Nasjonalt ID-senter

POLITIET
KRIPOS

ID:26

Status, trusler og sårbarheter i den norske ID-forvaltningen

Spørsmål eller innspill til rapportens innhold kan sendes til:
postmottak@nidsenter.no

Design: Nasjonalt ID-senter
Foto og illustrasjoner: Nasjonalt ID-senter, iStock og Adobe Stock

Sammendrag

ID:26 gir en bred og oppdatert oversikt over utviklingen i ID-misbruk i Norge og hvordan fenomenet påvirker både offentlig forvaltning, privat sektor og enkeltpersoner. ID-misbruk er et samfunnskritisk problem som kan svekke rettssikkerheten, undergrave vårt tillitsbaserte samfunn og er samtidig en muliggjører for kriminalitet. Rapporten viser at digitaliseringen av offentlige tjenester og den høye graden av tillit i det norske samfunnet skaper sårbarheter, der både fysiske ID-dokumenter og elektroniske identiteter (eID) misbrukes i økende omfang til ulike formål.

Rapporten peker på tre hovedområder som særlig preges av ID-misbruk: registerkriminalitet (også kalt registermanipulasjon), bedragerier mot enkeltpersoner og misbruk av identitet og dokumenter i migrasjonsrelaterte prosesser. Registermanipulasjon har utviklet seg til å bli en sentral modus for økonomisk motivert kriminalitet, der kriminelle utnytter offentlige tillitsbaserte systemer ved å opprette selskaper eller virksomheter i andres identiteter. I disse selskapene innrapporteres fiktiv aktivitet på disse utnyttede identitetene, hvilket medfører muligheter for statlige utbetalinger og lånopptak i finansinstitusjoner. Disse kriminelle strukturene drives av både enkeltaktører og større organiserte kriminelle nettverk.

Bedragerier mot enkeltpersoner er et voksende problem der privatpersoners eID, er et sentralt angrepspunkt. Modusene har utviklet seg fra at de kriminelle aktørene tar direkte kontroll over eID-informasjonen til enkeltpersoner, til at det nå i større grad benyttes sosial manipulering der de fornærmede selv lures til å godkjenne transaksjoner. Parallelt ser rapporten økt bruk av falske eller lekkede ID-dokumenter på internettforum innen ulike former for digital svindel, inkludert kjærlighets- og investeringsbedragerier.

Innen migrasjon viser rapporten at både falske dokumenter og misbruk av legale kanaler, som visum og arbeidstillatelsesordninger, er økende. Falske utdanningsdokumenter og fiktive arbeidskontrakter brukes som inngang til norsk arbeidsliv, ofte i saker der personer i tillegg utnyttes av kriminelle aktører enten før, underveis eller i etterkant av søknadsprosessen. Internasjonale forhold som krig og konflikter og politisk uro i mange deler av verden øker kompleksiteten ytterligere.

Samlet viser rapporten at ID-misbruket er både omfattende og i rask utvikling. Tiltak må være helhetlige og rette seg mot både teknologiske løsninger, juridisk regelverk og forståelse av menneskelig atferd. Fremtidig ID-sikkerhet krever styrket samarbeid på tvers av sektorer, bedre kontrollmekanismer og økt forståelse for hvordan identitet kan misbrukes i et stadig mer digitalisert samfunn.

Innholdsfortegnelse

ID-misbruk 2025

Statistikken er basert på Kripos og Nasjonalt ID-senter sin monitorering av ID-misbruk. Tallene inkluderer misbrukte ID- og underlagsdokumenter avdekket i Norge, i tillegg til norske dokumenter avdekket misbrukt i utlandet. I tillegg til dokumenter avdekket av politiet, inkluderer statistikken også ID-misbruk anmeldt av andre etater som for eksempel Skatteetaten, Statens vegvesen og Tolletaten.

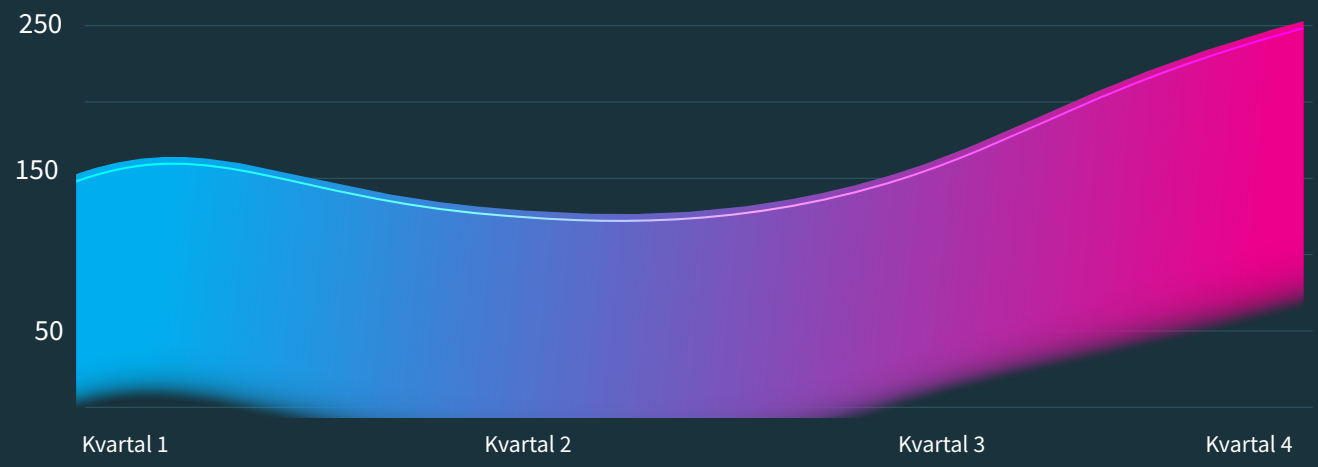
672

misbrukte dokumenter

av 522 personer

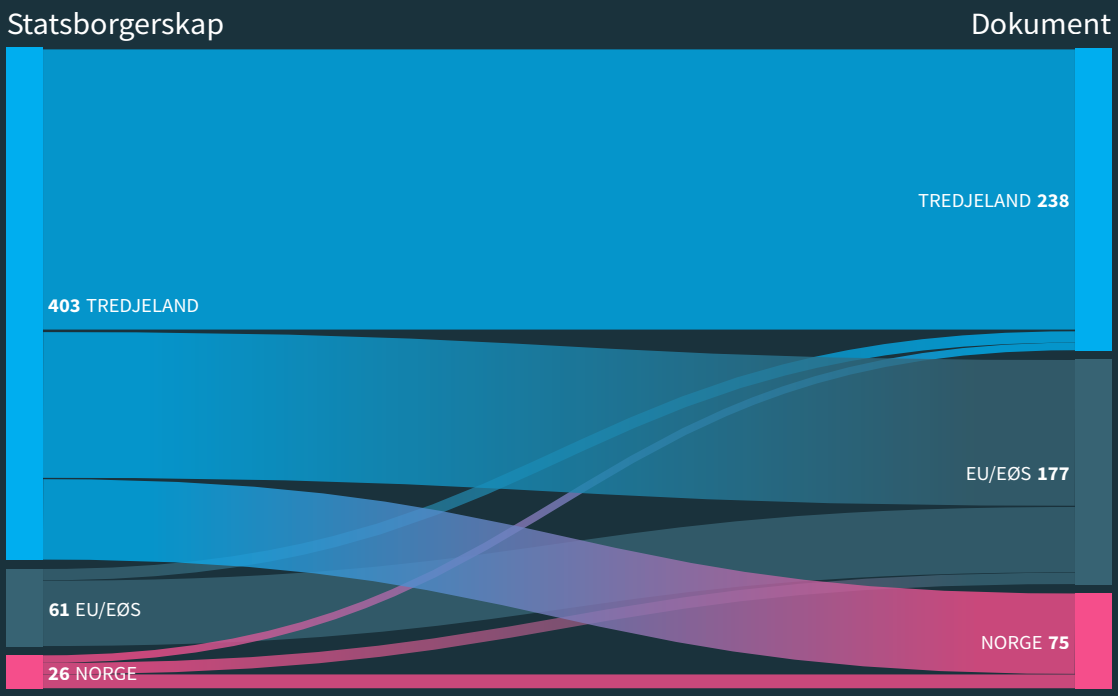
De resterende 93 dokumentene er reisebevis, ulike typer underlagsdokumenter, stempler og kopier eller bilder av ulike typer falske eller forfalskede ID-dokumenter.

Utviklingen gjennom året



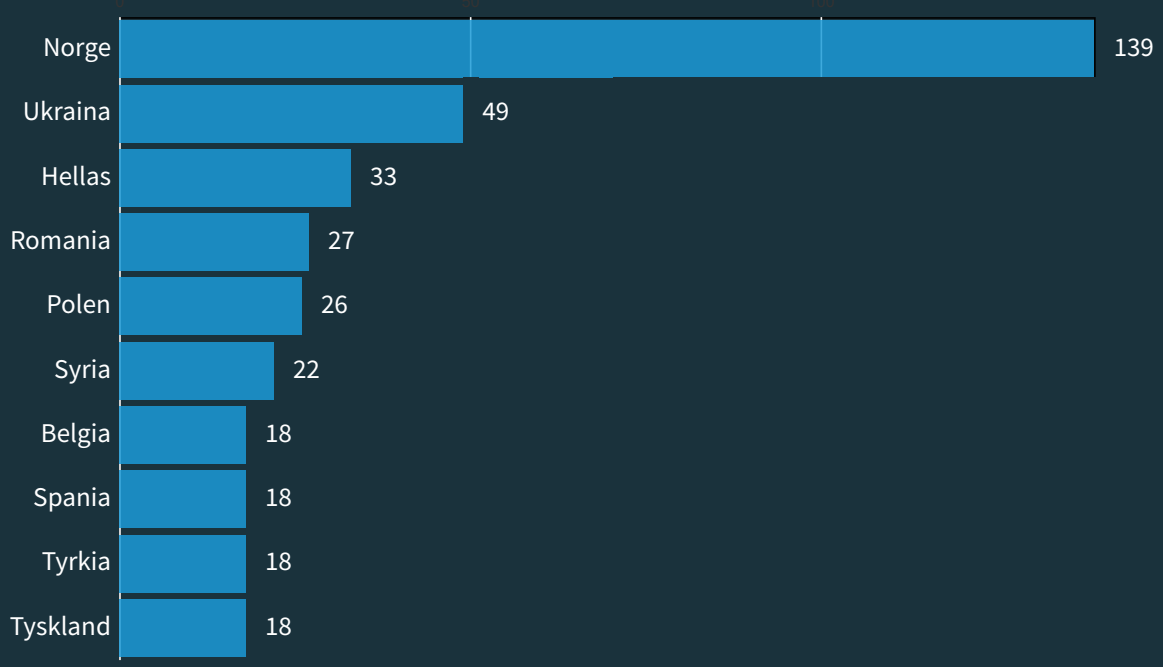
ID-misbruket var stabilt gjennom året, men fikk et tydelig oppsving fra tredje kvartal som fortsatte å øke frem til årsslutt.

Statsborgerskap versus dokumentnasjonalitet



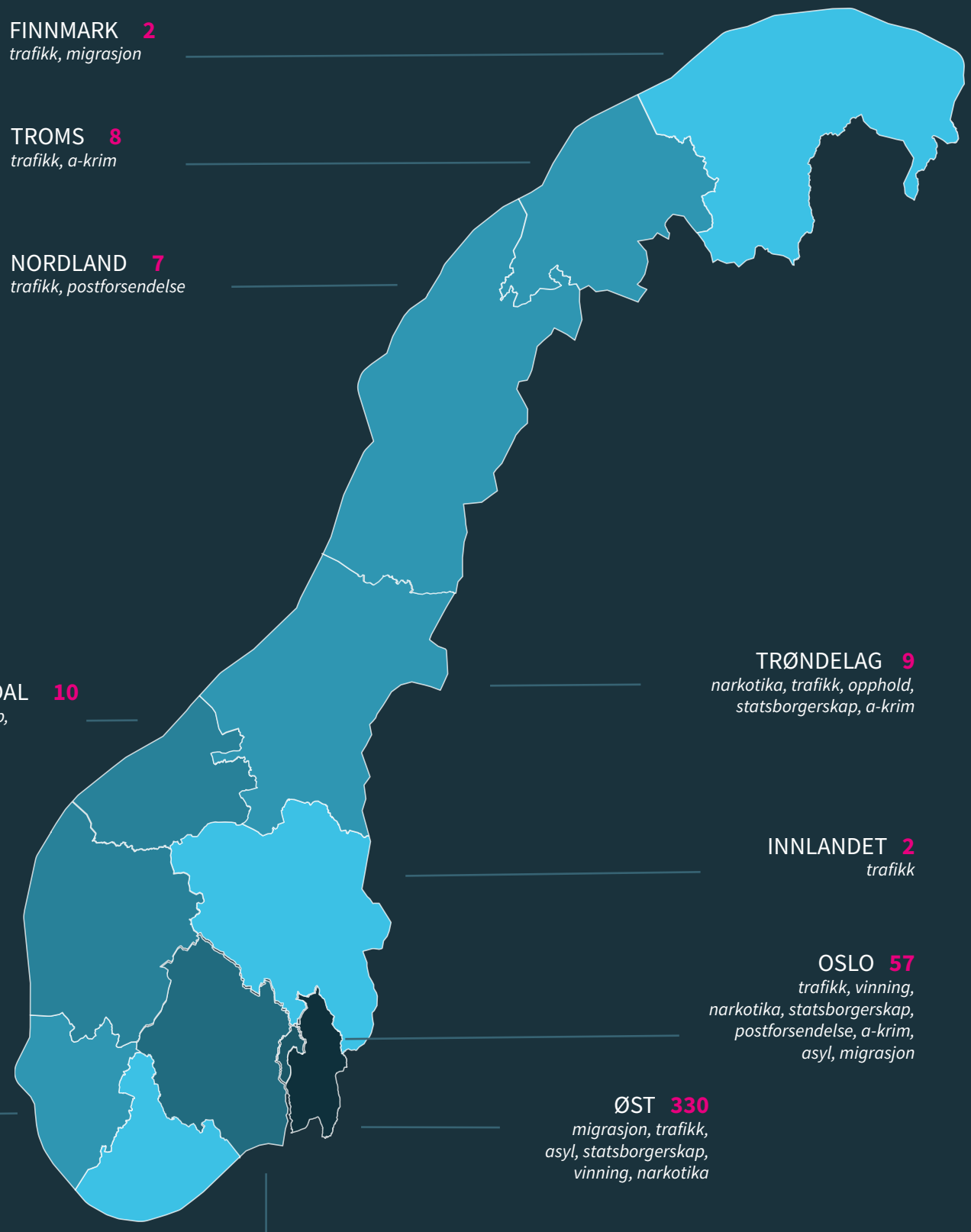
Det er en klar overvekt av tredjelandsborgere i statistikken. Mange i denne gruppen har misbrukt dokumenter fra eget eller andre tredjeland, men også dokumenter angivelig utstedt av land i EU/EØS eller Norge. Det er et antall personer i statistikken som vi ikke kjenner nasjonaliteten til og disse er ikke inkludert i denne fremstillingen.

Topp 10 dokumentnasjonaliteter



Dokumenter angivelig utstedt i EU/EØS og Norge utgjør litt over halvparten av de avdekkede dokumentene i 2025. Av dokumenter angivelig utstedt i tredjeland er Ukraina, Syria og Tyrkia på topp 10-listen.

Geografisk spredning og sakstyper



FINNMARK **2**
trafikk, migrasjon

TROMS **8**
trafikk, a-krim

NORDLAND **7**
trafikk, postforsendelse

TRØNDELAG **9**
narkotika, trafikk, opphold, statsborgerskap, a-krim

MØRE OG ROMSDAL **10**
trafikk, statsborgerskap, asyl, vinning

INNLANDET **2**
trafikk

VEST **10**
trafikk, migrasjon, vinning

OSLO **57**
trafikk, vinning, narkotika, statsborgerskap, postforsendelse, a-krim, asyl, migrasjon

SØR-VEST **6**
trafikk

ØST **330**
migrasjon, trafikk, asyl, statsborgerskap, vinning, narkotika

AGDER **3**
migrasjon, vinning

SØR-ØST **42**
trafikk, vinning, migrasjon, opphold, asyl

Å arbeide strukturert og forebyggende mot ID-misbruk er viktig, for godt ID-arbeid er et samfunnskritisk arbeid. Uten pålitelige identitetsavklaringer svekkes både rettssikkerheten, tilliten til forvaltningen og evnen til å ivareta nasjonal sikkerhet

Interessent- og brukeranalyse for Nasjonalt ID-senter (Oxford Research, 2025)

Innledning

Kripos og Nasjonalt ID-senter har siden 2020 arbeidet sammen for å skaffe til veie et helhetlig bilde over ID-misbruket i Norge og over misbruk av norske ID-dokumenter i utlandet. I løpet av disse årene har ID-misbruk blitt et stadig mer komplekst og dynamisk kriminalitetsområde. Digitaliseringen av både offentlige og private tjenester, konflikter i ulike deler av verden, personlig data på avveie, en rask utvikling i grensekryssende organisert kriminalitet og nye teknologiske muligheter bidrar til at trusselbildet utvikler seg raskt. For beslutningstakere i både offentlig og privat sektor er det derfor avgjørende å ha oppdatert kunnskap om hvordan kriminalitetsformen endres, hvilke drivere som påvirker utviklingen, og hvilke risikoer og sårbarheter som er strategisk mest relevante. For å forstå ID-misbruk er det også viktig å ha kunnskap om hvilke kriminalitetsområder fenomenet inngår i, og hvilke aktører som påvirker risikobildet.

ID-misbruk er et kriminalitetsverktøy som brukes på mange ulike samfunnsområder. Enkelte områder har stabile rutiner, god informasjonsflyt og struktur for registrering av ID-misbruk. Dette er typisk der en førstelinje kontrollerer eller registrerer personer. Dette skjer for eksempel i pass- og grensekontroller, ved registrering av søknader om beskyttelse, i søknader om skattekort og fødsels- eller d-nummer, og ved utstedelse av førerkort (Oxford Research, 2025). Samtidig finnes det mange områder der ID-misbruk er et sentralt kriminalitetsverktøy, men hvor manglende rutiner og fokus på ID gjør at vi ikke kjenner risikoene, sårbarhetene og omfanget av misbruket. Dette gjelder både i offentlig og privat sektor.

Til denne rapporten har vi mottatt informasjon fra flere ulike virksomheter som har ID som en prioritet i sitt arbeid, og som dermed også har god etatsspesifikk kunnskap om temaet. Blant de som har bidratt med informasjon til rapporten finner vi Arbeids- og velferdsdirektoratet (NAV), Brønnøysundregistrene, advokatfirmaet HELP, politidistrikter og særorgan, Skatteetaten, Statens vegvesen, Utlendingsdirektoratet (UDI), Utlendingsnemnda (UNE) og Utenriksdepartementet (UD). Deres kunnskap om ID-misbruk har vært fundamental for å gi et nyansert og oppdatert situasjonsbilde på ID-misbruk og vi er svært takknemlige for bidragene.

Formålet med rapporten er å gi et helhetlig bilde av dagens kriminalitetsbilde knyttet til ID-misbruk gjennom identifisering og beskrivelse av sentrale trender, aktører og drivkrefter, og synliggjøre hvilke aspekter ved utviklingen som har størst strategisk betydning for beslutningstakere i ulike virksomheter. Rapporten skal bidra med innsikt som kan brukes som grunnlag for strategiske vurderinger i relevante virksomheter, men den erstatter ikke etatenes egne analyser eller operative vurderinger.

Kripos og Nasjonalt ID-senter, mars 2026

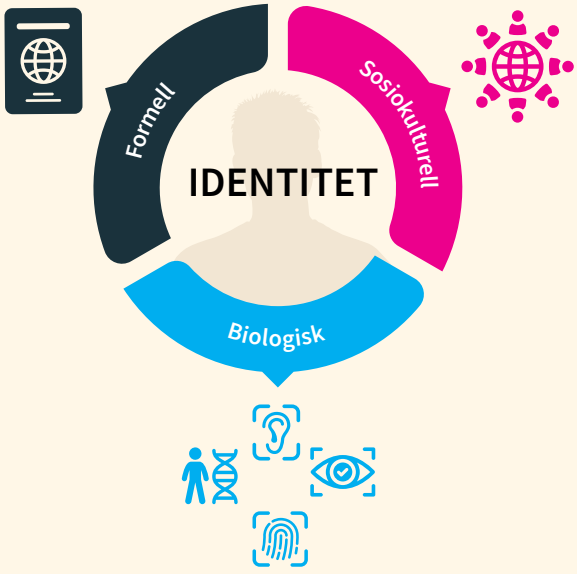
Hva er identitet?

At en befolkning består av personer med sikre og avklarte identiteter, er en grunnleggende forutsetning for utøvelsen av offentlige oppgaver. Dette reflekteres også i ID-forvaltningens målsetning om "én person - én identitet i Norge" (Kommunal- og distriktsdepartementet, 2023). Både offentlig forvaltning og tilgang til rettigheter og ytelser forutsetter at personer kan identifiseres på en pålitelig og etterprøvbar måte. Samtidig har misbruk av identiteter og dokumenter fått en stadig mer sentral rolle i ulike former for kriminalitet. For å forstå de ulike modusene for ID-misbruk som presenteres i denne rapporten, er det nødvendig med en presis begrepsavklaring. Dette kapittelet redegjør først for hvordan identitet forstås i rapporten, før begrepet ID-misbruk avgrenses. Deretter følger en beskrivelse av hvordan identitet kan fungere som et kriminalitetsverktøy, både på individnivå og som del av en bredere kriminell infrastruktur.

Identitetsbegrepet

Identitetsbegrepet brukes på tvers av en rekke fagdisipliner og spenner fra subjektive og selvopplevde forhold til objektive og formelle beskrivelser av en person. I rapporten avgrenses identitetsbegrepet til å omfatte identitet slik den forvaltes, dokumenteres og anvendes i offentlig sektor. Denne definisjonen av identitet kan inndeles i tre hovedkomponenter (Nasjonalt ID-senter, uten år):

1. **Formell identitet**
   Den delen av identiteten som er formalisert gjennom offentlige registre og ID-dokumenter. Dette omfatter blant annet opplysninger som fremgår av pass, som navn, fødselsdato, fødested, statsborgerskap/ nasjonalitet og kjønn.
2. **Biologisk identitet**
   En persons biologiske og genetiske opphav, som blant annet kommer til uttrykk gjennom fysiske kjennetegn og biometriske trekk.
3. **Sosiokulturell identitet**
   De delene av identiteten som kan endre seg gjennom livet og som formes av sosiale, kulturelle og samfunnsmessige forhold. Dette kan for eksempel være utdanning, arbeidserfaring, familiære relasjoner, klasse- eller gruppetilhørighet, politisk tilknytning, språk, livsstil og andre sosiale markører.



Identitet må altså forstås som et samspill mellom alle disse tre komponentene. De kan misbrukes hver for seg eller i kombinasjon, og gjør det mulig å konstruere, forsterke eller legitimere en falsk identitet. Misbruket kan også bestå i å konstruere en falsk historie rundt visse deler av identiteten.

Formell og biologisk identitet brukes i praksis sammen for å etablere og bekrefte en persons identitet i møte med offentlige og private systemer. Den formelle identiteten gir legitimitet og adgang gjennom ID-dokumenter, registre og digitale identitetsbevis, mens den biologiske identiteten brukes til å bekrefte at dokumentene tilhører riktig person gjennom en visuell sammenligning av for eksempel ansikt. Misbruk av de formelle og biologiske identitetskomponentene skjer for eksempel gjennom å søke asyl eller opphold i Norge med et forfalsket pass. Misbruk av den biologiske komponenten alene, kan skje om en person utgir seg for å være en annen ved å bruke denne personens ekte ID-dokumenter. Dette er en form for misbruk vi refererer til som imposter. Misbruk av den *sosiokulturelle komponenten* av identitet skjer typisk gjennom falske eller manipulerte attester, vitnemål og er særlig relevant i saker der formålet er å oppnå visse rettigheter, tillatelser eller ytelser som forutsetter en bestemt livssituasjon. Dette kan for eksempel skje ved å fremlegge falske dokumenter for utdanning og arbeidserfaring i en søknad om arbeidstillatelse. I slike tilfeller er det ikke uvanlig at det fremlegges ekte dokumenter som bekrefter den formelle og biologiske identitetskomponenten, men hvor de falske dokumentene konstruerer en fiktiv historie rundt den sosiokulturelle komponenten som gjør at personen oppfyller kravene til tillatelsen.

Hva er ID-misbruk?

Vår definisjon av ID-misbruk har utviklet seg i takt med endringer i kriminalitetsbildet og samfunnet ellers. I denne rapporten omfatter begrepet derfor både misbruk av fysiske ID- og underlagsdokumenter og misbruk av elektroniske identitetsbevis (eID).

ID-misbruk med bruk av fysiske dokumenter inkluderer blant annet:

- totalfalske eller forfalskede dokumenter
- totalfalske eller forfalskede digitale kopier av dokumenter
- misbruk av andres ekte ID-dokumenter (imposter)
- bruk av urettmessig utstedte dokumenter

Det er ikke et krav at en person skal være dømt for dokumentfalsk for at det inkluderes i vår statistikk over dokumentmisbruk. Det er tilstrekkelig at dokumentet er vurdert som totalfalskt eller forfalsket av en dokumentgransker. Det vil derfor være en forskjell mellom antallet personer som straffeforfølges for dokumentfalsk og tallene som presenteres i denne rapporten.

Misbruk av andre typer totalfalske eller forfalskede dokumenter som brukes til å skjule, endre eller konstruere deler av en identitet faller også innenfor vår definisjon av ID-misbruk når formålet er å oppnå rettigheter, tillatelser eller ytelser man ellers ikke har krav på. Dokumenter som ikke kategoriseres som ID-dokumenter, kalles ofte i rapporten for enten underlags- eller støttedokumenter.

Avslutningsvis omfatter ID-misbruk også opprettelse av falske identiteter i offentlige og private registre, samt utnyttelse av ekte identiteter i slike registre og deres tilhørende digitale identitetsbevis (eID).

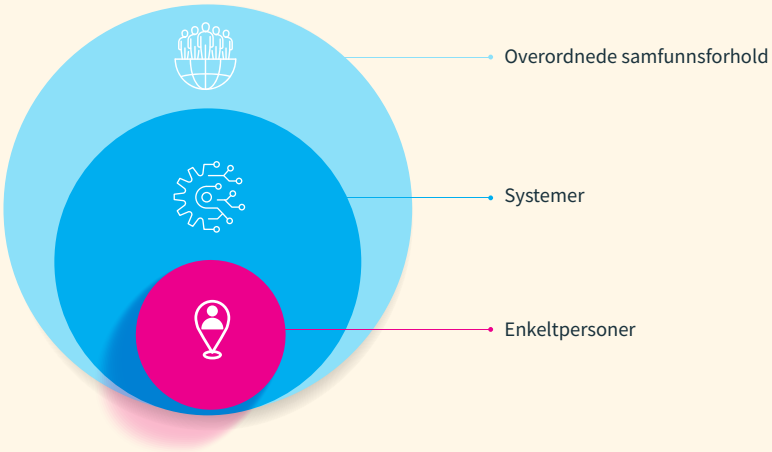
ID-dokumenter og identiteter i den kriminelle infrastrukturen

Europol definerer kriminell infrastruktur som de verktøyene og metodene som må være på plass for at kriminelle nettverk skal kunne utøve kriminalitet. I den nyeste trusselvurderingen av alvorlig organisert kriminalitet fremheves misbruk av legale forretningsstrukturer, utnyttelse av digital infrastruktur samt identiteter og dokumenter som viktige bestanddeler i infrastrukturen til europeiske kriminelle nettverk (Europol, 2025). Det er også et kjent trekk ved dagens kriminalitet at nettverk benytter seg av profesjonelle tilretteleggere som har spesialisert seg på å levere ulike tjenester til nettverkene, blant annet innen transport og logistikk, kryptert kommunikasjon og hvitvasking. Denne forretningsmodellen omtales ofte som «crime-as-a-service» (CaaS) (Politiet, 2023).

I nettverkene finnes også såkalte tilretteleggere som er spesialisert på svært avgrensede deler av infrastrukturen, for eksempel gjennom å fremskaffe produksjonsutstyr og materialer til fremstilling av falske dokumenter (Polismyndigheten, 2025). Andre gjennomfører datainnbrudd i databaser som inneholder personopplysninger og bilder av ID-dokumenter. Slike databaser finnes hos en lang rekke aktører, blant annet hos hoteller, reisebyråer, sosiale medier og finansinstitusjoner. Personopplysningene og bilder av ID-dokumenter selges videre til andre kriminelle aktører og nettverk, og brukes for eksempel til ID-tyverier og hvitvasking (Agenzia per l'Italia Digitale, 2025). Utnyttelsen av andres identiteter er også en metode for de kriminelle aktørene å skjule sine spor eller forlede politiet i sin etterforskning. Dette kan for eksempel skje ved at utbytte fra kriminalitet kanaliseres til ordinære bankkontoer eller kryptotjenester opprettet i andres identitet. Det finnes også eksempler på at unge personer rekrutteres via sosiale medier til å bruke identiteten sin til å opprette mobilabonnement og telefonnummer som de kriminelle nettverkene bruker til bedragerier (Telenor, 2024). I et slikt perspektiv er identitet en handelsvare som brukes både til å gjennomføre og til å skjule kriminalitet. Begge tilfeller medfører en risiko for at uskyldige tredjepersoner dras inn i alvorlig kriminalitet.

Sentrale drivkrefter for utviklingen i ID-misbruk

ID-misbruk som kriminalitetsfenomen er i konstant utvikling og både omfang og modus påvirkes av parallelle drivkrefter som virker på ulike nivåer. Fenomenet oppstår altså ikke som følge av én enkelt årsak, men utvikler seg i samspillet mellom individer, systemer og overordnede samfunnsforhold. I rapporten beskrives sentrale drivkrefter på tre nivåer: individ, gruppe og samfunn (illustrert i figur 1). I informasjonsinnhentingen til rapporten er de ulike virksomhetene bedt om å rapportere med utgangspunkt i drivkreftene som beskrives i det følgende.



Figur 1. ID-misbruk utvikler seg i samspillet mellom individer, systemer og overordnede samfunnsforhold og endringer i disse.

På samfunnsnivå påvirkes ID-misbruk av geopolitisk uro, konflikter og endringer i migrasjonsstrømmer. Ustabile regioner, korrupsjon blant ansatte i myndighetsorganer, grenseoverskridende kriminalitet og økt mobilitet bidrar både til tilbud og etterspørsel etter ekte, totalfalske og forfalskede dokumenter. Samtidig kan strengere innreise- og asylpolitikk øke risikoen for misbruk av legale migrasjonskanaler, blant annet gjennom bruk av falske underlagsdokumenter, korrupsjon eller utnyttelse av investeringsbaserte statsborgerskapsordninger.

Digitalisering og endret brukeratferd har samtidig flyttet store deler av identitetsforvaltningen over i digitale kanaler. Tilgang til eID er i dag en forutsetning for deltakelse i det norske samfunnet, noe som gjør digitale identiteter til attraktive mål for misbruk. Fremveksten av plattform- og delingsøkonomi har også skapt nye arenaer der identitetskontroll i stor grad baserer seg på selvregistrering og digitale tillitsmekanismer, og dermed åpner for bruk av falske eller stjålne identiteter.

På gruppe- og individnivå preges utviklingen av økt profesjonalisering og spesialisering blant kriminelle aktører. Kriminelle nettverk tilbyr i økende grad tjenester knyttet til identiteter og dokumenter som del av «crime-as-a-service», herunder salg av stjålne identiteter, forfalskede dokumenter og tjenester for registermanipulasjon. Teknologisk utvikling, inkludert kunstig intelligens, kan gjøre produksjonen av totalfalske ID-dokumenter mer overbevisende og vanskelige å avdekke i en kontroll.

Sentrale moduser for ID-misbruk

I dette kapittelet presenteres de modusene for ID-misbruk som har vært særlig fremtredende og av alvorlig art gjennom 2025. Disse er valgt fordi de illustrerer hvordan identitet misbrukes som et kriminalitetsverktøy på ulike måter:

- gjennom utnyttelse av offentlige registre og systemer for økonomisk vinning
- gjennom målrettet kriminalitet mot enkeltpersoner gjennom bedragerier. og
- gjennom misbruk av regelverk og legale ordninger for migrasjon.

Modusene har også til felles at vi forventer at de vil utgjøre en vedvarende trussel og/eller utvikle seg i både omfang og karakter det neste året.

I arbeidet med dette kapittelet er det særlig to forhold ved det norske samfunnet som har pekt seg ut som muliggjørere for den mest alvorlige og fremtredende kriminaliteten på ID-feltet: tillit og digitalisering. Disse to utgjør et viktig bakteppe for å forstå flere av modusene som presenteres i rapporten og forklares derfor på kapittelets start. Deretter følger beskrivelser av de tre utvalgte modusene for ID-misbruk og rapporten avsluttes med noen avsluttende refleksjoner.

ID-misbruk i et tillitsbasert og digitalisert samfunn

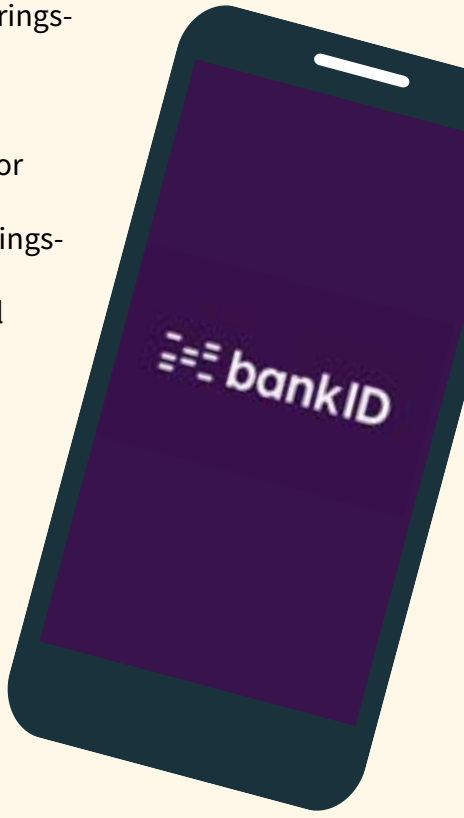
Norge ligger helt i verdenstoppen når det gjelder befolkningens tillit – både til hverandre og til offentlige myndigheter (Digitaliseringsdirektoratet, 2024). Innrapporteringen til denne rapporten viser at kriminelle aktører utnytter denne tilliten systematisk i forbindelse med ID-misbruk. Det skjer blant annet ved at de utgir seg for å være myndigheter i møtet med ofre i bedragerisaker, eller ved at de skjuler seg bak lovlydige personers identiteter i offentlige, digitale registre og systemer. I modusene som presenteres i dette kapittelet er misbruk av tillit et sentralt virkemiddel for de kriminelle aktørene, men tilliten angrepes fra ulike vinkler:

- myndighetenes tillit til innbyggerne,
- innbyggernes tillit til myndighetene og andre sentrale samfunnsfunksjoner som for eksempel finansinstituasjoner,
- og den gjensidige tilliten mellom innbyggere.

Tillit handler «(…) mest grunnleggende om å kunne stole på noen i situasjoner preget av usikkerhet eller risiko» (Krokan, 2019). Risikoelementet innebærer en sårbarhet for tap av noe man anser som viktig. I konteksten av ID-misbruk er dette ofte økonomi, tilganger og legitimitet, både som profitt for kriminelle og som tap for enkeltpersoner og institusjoner.

Tillit og digitalisering i det norske samfunnet

Tillit kan sies å være en grunnstein i det norske samfunnet. Den høye tilliten muliggjør enkle, raske og smidige prosesser i offentlige løsninger (Digitaliserings- og forvaltningsdepartementet, 2024). I tillegg til å være i verdenstoppen på tillit, er Norge blant Europas mest digitaliserte land og har som mål å bli det mest digitaliserte landet i verden innen 2030 (Digitaliserings- og forvaltningsdepartementet, 2024). Tillit er et fortrinn i dette arbeidet, men for at den skal fortsette å holde seg høy, må digitale løsninger ha kvalitet, være tilgjengelige og brukervennlige og utvikles innen trygge rammer (Digitaliserings- og forvaltningsdepartementet, 2024). En annen viktig side av dette er at digitaliseringen av offentlige tjenester er nødvendig for at forvaltningen skal kunne sikre effektivitet og sikre likebehandling i saker (NAV, 2025).



En forutsetning for å nå målsetningen om å bli det mest digitaliserte landet i verden, er den høye utbredelsen av eID i den norske befolkningen (Kommunal- og distriktsdepartmentet, 2023). Det er i dag BankID som er den mest brukte løsningen med om lag 4,6 millioner brukere (Stø, 2025). Tilgang på en eID er selve nøkkelen til deltakelse i det norske samfunnet. Innlogging med eID brukes til alt fra å ha tilgang til helsejournaler, til registrering av skilsmisse, til leie av bolig via Finn.no og overføring av utbytte fra Trumf-kontoen (FAFO, 2025; SODI, 2025). En rekke profesjoner bruker også sin private eID til innlogging på tjenester som brukes i forbindelse med arbeid, for eksempel for advokater for å få tilgang til straffesaksdokumenter gjennom Aktørportalen og for leger til å registrere dødsfall.

Misbruk av tillit er sentralt angrepspunkt for de kriminelle aktørene. De utnytter myndighetenes tillit til innbyggerne, innbyggernes tillit til myndighetene og andre sentrale samfunnsfunksjoner, og den gjensidige tilliten mellom innbyggere

I Norge finnes det flere private tilbydere av eID-løsninger der BankID, Commfides og Buypass ligger på det høyeste sikkerhetsnivået (Digitaliseringsdirektoratet, uten år). Digitaliseringsdirektoratet har ansvar for den offentlige utstedte MinID som ligger på det nest høyeste sikkerhetsnivået. Dette er et offentlig tilbud som kan brukes av personer som ikke oppfyller kravene til en eID på det høyeste sikkerhetsnivået (Digitaliseringsdirektoratet, uten år). Forskjellen mellom dem er at eID-løsningene på høyeste sikkerhetsnivå gir tilgang til et større tjenestetilbud enn de på de lavere nivåene. Det er de ulike tjenesteeierne som fastsetter hvilket sikkerhetsnivå som kreves for innlogging til tjenesten. En tjenesteeier kan for eksempel være HelseNorge eller Finn.no. Det er per i dag over 5000 offentlige tjenesteeiere som bruker eID som innlogging til sine tjenester (Digitaliseringsdirektoratet, 2025). At den norske befolkningen består av personer som ikke oppfyller kravene til eID på høyeste sikkerhetsnivå, har konsekvenser for den enkeltes deltakelse i samfunnet og mulighetene for blant annet integrering. FAFO fremhever i en nylig publisert rapport at personer med d-nummer ofte møter praktiske sperrer for å få utstedt en eID på høyeste sikkerhetsnivå og at de dermed for eksempel ikke har mulighet til å opprette depositumskonto for leie av bolig i Norge (FAFO, 2025).

Opprinnelig ble BankID utviklet i 2004 som felles infrastruktur for sikker pålogging i bank, men har gjennom sterk brukervekst og nettverkseffekter blitt en de facto nasjonal identitetsinfrastruktur i fraværet av en offentlig utstedt eID på høyeste sikkerhetsnivå. Et annet viktig ledd i digitaliseringsprosessen rundt identitet, er at digitaliseringen har ført til muligheter for økt anonymitet ettersom det blir stadig færre fysiske kontaktpunkt mellom myndighetene og innbyggerne. Denne anonymiteten gjør det enklere for kriminelle aktører å skjule eierskap til, eller kontroll over, virksomheter og falske identiteter som benyttes som verktøy i kriminell aktivitet (Polismyndigheten, 2025). Riksrevisjonen har også pekt på at økt digitalisering av offentlige og private utbetalingsordninger, for eksempel innen merverdiavgift, har endret risikobildet ved å muliggjøre misbruk i større omfang enn tidligere (Riksrevisjonen, 2025). Dagens identitetsforvaltning i Norge er derfor preget av en digitaliseringsprosess med målsetning om å gjøre alt mer sikkert og effektivt, men som dessverre også har åpnet opp for nye trusler, sårbarheter og større handlingsrom for misbruk av kriminelle aktører.

EKSEMPEL: digitale arbeidsplattformer

Også arbeidsplassene blir i stadig større grad digitale. Det kan medføre en risiko for at virksomheter ikke har tilstrekkelig kontroll på hvem som egentlig jobber for firmaet, for eksempel gjennom at flere personer jobber i samme identitet/bruker eller at det benyttes enkeltpersonforetak i stedet for tradisjonelle ansettelsesforhold. Tidligere gjaldt dette spesielt matleveringstjenester som eksempelvis Wolt og Foodora, men denne typen arbeidsform, og dermed samme risiko for misbruk, har nå også utbredelse i andre bransjer som for eksempel transport- og drosjebransjen med aktører som Uber og Bolt (Skatteetaten, 2025).

Parallelle EU-drevne digitaliseringsprosesser

På samme tid som denne digitaliseringsprosessen har pågått i forvaltningen, har det også skjedd store ting på området for grensekontroll i Norge og Schengen. I grenseforvaltningen ble Schengens Entry/Exit System (EES) faset inn fra oktober 2025. Dette er et system som registrerer biometri og grensepasseringer for tredjelandsborgere (EU, 2025; Politiet, 2025c). EES har som hovedmål i å blant annet forebygge at personer oppholder seg lenger i Schengen enn den perioden de er innvilget, og skal bidra til at ID-misbruk avdekkes på grensen. I forbindelse med utrulling av EES er de norske og europeiske grensene i økende grad basert på bruk av teknologiske løsninger som automatiserte grensekontrollporter (ABC-gates), ansiktssammenligningssystemer og elektroniske passlesere (EU, 2025).

Det er også andre store EU-prosjekter innen digitalisering og identitet på gang. Dette gjelder for eksempel eIDAS 2.0 som blant annet innebærer innføringen av digitale identitetslommebøker som skal fungere på tvers av medlemslandene i EU/EØS (Digitaliseringsdirektoratet, 2024). Digitaliseringsdirektoratet er ansvarlig for en konseptvalgutredning (KVU) som skal vurdere ulike alternative løsninger for identitetslommeboken. Formålet med KVUen er: "(...) å utrede hvilke konsepter som er best egnet til å oppfylle regjeringens mål om at eID på høyt sikkerhetsnivå kan gjøres tilgjengelig for flere og mål om å tilby alle en digital lommebok med eID." (Digitaliseringsdirektoratet, 2025b). De øvrige EU-landene har frist om å implementere den digitale lommeboken innen 21. november 2026, men det er per i dag ikke satt en frist for Norge.

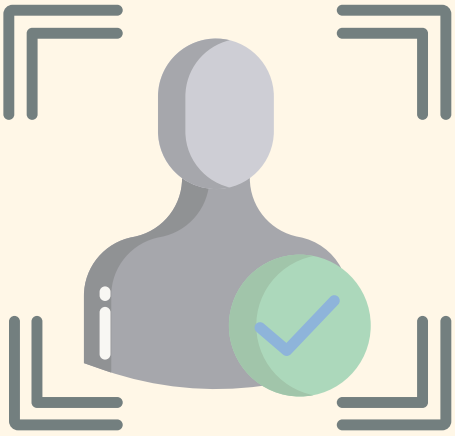
I tillegg har EU vedtatt et nytt førerkortdirektiv som vil medføre at digitale førerkort rulles ut til hele EU innen 2030. Det digitale førerkortet vil være en del av den europeiske identitetslommeboken (Regjeringen, 2025). Statens vegvesen fremhever i sitt svar til rapporten at man som følge av disse endringene bør være oppmerksomme på digitale forfalskninger av førerkort i tiden som kommer. Det er også grunnlag for videre analyser og risikovurderinger av hvordan disse digitaliseringsprosjektene endrer ID-misbrukets natur på generell basis i Norge.

ID-misbruk og registerkriminalitet

Registerkriminalitet eller registermanipulasjon har blitt et stadig større problem innen økonomisk kriminalitet og anses som å være en trussel mot velferdsstaten (NTAES, 2024; Politiet, 2025b). Registerkriminalitet skjer ved at kriminelle bevisst rapporterer inn feilaktige eller fiktive grunnlagsopplysninger til myndighetenes tillitsbaserte systemer, som skal brukes for å verifisere personers eller foretaks identitet og aktiviteter. At systemene er tillitsbaserte innebærer at myndighetene legger til grunn at den selvrapporterte dataen er korrekt. Gjennom å opprette selskaper ved utnyttelse av andres identiteter kan kriminelle aktører skaffe seg uberettigede offentlige utbetalinger, banklån eller andre økonomiske fordeler (Politiet, 2025b). Denne typen kriminalitet inngår ofte i mer omfattende kriminelle strukturer, inkludert hvitvasking av penger, og muliggjøres på grunn av svakheter i regelverk, et ensidig fokus på brukervennlighet i digitale løsninger og mangelfull informasjonsdeling mellom offentlige etater (NTAES, 2024).

Europol har pekt på at EU-baserte og nasjonale tilskudds- og støtteordninger er attraktive mål for profittmotivert kriminalitet, særlig i situasjoner der myndigheter raskt etablerer ordninger for å håndtere ekstraordinære hendelser (Europol, 2025). Kriminelle nettverk forventes å utnytte situasjoner der bedrifter eller enkeltpersoner har rett på økonomisk støtte, spesielt når kontrollmekanismer er svake eller nedprioritert i oppstartsfasen. Dette bekreftes av NAV, som i etterkant av koronapandemien har påpekt at nye ytelsesordninger innebærer betydelig risiko for misbruk uten tilstrekkelige tiltak i forkant (NAV, 2025). Under koronapandemien ble for eksempel den tillitsbaserte lønnskompensasjonsordningen, med automatisk saksbehandling basert på arbeidsgivers innrapportering i a-meldingen, utnyttet til å registrere fiktive arbeidsforhold og utløse utbetalinger ved bruk av andres identiteter. I ett tilfelle ble en person dømt for å ha svindlet til seg nærmere ti millioner kroner etter å ha utnyttet identitetene til over 300 personer (Aftenposten, 2021). Modusene som opprinnelig oppsto i forbindelse med pandemien, observeres fremdeles i dag (NAV, 2025).

Både Arbeidstilsynet, Brønnøysundregistrene, NAV og Skatteetaten har fremhevet denne formen for kriminalitet i sine svar til denne rapporten og ser utfordringen fra ulike perspektiver ut ifra sitt samfunnsoppdrag. Arbeidstilsynet beskriver utnyttelse av sårbare personer og manipulering av offentlige digitale registre innen sitt ansvarsområde (Arbeidstilsynet, 2025). Skatteetaten erfarer at identiteter blir misbrukt og er under andres kontroll, gjennom at de har blitt tiltvunget, stjålet, kjøpt eller tilegnet på annet vis (Skatteetaten, 2025). For NAV knyttes denne formen for kriminalitet hovedsakelig til feilaktige utbetalinger av velferdsytelser (NAV, 2025). For Brønnøysundregistrene omhandler denne kriminalitetsformen både registrering av selskaper og virksomheter som driver fiktiv aktivitet og registrering ved misbruk av identiteter. Virksomhetene og organisasjonsnumrene brukes så som et ledd i kriminaliteten (Brønnøysundregistrene, 2025).



Registerkriminalitet skjer ved at kriminelle bevisst rapporterer inn feilaktige eller fiktive grunnlagsopplysninger til myndighetenes tillitsbaserte systemer. Gjennom å opprette selskaper ved utnyttelse av andres identiteter kan kriminelle aktører skaffe seg uberettigede offentlige utbetalinger, banklån eller andre økonomiske fordeler

Denne formen for kriminalitet rammer derimot ikke bare det offentlige. En viktig del av modusene er også låneopptak i finansinstituasjoner via såkalte samtykkebaserte lånesøknader (Oslo politidistrikt, 2025). I samarbeid med finansinstitusjonene stanset Oslo politidistrikt i løpet av 2024 slike søknader til en samlet verdi av minst 46 millioner kroner. DNB skriver i sin årsrapport for 2025 at de har observert en dobling i antallet rapporterte forhold om hvitvasking knyttet til blant annet trygdeordninger og konkurskriminalitet, med samlede beløp i millionklassen. Til grunn ligger blant annet uriktig selskapsinformasjon, bruk av stråpersoner og eID-misbruk, i det som beskrives som et «profesjonalisert økosystem» (DNB, 2025).

Registerkriminalitet rammer altså både det offentlige og det private, men den er heller ikke bare lokal. Svenske myndigheter har observert den samme utviklingen og beskriver trusselen som både økende og alvorlig (Regeringen, 2025). I en rapport om det svenske situasjonsbildet på organisert kriminalitet fra 2025 beskrives det at den profittjagende organiserte kriminaliteten fungerer som en «parasitt» på de svenske samfunnsfunksjonene (Polismyndigheten, 2025). Svenske myndigheter beskriver også at denne kriminalitetsformen har koblinger til andre former for kriminalitet vi ikke tidligere har koblet til ID-misbruk, som for eksempel miljø- og avfallskriminalitet. Dette gjøres for eksempel ved at falske dokumenter og uriktige identiteter misbrukes for å unngå å bli oppdaget i tollkontroller (Polismyndigheten, 2025). Det er ikke kjent hvorvidt dette fenomenet kan kobles til miljø- og avfallskriminalitet ved Norges grenser, men tematikken knyttet til ID-misbruk er ikke nevnt i Tolletatens åpne trusselvurdering (Tolletaten, 2025).

Økokrim skriver imidlertid i sin trusselvurdering på miljøkriminalitet at anonymiseringsteknologi og digitale betalingsløsninger gir «(…) økt mulighet til å skjule identitet og transaksjoner, og kamuflere den økonomiske gevinsten fra miljøkriminalitet. Slik kan ulovlig virksomhet fremstå som lovlig og omgå toll- og kontrollregimer» (Økokrim, 2025). Undersøkelser i politiets registre viste også et interessant funn. En typisk indikasjon på registerkriminalitet er boligadresser med mange personer og virksomheter registrert på adressen. Politiet gjennomførte i 2025 en kontroll av en bolig der det var registrert 39 utenlandske borgere og 33 virksomheter på adressen. På plassen ble det også funnet avfall og spesialavfall av ukjent opprinnelse og en av beboerne på adressen brant deler av avfallet på et bål.

EKSEMPEL: Russisktalende nettverk i Sverige og omgåelsesekteskap

I Sverige er det også avdekket at et russisktalende nettverk som har vært svært aktivt innen registermanipulasjon, også har utnyttet identiteter i forbindelse med omgåelsesekteskap. Et omgåelsesekteskap er et ekteskap som inngås med formål om å skaffe oppholdstillatelse. De utnyttede identitetene er benyttet til å gifte seg med tredjelandsborgere som skal utvises fra Sverige eller med andre som ønsker opphold i landet (Polismyndigheten, 2025; Polismyndigheten, 2023; Sveriges radio, 2023). Vi er per i dag ikke kjent med at dette har forekommet i Norge.

Utviklingen har også en annen alvorlig side. Tidligere var økonomisk kriminalitet som oftest knyttet til hvitsnippkriminalitet uten særlig voldspotensiale. I dag er denne kriminaliteten derimot tett knyttet til organiserte kriminelle nettverk og aktører med høyt voldskapasitet (DNB, 2025). Politiets trusselvurdering for 2025 fremhever at denne formen for kriminalitet er «(...) samfunnstruende fordi den har vesentlige økonomiske konsekvenser for samfunnet, og potensielt store negative konsekvenser for enkeltpersoner som blir rammet eller utnyttet» (Politiet, 2025b). Prosjektet «Societal Security and Digital Identities» (SODI) ved Universitetet i Oslo har i en årrekke utforsket utfordringer knyttet til den digitale identitetsforvaltningen og eID i Norge og skriver i sin sluttrapport at problemene i den digitale identitetsforvaltningen i dag er så komplekse og omfattende at det på sikt kan komme til å utgjøre et alvorlig samfunnssikkerhets- og beredskapsproblem (SODI, 2025). NTAES (2024) sin rapport om registermanipulasjon gir en god oversikt over de samfunnssmessige forholdene rundt denne formen for kriminalitet. For å komplementere kunnskapen som allerede finnes i en lang rekke produkter, vil denne rapporten i det følgende fokusere på aktørbildet innen registerkriminaliteten og identitetsutnyttelsen.

Aktørbilde og utnyttede identiteter

For å kunne hente ut profitt fra denne kriminalitetsformen er kriminelle aktører avhengige av legale selskaper eller virksomheter hvor det innrapporteres fiktive eller falske opplysninger som gir inntrykk av reell virksomhet (Politiet, 2025b). Aktørbildet er sammensatt og varierer fra sak til sak, både når det gjelder omfang og grad av organisering. Enkelte saker kjennetegnes av involvering av mange personer, mens andre strukturer driftes av maksimalt én eller to personer. En analyse av kjente saker i politiets registre, supplert med en dom fra Midtre Hålogaland tingrett i 2025, indikerer at det hovedsakelig kan identifiseres fire roller eller funksjoner blant de kriminelle aktørene som bedriver registerkriminalitet:

1) **kriminelle entreprenører**
2) **profesjonelle tilretteleggere**
3) **operative hjelpere**
4) **stråpersoner/utnyttede identiteter**

Rollene og rollenavnene må forstås som analytiske kategorier. I praksis kan én og samme person fylle funksjon 1-3 og fordelingen kan også endre seg over tid. En nærmere beskrivelse av de ulike rollene følger på neste side.

Den kriminelle entreprenøren

De kriminelle entreprenørene planlegger og orkestrerer opplegg som kombinerer legale selskaper og virksomheter med innrapportering av fiktiv aktivitet på utnyttede identiteter. Disse aktørene har normalt høy kontroll over verdistrømmene og lav direkte eksponering mot myndighetene fordi de skjuler handlingene sine bak de utnyttede identitetene.

Den profesjonelle tilretteleggeren

Profesjonelle tilretteleggere bistår gjennom fagkompetanse, posisjon eller tilgang til sentrale funksjoner, til å muliggjøre eller opprettholde strukturer for registermanipulasjon. Tilretteleggerne kan for eksempel være regnskapsførere, revisorer, advokater, politikere og nåværende eller tidligere ansatte i statlige funksjoner (Oslo politidistrikt, 2025). Bistanden kan gjelde selskapsopprettelse, regnskapsføring, økonomisk rådgivning, kontraktsutforming eller håndtering av finansielle transaksjoner. Enkelte tilretteleggere markedsfører tjenestene sine via sosiale plattformer.

Den operative hjelperen

Operative hjelpere bistår blant annet med rekruttering av stråpersoner, innhenting av ID-dokumentene deres, bestiller timer for registrering av den utenlandske borgeren og følger personen til avtalen. I flere saker observeres det at hjelperen behersker samme språk som personene de rekrutterer og bistår med oversettelse i skranken. I større opplegg har denne funksjonen muligens mindre innsikt i den samlede virksomheten, og er samtidig vesentlig mer eksponert for myndighetene enn entreprenører og tilretteleggere.

Stråpersonene eller de utnyttede identitetene

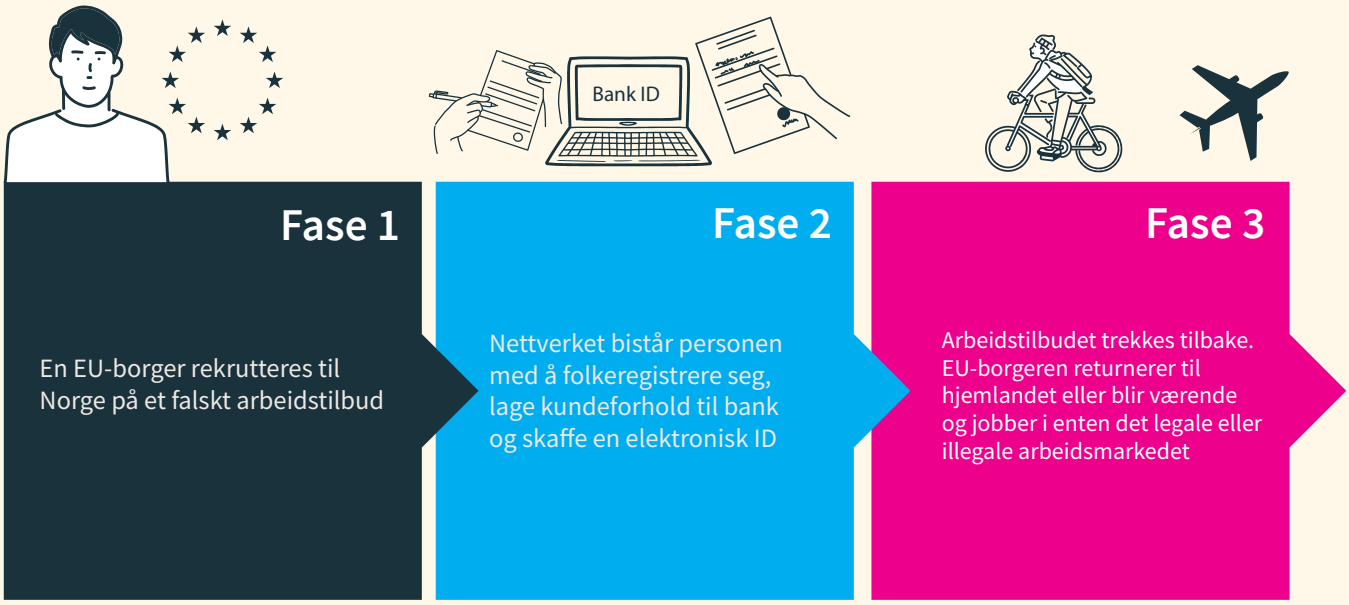
Stråpersoner eller utnyttede identiteter brukes som formelle eiere, styremedlemmer, daglige ledere eller kontohavere i selskapene. Identitetsmisbruket kan skje med eller uten personens samtykke og viten, og mange er EU-borgere som befinner seg i sårbare livssituasjoner, for eksempel knyttet til økonomi, språk eller oppholdsstatus (Arbeidstilsynet, 2025). Det forekommer også salg av «pakkeløsninger» som trekker disse personene til Norge, blant annet med mottak ved ankomst til landet, bistand til registrering hos Skatteetaten, arbeidskontrakt, telefonnummer og bostedsadresse, ofte mot betaling og med påfølgende gjeldsforpliktelser. Det er ikke uvanlig at identitetene omsettes mellom ulike kriminelle nettverk når de er blitt registrert (SODI, 2025).

Utnyttelse av andres identiteter

Utnyttelse av andres identiteter er et helt sentralt element i denne kriminalitetsformen. Identitetsmisbruket gjør det mulig for den kriminelle entreprenøren å distansere seg fra den faktiske kriminaliteten og redusere risikoen for straffeforfølgelse. Rekrutteringen skjer ofte blant sårbare EU/EØS-borgere som, i kraft av prinsippet om fri bevegelighet innen Schengen, har rett til å bo og arbeide i Norge. I flere norske saker går rumenske borgere igjen, men både identiteter fra andre nasjonaliteter og norske borgere forekommer. Personene som får sine identiteter misbrukt har ofte lav digital kompetanse, lese- og skrivevansker og begrensede språkferdigheter, noe som gjør dem særlig utsatt for å overlate identiteten til såkalte «hjelpere» eller arbeidsgivere (Arbeidstilsynet, 2025; Skatteetaten, 2025; SODI, 2025).

Fair Play Bygg beskriver i SODIs rapport at sårbare grupper blant arbeidsinnvandrere og personer i rusmiljøer er spesielt utsatt for omfattende identitetsmisbruk. I enkelte tilfeller utsettes de for press, tvang eller vold for å gi fra seg identitetsopplysningene sine, i det som omtales som et «moderne slaveri» (SODI, 2025). Fremgangsmåten fremstår som systematisk og langsiktig: kriminelle nettverk bygger opp troverdige historikker rundt utnyttede identiteter på tvers av saker og landegrenser, noe som indikerer en målrettet og profesjonalisert modus (Ekobrottsmyndigheten, 2025; Europol, 2025)

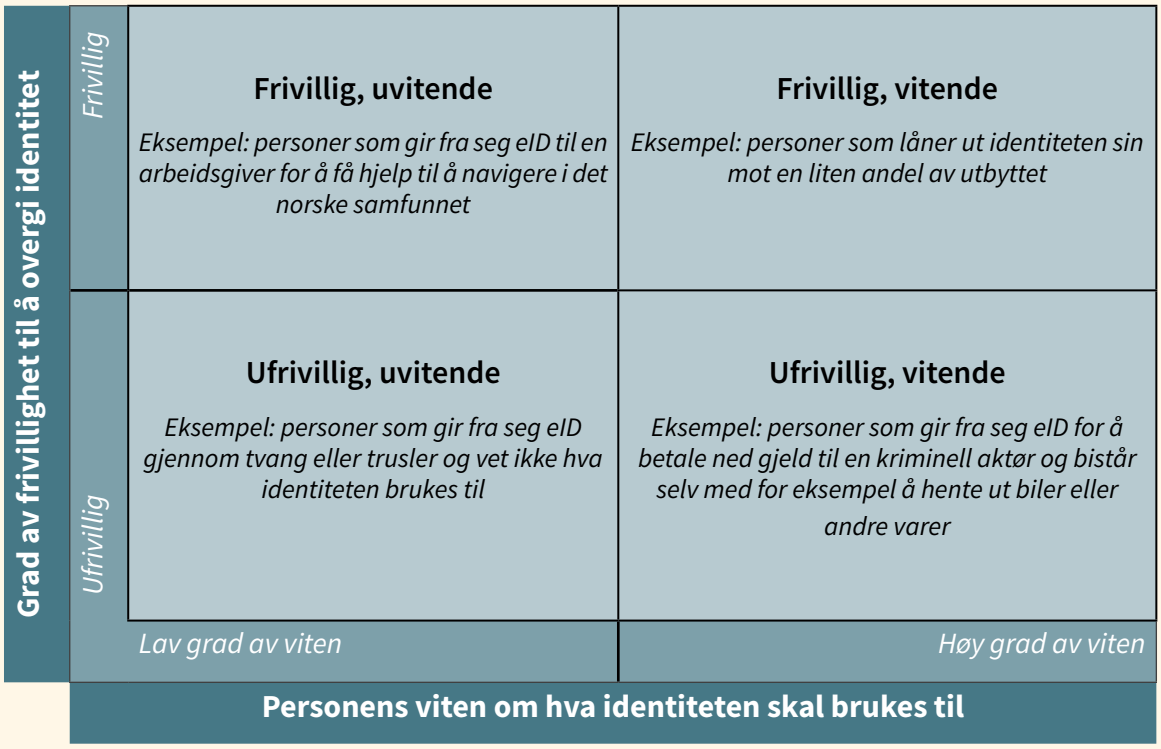
Det er også vanlig at flere identiteter med opprinnelse fra samme land registreres på de samme bostedsadressene i Folkeregisteret. Uformelle kontroller viser ofte at det ikke er fysisk mulig for så mange personer å bo på eiendommen. Brønnøysundregistrene har i tillegg observert at personer med d-nummer uten fast oppholdssted i Norge, benytter digitale markedsplasser, som Finn.no, for å finne adresser som kan brukes for registrering av virksomhetene. Dette gjelder for eksempel adresser knyttet til større boligprosjekter eller eiendommer som ligger ute for salg (Brønnøysundregistrene, 2025).



Figur 2. En forenklet illustrasjon av prosessen bak rekruttering av EU-borgere som får identiteten sin utnyttet i registermanipulasjon i Norge. Denne prosessen er basert på dommen som presenteres på side 27.

Ulike grader av medvirkning til utnyttelse av identitet

Analysene som ligger til grunn for rapporten viser at utnyttede identiteter befinner seg på et bredt spekter, både når det gjelder grad av kunnskap om utnyttelsen og hvorvidt identitetsopplysningene er overlatt frivillig. Dette spekteret er illustrert i firefeltsdiagrammet nedenfor, som kombinerer graden av frivillighet med graden av viten om hva identiteten skal brukes til. Det er viktig å påpeke at denne fremstillingen er analytisk og forenklet. I praksis beveger både frivillighet og viten seg langs et kontinuum fra fullt frivillig til fullt ufrivillig, og fra fullstendig vitende til fullt uvitende.



Figur 3. Diagrammet illustrerer analytiske kategorier for hvorvidt utnyttede identiteter har kunnskap om hva identiteten deres misbrukes til og hvorvidt de har gitt fra seg identitetsopplysninger eller eID frivillig.

De frivillige, men uvitende identitetene fremstår som den mest dominerende gruppen innen denne modusen. Dette underbygges både av saksgjennomgangen og rapporteringen til rapporten. Eksempler på denne modusen er tilfeller der arbeidstakere blir lurt til å gi fra seg ID-dokumenter og eID-opplysninger til arbeidsgiver, ofte under påskudd om hjelp til navigering i det norske systemet. Identiteten brukes deretter til å opprette selskaper i arbeidstakerens navn, samt til å kjøpe varer og tjenester på kreditt, uten arbeidstakerens viten og uten forståelse for det formelle ansvaret som følger med eierskap og gjeld (Fri fagbevegelse, 2024; Dagens Næringsliv, 2025). Dette er også et eksempel som viser hvordan tillit mellom individer misbrukes for å gjennomføre kriminalitet.

Arbeidstilsynet rapporterer at de i kontroller møter disse formelle bedriftseierne, som da fremstår som ordinære arbeidstakere uten kunnskap om virksomhetens drift og omtaler den reelle driveren av selskapet som sin «sjef» (Arbeidstilsynet, 2025).

Mange av de utenlandske borgerne som får sin identitet misbrukt er registrert med d-nummer i Norge. Et d-nummer er et midlertidig norsk identitetsnummer som gis til personer med kortvarig eller begrenset tilknytning til Norge, for eksempel ved midlertidig arbeid eller andre formelle oppdrag. Det tildeles utenlandske personer som oppholder seg i Norge i mindre enn seks måneder, eller som oppholder seg lenger, men ikke oppfyller vilkårene for å få et fødselsnummer. En rekke virksomheter og etater kan rekvirere d-nummer til en utenlandsk borger, som for eksempel Skatteetaten, NAV, Kartverket, Brønnøysundregistrene og banker (Skattetaten, uten år). Skatteetaten usteder MinID til mange av disse utenlandske arbeidstakerne i Norge i forbindelse med oppmøte for ID-kontroll og søknad om skattekort. I enkelte tilfeller avdekker etaten at det gis uriktige opplysninger, blant annet om kontaktinformasjon. I enkelte tilfeller viser det seg at MinID benyttes av andre personer enn av rettmessig eier (Skatteetaten, 2025).

Gruppen *frivillig og vitende* er mindre fremtredende, men er særlig observert i én spesifikk modus: misbruk av lønnskompensasjonsordningen under koronapandemien. Ordningen, som ble administrert av NAV, var basert på automatisert saksbehandling og arbeidsgivers innrapportering i a-meldingen, med mål om rask utbetaling. Kriminelle aktører utnyttet dette ved å opprette selskaper med fiktive identiteter og falske lønnsinnberetninger, og ordningen spredte seg raskt i ulike kriminelle miljøer (NAV, 2025). Det finnes også tilfeller der personer frivillig overlater sine personopplysninger mot betaling, men uten nødvendigvis å ha full innsikt i hvordan identiteten videre misbrukes (Arbeidstilsynet, 2025). Dette kan for eksempel gjelde utenlandske borgere som planlegger å forlate Norge, som kan selge identiteten for et mindre beløp.

Kategorien *ufrivillig og uvitende* ble også observert i lønnskompensasjonsbedrageriene. I ett tilfelle benyttet en gjerningsperson personnumrene til nærmere 300 stjålne identiteter, som ble registrert i ulike selskaper og brukt til å søke om lønnskompensasjon (Aftenposten, 2021; Nettavisen, 2021). Personer som er utsatt for ID-tyverier er derfor relevante innen denne kategorien. NRK publiserte for eksempel i 2024 en sak om en kvinne som opplevde at hennes identitet ble benyttet av kriminelle uten at hun hadde kunnskap om det. Gjennom fiktive lønnsinnberetninger fremsto den kreftsyke og pensjonerte kvinnen som at hun var i arbeid, og identiteten ble brukt til både handel av varer og lånopptak (NRK, 2024). Informasjon fra HELP til denne rapporten viser at personer som får identiteten sin misbrukt på denne måten risikerer å miste sine offentlige ytelser, fordi de står med fiktiv inntekt i offentlige registre (HELP, 2025). Kategorien omfatter også identiteter som er tilegnet gjennom tvang eller trusler, eksempelvis for å nedbetale gjeld til en kriminell aktør, uten at den berørte personen har kunnskap om hvordan identiteten brukes.

I kategorien *ufrivillig, men vitende* inngår personer som gir fra seg identitetsopplysningene sine under press eller tvang, og som i enkelte tilfeller også tvinges til å delta aktivt i kriminaliteten. Dette kan for eksempel innebære å hente ut kjøretøy eller andre verdier i eget navn, til tross for at de er klar over at handlingene er ledd i kriminalitet. Det legges derimot ikke til grunn at personene innen denne kategorien har fullstendig innsikt i hva den kriminelle aktiviteten er.

Konkret eksempel på selskapsstrukturer opprettet med utnyttede identiteter

I 2025 falt en dom i Midtre Hålogaland tingrett som illustrerer denne modusen godt. I den konkrete saken ble utenlandske borgere, hovedsakelig fra Romania, lokket til Norge med løfter om arbeid og fulgt til Skatteetaten med forhåndsutarbeidede fiktive arbeidskontrakter. Der gjennomgikk de identitetskontroll og fikk d nummer, skattekort og MinID, i den tro at de signerte dokumenter knyttet til lovlig arbeid og opphold.

Så snart registreringen var gjennomført, overtok den kriminelle entreprenøren og tilretteleggeren tilgangen til deres digitale identiteter. Med kontroll over MinID, e-postadresser, passord og andre identitetsbærere kunne han operere fullt ut på deres vegne. Dette gjorde det mulig å opprette en rekke enkeltpersonforetak i deres navn, registrere dem i mva-registeret og sende inn uriktige mva-meldinger. Foretakene var rene skallselskaper uten reell aktivitet, og ble brukt i et bedragerioppleg som omfattet krav om refusjon av merverdiavgift på mer enn fem millioner kroner, hvorav over 1,4 millioner ble utbetalt før Skatteetaten stanset utbetalingene.

Bakmannen misbrukte også eID-opplysningene til personer i egen familie. Under praktiske påskudd skaffet han seg tilgang til deres BankID, som han brukte til å sende inn krav mot lønnsgarantiordningen og fremsette søknader om dagpenger, samtidig som han opptrådte digitalt som familiemedlemmene overfor NAV. Misbruket var mulig fordi systemene er basert på selvrapportering og digital innlogging uten ytterligere verifikasjon av hvem som faktisk bruker identiteten.

Retten la i domsavsigelsen vekt på at dette ikke bare var økonomisk kriminalitet, men en alvorlig utnyttelse av mennesker og deres identiteter:

«Retten vil mene at hele opplegget ved denne grove utnyttelsen av personer vel må sies å være svært nær det en folkelig kan karakterisere som menneskehandel uten at det rammes av straffelovens definisjon av nettopp dette i dens § 257». (Midtre Hålogaland Tingrett, 2025).

De utenlandske borgerne ble ført til Norge under falske premisser, og deres identitet ble brukt i et omfattende svindelopplegg uten deres viten. Den kriminelle entreprenøren ble dømt til 3 år og 11 måneder ubetinget fengsel, i tillegg til å tåle en inndragning på i underkant av 1 million kroner og 570 000 kroner i erstatning til Skatteetaten (NRK, 2025; Midtre Hålogaland Tingrett, 2025).

ID-misbruk i bedragerier av enkeltpersoner

Ifølge politiets trusselvurdering for 2025 var rundt tre av fire bedragerier i 2024 digitale (Politiet, 2025b). I konteksten av ID-misbruk ser vi en tendens til at privatpersoners eID er et sentralt angrepspunkt for ulike kriminelle aktører som er aktive innen bedragerier. I dette kapittelet belyses hvordan identitetsopplysninger, ID-dokumenter og elektroniske identiteter (eID) misbrukes i bedragerier der privatpersoner er direkte ofre. Misbruk av eID kan blant annet innebære opptak av kreditt og lån, kjøp av varer og tjenester gjennom kredittløsninger, opprettelse av mobilabonnementer eller inngåelse av leieavtaler i en annen persons navn (SODI, 2024). Når slike handlinger først er gjennomført, kan det få betydelige økonomiske og praktiske konsekvenser for den som får sin identitet misbrukt. Fremstillingen tar utgangspunkt i hvordan høy tillit, utstrakt digitalisering og tilgjengeligheten av identitetsdata på nett samlet sett skaper sårbarheter som kan utnyttes av kriminelle aktører. Informasjonsgrunnlaget til rapporten består i hovedsak av studier gjort av SODI-prosjektet som har observert bedragerimoduser med bruk av eID gjennom en årrekke (SODI, 2025; SODI, 2024). I tillegg har advokatfirmaet HELP som arbeider med ID-tyverisaker vært en viktig bidragsyter til dette kapittelet. Disse rapporteringene er supplementert med saker fra politiets registre.

EKSEMPEL: eID og økonomisk vold

SODI-prosjektet har også belyst hvordan eID kan være et sentralt verktøy i økonomisk vold. Økonomisk vold er når noen handler slik at en person forhindres fra å styre egen økonomi og kan bestå i at en nærstående tar opp lån eller kreditt i partnerens identitet, eller fratar personen tilgang til egen eID (SODI, 2025). En svensk studie har også vist hvordan eID kan misbrukes som kontrollverktøy for å overta eller styre parets økonomiske ressurser, blant annet gjennom overføring av eiendeler, bestilling av kredittkort eller finansiering av spillavhengighet (Henrikson, Evertsson, & Nyman, 2023). Dette er også en risiko for eldre som deler eID-informasjonen sin med personer som hjelper den eldre med økonomi eller tilganger til digitale tjenester (Pensjonistforbundet, uten år).

I informasjonsinnhentingen til denne rapporten beskriver HELP at modusene for bedrageriene har endret seg i takt med sentrale rettsavgjørelser og påfølgende tiltak fra bankene. Frem til 2022 var bedragerisakene preget av at ofrene ble lurt til å gi fra seg eID-detaljene sine i det som ofte omtales som Olga-svindel. Navnet kommer av at det ofte var eldre kvinner med lav teknologisk forståelse som var de fornærmede i disse sakene. En Høyesterettsavgjørelse i 2022 la imidlertid det økonomiske

ansvaret for tapet på bankene. Bankene iverksatte en rekke tiltak og dette medførte at de kriminelle endret modusen til det vi i dag ofte omtaler som "sikker konto-svindel". I denne svindelformen, blir ikke de fornærmede lenger lurt til å gi fra seg eID-detaljene sine, men til gjennomføre de finansielle transaksjonene selv (HELP, 2025). Det kriminelle utbyttet fra disse bedrageriene er stort. Finanstilsynet har blant annet estimert at nordmenn overførte 667 millioner norske kroner til svindlere i løpet av 2024 (Finanstilsynet, 2025). Selv om svindelsituasjonen nå i stort er preget av sikker-konto svindel er det viktig å bemerke at politiet har informasjon om organiserte bedragerier der personer er lurt til å gi fra seg BankID-opplysninger så sent som våren 2025. Det bør derfor legges til grunn at de ulike svindelmodusene er dynamiske og kan endre seg.

Bruken av ID-dokumenter og eID i digitale prosesser forutsetter et høyt nivå av tillit. Personlig tillit er basert på relasjoner og erfaringer, mens institusjonell tillit i stor grad knytter seg til etablerte aktører som banker og offentlige myndigheter. I Norge er tilliten til bankvesenet høy, og denne tilliten er ofte like knyttet til institusjonen «bank» som sådan enn til den enkelte bank eller medarbeider (Krokan, 2019). I bedrageriutviklingen er det tydelig hvordan de kriminelle misbruker denne tilliten. Dette gjøres for eksempel ved å utgi seg for å være en ansatt i banken eller politiet, som gjennom sosial manipulasjon overbeviser den fornærmede at han eller hun er utsatt for en pågående svindel og må raskt overføre pengene fra sin egen konto til en sikker konto (Finans Norge, uten år; HELP, 2025). Modusen for bedragerier har dermed dreiet fra overtakelse av andres eID som sentralt angrepspunkt, til at man nå ser et større fokus på å manipulere de fornærmede til å selv utføre den finansielle transaksjonen med sin eID. Med eID-innlogging og signering er de digitale tjenestene brukervennlige, tilgjengelige, effektive og smidige, og det kan gå kort tid fra svindleren først tar kontakt med den fornærmede til transaksjonen er gjennomført. Et sårbart punkt i dette systemet er altså utnyttelsen av tillit, i kombinasjon med at helt vanlige mennesker er på egenhånd satt til å beskytte de økonomiske verdiene de kriminelle aktørene er ute etter.

Bedragerier utført med ID-dokumenter

Parallelt med at eID er en sentral angrepsflate for kriminelle aktører som bedriver bedragerier, viser informasjonsinnhentingen til rapporten at også de fysiske ID-dokumentene spiller en rolle i bedragerier og annen vinningskriminalitet. Utenriksstasjonene rapporterer om økt misbruk av norske ID-dokumenter i bedragerier, særlig gjennom bruk av digitale kopier av pass og nasjonale ID-kort som legitimasjon (Utenriksdepartementet, 2025). En analyse gjennomført av Kripos og Nasjonalt ID-senter i 2024 viste at bilder og kopier av norske ID-dokumenter som har kommet på avveie på internett, fungerer som en tilretteleggende faktor i en rekke digitale bedrageriformer, herunder bruktbilsvindel, digital seksuell utpressing, kjærlighetsbedragerier og investeringsbedragerier (Kripos og Nasjonalt ID-senter, 2024). Bedrageriene utført med norske ID-dokumenter foregår både nasjonalt og i utlandet.

Gjennom 2025 har Kripos og Nasjonalt ID-senter også observert en trend der fysiske falske ID-dokumenter og bilder av slike dokumenter er blitt benyttet til å hente ut mobiltelefoner på avbetalingsløsninger fra ulike elektronikkjeder. På disse ID-dokumentene benyttes identitetene til personer utsatt for ID-tyveri (Kripos og Nasjonalt ID-senter, 2025). I 2025 kom en ny forskrift som

skjerpet kravene for fremvisning av legitimasjon ved kjøp av kontantkort og mobilabonnement. Forskriften er et tiltak i å bekjempe svindel og ID-tyverier (NKOM, 2025). Imidlertid ser det ut til at de kriminelle aktørene enkelt tilpasser seg disse endringene, hvorpå de nå oppsøker butikkene fysisk og fremviser falske ID-dokumenter i andres identitet. En sentral sårbarhet i dette er at det kreves en viss kompetanse på ID-kontroll å kunne avsløre falske ID-dokumenter, og det er ikke gitt at butikkansatte har denne kompetansen eller eventuelt teknologisk utstyr for å avdekke falske dokumenter. Det er samtidig relativt enkelt å få tak i produksjonsutstyr for falske ID-kort på en rekke nettbutikker. ID-kort som produseres på denne måten kan være i god nok kvalitet til at de slipper gjennom en dokumentkontroll utført av noen med lav kompetanse på området. Erfaringer fra tidligere saker nasjonalt, viser at falske ID-kort produseres av én kriminell aktør på vegne av både seg selv og andre som en slags crime-as-a-service.

Som tidligere nevnt i rapporten finnes det også egne kriminelle miljøer som har spesialisert seg på datainnbrudd der personlig informasjon og bilder av ID-dokumenter stjeles (Agenzia per l'Italia Digitale, 2025). Sensommeren 2025 ble det kjent at et stort antall kopier av ekte pass ble lagt ut for salg på ulike undergrunnsforum etter lekkasjer fra databaser tilknyttet hoteller i Italia. Det er mulig at passkopier tilhørende norske borgere er lekket i denne saken, men dette er ikke bekreftet (Politiet, 2025). I tillegg til datalekkasjer, så finnes det både falske nettsider og profiler i sosiale medier som lurer personer til å laste opp eller sende bilder av ID-dokumentene sine. I løpet av 2025 har politiet blitt tipset om flere falske nettsider som utgir seg for å være offentlige myndighetssider for elektronisk visum eller innreisetillatelse. Storbritannia innførte en slik elektronisk innreisetillatelse for visumfrie reisende i april 2025. I søknaden må man fylle inn en rekke personopplysninger og opplysninger om formålet med reisen. Opplysningene sjekkes så mot en sikkerhetsdatabase før det gis tillatelse til innreise eller ikke. I tipsene til politiet fremkommer det at personer har brukt søkemotorer for å finne denne siden og blitt lurt av falske nettsider som kommer opp høyt i søket. På disse sidene har de blitt forledet til å laste opp bilde av reisedokumentet sitt. Det er ikke kjent for politiet at noen har opplevd å få sin identitet misbrukt som følge av dette, men det bør legges til grunn at det finnes en risiko for misbruk i disse tilfellene.

En lignende løsning for digital forhåndsgodkjenning for visumfrie reisende vil også innføres i Schengen, etter planen i løpet av siste kvartal 2026. Denne løsningen er kalt ETIAS - European Travel Information and Authorisation System (EU, uten år). USA og Canada har lignende digitale løsninger for sine visumfrie reisende. Verdensmesterskapet i fotball for menn avholdes i USA, Canada og Mexico sommeren 2026. Et slikt arrangement med mange internasjonale besøkende medfører en risiko for at flere slike falske nettsider vil oppstå og forlede personer til å gi fra seg bilder av reisedokumentene sine til ukjente aktører.

Bedragerimoduser med bruk av bilder av norske ID-dokumenter

Bilder av ID-dokumenter som er på avveie er observert misbrukt i ulike former for bedragerier, herunder kjærlighetsbedragerier, investeringsbedragerier og digital seksuell utpressing. Disse tre modusene forklares kort i det følgende og bygger på Kripos og Nasjonalt ID-senters analyse fra 2024. Selv om analysen er et par år gammel er disse modusene fortsatt aktuelle i dag.

Kjærlighetsbedragerier

I kjærlighetsbedrageri bygger svindleren først tillit til offeret i sosiale medier, gjerne gjennom en falsk identitet. Tillit kan etableres raskt dersom svindleren utgir seg for å være en kjent person eller tilhøre en profesjon med høy troverdighet, som soldat eller lege, eller gjennom langsiktig relasjonsbygging over flere måneder. Når tillit er etablert, fremsettes ofte krav om økonomisk støtte med ulike begrunnelser, for eksempel at svindleren har havnet i økonomiske vansker. Bilder av ID-dokumenter benyttes i denne konteksten for å gjøre den falske identiteten mer troverdig, og for å legitimere forespørsler om økonomisk bistand.

Investeringsbedragerier

Investeringsbedragerier kombinerer ofte identitetstyveri med sosial manipulasjon. Ofre blir lurt til å investere i kryptovaluta via falske vekslingstjenester, og må laste opp bilder av ID-dokumenter for å opprette konto. Underveis i denne formen for svindel er den fornærmede ofte i hyppig kontakt med en valutamegler, og det er et fellestrekk i sakene at denne megleren sender et bilde av passet sitt for å styrke sin legitimitet. Dette passet er som regel enten totalfalskt eller forfalsket. Det er avdekket misbruk av norske ID-dokumenter i denne typen bedragerier. Et av de norske dokumentene som har vært hyppig brukt stammer fra en datalekkasje tilhørende en legitim kryptovalutatjeneste. Våre undersøkelser tyder på at passet er manipulert og har vært benyttet med minst 7 ulike fiktive identiteter.

Digital seksuell utpressing (sextortion)

Digital seksuell utpressing innebærer at kriminelle aktører truer med å offentliggjøre seksuelt materiale for å presse et offer til å betale penger eller utføre handlinger mot sin vilje. I enkelte saker er ID-dokumenter brukt som virkemiddel for å øke troverdigheten og presset. Et eksempel fra datagrunnlaget viser en kvinne som ble lurt inn i et såkalt sugardating-forhold via Instagram. Etter at hun delte betalingsinformasjonen sin med det hun trodde var en sugardaddy, fikk hun tilsendt private bilder av seg selv, inkludert et bilde av passet sitt, som ble brukt for å true og kontrollere henne. Det er ukjent hvordan disse bildene hadde kommet på avveie. Eksemplet viser derimot hvordan kriminelle aktører bevisst kan digitalt oppsøke personer som får bilder av ID-dokumentene sine på avveie på nett.

I konteksten av ID-misbruk ser vi en tendens til at privatpersoners eID er et sentralt angrepspunkt for ulike kriminelle aktører. Dette gjør ID-misbruk i bedragerier mot enkeltpersoner til et omfattende samfunnsproblem.

ID-misbruk og migrasjonsstrømmer

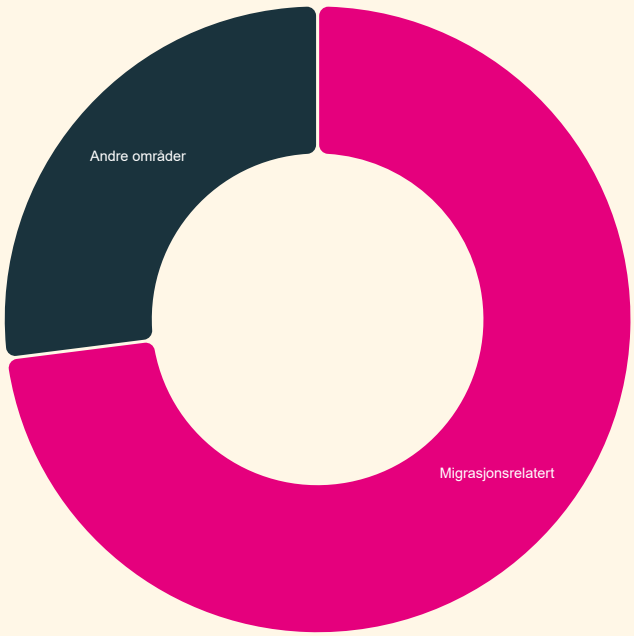
Utviklingen i ID-misbruk i konteksten av migrasjon er tett knyttet til utviklingen i de globale migrasjonsstrømmene, internasjonale konflikter, regionale situasjonsbilder og strukturelle forhold i ulike lands identitetsforvaltning. Norske myndigheter og identitetsforvaltning opererer dermed i et risikobilde som formes av forhold langt utenfor Norges grenser. Dette er også det feltet ID-misbruket tradisjonelt har blitt sterkest knyttet til, spesielt når det gjelder misbruk av fysiske ID-dokumenter. I en tid med økende og stor mobilitet, omfattende digitalisering og skjerpede internasjonale spenninger, blir identitet både en inngangsbillett og en barriere for mobilitet. Dette skaper et komplekst landskap der både enkeltpersoner, kriminelle aktører og statlige aktører kan utnytte de mulighetene og sårbarhetene som finnes.

For enkeltpersoner kan ID-misbruk i dette perspektivet være en inngangsbillett for å skaffe arbeid, opphold eller trygghet i Norge. For organiserte kriminelle aktører og nettverk er produksjon av falske ID-dokumenter en betydelig inntektskilde, ofte tett koblet til menneskesmugling inn og internt i Europa. I UDIs omverdensanalyse fra 2025 beskrives det i tillegg hvordan flyktningstrømmer kan fungere som en spillebrikke i et utenrikspolitisk spill som utnytter den betente innvandringsdebatten i flere europeiske land. Strategiske flyktningstrømmer inn i disse landene kan fungere destabiliserende og fyre opp under konflikter (Utlendingsdirektoratet, 2025b). Blant annet har Russland og Belarus blitt beskyldt for å strategisk lede større flyktningstrømmer mot Europas østlige grenser siden 2021 som et ledd i hybrid krigføring mot Europa (Eggen & Lavikainen, 2025). Russland ble også anklaget for å ha drevet store migrasjonsstrømmer til Storskog i 2015, da 5500 asylsøkere kom over grensen til Norge gjennom noen få måneder (Moe & Rowe, 2016). Selv om strategiske migrasjonsstrømmer i seg selv ikke har direkte betydning for ID-misbruk, så er det noe som legger stort press på migrasjonsmyndighetene og organene som er satt til å håndtere ankomstene. Politiet og de øvrige etatene i utlendingsforvaltningen bruker betydelige ressurser på innledende registrering og ID-undersøkelser av asylsøkere for å stadfeste rett identitet.

Situasjonsbildet på ID-misbruk knyttet til migrasjon er todelt. På den ene siden er en del av misbruket knyttet til bruk av falske dokumenter på individnivå, som for eksempel at en tredjelandsborger fremlegger falske dokumenter i en asylsøknad. På den andre siden ser vi en økende tendens til misbruk av såkalte legale kanaler for migrasjon. ID-misbruk i disse tilfellene kan for eksempel handle om å fremlegge falske dokumenter i en søknad om visum eller arbeidstillatelse. Dette kapittelet belyser enkelte slike moduser for ID-misbruk knyttet til migrasjon. Samlet gir kapittelet et bilde av hvordan globale forhold, migrasjonsstrømmer påvirker risikolandskapet og skaper nye sårbarheter i norsk identitetsforvaltning.

Regionale særtrekk som har påvirkning på ID-misbruk i Norge

Kripos og Nasjonalt ID-senters statistikk over ID-misbruk i 2025 viser at de to største områdene for ID-misbruk er knyttet til irregulær migrasjon (53 prosent) og søknader om asyl, opphold og statsborgerskap (20 prosent). Irregulær migrasjon viser her til personer som krysser grensen ved misbruk av ID-dokumenter, men hvor dette ikke er ulovlig fordi de er i en fluktsituasjon. Personene som kom til Norge i 2025 med falske dokumenter eller som fremla falske dokumenter til utlendingsforvaltningen i Norge har opprinnelse fra 51 ulike land i verden. De fleste er fra land utenfor EU/EØS-området og de fem hyppigst forekommende nasjonalitetene er Syria, Irak, Tyrkia, India og Pakistan. Statistikken for 2025 viser en stor variasjon i opphavsland for dem som misbruker ID-dokumenter. Dette viser at grense- og utlendingsforvaltningen i dag må håndtere et svært komplekst og sammensatt situasjonsbilde som setter høye krav til kompetanse på dokumentsituasjonen i ulike land, tilganger på referansedatabaser i tillegg til samarbeid og kunnskapsutveksling med andre etater både nasjonalt og internasjonalt.



Figur 4. Migrasjonsrelatert ID-misbruk utgjør om lag 75 prosent av det registrerte ID-misbruket.

Utenriksdepartementets ID-eksperter er stedsplassert i ulike regioner i verden og rapporterer ulike utfordringer knyttet til ID-misbruk.Utfordringsbildet knyttet til identitet har allikevel visse fellestrekk at mange av områdene preges av politisk uro og migrasjon ut av landene. I Øst-Afrika bidrar autoritær utvikling, økonomisk ustabilitet og en nedbygging av viktige institusjoner til disse urolighetene. Tilsvarende preges Sør-Øst-Asia av vedvarende konflikter, slik som i Myanmar, kombinert med ungdomsopprør. Dette skaper en kompleks regional kontekst der både migrasjon og ID misbruk inngår i et dynamisk trusselbilde. I Gulf-området finnes det få eller ingen muligheter for permanent opphold, noe som gjør at mange tredjelands arbeidsmigranter benytter regionen som et midlertidig stoppested før videre migrasjon, til blant annet Europa (Utenriksdepartementet, 2025).

Situasjonen i Syria er fortsatt ustabil og er sterkt preget av mange år med krig og konflikt. Registerkvaliteten er svekket, og dette svekker også legitimiteten til syriske underlagsdokumenter. ID-ekspertene peker også på hvordan digitalisering i flere regioner skaper nye former for sårbarhet. I Aserbajdsjan og Tyrkia er falske digitale plattformer for visumsøknader og arbeidstillatelse et økende problem. Det medfører en del henvendelser til visum-knutepunktet med spørsmål om bekreftelse på «innvilget» visum og arbeidstillatelser. Flere afrikanske land opplever risiko knyttet til digitalisering av sivile registreringer i kombinasjon med korrupsjon i offentlige institusjoner (Utenriksdepartementet, 2025). I flere afrikanske land anslår Utenriksdepartementet at korrupsjon på regionale flyplasser kan tilrettelegge for utreise ved bruk av falske ID dokumenter. Dette skjer ofte parallelt med økt aktivitet innen menneskesmugling, som ytterligere kompliserer det samlede risikobildet (Utenriksdepartementet, 2025).

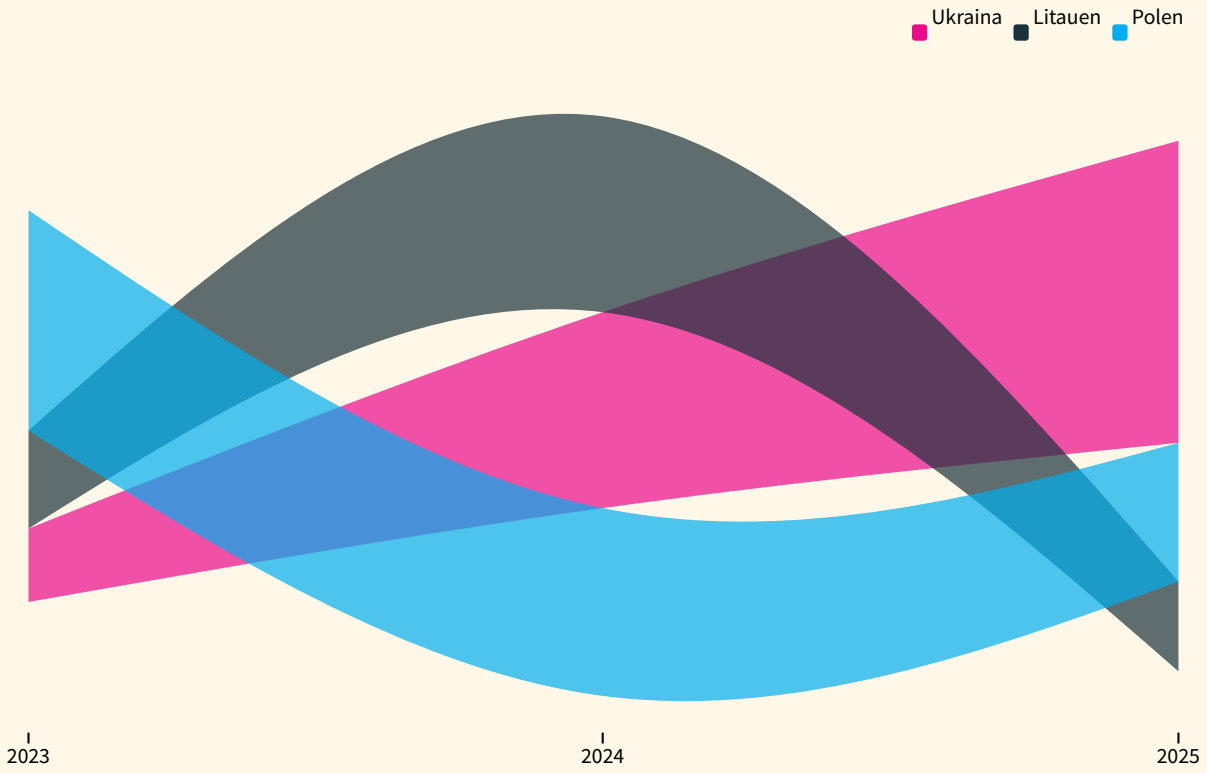
Situasjonen i våre nærområder har også påvirkning på ID-misbruket. Som allerede nevnt tidligere i rapporten har forvaltningen måtte håndtere en forhøyet innvandring av EU/EØS-borgere som registrerer seg og som blir utnyttet innen registermanipulasjon. Videre beskriver for eksempel Arbeidstilsynet i informasjonsinnhentingen at krigen i Ukraina påvirker det norske arbeidslivet. Det har for eksempel kommet frem at personer uten ukrainsk statsborgerskap har utnyttet krigen i Ukraina til å få opphold i Norge. Disse personene har ofte bodd eller jobbet i andre EU-land før krigen, men utgir seg for å være flyktninger for å få tilgang til velferdsordninger i Norge (Arbeidstilsynet, 2025). I en konkret sak som politiet har kunnskap om har det blitt fremlagt en falsk husleiekontrakt på en bolig i Ukraina, fra en ikke-ukrainsk familie som et ledd i å få kollektiv beskyttelse i Norge. Dette er en måte å forfalske den sosiokulturelle delen av identiteten sin, for å få opphold i Norge. Slike saker kan ende med tilbakekall av oppholstillatelsen.

EKSEMPEL: UNE og tilbakekallssaker

I sitt sitt svar til rapporten skriver UNE at et av deres arbeidsområder er knyttet til tilbakekall. Den største andelen av tilbakekallssaker er tilfeller der utlendingen har gitt uriktige opplysninger om sin identitet. Vurderingstemaet i disse sakene er om det er mest sannsynlig at klageren har gitt uriktige opplysninger eller fortiet forhold av vesentlig betydning for vedtaket. I mange tilbakekallssaker har utlendingen oppgitt å komme fra et land hvor det er krig/konflikt i søknaden om beskyttelse, og fått en beskyttelsestillatelse på det grunnlaget, men hvor det senere fremkommer informasjon om at personen kommer fra et trygt område i samme land, eller fra et trygt naboland.

I statistikken for 2025 er det også observert en økning i falske ukrainske førerkort. I Norge er hovedregelen at de fleste utenlandske førerkort må konverteres til norske førerkort innen en gitt periode. Statens vegvesen avdekker mange falske førerkort i saker som omhandler konvertering av utenlandsk førerkort til norske førerkort. I disse sakene er det en stor overvekt av falske førerkort angivelig utstedt i Polen. (Statens vegvesen, 2025). Ukrainske førerkort er imidlertid unntatt

kravene om innbytte så lenge ordningen om kollektiv beskyttelse gjelder (Statens vegvesen, uten år). Ettersom ukrainske førerkort ikke sjekkes systematisk, men kun ved tilfeldige kontroller, er det en faktor som kan påvirke personers tilbøyelighet til å anskaffe et falskt førerkort ettersom oppdagelsesrisikoen anses som lav. I tillegg er det slik at falske førerkort er enkle å bestille via nettsider på det åpne nettet og til relativt lave summer. Førerkortene kan personaliseres med riktig persondata og ansiktsfoto tilhørende personen som kjøper førerkortet. Gjennom 2025 har Nasjonalt ID-senter og Kripos undersøkt ulike aspekter ved misbruk av falske førerkort fra Ukraina. Analysene viser at disse førerkortene er hyppigere involvert i saker med farlig kjøring, inkludert ruspåvirket kjøring, i tillegg til trafikkulykker. Falske førerkort må derfor anses som å være en fare for trafikksikkerheten på norske veier.



Figur 5. Siden 2023 har totalfalske ukrainske førerkort hatt den mest markante økningen blant misbrukte førerkort i Norge.

Krigen i Ukraina og den skjerpede sikkerhetspolitiske situasjonen i verden generelt har medført strengere innreiserestriksjoner for borgere av visse land, for eksempel Russland. Nasjonalt ID-senter publiserte i 2025 en rapport om investeringspass, som viser at borgere fra land underlagt innreiserestriksjoner utnytter legale kanaler for å skaffe seg et nytt statsborgerskap og nytt pass som gjør at de kan reise visumfritt inn i Norge og Schengen (Nasjonalt ID-senter, 2025).

Identitetsrelatert visummisbruk og falske dokumenter i søknader om arbeidstillatelser

Misbruk av legale ordninger som kan gi opphold i Norge, vurderes som særlig relevante i forbindelse med ID-misbruk. I modusene for denne formen for ID-misbruk, er det oftere at det er den sosiokulturelle delen av identiteten som er gjenstand for misbruk. Det innebærer å manipulere eller oppgi falske opplysninger om den delen av identiteten som omhandler eksempelvis utdanning, arbeidserfaring eller familiære relasjoner. ID- og underlagsdokumenter misbrukes her på en måte som gjør at man manipulerer seg til et oppholdsgrunnlag som man egentlig ikke har krav på. Dette har for eksempel forekommet på områder som visumsøknader og misbruk av faglærtordningen.

Visumordningen kan misbrukes på ulike måter og det er viktig å presisere at ikke alle formene for visummisbruk vil falle innunder vår definisjon av ID-misbruk. Eksempler som typisk vil falle utenfor er dersom en person arbeider på et turistvisum eller om personen ikke reiser ut av landet innen gyldighetstiden for visumet. Identitetsrelatert visummisbruk knyttes til bruk av falske eller fiktive dokumenter i søknadsprosessen for visumet, hvilket kan resultere i et ekte visum utstedt på et uriktig grunnlag. Når visumene er ekte, men utstedt på bakgrunn av falske underlags- eller støttedokumenter, kan misbruket være vanskeligere å oppdage. Misbruket vil ikke kunne avdekkes gjennom en dokumentteknisk kontroll, men man er avhengig av å gjennomføre en taktisk ID-kontroll som for eksempel kan bestå av et intervju med den reisende om formålet med reisen eller kontrollere opplysningene som er vedlagt visumsøknaden. Dette er en tidkrevende prosess som ikke alltid lar seg gjøre i en hektisk arbeidshverdag og som dermed må anses som en risiko. Kripos og Nasjonalt ID-senter har i statistikken for 2025 observert en markant økning i antallet innrapporterte misbrukte visum ved innreise til Norge. Overvekten av disse er ekte visum. Det er viktig å påpeke at økningen i første omgang ser ut til å komme av endrede registrerings- og rapporteringsrutiner. Det kan derfor ikke hevdes at det har vært en faktisk økning innen visummisbruk det siste året.

De endrede registreringsrutinene gjør imidlertid at vi har fått mer kunnskap om fenomenet. En ting som peker seg spesielt ut er at det er observert ulike tilfeller der reiseplanen i visumsøknaden ser ut til å være generert av kunstig intelligens. I disse sakene er det fremlagt en svært detaljert plan for oppholdet, men ved muntlige spørsmål kan den reisende svært lite om planene for reisen. I enkelte tilfeller uttaler den reisende at reiseplanen er utarbeidet av et reisebyrå eller en agent. Kunstig intelligens representerer dermed en ny utfordring og det er grunnlag til å undersøke om dette også er et verktøy som misbrukes i andre kanaler for migrasjon til Norge.

UDs ID-eksperter rapporterer at norske utenriksstasjoner i Sør-Øst Asia og Gulf-området ser bruk av totalfalske eller forfalskede støttedokumenter som bankutskrifter, hotellreservasjoner og falske jobbtilbud i søknader om visum (Utenriksdepartementet, 2025). Det er også tilfeller hvor kopier av norske pass, både ekte og falske, benyttes sammen med falske invitasjonsbrev i søknader om visum til Schengen området. Det er mistanke om at digitale kopier av ekte pass kan være solgt av passinnehaver for dette formålet (Utenriksdepartementet, 2025). Politiet er kjent med at det foregår en viss organisering blant kriminelle som tilbyr falske dokumenter til bruk i visumsøknader, og at dette ofte er et ledd i menneskesmugling. De som står bak dette omtales ofte som agenter eller reisebyråer. Enkelte av grupperingene bruker sosiale medier til å reklamere for tjenestene sine og lover at migrantene raskt og enkelt kan få arbeid i landet de får visum til. Det er derfor mulig at migrantene som betaler for slike tjenester blir lurt og at det brukes som en metode for bedragerier.

I tillegg til saker om visum, viser ID-misbruk seg også innen arbeidsinnvandring til Norge. Legale

ordninger for arbeidsinnvandring til Norge forutsetter at søkerne legger frem dokumentasjon som viser at de oppfyller kravene for oppholdstillatelse, enten dette gjelder arbeidskontrakter, arbeidstilbud eller dokumentasjon på utdanning og kvalifikasjoner. De senere årene har imidlertid både de rapporterende etatene og politiet avdekket en økning i misbruk av slike dokumenter, noe som i økende grad omfatter både falske arbeidskontrakter, fiktive arbeidstilbud og manipulerte utdanningsdokumenter. Misbruket berører flere deler av arbeidsinnvandringssystemet, inkludert faglærtordningen, og involverer både enkeltpersoner, kriminelle nettverk og agenter som bistår søkere med å skaffe falsk dokumentasjon. Dette skaper utfordringer både for identitetsforvaltningen og for kontrollen av arbeidslivet.

Utenlandske borgere som skal arbeide i Norge skal fremlegge en arbeidskontrakt for å sannsynliggjøre arbeidsforholdet. Dersom vilkårene er oppfylt vil personen bli tildelt et norsk identifikasjonsnummer, i form av et fødsels- eller d-nummer. Det er ulike regler for hvorvidt personen blir tildelt et fødsels- eller d-nummer. Personer som skal jobbe i Norge og søker skattekort får tildelt d-nummer dersom de ikke skal bosettes. Personer som flytter til Norge og skal bosettes, det vil si at de skal være i Norge og bo her i over 6 måender vil få tildelt fødselsnummer dersom de øvrige vilkårene er oppfylt (Skattetaten, uten år; FAFO, 2025). Skatteetaten har de senere årene identifisert en økning i bruken av falske og fiktive arbeidskontrakter. Mellom 2023 og 2025 ble det avdekket 108 falske arbeidskontrakter, hvorav nesten halvparten ble avdekket i 2025 (Skatteetaten, 2025). Dette er derfor en modus som må anses for å være høyaktuell og pågående. Selv om arbeidskontrakter i seg selv ikke er ID-dokumenter, brukes de i praksis til å skaffe identitetsnummer og eID på uriktig grunnlag og fungerer dermed som en døråpner til det norske samfunnet. Ettersom arbeidskontrakter ikke følger et standardisert format, er man også i disse sakene ofte avhengig av at førstelinjen gjennomfører en taktisk kontroll for å avdekke misbruket.

Falske arbeidskontrakter forekommer særlig i bransjer som driver matlevering, drosjenæringen og massasjestudioer, hvor behovet for fleksibel arbeidskraft og muligheten for omgåelser skaper grobunn for misbruk (Skatteetaten, 2025). Det er viktig å legge til at falske arbeidstilbud i visse tilfeller også kan kobles til mer alvorlige former for kriminalitet, som menneskesmugling, menneskehandel og sosial dumping. Aftenposten har omtalt saker hvor personer har betalt bakmenn for lovnader om arbeid som aldri blir realisert, og hvor enkelte arbeidssøkere også har forsvunnet (Aftenposten, 2025). UDI har i informasjonsinnhentingen rapportert om tilsvarende bruk av falske arbeidstilbud både i faglærtsøknader og i sesongarbeid, og har publisert en oversikt over berørte virksomheter på sine nettsider (Utlendingsdirektoratet, 2025). Flere aktører peker også på at man i sakene ser at det er agenter og mellommenn i bakgrunnen som bistår med å fremskaffe de falske dokumentene.

Norge, som mange andre europeiske land, har et stort og voksende behov for arbeidskraft. Dette som følge av befolkningsutviklingen og samfunnsendringer knyttet til omstilling, grønn økonomi og kompetansemangel i kritiske samfunnsfunksjoner. For å tiltrekke seg kvalifiserte arbeidstakere er det et politisk mål å effektivisere saksbehandlingen, særlig innen det som kalles faglærtordningen (Utlendingsdirektoratet, 2025b). En faglært er en person som har fullført utdanning i et yrke eller yrkesfag som ofte gir et fagbrev eller svennebrev. En typisk utdanningsmodell for faglærte er to år på skole og to år som lærling i en bedrift, men dette varierer (Store norske leksikon, 2025). Mange tredjelandsborgere søker seg inn i faglærtordningen via bransjer med særlig arbeidskraftsbehov,

slik som restaurant, bygg og anlegg, bilmekanikk og andre yrkesfag. UDI beskriver i informasjonsinnhentingen til rapporten at mange av søkerne i faglærtordningen kommer fra India, Pakistan, Kosovo, Vietnam, Kina, Bangladesh og Tyrkia og at det også er en voksende trend med farmasøyt-søknader fra Pakistan (Utlendingsdirektoratet, 2025).

I tiden etter koronapancdemien har Kripos og Nasjonalt ID-senter gjennom sin monitorering sett mange saker med falske utdanningsdokumenter i søknader om opphold og arbeidstillatelse som faglært. Sakene ser ut til å ha en viss grad av organisering, da flere søkere for eksempel har fremlagt dokumenter fra samme universitet eller skole og er tilknyttet samme arbeidsgiver i Norge. Enkelte utdanningsdokumenter og vitnemål er i tillegg knyttet til universiteter i utlandet som er fullstendig fiktive. Disse vitnemålene er gjerne utstedt med QR-koder som gjør det mulig å «verifisere» ektheten av vitnemålet via en digital løsning på det fiktive universitetets nettside. Dersom norske myndigheter ikke gjør grundige undersøkelser rundt eksistensen til utdanningsstedet, men stoler på verifiseringsløsningen, er det en risiko for at det godkjennes søknader til personer uten tilstrekkelig kompetanse. Dette er en situasjon hvor det fort kan oppstå konflikt mellom å gjøre en grundig vurdering av dokumentene i saken, samtidig som det er høye krav til effektiv saksbehandling da arbeidsinnvandring gjennom faglærtordningen er en villet politikk for å dekke kompetansehullene i arbeidsmarkedet (FAFO, 2022).

EKSEMPEL: Det fiktive Yeni Pazar-universitetet

Yeni Pazar-universitetet er et eksempel på et fiktivt universitet. I 2024 dukket det opp flere saker i tyrkiske medier som beskrev at Yeni Pazar utga seg for å være en utenlandsk utdanningsinstitusjon med om lag 4000 online-studenter fra rundt 168 land. Undersøkelser avdekket at det ikke fantes noe fysisk campus, akademisk stab eller reelle grader, og vitnemålene som ble utstedt var falske. Rådet for høyere utdanning i Tyrkia (Yükseköğretim Kurulu) bekreftet i 2024 at Yeni Pazar var en svindel og at det var opprettet straffesak mot bakmennene (Hürriyet Daily News, 2024)

Oslo politidistrikt rapporterer i sin lokale trusselvurdering for 2025 at faglærtordningen i økende grad misbrukes som kanal for menneskesmugling, hvor forfalskede arbeids- eller utdanningsdokumenter brukes for å gi innreisemuligheter til personer som ellers ikke ville fått opphold. Organiserte kriminelle aktører benytter de falske dokumentene for å smugle inn familie, bekjente eller arbeidskraft. Oslo politidistrikt skriver også i trusselvurderingen at personer som kommer til Norge på denne måten står i økt fare for utnyttelse i arbeidslivet (Oslo politidistrikt, 2025). Det er observert flere eksempler på dette gjennom 2025. I en sak ble det avdekket falske utdanningsdokumenter hos to serbiske borgere som ifølge søknadene arbeidet som kokker i Norge. I en etterkontroll ble de falske vitnemålene avdekket, og det ble også raskt klart at restauranten brøt vilkårene for faglærttillatelsen. Tillatelsen krever at de ansatte arbeider i en heltidsstilling og med arbeidsoppgaver på faglært

kompetansenivå. I realiteten jobbet disse kokkene i lavere stillingsprosenter og med oppgaver tilegnet personer på et lavere kompetansenivå.

Det er også viktig å legge til at personene som misbruker falske utdanningsdokumenter kan ha betalt store summer for de falske dokumentene, og dermed ha gjeld som de er avhengige av en jobb for å kunne nedbetale. Det setter dem i en ekstra sårbar posisjon. Det er ikke mulig å estimere hvor mye disse personene betaler for de falske dokumentene, men i en konkret sak fra 2025 kom det frem at en ukrainsk borger hadde betalt om lag 30 000 kroner for et falskt vitnemål som ingeniør (Trønder-Avisa, 2025; Khrono, 2025b). Oppsummert viser eksemplene med falske dokumenter i visumsøknader og i søknader om arbeidstillatelser at det finnes et marked med personer som er villige til å betale for falske dokumenter, og at det finnes kriminelle aktører og nettverk som bistår dem i produksjonen

av slike dokumenter. De ulike modusene og sakene som omtales i dette kapittelet viser at det finnes sårbarheter i norske innvandringssystemer og -ordninger som kan utnyttes. Den norske identitetsforvaltningen befinner seg dermed i en kompleks situasjon, der det er avgjørende å finne en hensiktsmessig balanse mellom effektiv saksbehandling og grundige vurderinger av dokumenters ekthet, i en tid preget av høyt migrasjonspress, for å kunne avdekke og forebygge ID-misbruk.

Avsluttende refleksjoner

Denne rapporten bygger på erfaringer med ID-misbruk fra en lang rekke offentlige myndigheter og private aktører. Særlig illustrerende er det hvordan ID-misbruk både fungerer som et verktøy i seg selv, og som en tilretteleggende faktor for andre former for kriminalitet som både preger og truer samfunnet vårt.

Økt digitalisering, færre fysiske oppmøter og utbredt bruk av elektroniske ID-løsninger har bidratt til at nye angrepsflater er blitt tilgjengelige for profittmotiverte kriminelle nettverk. Dette har også endret de kriminelle aktørenes metoder for å oppnå økonomisk vinning. I Norge hører vi i dag ikke lenger om kriminelle gjenger som planlegger eller gjennomfører store bankran. Den økonomiske profitten er tilgjengelig på mer skjulte og smidige måter, og det kriminelle utbyttet kan hentes stille og rolig ut av statskassen gjennom ulike former for registermanipulasjon eller gjennom bedragerier rettet mot enkeltpersoner.

Innføringen av eID-løsninger har bidratt til et skifte i ansvar for tilgang til samfunnets økonomiske verdier. Der dette tidligere i stor grad var ivaretatt gjennom institusjonelle kontrollmekanismer, er ansvaret i dag i økende grad individualisert og knyttet til den enkelte bruker. Dette representerer ikke nødvendigvis en eksplisitt ansvarsoverføring, men en strukturell konsekvens av digitalisering og økt bruk av eID som tilgangsmekanisme. Dette understreker behovet for helhetlige og forebyggende tiltak som tar høyde for både teknologiske, organisatoriske og menneskelige sårbarheter i identitetsforvaltningen.

Rapporten har også vist hvordan kriminelle aktører raskt tilpasser sin virksomhet i takt med nye tiltak, slik det blant annet fremgår av sakene knyttet til såkalte Olga-bedragerier. Misbruket av lønnskompensasjonsordningen under koronapandemien illustrerer på tilsvarende måte hvordan kriminelle raskt identifiserer og utnytter nye økonomiske muligheter når samfunnet endrer seg, og etablerte kriminalitetsformer ikke lenger er tilgjengelige.

Eksempelsakene med misbruk av over 300 ulike identiteter og et samlet utbytte på over 10 millioner kroner, viser at tilgangen på identiteter som kan utnyttes er betydelig innenfor den kriminelle infrastrukturen. Elektroniske ID-løsninger som BankID gir en effektiv måte å verifisere identitet på, men kan samtidig skape en illusjon av faktisk identifikasjon. Slik systemene er utformet i dag, er det ikke mulig å fastslå om personen som handler i en identitets navn i offentlige registre, faktisk er den rette innehaveren av identiteten. Som rapporten har vist, er det mulig både for én person å opptre med flere identiteter i registrene, og for flere personer å utnytte én og samme identitet.

Fremover vil teknologiske endringer og nye EU-initiativer, som eIDAS 2.0 og digitale identitetslommebøker, kunne bidra til tryggere og mer smidig identifikasjon på tvers av landegrensene i Europa. Samtidig må det legges til grunn at disse løsningene skal bygges videre på en nasjonal identitetsinfrastruktur som allerede er under betydelig press fra kriminelle aktører.

Digitaliseringen av grensekontrollen, blant annet gjennom økt bruk av automatisert ansiktssammenligning, vil også påvirke hvordan ID-misbruket arter seg. Økt bruk av teknologi bidrar samtidig til høyere kvalitet på forfalskede dokumenter, noe som vanskeliggjør arbeidet med å avdekke ID-misbruk. Dette kan også innebære at det er andre deler av ID-dokumentene som blir utsatt for manipulasjon og misbruk, som for eksempel den elektroniske chipen som finnes i mange pass og ID-kort. Nasjonalt ID-senter har de siste tre årene observert det som fremstår som en økning i falske dokumenter som inneholder en falsk chip. Per i dag avdekkes disse dokumentene primært gjennom kontrollørens kompetanse i vurderingen av de øvrige delene av det fysiske dokumentet.

Kontroll av den elektroniske delen av dokumentene innebærer imidlertid flere utfordringer:

- ikke alle land har innført chipteknologi i sine reisedokumenter
- ikke alle land deler sine utstedersertifikater
- mange land gjør feil under utstedelsen av chipen

Dette fører til en rekke avviksmeldinger i passlesere som ikke er relevante og dette kan svekke kontrollørens tillit til de elektroniske systemene. Vurderingen av om et avvik skyldes utstederfeil ellerom det faktisk er et falskt dokument, er ofte krevende. I tillegg forekommer det utstederfeil som i praksis umuliggjør en sikker ekthetsvurdering. Dette er sentrale utfordringer knyttet til chipteknologi som norske myndigheter bør ha særlig oppmerksomhet på i årene som kommer.

Rapporteringen viser også at ID-forvaltning er et komplekst samspill mellom offentlige og private aktører. Systemer, prosesser og teknologiske løsninger er ofte tett integrert, noe som gir effektive tjenester, men samtidig kan skape sårbarheter dersom risikoen for misbruk ikke vurderes tilstrekkelig. Dette illustrerer at fremtidige tiltak mot ID-misbruk må kombinere tekniske sikkerhetstiltak med organisatoriske og juridiske løsninger, samt en forståelse for hvordan både menneskelig og institusjonell tillit kan utnyttes.

Samlet peker utviklingen mot et kriminalitetsbilde som er både komplekst og tilpasningsdyktig. Tiltak må derfor utformes med kunnskap om samspillet mellom teknologiske løsninger, regelverk og menneskelig atferd. Erfaringene som presenteres i denne rapporten gir et viktig grunnlag for beslutningstakere i både offentlig og privat sektor, men fremtidig ID-sikkerhet vil kreve kontinuerlig overvåking, vurdering av nye trusler og tett samarbeid mellom offentlige etater og private aktører.

Datagrunnlag og metode

Informasjon om datagrunnlag

Til denne rapporten har vi etterspurt informasjon om ID-misbruk fra tolv offentlige aktører og fire private aktører. Informasjonsinnhentingen har pågått i perioden 30. oktober 2025 til 20. desember 2025. Totalt har vi mottatt svar fra åtte offentlige aktører og en privat aktør:

- Arbeidstilsynet
- Arbeids- og velferdsdirektoratet (NAV)
- Brønnøysundregistrene
- HELP
- Skatteetaten
- Statens vegvesen
- Utlendingsdirektoratet (UDI)
- Utlendingsnemnda (UNE)
- Utenriksdepartementet (UD)

Informasjon fra organisasjonene i listen ble innhentet gjennom elektronisk kommunikasjon direkte med aktørene. Samtlige mottok et vedlegg med en definisjon av ID-misbruk, et dokument med beskrivelse av sentrale drivkrefter for ID-misbruk og spørsmål knyttet til hvordan deres etat vurderer utviklingen av ID-misbruk sett opp mot disse drivkreftene. Beskrivelsene av drivkreftene finnes i vedlegg 1 i denne rapporten. Disse er basert på observasjoner om utvikling oppdaget i Nasjonalt ID-senter og Kripos' løpende monitorering av politiets registre og er sett i konteksten av generelle, relevante utviklingstrekk i samfunnet.

De ulike etatene som har rapportert til rapporten har svært ulike roller i ID-forvaltningen og det er derfor stor variasjon i hvilke drivkrefter som treffer deres etat. I tillegg til å besvare spørsmålene i kvalitativt format, sendte enkelte av aktørene inn statistikk på avdekkede misbrukte ID-dokumenter. Disse tallene er blitt inkludert i datagrunnlaget for rapporten. Samtlige svar er samlet i en samleoversikt og deretter analysert og presentert i denne rapporten.

Av kostnadseffektive hensyn ble det besluttet å ikke sende ut informasjonsforespørsler til politidistrikter og særorgan. I stedet er det gjort egne undersøkelser i politiets sentrale registre. Dette er en oppgave som Kripos og Nasjonalt ID-senter utfører fortløpende gjennom året uavhengig av denne rapporten.

I tillegg er det innhentet informasjon fra åpne kilder via offentlige rapporter, nyhetsartikler og forskning. Disse kildene er tilgjengelig via litteraturlisten og er referert til fortløpende gjennom rapporten. Rapporten er avslutningsvis kvalitetssikret i både Nasjonalt ID-senter og Kripos, og aktuelle deler av teksten er sendt til sitatsjekk og godkjenning hos bidragsyterne til rapporten.

Vurdering av datagrunnlaget

Misbruk av ID-dokumenter og identiteter er fenomener som foregår og observeres av en lang rekke offentlige og private aktører. Ifølge en interessentanalyse utført av Oxford Research Centre på

oppdrag av Nasjonalt ID-senter i 2025, er det kommet frem til at det er om lag 24 virksomheter eller organisasjoner i Norge som har konkrete ID-oppgaver i norsk forvaltning (Oxford Research, 2025). ID-forvaltningen i Norge har i en årrekke blitt beskrevet som fragmentert. Dette fremheves blant annet i områdegjennomgangen av ID-forvaltningen fra 2019 (Capgemini, 2019), og også i etterevalueringen gjennomført i fem år senere (Direktoratet for forvaltning og økonomistyring, 2025).

At ID-forvaltningen er fragmentert betyr blant annet at det offentlige ansvaret for identitetsstyring er spredt på mange aktører som igjen er organisert under ulike departementer og politikkområder. Dette begrenser mulighetene for å skaffe til veie et helhetlig bilde over ID-misbruket i Norge.

Fragmenteringen av ID-forvaltningen medfører også at det ikke finnes en felles nasjonal tilnærming til innsamling, kategorisering og rapportering av data om ID-misbruk. Ulike aktører benytter ulike definisjoner av hva som inngår i begrepet ID-misbruk, og registrerer hendelser på ulike nivåer av detaljeringsgrad. Dette innebærer at data fra ulike kilder i begrenset grad lar seg sammenstille uten betydelig metodisk tilpasning.

Videre er tilgjengelige datakilder i hovedsak utviklet for administrative, operative eller kontrollrelaterte formål, og ikke for statistisk eller analytisk bruk. Som følge av dette kan dataene være mangelfulle når det gjelder variabler som er sentrale for å analysere omfang, utviklingstrekk og mønstre i ID-misbruk over tid.

Det må tas høyde for betydelige mørketall knyttet til ID-misbruk. Ikke alle former for misbruk avdekkes, og ikke alle avdekkede hendelser rapporteres videre til relevante myndigheter eller felles statistikkgrunnlag. Dette gjelder særlig i saker der økonomisk tap er begrenset, eller der misbruket håndteres internt av private aktører.

Samlet sett innebærer disse forholdene at tall og analyser som presenteres i rapporten må tolkes med varsomhet. Datagrunnlaget gir indikasjoner på utviklingstrekk og problemområder, men kan ikke uten videre gi et fullstendig eller uttømmende bilde av omfanget av ID-misbruk i Norge. Resultatene bør derfor forstås som et best mulig kunnskapsgrunnlag gitt dagens tilgjengelige data.

Referanser

Aftenposten (2021). *35-åring tiltalt for å ha lurt til seg mange millioner i koronastøtte – utnyttet 300 stjålne identiteter.* Hentet 23.12.25 fra https://www.aftenposten.no/norge/i/5nyqbO/35-aaring-tiltalt-for-aa-ha-lurt-til-seg-mange-millioner-i-koronastoette-utnyttet-300-stjaalne-identiteter

Aftenposten (2025). *Over 27.000 sesongarbeidere til Norge: - Enkelt å forfalske kontrakter.* Hentet 17.12.25 fra https://www.aftenposten.no/norge/i/6qwjb8/over-27000-sesongarbeidere-til-norge-enkelt-aa-forfalske-kontrakter

Agenzia per l'Italia Digitale (2025). *In vendita documenti di identità trafugati da hotel italiani.* Hentet 19.12.25 fra https://cert-agid.gov.it/news/in-vendita-documenti-di-identita-trafugati-da-hotel-italiani/

Arbeidstilsynet (2025). *Svar på forespørsel om informasjon til årsrapport om ID-misbruk.* Elektronisk kommunikasjon til Nasjonalt ID-senter.

Brønnøysundregistrene (2025). *Svar på forespørsel om informasjon til årsrapport om ID-misbruk.* Elektronisk kommunikasjon til Nasjonalt ID-senter.

Capgemini (2019). *Områdegjennomgang ID-forvaltningen.* Hentet 26.11.25 fra https://www.regjeringen.no/contentassets/fc0f9e0edef4440cb1ef5e8dd8ffad0e/07-09-2021-hovedrapport.pdf

Dagens Næringsliv (2025). *Støre om bedrageribølgen: – Alle politidistriktene jeg besøker ser spor etter svenske gjenger.* Hentet 26.11.25 fra https://www.dn.no/politikk/store-om-bedrageribolgen-alle-politidistriktene-jeg-besoker-ser-spor-etter-svenske-gjenger/2-1-1785821

David, P. A. (1985). *Path Dependence and Technology Lock In.* Hentet 23.12.25 fra https://static1.squarespace.com/static/5e582b6d525bce01a6016637/t/604a6721207b9c2c4eb3d0a8/1615488801936/David+FINAL+articles+with+Intro.pdf

Digitaliserings- og forvaltningsdepartementet (2024). *Fremtidens digitale Norge. Nasjonal digitaliseringsstrategi 2024-2030.* Hentet 23.12.25 fra https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi_ny.pdf

Digitaliseringsdirektoratet (2024). *Et viktig skritt nærmere digital lommebok.* Hentet 15.12.25 fra https://www.digdir.no/digital-identitet/et-viktig-skritt-naermere-digital-lommebok/5559

Digitaliseringsdirektoratet (2024). T*illit i befolkningen og til det offentlige.* Hentet 17.12.25 fra https://www.digdir.no/rikets-digitale-tilstand/tillit-i-befolkningen-og-til-det-offentlige/4060

Digitaliseringsdirektoratet (2025a). *Kunnskapsinnhenting på eID-området.* Hentet 06.02.26 fra https://www.digdir.no/digital-identitet/kunnskapsinnhenting-pa-eid-omradet/7757

Digitaliseringsdirektoratet (2025b). *Konseptvalgutredning.* Hentet 27.02.26 fra https://samarbeid.digdir.no/digital-lommebok/konseptvalgutredning/2924

Digitaliseringsdirektoratet (uten år). *MinID.* Hentet 12.12.25 fra https://eid.difi.no/nb/minid

Digitaliseringsdirektoratet (uten år). *Slik skaffer du deg elektronisk ID.* Hentet 06.02.26 fra https://eid.difi.no/nb/id-porten/slik-skaffer-du-deg-elektronisk-id

Direktoratet for forvaltning og økonomistyring (2025). *DFØ-notat 2025:4 Etterevaluering av*

områdegjennomgang av ID-forvaltningen fra 2019. Hentet 05.01.26 fra https://www.dfo.no/dfo-notat-20254-etterevaluering-av-omradegjennomgang-av-id-forvaltningen-fra-2019

Direktoratet for høyere utdanning og kompetanse (2023). *Falske dokumenter.* Hentet 17.12.25 fra https://hkdir.no/utdanning-fra-utlandet/falske-dokumenter

DNB (2025). *Finansiell trygghet: Hvem kan du stole på?* Hentet 05.12.25 fra https://www.dnb.no/portalfront/nedlast/no/om-oss/samfunnsansvar/finansiell-trygghet/113640_DNB_Finansiell_trygghet.pdf

Eggen, K.-A., & Lavikainen, J. (2025). *Implementing a new tool: Russia's strategiv use of migrants towards Norway and Finland 2015/16.* European Journal of International Security, s. 24. doi:10.1017/eis.2025.10029

Ekobrottsmyndigheten (2025). *Ekonomisk brottslighet. Ekobrottsmyndighetens lägesbild 2025.* Hentet 28.11.25 fra https://www.ekobrottsmyndigheten.se/wp-content/uploads/2025/05/ebm-lagesbild-2025.pdf

EU (2025). *What is the EES?* Hentet 13.01.26 fra https://travel-europe.europa.eu/ees/what-is-the-ees

EU (uten år). *ETIAS in a nutshell*. Hentet 01.03.26 fra https://travel-europe.europa.eu/etias/about-etias/what-is-etias

European Labour Authority (uten år). *Posting of third-country nationals: contracting chains, recruitment patterns, and enforcement issues. Insights from case studies.* Hentet 29.12.25 fra https://www.ela.europa.eu/sites/default/files/2025-06/Third_country_nationals_report.pdf

Europol (2025). *The changing DNA of serious and organized crime.* Hentet 28.11.25 fra https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

FAFO (2022). *Arbeidsinnvandring fra tredjeland.* Hentet 07.02.26 fra https://www.fafo.no/images/pub/2022/20820.pdf

FAFO (2025). *Kartlegging av innvandrere med d-nummer og langvarig tilknytning til Norge.* Hentet 01.12.25 fra https://www.fafo.no/publikasjoner/fafo-rapporter/kartlegging-av-innvandrere-med-d-nummer-og-langvarig-tilknytning-til-norge

Finans Norge (uten år). *Sikker konto svindel.* Hentet 18.12.25 fra https://www.svindel.no/selvforsvar/svindelmetoder/sikker-konto-svindel/

Finanstilsynet (2025). *Svindelstatistikk andre halvår 2024.* Hentet 06.02.26 fra https://www.finanstilsynet.no/publikasjoner-og-analyser/svindel-og-svindelstatistikk/2024/h2/svindelstatistikk-andre-halvar-2024/#tap-ved-svindel-der-betaler-manipuleres-til-aa-initiere-en-transaksjon

Fri fagbevegelse (2024). *Arbeidslivskriminalitet: Hamid ble lurt av sjefen. Nå skylder han staten 200.000 kr*oner. Hentet 26.11.25 fra https://frifagbevegelse.no/nyheter/hamid-ble-lurt-av-sjefen-na-skylder-han-staten-200000-kroner-6.158.1030267.e7b3f97db4

HELP (2025). *Svar på forespørsel om informasjon til årsrapport om ID-misbruk.* Elektronisk kommunikasjon til Nasjonalt ID-senter.

Henrikson, A.-S., Evertsson, L., & Nyman, C. (2023). *E-legitimation som verktyg för ekonomisk våld.* Hentet 08.12.25 fra https://svjt.se/svjt/2023/579

Hürriyet Daily News. (2024). *Students file complaints as university found to be fake.* Hentet 12.01.26 fra https://www.hurriyetdailynews.com/students-file-complaints-as-university-found-to-be-fake-198456

Justis- og beredskapsdepartementet (2024). *Meld. St. 15 (2023-2024) Felles verdier - felles ansvar. Styrket innsats for forebygging og bekjempelse av økonomisk kriminalitet.* Hentet 11.12.25 fra https://www.regjeringen.no/contentassets/4ad80f7323ce4a8ea6ec3b57d68463e4/no/pdfs/stm202320240015000dddpdfs.pdf

Khrono (2025a). *Dobling av anmeldelser for svindel med vitnemål.* Hentet 18.12.25 fra https://www.khrono.no/dobling-av-anmeldelser-for-svindel-med-vitnemal/1018999

Khrono (2025b). *Leverte falskt vitnemål fra utlandet, må i fengsel.* Hentet 17.12.25 fra https://www.khrono.no/leverte-falskt-vitnemal-fra-utlandet-ma-i-fengsel/1017576

Kommunal- og distriktsdepartmentet (2023). *Nasjonal strategi for eID.* Hentet 23.12.25 fra https://www.regjeringen.no/contentassets/f3f51d0207f04296b8192636cf4a4521/h-2540_nasjonal-strategi-for-eid-i-offentlig-sektor.pdf

Kripos og Nasjonalt ID-senter (2024). *Bilder av ID-dokumenter på internett som tilretteleggende faktor for kriminalitet* (unntatt offentlighet).

Kripos og Nasjonalt ID-senter (2025). *Halvårsrapport ID-misbruk, første halvår 2025.* Unntatt offentlighet.

Krokan, A. (2019). *Deling, plattform, tillit. Perspektiver på delings- og plattformøkonomi.* Oslo: Cappelen Damm Akademisk.

Midtre Hålogaland Tingrett (2025). *Midtre Hålogaland tingrett - Dom: TMHA-2024-197006.* Hentet desember 09.12.25 fra https://lovdata.no/dokument/TRSTR/avgjorelse/tmha-2024-197006?q=rumenske

Moe, A., & Rowe, L. (2016). *Asylstrømmen fra Russland til Norge i 2015: Bevisst russisk politikk?* Hentet 02.02.26 fra https://tidsskriftet-nof.no/index.php/noros/article/view/432/912

Nasjonalt ID-senter (uten år). *Hva er identitet?* Hentet 16.12.25 fra https://www.nidsenter.no/vedlegg/utlopt/utlopt-innhold/hva-er-identitet/

NAV (2025). *Svar på forespørsel om informasjon til årsrapport om ID-misbruk.* Elektronisk kommunikasjon til Nasjonalt ID-senter.

Nettavisen (2021). *Oslomann dømt for å ha svindlet Nav for ti millioner kroner i koronastøtte.* Hentet 23.12.25 fra https://www.nettavisen.no/nyheter/oslomann-domt-for-a-ha-svindlet-nav-for-ti-millioner-kroner-i-koronastotte/s/12-95-3424214630

NKOM (2025). *Nye regler skal hindre ID-tyveri.* Hentet 18.12.25 fra https://nkom.no/aktuelt/nye-regler-skal-hindre-id-tyveri

NRK (2024). *Kreftsyke Magnhild (71) utnyttes av kriminelle.* Hentet 22.12.25 fra https://www.nrk.no/norge/kreftsyke-magnhild-_71_-utnyttes-av-kriminelle-1.17076557

NRK (2025). *Nesten fire års fengsel for bedrageri: – Grenser til menneskehandel.* Hentet 09.12.25 fra https://www.nrk.no/nordland/mann-domt-til-ubetinget-fengsel-for-omfattende-bedragerier-1.17429375

NTAES (2024). *Registermanipulasjon.* Hentet 11.11.25 fra https://www.ntaes.no/reports/NTAES%20Rapport%20Registermanipulasjon.pdf

Oslo politidistrikt (2025). *Lokal trusselvurdering 2025 for Oslo, Asker og Bærum.* Hentet 16.12.25 fra https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/oslo/rapporter/lokal-trusselvurdering/lokal-trusselvurdering-2025-oslo-politidistrkt.pdf

Oxford Research (2025). *Interessent- og brukeranalyse for Nasjonalt ID-senter.* Hentet 16.12.25 fra https://www.nidsenter.no/aktuelt/nyhetsarkiv/2025/interessent--og-brukeranalyse-for-nasjonalt-id-senter/

Pensjonistforbundet (uten år). *Økonomiske overgrep mot eldre.* Hentet 06.02.26 fra https://www.pensjonistforbundet.no/rad-og-tips/sikkerhet/okonomiske-overgrep-mot-eldre

Polismyndigheten (2023). *Operativa Rådsinsatsen Robert*. Hentet 18.12.25 fra https://www.youtube.com/watch?v=iw5SSYZtJzQ

Polismyndigheten (2025). Organiserad brottslighet 2025. Hentet 16.11.25 fra https://polisen.se/siteassets/dokument/organiserad_brottslighet/myndighetsgemensam-lagesbild---organiserad-brottslighet-2025.pdf

Politiet (2023). *Politiets trusselvurdering 2023.* Hentet 19.12.25 fra https://www.politiet.no/globalassets/tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2023.pdf

Politiet (2025). *Italienske hoteller utsatt for datainnbrudd – kopier av reisedokumenter på avveie.* Hentet 19.12.25 fra https://www.politiet.no/nyheter-og-presse/politidirektoratet/nyhet/2025-08-25/italienske-hoteller-utsatt-for-datainnbrudd-kopier-av-reisedokumenter-pa-avveie

Politiet (2025b). *Politiets trusselvurdering 2025.* Hentet 11.11.25 fra https://www.politiet.no/globalassets/tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2025.pdf

Politiet (2025c). *Entry/Exit System – et nytt system for grensekontroll i Schengenområdet.* Hentet 13.01.26 fra https://www.politiet.no/rad/grensepassering/entry-exit

Regeringen (2025). *Arbetslivskriminalitet. Upplägg, verktyg och åtgärder, fortsatt arbete.* Hentet 26.11.25 fra https://www.regeringen.se/contentassets/5dd9d5f20beb4ca98b249f9f55a2eddb/arbetslivskriminalitet--upplagg--verktyg-och-atgarder--fortsatt-arbete-sou_2025_25.pdf

Regjeringen (2025). *Førerkortdirektivet.* Hentet 17.12.25 fra https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2023/mars/forerkortdirektivet/id2996254/

Riksrevisjonen (2025). *Riksrevisjonens undersøkelse av Skatteetatens kontroll med merverdiavgift.* Hentet 23.12.25 fra https://www.riksrevisjonen.no/globalassets/rapporter/no-2025-2026/skatteetatenskontrollmedmerverdiavgift.pdf

Skatteetaten (2025). *Svar på forespørsel om informasjon til årsrapport om ID-misbruk.* Elektronisk kommunikasjon til Nasjonalt ID-senter.

Skattetaten (uten år). *D-nummer.* Hentet 06.02.26 fra https://www.skatteetaten.no/person/folkeregister/identitetsnummer-og-elektronisk-id/d-nummer/

SODI (2024). *Sluttrapport for rettshjelptilbudet ID-juristen.* Hentet 03.12.25 fra https://www.karnovgroup.no/hubfs/Norway/downloads/Bruk%20og%20misbruk%20av%20elektronisk%20identifikasjon/9.%20Sluttrapport%20for%20rettshjelpsprosjektet%20ID-juristen.pdf

SODI (2025). *Helhetlig, trygg og inkluderende digital identitetsforvaltning i Norge: Anbefalinger fra SODI-prosjektet.* Hentet 05.12.25 fra https://www.jus.uio.no/ifp/forskning/prosjekter/sodi/publikasjoner/rapporter-mv/sodi-rapport-5-2025.pdf

Statens vegvesen (2025). *Svar på forespørsel om informasjon til årsrapport om ID-misbruk.* Elektronisk kommunikasjon til Nasjonalt ID-senter.

Statens vegvesen (uten år). *Førerkort og yrkessjåførkompetanse fra Ukraina.* Hentet 07.02.26 fra https://www.vegvesen.no/forerkort/har-forerkort/utenlandsk-forerkort-i-norge/bruk-av-forerkort-fra-land-utenfor-eu-eos-i-norge/forerkort-fra-ukraina/

Store norske leksikon (2025). *Faglært*. Hentet 07.02.26 fra https://snl.no/fagl%C3%A6rt

Stø (2025). *BankID sparer samfunnet for milliarder.* Hentet 23.12.25 fra https://stoe.no/nyheter/bankid-sparer-samfunnet-for-milliarder

Sveriges radio (2023). *Rysktalande nätverk fixar skenäktenskap för att begå brott.* Hentet 18.12.25 fra https://www.sverigesradio.se/avsnitt/ryska-natverk-bakom-vag-av-skenaktenskap-och-skapade-identiteter-exploatering-vald-kriminalitet

Telenor (2024). *Advarer om ny svindelmetode: Slik kan kriminelle opprette abonnement i ditt navn.* Hentet 06.02.26 fra https://www.telenor.no/privat/artikler/sikkerhet/slik-kan-kriminelle-oprette-abonnement-i-ditt-navn/?srsltid=AfmBOorLh1t9w2jXZjb1fQ4jY_J5MFhZXNV_fpSFWkez525wFGQrwgy-

The Council for Higher Education Accreditation (uten år). *Degree Mills: An Old Problem & A New Threat.* Hentet 17.12.25 fra https://www.chea.org/degree-mills-old-problem-new-threat

Tolletaten (2025). *Trusselvurdering 2025.* Hentet 15.12.25 fra https://www.toll.no/files/628bd081966d88b036f8b0b92471f397084efd21.pdf

Trønder-Avisa (2025). *Betalte 30.000 kroner - fikk falske papirer som spesialist.* Hentet 17.12.25 fra https://www.t-a.no/betalte-30-000-kroner-fikk-falske-papirer-som-spesialist/s/5-116-2260214

UNE (2024). *Sammendrag: Tilbakekall.* Hentet 12.01.26 fra https://www.une.no/kildesamling/praksisbase-landingsside/2024/november/pb804254/

Utenriksdepartementet (2025). *Svar på forespørsel om informasjon til årsrapport om ID-misbruk.* Elektronisk kommunikasjon til Nasjonalt ID-senter.

Utlendingsdirektoratet (2025). *Svar på forespørsel om informasjon til årsrapport om ID-misbruk.* Elektronisk kommunikasjon til Nasjonalt ID-senter.

Utlendingsdirektoratet (2025b). *Omverdensanalyse 2025.* Hentet 22.12.25 fra https://www.udi.no/globalassets/om-udi/omverdensanalyse-v-2.0-var-2025.pdf

Utlendingsnemda (2025). *Svar på forespørsel om informasjon til årsrapport om ID-misbruk.* Elektronisk kommunikasjon til Nasjonalt ID-senter.

VG (2023). *Unge leier biler gjennom apper ulovlig.* Hentet 03.12.25 fra https://www.vg.no/nyheter/i/RGoLMO/unge-leier-biler-gjennom-apper-ulovlig

Økokrim (2025). *Trusselvurdering miljøkriminalitet 2025.* Hentet 06.02.26 fra https://img8.custompublish.com/getfile.php/5462918.2528.asbapuqmqpajs7/2025_Trusselvurdering%2B-%2BMilj%C3%B8kriminalitet-nett.pdf?return=www.okokrim.no

Nasjonalt ID-senter

POLITIET

KRIPOS