74. Mennesker i sårbare posisjoner som velger å anmelde, må tilbys praktisk hjelp og bistand.
75. Det gjennomføres en utredning med sikte på å foreslå tiltak som reduserer de negative konsekvensene av at svindelofre står i en uavklart økonomisk posisjon mens de strafferettslige forholdene er under etterforskning og evt. påtale. Svindelofre bør kunne kreve berostillelse av omstridt gjeld uten at verken avtalte renter eller forsinkelsesrenter løper i denne perioden.
76. Bedragerienheten på Gjøvik bør utarbeide retningslinjer for effektiv etterforskning og påtale av digitale bedragerier og identitetskrenkelser på tvers av politidistrikt, og innta en koordinerende rolle for nasjonal bekjempelse av kriminalitetsformen.
77. Politidirektoratet bør utarbeide rundskriv og sørge for opplæring som sikrer tilstrekkelig kunnskap i politiets førstelinje om privatrettslige konsekvenser av digitalt bedrageri og identitetskrenkelse, slik at svindelofre kan veiledes og henvises til relevante ressurser.

Mangler ved systemer for å rette feil opplysninger i registre

78. Det gjennomføres en utredning av reglene for alle relevante registre, herunder Gjeldsregistreret og Brønnøysundregistrene, for å sikre at mekanismer er på plass for retting av feil opplysninger.

Styringsprinsipp 4: Autonomi: Selvbestemmelse og personvern

Manglende innsyn i og kontroll over egen eID og personopplysninger

79. Alle bør ha rett til en brukerstyrt eID med mulighet for bruksbegrensninger og tilgang til logg som viser når, hvor og til hva eID'en er brukt, se også 5.2.6.[215] Loggen bør bare være

[215] Dette er også foreslått av Finans Norge, Status og tiltak mot svindel for 2025

tilgjengelig for brukeren selv og gjelde for den enkelte eID. Brukeren bør kunne reservere seg mot registrering av opplysninger som ellers skjer av hensyn til brukeren.

80. Kontakt- og reservasjonsregisteret bør utvides med opplysninger om hvorvidt brukeren har fått utstedt en eID på nivå høy (og som ikke er trukket tilbake) og hvem som har utstedt eID'en eller eID'ene. Oversikten må være tilgjengelig for brukeren selv og for avsendere som har rett (og plikt) til å benytte kontakt- og reservasjonsregisteret for å sende elektroniske meldinger slik at de (f.eks. forvaltningen, et legekontor eller inkassoselskap) ikke sender en melding på sikkerhetsnivå høyt til en person som ikke kan få tak i meldingen fordi vedkommende ikke har eID på riktig sikkerhetsnivå. Se også om meldinger som ikke kommer frem i punkt 5.4.3.

Teknologien overstyrer den juridiske privatautonomien

81. Alle må ha rett til eID på samme måte som alle har rett til fysisk ID-bevis, uavhengig av funksjonsnedsettelser og digitale og fysiske ferdigheter. Dette kan om nødvendig gjøres ved å utstede eID-er med begrenset bruksområde eller rettigheter, eller ved å kunne registrere bruksbegrensninger i sertifikat-/eID-katalogen og utlevere bruksbegrensningene sammen med status for eID-en når den benyttes.

Digitalisering og bruk av eID kan føre til rettstap fordi informasjon ikke kommer frem til mottakeren

82. Det må aktivt informeres om muligheten for å reservere seg mot digital post fra forvaltningen, hvordan det gjøres og konsekvensene av det.
83. Reservasjonsretten bør utvides til å kunne gjøres gjeldende for flere typer meldinger og tjenester enn i dag, og overfor både offentlige og private virksomheter. Det bør være mulig å reservere seg bare mot noen tjenester, eller å oppheve reservasjon bare for enkelte tjenester.
84. Alle typer meldinger som må antas å ha stor betydning for den enkelte bør omfattes av kravene til varsling og oppfølging hvis de ikke leses, ikke bare de meldingene som omfattes av eForvaltningsforskriftens § 8. Dette kan muligens baseres på den kategorisering som avsender uansett må gjøre i forbindelse med valg av varslingsmetode og sikkerhetsnivå mv, f.eks. at alle meldinger på sikkerhetsnivå høyt må følges opp av avsender.
85. Det bør vurderes å gjeninnføre ettersending av meldinger i fysisk post, dersom digital post ikke åpnes, slik løsningen var i henhold til eforvaltningsforskriften § 8 frem til 2014 (fra 2004, og tilsvarende i § 7 i 2002-forskriften frem til 2004). Det bør også vurderes andre former for oppfølging hvis digital post ikke leses, f.eks. per telefon når forholdene gjør det hensiktsmessig og trygt.
86. Det bør utredes om kontakt- og reservasjonsregisteret kan inneholde opplysninger om den enkelte har eID på nivå høy og om denne er i aktiv bruk slik at avsender kan sjekke dette før melding sendes digitalt på sikkerhetsnivå høyt, slik det er foreslått under punkt 5.4.1.

Styringsprinsipp 5: Transparens: Åpenhet og gjennomsiktighet

87. Finanstilsynet bør offentliggjøre detaljert statistikk for svindelhåndtering, inkludert hvordan det svindelforebyggende arbeidet virker, hvor mange svindler som gjennomføres og hvem som tar tapet i svindlene
88. Myndighetene bør pålegge eID-leverandørene å være transparente om den tekniske funksjonaliteten til eID-ene, herunder arkitektur og tekniske detaljer. Det kan gis snevre unntak for detaljer om sikkerhetsmekanismer som slutter å fungere hvis angriperne kjenner disse detaljene.

Styringsprinsipp 6: Ansvar: tilsyn, kontroll og sanksjoner

89. Etter selvdeklarasjonsforskriften § 10 annet ledd, kan NKOM pålegge tilbyder av eID-løsning å gjennomføre revisjon for å dokumentere oppfyllelse av kravene til nivå høyt. Denne muligheten til å kreve revisjon bør benyttes i større grad enn i dag for å sikre at kravene faktisk blir, og holdes, oppfylt.
90. Finanstilsynet og/eller Forbrukertilsynet gjennomfører tilsyn med bankenes praksiser knyttet til nektelse og inndragning av BankID.
91. Det gjennomføres en utredning av totaliteten i tilsyns- og sanksjonssystemet med en vurdering og avklaring av ulike tilsynsmyndigheters rolle og ansvar.

Styringsprinsipp 7: Innovasjon: interoperabilitet, valgfrihet og konkurranse

92. Det bør settes av midler til å gjennomføre en innovasjonskonkurranse for inkluderende eID-løsninger.
93. Det bør utredes om ID-porten kan legge til rette for at alle eID-er som oppfyller en felles kravspesifikasjon og forretningsmessige standardvilkår kan knyttes til ID-porten uten å måtte gå veien om nye offentlige anskaffelser.
94. Det må bli en rettslig plikt til at banker og andre finansvirksomheter må godta eID-løsninger på tilstrekkelig sikkerhetsnivå, eventuelt basert på felles godkjenning i finanssektoren.
95. Tydeligere reguleringer av dominerende markedsaktører når det gjelder sikkerhet og tilgjengelighet for alle grupper.

Styringsprinsipp 8: Samfunnssikkerhet og beredskap

96. Det må etableres beredskapsplaner som sikrer redundans og alternative løsninger dersom én identitetsleverandør skulle falle ut.

Styringsprinsipp 9: Demokratisk forankring

97. Nedsett et offentlig utvalg med mandat å gjennomgå den digitale identitetsforvaltningen

Etabler et nasjonalt råd eller forum for digital identitet med bredt sammensatt deltakelse, inkludert sivilsamfunn og sårbare grupper.

Styringsprinsipp 10: Helhetlig styring: Systemtenkning og samhandling

98. Gi én statsråd, ett departement og én etat (eventuelt direktorat) et helhetlig ansvar for ID-forvaltningen. Forslaget er nærmere beskrevet i områdegjennomgangen fra 2019, pkt. 16.1.7. Vi slutter oss til anbefalingen.
99. Det må bevilges tilstrekkelige midler til en forsvarlig, helhetlig digital identitetsforvaltning.
100. Et statlig organ bør jevnlig gjennomføre en helhetlig risikovurdering av eID forvaltningen i Norge, der blant annet systemisk risiko vurderes og risikoreduserende tiltak drøftes i dialog med representanter for relevante brukergrupper.
101. Midler til evaluering, forskning og innovasjon innen cybersikkerhet og rettshjelp bør fordeles av regjeringen for å styrke kunnskap, cybersikkerhet, transparens og rettssikkerhet i systemet.