

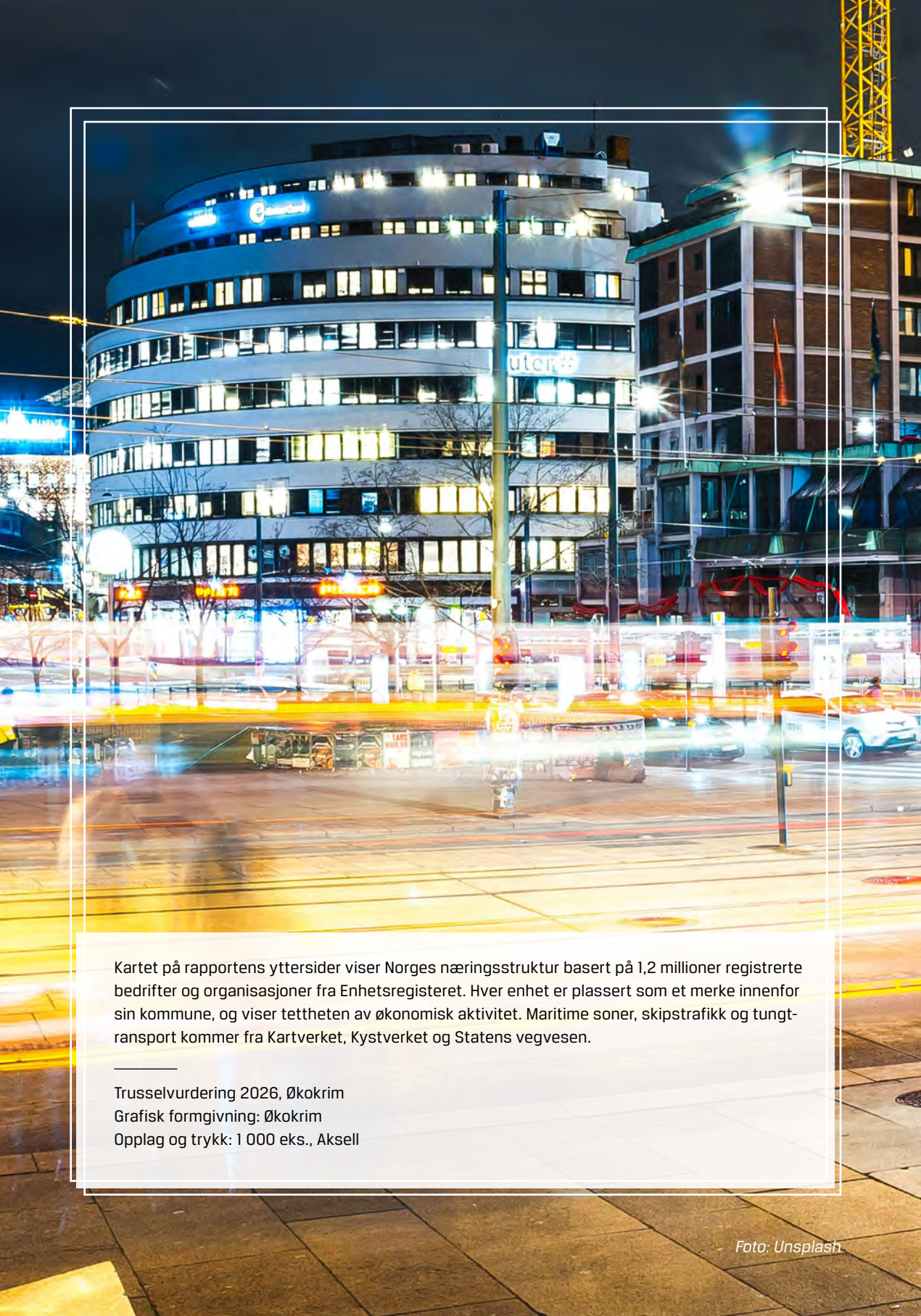


ØKOKRIM

TRUSSEL- VURDERING | 2026

Økonomisk kriminalitet





Kartet på rapportens yttersider viser Norges næringsstruktur basert på 1,2 millioner registrerte bedrifter og organisasjoner fra Enhetsregisteret. Hver enhet er plassert som et merke innenfor sin kommune, og viser tettheten av økonomisk aktivitet. Maritime soner, skipstrafikk og tungtransport kommer fra Kartverket, Kystverket og Statens vegvesen.

Trusselvurdering 2026, Økokrim
Grafisk formgivning: Økokrim
Opplag og trykk: 1 000 eks., Aksell

Forord

Kriminelle maksimerer utbytte ved å misbruke teknologi og ordninger og systemer som er selve fundamentet i det åpne og tillitsbaserte samfunnet vi har. Samtidig blir utbyttehåndteringen og hvitvaskingsprosessene stadig mer sofistikerte. Utviklingen skjer raskere enn før, nettverk tilpasser seg og bygger seg opp igjen i et tempo som utfordrer vår evne til å henge med. Konsekvensene er alvorlige og kan innebære store økonomiske tap, konkurransevridning, omdømmetap og svekket tillit til institusjonene vi er avhengige av.

Utbytte fra bedrageri, utnyttelse av arbeidstakere og narkotikasalgs investeres i norske bedrifter og eiendommer, og får et lovlig ytre. I virksomhetene begår de økonomisk kriminalitet. På denne måten viskes grensene mellom økonomisk kriminalitet og annen alvorlig kriminalitet ut.

Svenske kriminelle nettverk har for lengst etablert seg i Norge. Nettverkenes volds- og fryktt kapital brukes til å sikre posisjoner i et lukrativt narkotikamarked, og omsetningen genererer utbytte som norske aktører bistår med å hvitvaske. Europol beskriver hvordan de mest truende nettverkene ikke opptrer isolert, men inngår i et kriminelt økosys-

tem som legger til rette for samarbeid, motstandsdyktighet og rask tilpasning. Vi ser samme mønster i Norge.

Ingen enkeltaktør kan bekjempe denne trusselen alene. Det krever vedvarende samarbeid mellom politi, kontrolltater og privat sektor, noe etableringen av Ø-krim senteret er et uttrykk for. Et slikt samarbeid må bygge på en felles forståelse av hvem trusselaktørene er, hvilke sårbarheter de utnytter og utviklingen vi må forberede oss på å møte. Det er denne forståelsen vi håper at trusselvurderingen kan bidra til.



Pål K. Lønseth // Sjef for Økokrim



Innhold

Innledning.....	7	Risiko for at norske borgere begår korrupsjon i utlandet.....	45
En verdensorden i endring	11	Sårbarheter knyttet til korrupsjon og misbruk av myndighet.....	47
Økt risiko for økonomisk kriminalitet i forsvarssektoren	12	Kriminelle nettverk i næringslivet.....	49
Kriminelle nettverk bygger opp industrialisert bedragerivirksomhet ...	13	Kriminelle nettverk i velferds- foretak rettet mot unge	50
Kriminelle aktører etablerer seg i turistnæringen	15	Kriminelle nettverk i drosje- næringen	52
Skjult eierskap og mistenkelige transaksjoner i norsk fiskerinæring ...	16	Kriminelle nettverk i det app- baserte næringslivet	53
Informasjon, kompetanse og anonymitet til salgs.....	19	Sårbarheter knyttet til kriminelle nettverk i næringslivet	55
Profesjonelle tilretteleggere.....	20	Misbruk av fellesskapets midler	57
Kriminalitet som handelsvare.....	22	Kriminelle nettverk bedrar offentlige velferdsordninger	58
Innsidere	23	Misbruk av refusjonsordninger	59
Pengemuldyr	25	Skatte- og avgiftsunndragelse	61
Stråpersoner.....	26	Sårbarheter knyttet til misbruk av fellesskapets midler	63
Sårbarheter ved kontrollsystemer ..	29	Digitale bedragerier	65
Hvitvasking	31	Investeringsbedrageri	66
Handelsbasert hvitvasking	32	Nettbankbedragerier	67
Hvitvasking og verdioverføring gjennom digitale valutaer og verktøy	34	Annonsebedrageri	68
Hvitvasking via eiendom	36	Falsk nettjobb.....	69
Kriminelle benytter undergrunns- banktjenester	38	Sårbarheter knyttet til digitale bedragerier.....	71
Sårbarheter som utnyttes til hvitvasking	41	Begrepsliste	73
Korrupsjon og misbruk av myndighet ...	43	Anbefalt viderelesing	78
Korrupsjon i plan- og bygge- saksbehandling	44		



Foto: KI-generert, Økokrin

Innledning

Omfanget av *økonomisk kriminalitet* i Norge er ukjent siden mange lovbrudd aldri blir kjent eller anmeldt til politiet. Politiet erfarer likevel at kriminaliteten rammer bredt.

Anslag fra andre land illustrerer størrelsesordenen. En svensk analyse fra 2026 anslår den kriminelle økonomien i Sverige til 352 milliarder kroner i årlig omsetning og 185 milliarder i årlig utbytte, hvorav svart arbeid alene står for over halvparten av utbyttet.¹ Tallene understreker at økonomisk kriminalitet samlet sett utgjør en trussel mot vår velferdsstat og våre felles verdier.

Vi presenterer trusselbildet for økonomisk kriminalitet i Norge i åtte kapitler. Det første kapitlet beskriver hvordan geopolitisk utvikling påvirker trusselbildet i Norge, og trekker frem fire eksempler på dette. De øvrige syv kapitlene går nærmere inn på hvert kriminalitetsområde, og beskriver også tilretteleggere for kriminalitet som gjør det mulig for kriminelle nettverk å gjennomføre kriminaliteten.

Fordi truslene henger tett sammen, vil enkelte kapitler ha overlappende innhold. Vi trekker i rapporten særlig frem *sårbarheter* kriminelle utnytter innenfor de ulike kriminalitetsområdene. De presenteres i slutten av kapitlene. For noen av disse er tiltak allerede iverksatt, mens andre krever videre samarbeid eller ytterligere oppfølging.

Der ikke annet er angitt, bygger teksten på politiets interne informasjonskilder, inkludert hvitvaskingsregisteret. I tillegg har vi benyttet en rekke åpne kilder. Rapporten inneholder også en begrepsoversikt. Begreper som forklares i begrepsoversikten er merket med kursiv i teksten.

¹ Rostami, Mondani, Mellberg og Roine. 2026. *Svarta siffror – ESO-rapport om den kriminelle økonomiens omfattnng*.

Sentrale utviklingstrekk

I denne delen av rapporten beskriver vi de viktigste endringene i trusselbildet siden forrige trusselvurdering og de truslene vi vurderer vil bli mest fremtredende i årene som kommer.

Misbruk av foretak som sentral del av kriminell virksomhet

I 2024 beskrev vi hvordan kriminelt utbytte reinvesteres i den legale økonomien, og at skillet mellom kriminelle nettverk og legalt næringsliv gradvis viskes ut. To år senere er foretak i legalt næringsliv en sentral del av flere kriminelle nettverks virksomhet, og nettverkene er mer involvert i økonomisk kriminalitet enn tidligere.

Kriminelle nettverk har etablert seg i flere norske næringer og beveger seg dit kontrollen er svakest. I fiskerinæringen kan utenlandske nettverk oppnå kontroll i flere ledd av verdikjeden gjennom skjult eierskap i komplekse selskapsstrukturer. I app-baserte næringer gir arbeidslivskriminalitet og utnyttelse av sårbar arbeidskraft høy profitt med lav risiko. Vi forventer at flere kriminelle aktører vil etablere seg i nye næringer fremover.

Grensene mellom kriminalitetsområdene viskes samtidig ut. De samme aktørene, metodene og foretakene går igjen på tvers. Ett og samme foretak kan fungere som fasade utad, som verktøy for å flytte og skjule penger, og som arbeidsgiver for å utnytte ansatte eller sårbare grupper.

Et dynamisk kriminelt økosystem

I 2024 beskrev vi løst sammensatte nettverk med ad hoc-samarbeid tuftet på hvilke tjenester det til enhver tid var behov for. Europol omtaler nå de mest truede nettverkene som del av et dynamisk kriminelt økosystem preget av utstrakt samarbeid, stor motstandsdyktighet og rask tilpasning, der utslåtte nettverk raskt erstattes av nye.² Det som har endret seg er ikke hvordan nettverkene er organisert, men hvor raskt de reetableres.

² Europol. 2026. *The blueprint of criminal opportunism. Issue 2.*

En omfattende kriminell økonomi

Den kriminelle økonomien er av betydelig omfang. Utbytte fra kriminalitet konverteres inn i den lovlige økonomien, eller reinvesteres i ny kriminell virksomhet, og vokser i takt med den lovlige økonomien for øvrig.³

Hvitvasking finner stadig nye former utenfor det formelle finanssystemet, gjennom uformelle betalingstjenester og verdioverføring via ikke-finansielle tjenester. Samtidig forblir foretak, eiendom og internasjonal handel sentrale hvitvaskingsmetoder.

Korrupsjonsrisikoen ved anskaffelser forsterkes

I 2024 pekte vi på offentlige anskaffelser som var særlig utsatt for korrupsjon. Svekket internasjonal håndheving av antikorrupsjonsregelverk gir nå større spillerom for slik kriminalitet globalt, inkludert i Norge. Vi forventer at risikoen forsterkes innenfor forsvarssektoren. Svært store midler skal forvaltes raskt, ofte med hemmelighold og begrenset konkurranse.

KI effektiviserer kriminaliteten

I 2024 var kunstig intelligens (KI) først og

fremst noe kriminelle brukte for å skalere kjente modus. I dag settes deler av kriminalitetsutøvelsen bort til selvgående systemer, særlig innen bedrageri, som blir mer automatisert og treffer bredere.

Også misbruk av offentlige midler effektiviseres gjennom digitale verktøy og KI. Teknologien gjør det enklere å produsere fiktiv dokumentasjon og opprette eller misbruke identiteter, slik at flere separate søknader og ordninger kan styres av samme aktør uten at koblingen oppdages.

Overordnet utvikling

De neste årene vil trolig forsterke dette bildet. Kriminelle nettverk vil fortsette å integrere sine aktiviteter i den legale økonomien og etablere seg der kontrollen er svakest. Sammen med nettverkens evne til raskt å bygge seg opp, og en teknologiutvikling som forkorter veien fra plan til gjennomføring, endrer trusselbildet seg raskere enn kontrollapparatet. Dette krever at myndigheter og privat sektor evner å se sammenhengene på tvers av kriminalitetsområder, sektorer og landegrenser, fremfor å møte hver trussel isolert.

³ Europol. 2025. *Serious and Organised Crime Threat Assessment (SOCTA) - The Changing DNA of Serious and Organised Crime*.



Etterforskning av anskaffelse av sanitetsmateriell til Ukraina

Økokrim har siden april 2026 etterforsket en offiser i Forsvaret og en daglig leder i et privat selskap i forbindelse med en offentlig anskaffelse av sanitetsmateriell til Ukraina. Kontrakten, som er finansiert gjennom Nansen-programmet, har en verdi på mellom 30 og 40 millioner kroner. Offiseren er siktet for myndighetsmisbruk etter at han skal ha involvert seg i anskaffelsesprosessen til tross for forbindelser både til produktet som ble kjøpt inn og til personer i selskapet som fikk kontrakten. Den daglige lederen er siktet for økonomisk utroskap. Begge de siktede avviser anklagene og nekter straffskyld.

En verdensorden i endring

Forholdet mellom USA og Europa er under press og kompliseres av den vedvarende krigen i Ukraina. Krigføringen i Midtøsten bidrar til ytterligere global usikkerhet. Samtidig svekkes internasjonale institusjoner og normer i takt med at stormakter i økende grad prioriterer egne interesser fremfor etablerte spilleregler.⁴

Dette kan bli utnyttet av organiserte og opportunistiske kriminelle aktører som opererer på tvers av landegrenser.

Amerikanske myndigheter har endret håndhevingen av antikorrupsjonsloven Foreign Corrupt Practices Act (FCPA). Endringene i USA har utvidet mulighetsrommet for korrupsjon og hvitvasking i internasjonal handel.

Svekket internasjonal håndheving av antikorrupsjonsregelverk gir også større spillerom for statlige aktører som benytter økonomisk kriminalitet som virkemiddel. Dette gjelder også Norge.

Trusselbildet mot Norge preges også av at stater som Kina, Russland og Iran bruker en rekke virkemidler for å fremme egne interesser, inkludert kriminelle nett-

verk som *proxy-aktører*.⁵ Skjult eierskap i eiendom og selskaper, strategiske oppkjøp, bruk av innsidere, handelsbasert hvitvasking, korrupsjon og sanksjonsomgåelser er eksempler på dette.⁶

I den nye verdensordenen fungerer korrupsjon som en betydelig sikkerhetsrisiko fordi den undergraver demokratiske institusjoner, svekker staters motstandskraft mot ytre påvirkning og åpner døren for grenseoverskridende kriminalitet og autoritære krefter. Dette påvirker trusselbildet politiet møter på mange områder. I dette kapitlet trekker vi frem fire områder hvor vi forventer at kriminalitetsbildet vil påvirkes.

4 Etterretningstjenesten. 2026. *Fokus 2026*.

5 Politiets sikkerhetstjeneste. 2026. *Nasjonal trusselvurdering 2026*.

6 Tax Justice Norge. *Skjult eierskap i Norge. Analyse av det nye eierregisteret*.

Økt risiko for økonomisk kriminalitet i forsvarssektoren

Forsvarsbudsjettene i Norge og Europa øker betydelig, og ventes å øke ytterligere. Det er avsatt betydelige midler til utvikling av forsvarsmateriell, i tett samarbeid mellom næring, forskning og forsvarssektoren. Behovet for rask teknologiutvikling og anskaffelser kan gi økt handlingsrom for aktører som søker egen vinning.

Transparency International har vist at økte forsvarsutgifter generelt øker korrupsjonsrisikoen,⁷ og norske bidrag kan bli kanalisert til formål i områder med høyt korrupsjonsnivå. Ukraina er et land med kjent høy korrupsjonsrisiko.⁸ Samtidig gir Norge omfattende sivil og militær støtte til Ukraina. Et element som særlig øker korrupsjonsrisikoen ved forsvarsrelaterte anskaffelser er stort hemmelighold.

Det har over tid vært svakheter ved styring og internkontroll ved innkjøp av forsvarsmateriell i Norge. En ekstern evaluering av Forsvarets varslingsssystem fra 2022 viste at varslingsordningen burde styrkes, blant annet gjennom bedre retningslinjer og tydeligere ansvarsfor-

deling. *Korrupsjon* inngikk som en av flere kategorier av alvorlige forhold varslingsordningen skulle fange opp.⁹ I desember 2025 ble det kjent at Forsvarsmateriell graderte dokumenter om et overforbruk på flere hundre millioner kroner for å unngå offentlig kjennskap. Slike svakheter, sammen med svake varslingskanaler gir et betydelig handlingsrom for korrupsjon og annen uetisk adferd.

Korrupsjon eller andre økonomiske misligheter i forsvarsrelaterte anskaffelser kan føre til overprising eller urettmessige betalinger, samt leveranser av materiell med lavere kvalitet enn forutsatt.¹⁰ Samlet sett kan dette få alvorlige konsekvenser for nasjonal sikkerhet, Forsvarets operative evne og befolkningens tillit til sektoren.

7 Transparency International. 2024. *Trojan Horse Tactics: Military spending, corruption and the need for transparency and good governance*.

8 Norad. 2026. *50 millioner til anti-korrupsjon i Ukraina*.

9 PWC. 2022. *Det skal nytte å si ifra. Evaluering av forsvarets varslingsordning*.

10 Økokrim. 2026. *Økokrims vurdering av økt korrupsjonsrisiko i forsvarssektoren*.

Kriminelle nettverk bygger opp industrialisert bedragerivirksomhet

De siste årene har det vokst frem en form for organisert kriminalitet som ofte omtales som «industrialisert bedragerivirksomhet». Den kjennetegnes av stor skala, profesjonelle strukturer, klare arbeidsoppgaver og høy grad av organisering. Fremveksten av denne virksomheten henger sammen med svekket statlig kontroll i enkelte regioner i Sørøst-Asia. Særlig i deler av Kambodsja, Myanmar og Laos har det utviklet seg territorier hvor kriminelle nettverk driver systematisk bedragerivirksomhet.¹¹ Aktiv bruk av moderne teknologi som for eksempel kunstig intelligens, gjør det mulig for kriminelle nettverk å gjennomføre bedrageri i stor skala gjennom telefon, e-post og digitale tjenester.

Virksomhetene har ofte likhetstrekk med ordinær næringsvirksomhet, med klare roller, opplæring og resultatkrav. Mange arbeider under tvang og er ofre for menneskehandel. FNs høykommissær for menneskerettigheter har dokumentert at personer som ikke når de fastsatte bedragerimålene, straffes med vold, seksuell vold, tortur og innesperring.¹²

Også i Øst-Europa har det blitt avdekket at kriminelle har etablert store call-sentre som har blitt brukt til å bedra ofre i stor skala. Europol avdekket et slikt call-senter i Albania som opererte som et foretak med opptil 450 ansatte. De anslår at tapene knyttet til investeringsbedrageri fra dette senteret er 50 millioner euro.¹³ Det som skiller dette fra virksomheten i deler av Sørøst-Asia, er både omfanget og graden av tvang mot dem som utfører arbeidet. Senteret i Albania fremstår som kriminell virksomhet drevet av noen hundre ansatte, mens de asiatiske bedragerisentrene i langt større grad er koblet til menneskehandel og tvang, og opererer med flere tusen arbeidere.

Bedragerioperasjonene genererer flere milliarder euro i inntekter og rammer ofre i Norge, Europa og andre deler av verden. FN peker på at slike bedragerioperasjoner er tett knyttet til profesjonelle hvitvaskingsnettverk, der midlene kanaliseres gjennom flere land og finansielle systemer for å skjule opprinnelsen.¹⁴ Dette kan inkludere bruk av kryptovaluta, stråpersoner og uformelle betalingssystemer.

11 United Nations Office on Drugs and Crime. 2025. *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*.

12 FN (20.02.2026). *UN report details grave abuses against those trafficked into scam centres*.

13 Europol. 2026. *Call centres dismantled and ten arrested in EUR 50 million online fraud case*.

14 FN (21.05.2025). *Scam centres are a 'human rights crisis', independent experts warn*.



Kriminelle aktører etablerer seg i turistnæringen

I takt med veksten i utenlandsk turisme har reiselivsnæringen i Norge blitt en internasjonal næring, der en betydelig andel av bedriftene er utenlandske. Særlig Nord-Norge opplever stor tilstrømming av utenlandske turister gjennom blant annet nordlysturisme.

Kontrolletatene har de siste årene avdekket manglende transportløyver og kjøresedler, skatte- og avgiftsunndragelser, hvitvasking og et stort omfang av svart arbeid i denne næringen. Enkelte arrangører opererer mer organisert, blant annet gjennom *skallselskaper* for å skjule aktivitet og unndra skatt. Flere av de kriminelle aktørene er utenlandske, og en rekke av disse har blitt utvist fra Norge som følge av lovbruddene de har begått.

Økokrim har informasjon om at deler av næringen brukes til organisert økonomisk kriminalitet med omfattende handelsbasert hvitvasking med kobling til kinesiske myndigheter. Bruk av kontanter og kinesiske betalingsplattformer bidrar til å tilslore pengestrømmer. Det er også

indikasjoner på at enkelte turistguider er delaktige og får betalt for å lede turister til utvalgte butikker hvor kontanter hvitvaskes.

Samtidig har Nord-Norge en viktig militærstrategisk rolle, med betydelig tilstedeværelse av allierte styrker gjennom øvingsaktivitet og allierte anløp. Etterretningstrusselen fra Kina er stor og PST forventer at den vil tilta, drevet særlig av økonomiske virkemidler som investeringer og oppkjøp.¹⁵ Reiselivsnæringen kan by på et mulighetsrom for slike aktører fordi det er krevende å skille mellom legitim næringsvirksomhet og aktører med andre motivasjoner.

15 Politiets sikkerhetstjeneste. 2025. *Nasjonal Trusselvurdering 2025*.

Skjult eierskap og mistenkelige transaksjoner i norsk fiskerinæring

Utenlandsk eierskap i norsk fiskerinæring er i seg selv ikke ulovlig. Regelverket åpner for at utenlandske aktører kan eie inntil 40 prosent i norske fiskefartøy eller rederier som direkte eller indirekte eier slike fartøy.¹⁶

Utenlandsk eierskap i fiskeflåten er økende, selv om det fortsatt er lavt samlet sett.^{17,18} Det som særlig kjenner seg ut i situasjonsbildet i 2026, er ikke omfattende utenlandsk overtakelse, men mer komplekse eierstrukturer og større uklarhet om hvem som i praksis styrer virksomheten. Dette utfordrer et grunnleggende prinsipp i norsk fiskeripolitikk: at fiskeflåten i hovedsak skal være eid av aktive fiskere, og at kontrollen over ressursene skal ligge i Norge.

Når selskaper er bygget opp gjennom flere ledd og på tvers av land blir det også vanskeligere for myndighetene å følge pengestrømmer og se hvem som faktisk har innflytelse. Slik kontroll fremgår ikke nødvendigvis av eierstrukturen. Den kan i stedet ligge i aksjonæravtaler, kontrakter og gjeldsforhold.

Økokrim har informasjon om at norske

sjømatelskaper blir kjøpt opp via land med begrenset åpenhet om eierskap, etterfulgt av omfattende pengeoverføringer uten tydelig kommersiell begrunnelse. Det er avdekket tilfeller av selskaper registrert i norske kommuner uten ansatte eller påvist drift, men med høy finansiell aktivitet og eierforbindelser til selskaper i høyrisikoområder.

I et tilfelle mistenkes både norske og utenlandske eiere av flere selskaper å inngå i et kriminelt nettverk. Nettverket knyttes til fiktive lån, bruk av midler med ukjent opphav, hyppig kjøp og salg av fiskefartøy og manglende sammenheng mellom fartøy, kvoter og fangst. Nettverket mistenkes også for *handelsbasert hvitvasking*, gjennomført over flere ledd og landegrenser, ved bruk av skall-selskap i utlandet og norske bedrifter i fiskerinæringen. Eierskap i fiskerinæringen gir både legitim inntekt og mulighet for økonomisk kriminalitet.

Det kan også være uklart hvem som kjøper norsk fisk. Handelsmønstre viser at norske foretak i flere tilfeller inngår i transaksjoner der motpartens rolle eller

¹⁶ Lov om retten til å delta i fiske og fangst.

¹⁷ Riksrevisjonen. 2020. *Undersøkelse av kvotesystemet i kyst og havfisket: Kap. 2.2.4 Utenlandsk eierskap i fiskeflåten er økende, men fortsatt lavt.*

¹⁸ Nærings- og fiskeridepartementet. 2024. *Meld. St. 7. Folk, fisk og felleskap – en kvotemelding for forutsigbarhet og rettferdig fordeling.*

forretningsområde ikke samsvarer med varetypen. Eksempler er fakturering av laks til et teknologiselskap, og eksport til en svært begrenset kundebase, med betalinger nesten utelukkende i runde beløp. Denne typen mistenkelige transaksjoner kan være handelsbasert hvitvasking, men det kan også være *sanksjonsomgåelser*. Dette er særlig relevant i næringer med utstrakt internasjonal handel, som fiskerinæringen. De samme

komplekse eierstrukturene som skjuler hvem handelspartneren er, kan også skjule varens opprinnelse.

Tolletaten vurderer det som en økende risiko at russisk fisk gis ny opprinnelse i tredjeland før videresalg til norske aktører.¹⁹ Konsekvensene kan bli svekket etterlevelse av sanksjonsregimet mot Russland, redusert tillit til norsk sjømatnæring og økte muligheter for økonomisk kriminalitet.

Kontroll gjennom gjeld

Norske fiskekvoter er blant verdens mest verdifulle fiskerettigheter. For å sikre at ressursen forblir under norsk kontroll, setter deltakerloven en grense for hvor stor eierandel en utenlandsk aktør kan ha. Loven regulerer eierskap, men ikke verdien av kvotene. Det skaper et gap. En utenlandsk investor kan stifte eller kjøpe et norsk fiskeriselskap, men holde eierandelen innenfor lovens grense. Den samme investoren finansierer resten av selskapet, via et lån som er mange ganger større enn verdien av eierandelen.

I eierskapsregistrene fremstår det som en liten, lovlig eierandel, men i praksis har investoren, som långiver, betydelig innflytelse over selskapet. Hverken kontrollmekanismer eller eierskapsregister fanger dette opp fordi de registrerer og viser eierskap gjennom aksjer, ikke gjeld. Kontrollen som utøves gjennom lånevilkår er dermed usynlig.

19 Tolletaten. 2025. *Trusselvurdering 2025*.



Informasjon, kompetanse og anonymitet til salgs

Kriminelle nettverk organiseres i dag etter en forretningsmodell, der tjenester, kompetanse og digitale verktøy kjøpes og selges på tvers av landegrenser.²⁰

Nettverkene søker også aktivt å etablere relasjoner som kan gi tilgang til informasjon, innflytelse og strategiske fordeler²¹ og benytter tilretteleggere som tilbyr spesialiserte tjenester, for eksempel innen hvitvasking, cyberkriminalitet og korrupsjon.

Disse tilretteleggerne bidrar med kompetanse som gir kriminaliteten et lovlig ytre, relasjoner som gir tilgang til personer i maktposisjoner, tilganger som gir innsyn i og kontroll over systemer, og identiteter som kan stilles til disposisjon for å skjule hvem som reelt sett står bak. Tilretteleggerne utgjør dermed en usynlig, men avgjørende infrastruktur for

den kriminelle økonomien. Deres tjenester binder sammen lovlige og ulovlige aktiviteter og gjør det mulig for kriminelle nettverk å operere effektivt.

Denne forretningsmessige organiseringen forutsetter tilgang til personer, som bevisst eller ubevisst, kan bidra til å gjennomføre den enkelte kriminelle handlingen. I dette kapitlet går vi nærmere inn på ulike typer aktører og kompetanse som kriminelle nettverk benytter seg av for å gjennomføre økonomisk kriminalitet.

20 Europol. 2025. *Serious and Organised Crime Threat Assessment (SOCTA) - The Changing DNA of Serious and Organised Crime*.

21 Berge og Humlesjø. 2024. *Honungsfällan: Historien om Swedbank, Ryssland og världens största penningstvåttskandal*.

Profesjonelle tilretteleggere

Profesjonelle tilretteleggere gir kriminell virksomhet et lovlig ytre. Dette er personer med spesialisert kompetanse innen områder som regnskap, finans, skatt, offentlige ordninger, teknologi eller jus, men også leger og andre fagpersoner som kan utstede dokumentasjon med høy grad av tillit. Det gjelder både profesjoner med rapporteringsplikt etter hvitvaskingsregelverket og andre spesialiserte roller i det offentlige og i næringslivet.

Europol peker på at aktører som advokater, regnskapsførere, eiendomsmedglere og logistikktilretteleggere kan være avgjørende for kriminelle nettverks evne til å vokse, hvitvaske utbytte og unngå avdekking.²²

Tilretteleggerne er særlig nyttige for kriminelle som opererer i næringslivet. De bistår med å tilpasse drift og rapportering til regelverket, slik at selskapsstrukturer fremstår som lovlig næringsvirksomhet. Metodene omfatter bruk av falske, fiktive eller manglende underlagsdokumenter, fiktive lønnskostnader eller uriktige verdifastsettelse, samt rådgivning rettet mot skatteunndragelse.

Enkelte regnskapsførere fremstår i praksis som drevet av kriminelle nettverk, og være en sentral del av nett-

verkets forretningsmodell. I noen tilfeller fungerer regnskapsførere og revisorer som en felles ressurs for flere kriminelle nettverk som ellers ikke har forbindelser til hverandre. I slike tilfeller er de ikke bare tilretteleggere for enkeltkriminelle, men sentrale bindeledd som kobler sammen virksomheter, personer og pengestrømmer, og bidrar til å koordinere kriminalitet som hvitvasking, skatte- og avgiftsunndragelse og bedrageri.

Advokater kan muliggjøre hvitvasking ved å åpne kontoer, tilrettelegge for lån eller «lukke øynene» i portvokterroller. Risikoen knyttet til advokaters *klientkontoer* er særlig betydelig, fordi transaksjonene der til dels er skjermet av taushetsplikten. Det er også attraktivt for kriminelle nettverk å nyttiggjøre seg av advokaters informasjonstilgang og status. Taushetsbelagt informasjon kan brukes som kapital i kriminelle nettverk for å kontrollere underordnede eller motstandere. Økokrim kjenner til flere tilfeller der advokater har bistått kriminelle nettverk, blant annet ved å gi dem tilgang til taushetsbelagte politiopplysninger mot betaling, og ved å bidra til å hvitvaske utbytte gjennom oppkjøp av virksomheter.

²² Europol. 2026. *Decoding the EU's most threatening criminal networks*.



Regnskapsfører dømt til seks års fengsel for grove økonomiske lovbrudd

En regnskapsfører ble i 2025 dømt til seks års ubetinget fengsel og rettighetstap på ubestemt tid. Regnskapsbyrået ble omtalt som en «svindelmaskin» som ble brukt til å bistå kunder og kriminelle aktører med skatteunndragelser og hvitvasking, blant annet ved bruk av fiktive underleverandører, stråmenn, falske fakturaer og uriktige avtaler. Totalt seks personer ble domfelt i sakskomplekset, for blant annet grove skattesvik, grov økonomisk utroskap, bruk av uriktige dokumenter for skatteformål, grove regnskapsovertredelser, grov hvitvasking og ulovlig betalingstjeneste. Retten la til grunn at overtredelsene var særlig alvorlige fordi de ble begått av en betrodd profesjonell aktør.

Kilde: LB-2024-18407

Kriminalitet som handelsvare

Der de profesjonelle tilretteleggerne bruker en lovlig yrkesrolle til å dekke over kriminalitet, representerer *kriminalitet som handelsvare* en modell der kriminelle tjenester tilbys og selges i et marked, på samme måte som varer og tjenester i lovlig næringsvirksomhet. Korrupsjonsmeglere og spesialiserte hvitvaskingsaktører er to eksempler på slike tilbydere.

Korrupsjonsmeglere setter kriminelle nettverk i kontakt med personer i maktposisjoner som de ønsker å påvirke. Verdien til korrupsjonsmeglerne ligger ikke i fagkompetanse, men i posisjon og nettverk. De kjenner både den som ønsker å påvirke og den som skal påvirkes, og fungerer som mellomledd som formidler og skjærer kontakten mellom partene. Europol omtaler korrupsjon som et sentralt virkemiddel for å muliggjøre eller skjule øvrig kriminalitet.²³ Korrupsjonsmeglere tilrettelegger for dette og bidrar dermed til å opprettholde og styrke kriminell virksomhet.

Spesialiserte hvitvaskingsaktører sikrer det kriminelle utbyttet, og er selve forutsetningen for at kriminalitet kan videreføres og vokse. Tjenestene har utviklet seg til en profesjonalisert bransje der enkeltaktører og nettverk påtar seg

hvitvaskingsoppdrag etter behov, blant annet gjennom transport av kontanter, organisering av muldyrsaktivitet og veksling mellom kontanter og kryptovaluta. Tilbys dette løpende fremfor enkeltstående oppdrag, kalles det *illegal undergrunnsbankvirksomhet*.

I det norske markedet tilbys hvitvaskingstjenester både av enkeltaktører og av organiserte nettverk. Enkeltaktørene håndterer gjerne mindre oppdrag, mens de organiserte nettverkene tilbyr hvitvasking av større beløp gjennom mer komplekse metoder, ofte ved å utnytte lovlige selskapsstrukturer og handelsbasert hvitvasking. I 2025 ble flere personer i et slikt nettverk i Norge pågrepet, og betydelige verdier i kontanter, gull og andre verdigjenstander ble tatt i beslag. En sentral person skal ha hentet ut minst 180 millioner kroner de siste tre årene.

²³ Europol. 2025. *Serious and Organised Crime Threat Assessment (SOCTA) - The Changing DNA of Serious and Organised Crime*.

Innsidere

Bruk av *innsidere* er sentralt for gjennomføring og fordekking av organisert kriminalitet, fordi tilgang til innsiden kan undergrave selv godt utviklede kontrollsystemer. Det er mye som tyder på at innsidevirksomhet er mer omfattende og utgjør en større utfordring enn det som fremkommer i offentlig statistikk og rapportering.²⁴

Økokrim er kjent med at innsidere, mot en økonomisk kompensasjon, har innvilget lånesøknader til kriminelle aktører på urettmessig grunnlag. I tillegg har Økokrim også informasjon om at innsidere i kredittselskaper har samarbeidet med aktører i eiendomsbransjen ved å manipulere inntektsopplysninger for å sikre at lånesøkere får innvilget lån de ikke er berettiget til.

Økokrim mottar også jevnlig informasjon om at kriminelle aktører og nettverk har nære knytninger til ansatte i ulike offentlige etater som har tilgang til sensitiv informasjon som kan være nyttig for nettverkene. Ansatte med tilgang til sensitive opplysninger kan både bevisst og ubevisst gi ifra seg informasjon som er attraktiv for kriminelle men også manipulere eller endre opplysninger i egne systemer.

Utviklingen i Norge må ses i sammenheng med situasjonen i Sverige, der man blant organiserte kriminelle ser en kontinuerlig etterspørsel etter innsidere.²⁵ Her jobber kriminelle målrettet for å skaffe seg tilgang i alle samfunnssektorer, inkludert bank, politi og rettsvesen.

Videre har man sett flere eksempler på at havneansatte har blitt brukt for smugling av narkotika, og mye tyder på at kriminelle nettverk er avhengige av innsidere for å få gjennomført narkotikasmugling og for å unngå toll- og grensekontroller.²⁶ Havneansatte er viktige innsidere fordi de innehar verdifull informasjon om sikkerhetsvakter og tollpersonells plassering og arbeidstid. I Danmark har det blitt avdekket at flere ansatte ved Aarhus havn har vært del av et kriminelt mc-miljø, eller hatt tette knytninger til aktører i dette miljøet som er dømt for narkotikakriminalitet. Vi ser at ansatte ved havner har denne typen knytninger også i Norge.

24 KPMG. 2025. *Innsiderisiko. Dybdeundersøkelse om økonomisk kriminalitet og innsidetrusselen.*

25 Brå. 2024. *Möjliggörare för kriminella nätverk, Rapport 2024-2.*

26 World Customs Organization. 2025. *Infiltration of maritime cargo supply chains.*



Pengemuldyr

Pengemuldyr er personer som stiller bankkontoen sin eller tilgangen til andre betalingsløsninger til disposisjon for å motta og videreformidle penger på vegne av andre.

Omfanget av kriminelles bruk av pengemuldyr er ukjent, men fremstår å ha økt i takt med økningen i digital kriminalitet. Europeiske politiaksjoner har identifisert at mer enn 90 prosent av pengemuldyrtransaksjonene har vært knyttet til nettopp digital kriminalitet.²⁷ Fenomenet finnes også på tvers av landene i Norden. Det har vært en økning i bruken av svenske pengemuldyr de siste årene.

Transaksjonene kan bevege seg raskt mellom flere muldyr, kontoer, betalingsløsninger og land. Hver overføring skaper et nytt ledd i kjeden og gjør det vanskeligere å følge pengene tilbake til den opprinnelige kriminaliteten. For kriminelle nettverk er denne rollen derfor en enkel måte å skape avstand mellom seg selv og det straffbare utbyttet på.

Kriminelle nettverk rekrutterer i stor grad pengemuldyr via sosiale medier,

i meldingstjenester eller gjennom annonser som lover enkle arbeidsoppgaver og raske penger. Datingtjenester brukes også som rekrutteringsarena.²⁸

I mange tilfeller er personer som rekrutteres til denne rollen i en økonomisk sårbar livssituasjon.²⁹ Både unge og eldre rekrutteres. Politiet har sett at barn helt ned i 10-årsalderen har blitt benyttet som pengemuldyr, ofte etter løfter om å tjene raske penger. Kontakten kan komme fra kriminelle aktører på nett, men også fra jevnaldrende eller andre ungdommer de allerede kjenner. En del eldre rekrutteres eller manipuleres på tilsvarende måte til å bistå som pengemuldyr. I enkelte tilfeller som del av bedragerier rettet mot dem selv.

Motivasjonen for å gjennomføre transaksjoner er ofte profitt, men i noen tilfeller blir pengemuldyrene manipulert, truet eller tvunget inn i rollen. Enkelte er også uvitende om sin egen rolle, for eksempel ved identitetsmisbruk.

²⁷ Europol. 07.08.2025. *Money Muling*.

²⁸ Kripas. 2024. *Cyberkriminalitet 2024*.

²⁹ Europol. 2025. *Serious and Organised Crime Threat Assessment (SOCTA) - The Changing DNA of Serious and Organised Crime*.

Stråpersoner

For å skjule hvem som egentlig står bak en virksomhet eller en aktivitet kan kriminelle bruke stråpersoner eller stråelskaper.³⁰

Stråpersoner og *stråelskaper* benyttes av kriminelle aktører som opererer i en rekke bransjer og flere sentrale kriminelle aktører i ulike kriminelle nettverk benytter aktivt stråpersoner i sin virksomhet. Omfanget av bruk av stråpersoner fremstår for politiet som betydelig og legger grunnlaget for at kriminelle nettverk kan operere i næringslivet på den måten de gjør i dag.

Praksisen er ofte mer systematisk enn enkeltstående stråpersoner. I flere tilfeller plasseres nærstående: ektefeller, svigerforeldre eller andre i familie- eller lojalitetsrelasjon, i sentrale formelle roller på tvers av et helt nettverk av selskaper, uten at den reelle aktøren selv innehar noen formell posisjon. En og samme stråperson kan inneha et betydelig antall slike roller samtidig.

Stråpersoner er eksempelvis mye brukt av aktører innen *arbeidslivskriminalitet* som tidligere er straffet og fradømt retten til å drive selvstendig nærings-

virksomhet. Kriminelle nettverk knyttet til drift av velferdsforetak for barn benytter også stråpersoner for å kamuflere sin tilknytning til foretakene ved eksempelvis søknad om offentlige midler og anbud. Også i fiskerinæringen benyttes stråpersoner for å kamuflere utenlandsk eierskap.

Noen stråpersoner vet at identiteten deres brukes og får betaling for det eller hjelper bakmannen av lojalitet. De kriminelle utnytter også sårbare personer, både norske og utenlandske. I enkelte tilfeller er ikke de som får sin identitet misbrukt klar over det.

Bruk av stråpersoner gjør det mulig å drive virksomhet videre selv etter at aktøren er dømt eller fratatt næringsrett. Dermed mister sanksjoner som *konkursskarantene* og næringsforbud mye av sin effekt. Stråpersoner er dessuten lette å skifte ut, noe som gjør nettverkene bak dem vanskelige å ramme varig. Kriminelle aktører kan bli sittende igjen som reelle eiere av norsk næringsliv, uten at det noen gang kommer til syne i offentlige registre.

30 Nasjonalt tverretattlig analyse- og etterretningssenter (NTAES). 2026. *Profittmotiverte lovbrudd i arbeidslivet. Risikovurdering arbeidslivskriminalitet*.



Identitet som handelsvare

Identitet er blitt en handelsvare som brukes både til å gjennomføre og skjule kriminalitet, og anses for å være en sentral del av den kriminelle infrastrukturen. Med kontroll over en annen persons elektroniske ID (eID) kan nettverkene opprette selskaper i andres navn, rapportere inn fiktiv aktivitet og hente ut uberettigede utbetalinger, momsrefusjon og banklån.

En fremtredende utsatt gruppe er personer som overlater ID og dokumenter frivillig, men uten å forstå konsekvensene. Dette er ofte arbeidsinnvandrere som lures under påskudd om hjelp til å navigere det norske systemet. En annen utsatt gruppe er ressursvake EU/EØS-borgere som rekrutteres til Norge på falske arbeidstilbud, og som bistås med folkeregistrering, bankkundeforhold og eID før nettverkene overtar kontrollen. Når kontroll over sårbare personers identiteter tilegnes på denne måten, er grensen mot menneskehandel uskarp.

Siden forrige trusselvurdering har politiet avdekket at eID i flere tilfeller blir brukt som oppgjør for kriminell gjeld. I en intern gjennomgang av nærmere tusen identiteter misbrukt til bedrageri og registermanipulasjon, fant politiet at størstedelen tilhørte unge menn med narkotikagjeld. Gjennom trusler og vold tar nettverkene kontroll over offerets eID, og bruker den til å søke lån og offentlige ytelser, registrere virksomheter, signere kontrakter og endre adresser. Misbruket anmeldes sjelden, og ofrene blir sittende igjen med betydelig gjeld i eget navn, ofte i millionklassen.



Stråselskap basert på misbrukt identitet – et fiktivt eksempel

En person kom til Norge etter å ha blitt forespeilet arbeid i bygg- og anleggsbransjen. Med hjelp fra en kontakt i Norge opprettet han et kundeforhold i en bank og fikk norsk BankID. Han arbeidet imidlertid svart, og kort tid etter flyttet han tilbake til hjemlandet. Etter at han flyttet, ble hans BankID overtatt og brukt av andre. Identiteten ble registrert på en adresse og brukt til å opprette og registrere vedkommende som daglig leder og styreleder i flere foretak. Gjennom disse foretakene ble det rapportert fiktive lønnsopplysninger. Med dokumentert (men fiktiv) inntekt ble det innvilget lån i en rekke banker. Lånebeløpene ble utbetalt, men aldri tilbakebetalt.

De samme opplysningene ga også grunnlag for Nav-ytelser som sykepenger, arbeidsavklaringspenger og foreldrepenger. I tillegg ble det sendt inn merverdiavgiftsoppgaver for å få urettmessig utbetalt inngående merverdiavgift.

Sårbarheter ved kontrollsystemer

Kapitlet har vist at kriminelle nettverk er avhengige av personer og tjenester utenfor selve nettverket for å gjennomføre og skjule sin virksomhet. Felles for disse er at de utnytter svakheter i kontrollsystemer som skulle vært en hindring for dem. Nedenfor pekes det på sentrale sårbarheter som gjør denne typen tilrettelegging mulig.

Manglende etterkontroll av digital identitet

Digitale identitetsløsninger (eID), som BankID, forutsetter at den som bruker identitetsbeviset, faktisk er den rettmessige innehaveren. Når en eID først er etablert, er det imidlertid lite kontroll med hvem som faktisk bruker den. Dette gjør det mulig for kriminelle å overta og misbruke andres eID over tid uten at det oppdages, blant annet for å inneha eierskap, styreverv og ansettelsesforhold i virksomheter, samt til å begå bedragerier.

Manglende bakgrunnssjekk ved ansettelser

For mange stillinger er det ikke krav om bakgrunnssjekk før ansettelse, og der politiattest kreves, dekker den bare den mest alvorlige kriminalhistorikken registrert i Norge. Den fanger i liten grad opp mengdekriminalitet, kriminalitet begått i utlandet, praktisk skikkethet, lojalitetsbånd til kriminelle nettverk eller reell rollebruk over tid. Svakheten forsterkes ved bemanningsselskaper, underleverandører eller parallelle ansettelsesforhold, fordi

ansvaret for egnethetsvurderingen da lett pulveriseres. Personer med kriminell bakgrunn eller tette knytninger til kriminelle nettverk kan få tilgang til sårbare grupper, sensitiv informasjon, havner og grensepasseringer eller økonomiske verdier.

Manglende kobling mellom konsesjonskrav og reelt eierskap

Enkelte typer virksomhet krever tillatelse (konsesjon). Et vilkår for å få denne er ofte at eieren anses egnet, blant annet at vedkommende ikke er straffet eller tidligere har mistet tillatelser. For finansforetak må den som vil erverve en betydelig eierandel, meldes og godkjennes av Finanstilsynet på forhånd. Kontrollen retter seg imidlertid mot hvem som står oppført som eier, ikke mot hvem som faktisk tar avgjørelsene. En person som selv ikke ville fått konsesjon kan derfor sette inn en stråperson som formell eier, slik at egnethetsvurderingen består på papiret mens den reelle bakmannen likevel styrer virksomheten.



Hvitvasking

Hvitvasking gjør det mulig for kriminelle å sikre, skjule og bruke utbytte fra kriminalitet. Utbyttet reinvesteres i kriminell virksomhet eller føres inn i den legale økonomien. Internasjonale anslag tilsier at det årlig hvitvaskes verdier tilsvarende mellom 2 og 5 prosent av globalt bruttonasjonalprodukt (BNP).³¹

Kriminelle benytter ulike metoder for å hvitvaske utbytte. Metodene endres i takt med regulering, teknologi og markedsforhold. Kontanter utgjør fortsatt en sentral del av den kriminelle økonomien. Strengere krav til dokumentasjon av kontanters opprinnelse de siste årene har trolig ført til at mer utbytte hvitvaskes innenlands eller veksles til kryptovaluta og annen valuta, kostbare klokker og smykker, bruktbiler og kunst.

Foretak brukes også til å hvitvaske kriminelt utbytte. Gjennom foretak kan kriminelle skjule hvem som kontrollerer verdiene, blande lovlige og ulovlige midler og gjennomføre større transaksjoner som fremstår som legitime. Mulighetene dette gir, kan være en viktig årsak til at kriminelle etablerer seg i næringslivet. Handelsbasert hvitvasking innebærer at handel med varer eller tjenester brukes til å skjule eller flytte kriminelt utbytte. Foretak kan også brukes til å investere

utbytte i eiendom og tilsløre hvem som reelt eier eller kontrollerer verdiene.

Strengere bankkrav og kontantrestriksjoner gjør samtidig alternative kanaler for verdioverføring mer attraktive. Verdioverføring gjennom ikke-finansielle kanaler og *uformelle verdioverførings-systemer* gjør det mulig å flytte verdier raskt over landegrenser og gjør det vanskeligere å identifisere avsendere, mottakere og pengenes opprinnelse. Utviklingen peker mot en parallell finansiell økonomi der utbytte både skjules, flyttes og forvaltes utenfor det regulerte finansielle systemet.

Kapitlet beskriver handelsbasert hvitvasking og hvitvasking gjennom eiendom, samt hvordan digitale løsninger brukes til å flytte og skjule kriminelt utbytte. Det tar også opp hvordan spesialiserte aktører tilbyr undergrunnsbank tjenester til kriminelle nettverk.

31 United Nations. 2011. *Illicit money: how much is out there?*

Handelsbasert hvitvasking

Handelsbasert hvitvasking er en samlebetegnelse for metoder der handelssystemet misbrukes til å flytte økonomiske verdier i form av varer og tjenester. Det skiller seg fra annen handelsrelatert kriminalitet som eksempelvis smugling – som omhandler illegal flytting av varer – ved at handelsbasert hvitvasking utelukkende handler om å flytte verdier.³² Det anses som en av de mest avanserte formene for hvitvasking. Metodene omfatter blant annet over- og underprising, tredjepartsbetalinger, gjenbruk av fakturaer og manipulering av handelsdokumenter, og kan benyttes hver for seg eller kombineres.

Handelsbasert hvitvasking er effektivt fordi store verdier kan flyttes gjennom tilsynelatende normale handelstransaksjoner. Hver dag flyttes enorme verdier over landegrenser, og FN anslår at det i 2025 ble handlet for rundt 35 billioner dollar globalt.³³ Det store omfanget av internasjonal handel gjør kontrollarbeidet krevende og mistenkelige transaksjoner vanskelige å identifisere. Valutaveksling, digitale finansielle tjenester og komplekse forsyningskjeder øker utfordringene ytterligere.³⁴

Handelsbasert hvitvasking gjør det mulig for kriminelle nettverk å legitimere store utbytteverdier fra straffbare handlinger og reinvestere dem i den kriminelle økonomien.

Enkelte bransjer er særlig sårbare for handelsbasert hvitvasking på grunn av store internasjonale varestrømmer, komplekse handelsforhold og utfordringer med å fastslå reell vareverdi. Sjømatsektoren er en slik sektor. Den er preget av omfattende internasjonal handel, og produktene kan variere i pris, kvalitet og bearbeidingsgrad. Samtidig er leverandørkjedene ofte komplekse og lite transparente. Det er vanskelig å kontrollere om varer er korrekt priset, og dermed lettere å skjule ulovlig verdioverføring gjennom tilsynelatende legitime handelstransaksjoner.

Også immaterielle produkter benyttes til handelsbasert hvitvasking. I andre tilfeller går det ingen varer i det hele tatt, varestrømmen det betales for er fiktiv. Økokrim er kjent med at begge metodene forekommer i Norge.

32 Hvidvasksekretariatet. 2022. *Temarapport: Handelsbasert hvidvask*.

33 UN Trade and Development. April 2026. *Global Trade Update (April 2026): Global trade growth continues, but fragility rises*.

34 Financial Action Task Force (FATF). 2020. *Trade-Based Money Laundering: Trends and Developments*.

Handelsbasert hvitvasking i sjømatnæringen – et fiktivt eksempel

Et kriminelt nettverk ønsker å hvitvaske utbytte fra kriminalitet i utlandet som de kan nyttiggjøre seg av i Norge. De etablerer derfor et norsk eksportfirma som tilsynelatende driver lovlig eksport av fisk. Eksportfirmaet kjøper fisk fra ordinære, uavhengige aktører i sjømatnæringen, slik at varestrømmen fremstår som reell og i tråd med vanlig eksportvirksomhet.

Fisken selges deretter videre til et samarbeidende selskap i utlandet, som nettverket selv kontrollerer. I salgsdokumentene manipuleres verdien på varene, for eksempel ved overfakturerings slik at fisken faktureres med en høyere kilopris enn den reelle markedsverdien. På papiret fremstår dette som ordinær handel, men i realiteten brukes fisken som et verktøy av det kriminelle nettverket for å overføre penger som stammer fra kriminalitet over landegrenser.

Ved å manipulere handelsdokumenter kan verdier flyttes mellom selskapene på tvers av landegrenser. Pengestrømmene benyttes for å betale varer, men hovedformålet med transaksjonen er å skjule midlenes opprinnelse og integrere pengene i det finansielle systemet. Deretter kan midlene benyttes videre for eksempel til investeringer eller videre næringsvirksomhet.

Hvitvasking og verdioverføring gjennom digitale valutaer og verktøy

Det lanseres stadig nye digitale løsninger for overføring av penger på tvers av landegrenser. Heldigitale betalingsløsninger gjør det lettere å opprette kontoer i eget og andres navn, uten at misbruket oppdages. Også i den tradisjonelle banksektoren har det kommet nye digitale løsninger. *vIBAN* forenkler internasjonale betalinger for avsender og mottaker, men kan samtidig gjøre det mer krevende å spore hvor pengene faktisk havner. Dette skaper et handlingsrom for økonomisk kriminalitet.

Kriminelle nettverk benytter digitale valutaer som del av sine hvitvaskingsmetoder, og som betalingsmiddel for ulike kriminelle varer og tjenester. Det er en utfordring at mange av tjenestene som brukes er basert i utlandet, noe som svekker norske myndigheters innsyn og gjør informasjonsinnhenting og samarbeid mer krevende.³⁵

Siden Økokrims forrige trusselvurdering har fremveksten av flere digitale produkter og plattformer utvidet mulighetene for å flytte verdier på alternative måter. En rekke ikke-finansielle tjenester legger i dag til rette for verdioverføring mellom brukere. Noen plattformer tilbyr direkte overføringer mellom brukere, mens andre legger til rette for verdi-

flytting gjennom gaver, abonnementer, pengeinnsamlinger eller kjøp og salg av varer og tjenester. De er legitime, men kan også misbrukes til hvitvasking. Betalingen går ofte via flere ledd, fra bruker til betalingsleverandør, til plattform, og til slutt til mottaker. Ingen av leddene har nødvendigvis oversikt over hele kjeden, noe som gjør det vanskelig å avdekke mistenkelige transaksjoner.

På sosiale medier og meldingstjenester brukes chattefunksjoner og lukkede grupper til å organisere kriminalitet, inkludert hvitvasking. Utbredt bruk av ende-til-ende-kryptert kommunikasjon gjør slik aktivitet utfordrende å avdekke. Flere av disse kanalene har allerede etablert funksjoner for direkte verdioverføring i sine apper.

Fremover ventes nye digitale betalingsløsninger og kryptovaluta å gjøre det stadig vanskeligere å spore verdioverføringer og identifisere reelle mottakere. Norske myndigheters innsyn ventes å bli ytterligere utfordret av at mye av denne aktiviteten skjer gjennom utenlandsbaserte tjenestetilbydere, mens bruken av sosiale medier og digitale plattformer til verdioverføring trolig vil fortsette å øke.

35 Økokrim. 2026. *Nasjonal Risikovurdering Hvitvasking*.



Bakmannen for Incognito Bank dømt til 30 års fengsel i 2026

I 2026 ble bakmannen til et av verdens største nettbaserte narkotikamarkeds-plasser dømt til 30 års fengsel. Markedsplassen, som befant seg på det mørke nettet og ble kalt Incognito Market, hadde et internt banksystem basert på kryptovaluta. Det opererte som et globalt, anonymt narkotikamarked med kunder over hele verden, og en omsetning på mer enn 105 millioner amerikanske dollar mellom oktober 2020 og mars 2024.

En sentral del av infrastrukturen var Incognito Bank, et internt banksystem, som lot brukere sette inn kryptovaluta på individuelle kontoer på plattformen. Betalingsløsningen hadde et escrow-system der betalinger ble holdt tilbake til kjøperen bekreftet mottak, noe som reduserte risiko for bedrageri og ga plattformen kontroll over pengestrømmen. Betalingene gikk gjennom et system av kryptovalutatransaksjoner som vanskeliggjorde sporing. Incognito Market skal ha hatt mer enn 400 000 kjøperkontoer, 1 800 narkotikaleverandører og 640 000 enkelttransaksjoner.

Kilde: U.S. Attorney's Office.

Hvitvasking via eiendom

Eiendom er en kilde til flere og potensielt lønnsomme hvitvaskingsmetoder. Kriminelle aktører og nettverk kjøper eiendom og betaler ned boliglån med penger som stammer fra straffbare handlinger, eller med en kombinasjon av lovlige og ulovlige midler. Verdier kan også overføres mellom kjøper og selger gjennom kunstig over- og underprising. Videre er utleie og fremleie utsatt for misbruk gjennom fiktive leieforhold og kunstig justerte leiepriser. Oppussing finansieres også med kriminelt utbytte. En eventuell verdistigning av eiendommen gjør i tillegg hvitvaskingen lønnsom.

Eiendomssektoren i Norge preges av høyt transaksjonsvolum og store verdier. I 2024 ble eiendommer for en samlet verdi av rundt 710 milliarder kroner formidlet gjennom eiendomsformidlingsforetak og advokater.³⁶ Gjennom bruk av tredjeparter skjuler kriminelle sin egen tilknytning til eiendommen ved å la andre stå for innbetaling av egenkapital, kostnader til oppussing, løpende leiebetalinger eller nedbetaling av lån. Politiet har avdekket hvordan fiktive lønnsinnberetninger og manipulerede regnskap i foretak brukes til å begå lånebedragerier, som videre brukes til å kvalifisere for boliglån.

Boliglånene er registrert på identiteter som de kriminelle har kontroll over. Disse mellompersonene fungerer som et lag mellom de kriminelle midlene og den formelle økonomien, og bidrar dermed til å tilsløre pengenes opprinnelse og gjøre transaksjonene vanskeligere å spore. Økokrim kjenner også til enkelte ansatte i finansforetak som seg imellom videreforder søknader fra kriminelle nettverk, til tross for at dokumentasjonen som ligger til grunn kan være forfalsket.

Eiendomskjøp gjennom selskaper gjør det også mulig å skjule reell eier. Dette skjer blant annet gjennom bruk av komplekse selskapsstrukturer, *skallselskaper*, *skatteparadiser* og *blankoskjøter*. Det åpner også for *selvvasking*, ved at en person som selv har oppnådd utbytte fra straffbare handlinger overfører eiendom mellom parter som fremstår som ulike, men som i realiteten er knyttet til vedkommende selv.

Flere godt etablerte kriminelle aktører og deres familiemedlemmer har ervervet betydelige eiendomsporteføljer i den legale økonomien på denne måten.

36 Økokrim 2026. *Nasjonal risikovurdering hvitvasking*.



Kriminelle benytter undergrunnsbanktjenester

Kriminelle nettverk benytter seg av en rekke *undergrunnsbanktjenester* for å flytte, oppbevare og gjøre opp verdier utenfor det formelle banksystemet. Noen tjenester leveres av spesialiserte hvitvaskingsaktører, som omtales i kapitlet om kriminalitet som handelsvare, mens andre leveres av uregulerte finanstilbydere som kan være uvitende om midlenes kriminelle opphav.

En sentral form for undergrunnsbankvirksomhet er *uformelle verdioverføringssystemer*. Slike systemer formidler penger på vegne av en sender og gjør pengene, eller tilsvarende verdi, tilgjengelig for en mottaker et annet sted. Eksempler er hawala i Midtøsten og Øst-Afrika, hundi i Sør-Asia og feiqian i Kina. Systemene er i utgangspunktet

lovlige dersom de har konsesjon, men de kan også misbrukes til hvitvasking og terrorfinansiering.³⁷

For kriminelle nettverk er undergrunnsbanktjenester attraktive fordi transaksjonene kan være vanskelige å spore. Undergrunnsbankaktører kan balansere tilbud og etterspørsel av kriminelle kontanter mellom ulike land uten at pengene fysisk må krysse landegrenser. Dette gjør tjenestene særlig relevante for internasjonal narkotikahandel og annen kriminalitet med store kontantstrømmer.

Hvitvasking via undergrunnsbanker brukes ofte sammen med andre metoder, som hvitvasking via kontanter, foretak, kryptovaluta og handelsbasert hvitvasking. Tiltak rettet mot ett ledd kan føre til at aktørene tilpasser seg andre

Undergrunnsbanktjenester er finansielle tjenester som leveres systematisk og i stort omfang utenfor den regulerte banksektoren. Eksempler er transport av kontanter, overføringer til andre land og veksling av kontanter og kryptovaluta. Tjenestene er *illegale* når verdiene som formidles stammer fra kriminalitet. *Uformelle verdioverføringssystemer* er en konkret type av undergrunnsbank. Organiserte nettverk formidler penger eller tilsvarende verdier mellom personer i ulike land, ofte uten at pengene flyttes fysisk. Hawala, hundi og feiqian er eksempler på slike systemer.

37 Europol. 2023. *European financial and economic crime threat assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime*.

ledd, fremfor at risikoen forsvinner.

Et eksempel er kinesiske hvitvaskingsnettverk som kombinerer *illegal undergrunnsbankvirksomhet* med daigou-handel. Daigou innebærer at varer, ofte luksusvarer, kjøpes i vestlige land og smugles inn i Kina for videresalg.³⁸ Når varene kjøpes med kontanter fra kriminalitet, fungerer handelen som hvitvasking gjennom kjøp av verdigjenstander. Når handelen også brukes til å overføre eller gjøre opp verdier mellom kriminelle aktører, er det handelsbasert hvitvasking, se eget kapittel om dette.

Høye importavgifter og store prisforskjeller mellom Kina og Europa gjør daigou-handel lønnsom. I 2023 ble importverdien til Kina gjennom daigou anslått til rundt 81 milliarder amerikanske dollar, tilsvarende om lag 760 milliarder norske kroner.³⁹

Betalinger utenfor det formelle norske banksystemet er observert i reiselivsnæringen i Nord-Norge, der kinesiske aktører i enkelte tilfeller mottar oppgjør kontant eller via kinesiske betalingsplattformer. Dette omtales nærmere i kapitlet om turistnæringen.

Avdekket nettverk for ulovlige finansielle tjenester

I 2025 ble verdier tilsvarende 4,5 millioner euro beslaglagt i en Europol-støttet operasjon mot illegal bankvirksomhet i flere europeiske land. Beslaget inkluderte eiendom verdt 2,5 millioner euro, omtrent 420 000 euro fordelt på flere titalls bankkontoer og 200 000 euro i kontanter, i tillegg til kryptovaluta, kjøretøy og ulike verdigjenstander.

Det aktuelle kriminelle nettverket skal ha tilbudt tjenester innen ulovlig hawala, innsamling og transport av kontanter og veksling mellom kryptovaluta og kontanter. Hvitvaskingsnettverket antas å ha flyttet over 21 millioner euro som stammet fra menneskesmugling og narkotikakriminalitet.

Kilde: Europol

³⁸ National Crime Agency. 2019. *Chinese Underground Banking and 'Daigou'*.

³⁹ Netherlands Police, Dutch Public Prosecution Service and the Fiscal Intelligence and Investigation Service. 2024. Daigou and criminal underground banking.



Sårbarheter som utnyttes til hvitvasking

Kapitlet har vist at kriminelle aktører og nettverk hvitvasker utbytte gjennom handel, eiendom, digitale valutaer og undergrunnsbanktjenester, blant annet ved å skjule reelt eierskap bak foretak og mellompersoner. Hvitvasking er avhengig av at pengenes opprinnelse forblir usynlig gjennom hele transaksjonskjeden fra kriminell handling til tilsynelatende lovlig formue. Det finnes ingen enkelt kontrollmyndighet som følger en verdi gjennom hele denne veien, og de tre sårbarhetene under oppstår nettopp i overgangen der ansvaret og oversikten er delt mellom flere parter.

Opplysninger om handel og betalinger er spredt mellom flere aktører

Opplysninger som er nødvendige for å kontrollere handelstransaksjoner er spredt mellom flere aktører. Fakturaer, varepriser, tolldokumenter og betalingsopplysninger kan befinne seg hos blant annet toll- og skattemyndigheter, banker og andre rapporteringspliktige, ofte i forskjellige land. Det finnes ikke ett samlet system som gjør det mulig å sammenstille og kontrollere opplysninger i sanntid. Dette gjør det krevende å avdekke avvik mellom varer, dokumentasjon og betalinger, og dermed identifisere handelsbasert hvitvasking.

Skjult eierskap i eiendomsmarkedet

Ved å kjøpe eiendom gjennom foretak kan man skjule det reelle eierskapet bak komplekse selskapsstrukturer og *skatte-*

paradis. Oversikten over hvem som juridisk sett eier norske selskaper er dessuten begrenset, siden aksjonærregisteret kun oppdateres én gang i året. Manglende tinglysingsplikt og bruk av *blankoskjøtte* forsterker dette, og gjør det vanskelig å få full oversikt over hvem som faktisk kontrollerer eiendom i Norge.

Manglende helhetlig innsyn i digitale betalingskjeder

Digitale betalinger går ofte gjennom flere ledd, fra bruker til betalingsleverandør, videre til plattform og til slutt til mottaker. Hvert ledd ser bare sin egen del av transaksjonen, og ingen av dem har oversikt over hele kjeden fra avsender til mottaker. Dette gjør det vanskelig å avdekke mistenkelige transaksjoner, fordi mistanke som oppstår hos ett ledd ikke nødvendigvis følger pengene videre til neste.



Korrupsjon og misbruk av myndighet

De siste års saker og avsløringer har vist at Norge er eksponert for *korrupsjon*. Det brede spekteret av saker viser at korrupsjon er til stede i stort sett alle deler av samfunnet.

Risikoen øker der det er små forhold, svake kontrollmekanismer og tette bånd mellom aktører, og der øvrige ansatte har høy tillit til ledere på ulike nivåer. Korrupsjonssaker som involverer personer i høyhengende tillitsverv er egnet til å svekke den høye graden av tillit vi har i samfunnet vårt.

For kriminelle nettverk er korrupsjon et sentralt virkemiddel, og ofte en forutsetning for gjennomføringen av alvorlig og organisert kriminalitet.⁴⁰ Ifølge Europol driver de fleste kriminelle nettverk i en eller annen grad med korrupsjon, mens en mindre andel av dem driver hyppig og målrettet korrupsjon rettet mot offentlige tjenestepersoner eller bestemte sektorer som en integrert del av sin forretningsstrategi.⁴¹

I Norge har flere saker vist en vedvarende risiko for korrupsjon der det offentlige og private møtes, blant annet der det offentlige utøver myndighet, gir lån, tilskudd, andre støtteordninger, eller foretar innkjøp og anskaffelser.⁴²

Korrupsjon vil fortsatt være en risiko der offentlige beslutninger, store verdier og kommersielle interesser møtes. Risikoen for korrupsjon ved forsvarsrelaterte anskaffelser, som følge av økte forsvarsbudsjetter og hemmelighold, er omtalt tidligere i kapitlet «En verdensorden i endring». I dette kapitlet ser vi nærmere på korrupsjon i plan- og byggesaksbehandlingen og i norske aktørers internasjonale virksomhet.

40 Europol. 2023. *European financial and economic crime threat assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime*.

41 Europol. 2025. *Serious and Organised Crime Threat Assessment (SOCTA) - The Changing DNA of Serious and Organised Crime*.

42 Transparency International Norge. 2026. *Korrupsjonsdommer i Norge 2003-2026*.

Korrupsjon i plan- og byggesaksbehandling

Plan-, bygg- og arealforvaltning innebærer store økonomiske interesser, hyppige private-offentlige møter og mange skjønsmessige avgjørelser. Dette gjør feltet spesielt utsatt for interessekonflikter, utveksling av uformelle fordeler og korrupsjon. Slik korrupsjon kan foregå både på politisk og administrativt nivå. I en undersøkelse om korrupsjon i kommunesektoren oppgir ansatte at tilbud om bestikkelser eller press om uetisk atferd som oftest kommer fra virksomheter innen bygg og anlegg samt eiendomsforvaltning.

Korrupsjonsrisikoen forventes å være stor ved kjøp og salg av eiendom, se avsnitt om innsidere.

Å få tilgang til informasjon fra kommuners arbeid med plan- og byggesaker kan være svært verdifullt, særlig tidlig i planprosesser. I større hyttekommuner opplever eksempelvis flere at det er tette bånd mellom utbyggere og beslutningstakere i kommunen.⁴³ Korrupsjon kan også oppstå under søknadsbehandling og ved oppfølging av lovlige og ulovlige tiltak. Risikoen øker ved små forhold, ved svak eller fraværende internkontroll, og med kapasitets- og kompetansemangel.

Det er fra tid til annen medieoppslag om inhabile folkevalgte, ledere og ansatte som tilrettelegger for eller fatter beslutninger når de skulle meldt seg inhabile. I flere tilfeller fremstår det som at aktørene har holdt egne interesser skjult, med profittmotiv. Det kan dreie seg om mistanke om korrupsjon, økonomisk utroskap eller misbruk av stilling til egen vinning. Fra Sverige har man sett eksempler på at kriminelle reklamerer med tilgang til innsidere i kommunale byggesakskontorer.⁴⁴

Korrupsjon i plan- og byggesaker undergraver tilliten som plan- og byggesakssystemet bygger på. Kriminaliteten på dette området får store samfunnsmessige omkostninger, i form av for eksempel feilaktig bruk av arealer, irreversible endringer av sårbar natur, rasering av uerstattelige kulturminner, eller oppføring av bygg til fare for liv og helse.

43 Kasin. 2024. *Naturparadokset - om naturen vi mister og hvordan vi kan få den tilbake*.

44 Brå. 2024. *Möjliggörare för kriminella nätverk*.

Risiko for at norske borgere begår korrupsjon i utlandet

Norske borgere kan også begå korrupsjon i utlandet og i forbindelse med ulike former for internasjonal virksomhet.

Korrupsjon i bistandssektoren er et internasjonalt problem som utfordrer effektiviteten og legitimiteten til utviklingshjelp. Bistand gis ofte i land med svake institusjoner, lav grad av rettssikkerhet og utbredt maktmisbruk, noe som øker risikoen for at midler misbrukes. I tillegg kan bistand brukes for å opprettholde korrupte statsledere. Store internasjonale organisasjoner har også vært gjenstand for korrupsjon i egne rekker.

Riksrevisjonen har konkludert med at det er vesentlige mangler i hvordan Utenriksdepartementet og Norad forebygger, avdekker og reagerer på økonomiske misligheter.⁴⁵ I 2026 er det på nytt rettet søkelys mot Norges bruk av bistandsmidler, og særlig fravær av oppfølging av tilskudd på tross av røde flagg.

Når norske virksomheter skal etablere eller drive forretningsvirksomhet med regimer med *endemisk korrupsjonsnivå* er det åpenbart høy risiko for korrupsjon,

også *høynivåkorruptsjon*. Økokrim tok tidlig i 2026 ut tiltale i en korrupsjonssak som gjelder bestikkelser i Republikken Kongo i perioden fra 2016 og fremover. Bestikkelsene fant ifølge Økokrims tiltale sted samtidig som de tiltalte søkte om, og fikk, deltakerlisens for oljeutvinning i landet. Ved *høynivåkorruptsjon* vil bestikkelser kunne bidra til at landets ledelse misbruker sin makt til å berike seg selv på bekostning av landets innbyggere.

Risikoen for korrupsjon i forbindelse med idrett er en internasjonal utfordring. Utfordringen gjelder også Norge, noe dommen mot den tidligere presidenten i det internasjonale skiskytingsforbundet (IBU) illustrerer. I tillegg til utfordringer som kampfiksing, benytter flere regimer idrett som en arena for å hvitvaske midler og eget omdømme, gjennom såkalt sportsvasking. Det har vært korrupsjonsmistanker knyttet til tildelingsprosessen ved flere store mesterskap.⁴⁶

45 Riksrevisjonen. 2024. *Håndteringen av risikoen for økonomiske misligheter i forvaltningen av bistanden*.

46 Fifa Ethics and Regulation Watch. 2025. *FIFA Accused of Covering Up Corruption in 2018 and 2022 World Cup Host Selections*.

Hva er korrupsjon?

Transparency International og Europol definerer korrupsjon som misbruk av betrodd makt for privat gevinst. Dette kan innebære tette bånd, interessekonflikter og dobbeltroller. Mye kan imidlertid være kritikkverdig uten å være straffbart.

Straffeloven §§ 387 og 388 beskriver hva korrupsjon er i strafferettslig forstand. For å kunne straffes for korrupsjon må gjerningspersonen ha gitt, tilbudt, krevd, fått eller akseptert en utilbørlig fordel i anledning av stilling, verv eller oppdrag. Uttrykket «utilbørlig fordel» er lovens betegnelse for bestikkelsen. Nærmest alle tenkelige fordeler kan i prinsippet rammes, både fordeler som har økonomisk verdi (for eksempel penger, gratis ferie, lån eller gratis oppussing) og fordeler av ikke-økonomisk verdi (for eksempel seksuelle tjenester eller medlemskap i en forening).

Det er videre krav om sammenheng (tilknytning) mellom bestikkelsen og motpartens posisjon. Dette følger av at fordelene må være gitt eller mottatt i anledning av motpartens stilling, verv eller oppdrag. Så lenge det er sammenheng mellom fordelene og motpartens stilling, verv eller oppdrag, er det uten betydning hvem som faktisk mottar fordelene. Dette kan for eksempel være et selskap vedkommende har interesser i eller et familiemedlem.

Det kan være en flytende og uklar grense mellom handlinger som utgjør korrupsjon, hvor det skjer en overføring av en utilbørlig fordel i kraft av stilling, og handlinger som utgjør ulovlig misbruk av stilling til egen vinning og økonomisk utroskap. Misbruk av offentlig myndighet går på at man har en stilling hvor man kan utøve makt og bryter en eller annen tjenesteplikt.

Kilde: Transparency International og straffeloven §§ 387–388, og § 173.

Sårbarheter knyttet til korrupsjon og misbruk av myndighet

Korrupsjon og myndighetsmisbruk er vanskelig å avdekke, fordi det sjelden etterlater spor og skjer mellom aktører med sammenfallende interesser. I Norge forsterkes dette av at strafferettslige reaksjoner på myndighetsbruk sjelden benyttes, at det systematiske antikorrupsjonsarbeidet har svakheter, og at varslervernet ikke er godt nok. Nedenfor beskrives tre sentrale sårbarheter.

Lite brukt straffebud om myndighetsbruk

Misbruk av offentlig myndighet kan omfatte situasjoner der personer i makt- eller tillitsposisjoner bruker rollen sin til å favorisere enkelte aktører, ta utenforliggende hensyn eller ivareta egne interesser. Straffebudet er lite brukt i praksis, og slike forhold kan derfor i større grad bli håndtert som interne feil, dårlig dømmekraft eller brudd på etiske retningslinjer, heller enn som mulig straffbare handlinger. Det er i ulike sammenhenger fremhevet at terskelen for å få dom i korrupsjonssaker oppleves som høy, og at forholdene derfor heller subsumeres under andre straffebud enn korrupsjon.⁴⁷

Norge har strukturelle svakheter i sitt systematiske arbeid mot korrupsjon

Internasjonale evalueringer har påvist svakheter i Norges oppfølging av inter-

nasjonale forpliktelser i antikorrupsjonsarbeidet. I 2025 viste OECD og GRECOs gjennomgang av norske forhold vedvarende strukturelle mangler på tre punkter: manglende systematisk arbeid mot korrupsjon, fraværende konsekvenser ved interessekonflikter på politisk toppnivå og liten vilje til å sikre åpenhet rundt lobbyisme rettet mot statens mektigste.^{48,49}

Fravær av gode varslingskanaler

Det norske varslervernet har over tid blitt kritisert, blant annet fordi varslerne har blitt utsatt for represalier. Dette gir korrupsjon og annen uetisk adferd større spillerom. Et svakt varslervern kan dermed gjøre det mindre sannsynlig at fremtidige korrupsjonsforhold kommer for dagen, fordi potensielle varslere kan velge å tie av frykt for konsekvensene.

47 Transparency International Norge. 2023. *Hva hindrer politiets etterforskning av korrupsjonssaker*.

48 OECD. 2024. *Anti-Corruption and Integrity Outlook 2024 – Country Notes*.

49 Group of States against Corruption (GRECO). 2025. *FEMTE EVALUERINGSRUNDE*.



Kriminelle nettverk i næringslivet

Både i Norge og i Europa for øvrig ser politiet at *kriminelle nettverk* utnytter legale foretaksstrukturer til å begå økonomisk kriminalitet, eller for å fordekke eller tilrettelegge for annen organisert kriminalitet. Ifølge Europol bruker 86 prosent av de mest truende kriminelle nettverkene i EU slike virksomhetsstrukturer.⁵⁰

Virksomheter brukes blant annet som ledd i bedragerier og skattekriminalitet, og til å hvitvaske verdier som stammer fra kriminell virksomhet.⁵¹ Ved å fremstå som lovlidige og seriøse aktører kan kriminelle nettverk vinne offentlige anbud. Dette gir økonomisk profitt, samtidig som det virker konkurransevidende for hele bransjer og næringslivet generelt.

For å skjule hvem som reelt kontrollerer virksomheten, begås kriminaliteten ofte gjennom foretak med kompliserte eierskapsstrukturer, skjulte avtaler, stråelskap og stråpersoner. Det benyttes også *registermanipulasjon*, der opplysninger om blant annet eierskap og roller endres for å skjule de faktiske forholdene.

Arbeidslivskriminalitet og utnyttelse av arbeidstakere utgjør ofte en vesentlig del av virksomheten, blant annet ved å

minimere driftskostnader knyttet til lønn og sikkerhet, unndra skatt og avgifter, eller urettmessig tilegne seg ytelser eller refusjoner.

Slike nettverk er i dag etablert i flere norske næringer. Tilpasningsevnen gjør dem i stand til å bevege seg mellom bransjer og etablere seg der kontrollen er svakest. Dette gir høy profitt med relativt lav risiko, og vi forventer at flere næringer vil bli infiltrert i årene fremover.

Kriminelle nettverk kan også utnytte konkurser, blant annet ved å overta eller tømme selskaper for verdier og videreføre aktiviteten i nye foretak etter konkurs. Dette gir nettverkene mulighet til å unndra seg gjeldsansvar og fortsette den kriminelle virksomheten med lav oppdagelsesrisiko.

⁵⁰ Europol. 2024. *Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures*.

⁵¹ Ekobrottsmyndighet. 2025. *Økonomisk brottslighet. Lagesbild 2025*.

Kriminelle nettverk i velferdsforetak rettet mot unge

Norske myndigheter har avdekket at kriminelle aktører har fått sentrale roller i private barnevernsforetak.⁵² Riksrevisjonen har pekt på en rekke strukturelle svakheter i barnevernet som gjør sektoren sårbar for slik utnyttelse.⁵³ Utviklingen har paralleller til Sverige, der myndighetene over tid har avdekket at kriminelle nettverk søker innpass i foretak som leverer helse-, omsorgs- og barnevernstjenester til det offentlige.

I Norge har politiet informasjon om at kriminelle aktører etablerer seg gjennom lovlige virksomheter og tilpasser seg systematisk et system som er presset og tillitsbasert. Over tid bygger de legitimitet, inntekter og kontroll innenfor formelt lovlige rammer. Kriminelle aktører vinner offentlige anbud og leverer ulike former for barnevernstjenester til det offentlige. Dette gir de kriminelle en posisjon der de kan kanalisere offentlige midler inn i kriminell økonomi, hvitvaske utbytte fra annen kriminalitet, og redusere avstanden mellom legal virksomhet og kriminelle miljøer. Dette gir dem også tilgang til barn og unge i sårbare situasjoner.

Mønsteret er ikke unikt. Kriminelle aktører etablerer seg systematisk gjennom lovlige virksomheter, og tilpasser seg et system som er presset, tillitsbasert og fragmentert. Svakheter i kontrollmekanismene, som skal sikre seriøsitet ved offentlige innkjøp, gjør at useriøse og kriminelle aktører kan vinne markedsandeler på bekostning av seriøse barnevernsforetak. De legger seg lavere i pris og fremstår som løsninger på akutte behov i et system med høyt tempo og få alternativer.

I en svensk fenomenrapport fra 2025 ble det vurdert at rundt 70 prosent av aksjeselskapene, som fikk tillatelse til å levere personlig assistanse i perioden 2021 til 2024, mest sannsynlig ble brukt til kriminalitet, ofte med koblinger til etablerte kriminelle nettverk.⁵⁴

52 Økokrim. 2026. *Kriminelle aktører med sentrale roller i barnevernsbransjen*.

53 Riksrevisjonen. 2025. *Riksrevisjonens undersøkelse av årsaker til utfordringer i barnevernet*.

54 Polisen. 2025. *Hälften av granskade assistansbolag kopplas till organiserad brottslighet*.



Kriminelle aktører vinner anbud og selger private barnevernstjenester til det offentlige

Politiet har informasjon om koblinger mellom bemanningsselskap, eiendoms-selskap og aktører med tilknytning til vold, narkotika og kriminelle nettverk. Aktørene og deres nærstående har roller i virksomheter som leverer tjenester innen helse, omsorg og barnevern, samtidig som eiendom leid ut til institusjonsformål kontrolleres av personer med tilsvarende tilknytning. Oppussing og vedlikehold av eiendom, som bekostes av det offentlige, og som leies ut til institusjonsformål gjøres dessuten av virksomheter som knyttes til hvitvas-king. Virksomhetene har en høy og stabil årlig omsetning som i stor grad er finansiert av det offentlige.

Kriminelle nettverk i drosjenæringen

Drosjenæringen innbefatter foretak som driver med persontransport, inkludert spesialtransport som pasientreiser og tilrettelagt transport. For å drive lovlig kreves gyldig drosjeløyve, noe som forutsetter fast og varig virksomhet i Norge, god vandel og tilfredsstillende økonomisk evne.

Drosjenæringen er omtalt som en bransje med utstrakte brudd på skatte- og avgiftsregler og regelverk knyttet til arbeidsmiljø og arbeidstakerrettigheter.⁵⁵ Økokrims informasjon tilsier at risikoen også knytter seg til bruk av fiktive løyver og kjøresedler, svart og ulovlig arbeid og hvitvasking.

Det er særlig koblingen til kriminelle nettverk som gjør trusselbildet alvorlig. Enkelte aktører benytter drosjeforetak

som distribusjonsledd for narkotika og hvitvasker fortjenesten gjennom tilsynelatende legale foretak. Det varierer om foretakene har reell drift, eller om de først og fremst fungerer som *skallselskap* og fasade. Kriminalitet i drosjenæringen kan til dels knyttes til kriminelle nettverk som bevisst utnytter sårbarheter i næringen.

Kriminelle aktører bidrar til konkurransevridning og dårligere vilkår for de som drifter legalt. Noen drosjeforetak benytter seg av profesjonelle tilretteleggere som bistår med skatte- og avgiftsunndragelse og hvitvasking for drosjeforetak.

Kriminelle nettverk misbruker drosjenæringen

Politiet har indikasjoner på at et kriminelt nettverk utnytter drosjeforetak som distribusjonskanal for narkotika, samt til hvitvasking, bedrageri, arbeidslivs- og skattekriminalitet. Nettverket opererer gjennom flere samarbeidspartnere og tilretteleggere i både Norge og utlandet. Virksomheten omfatter blant annet systematisk kredittmisbruk ved kjøp av kjøretøy, der lån misligholdes. Det observeres også en uforholdsmessig høy andel ansatte med offentlige ytelser, og enkelte foretak mistenkes for å fasilitere fiktivt arbeid.

55 Samferdselsdepartementet. 2024. *En bedre regulert drosjenæring* (NOU 2024:15).

Kriminelle nettverk i det app-baserte næringslivet

Plattformselskaper stykker opp arbeidet i avgrensede oppdrag som utføres på etterspørsel av kunden. Modellen brukes til alt fra hjemlevering av mat, drosjeturer og renhold i private hjem til barne- og dyrepass, vaktmestertjenester, digitale legetjenester og IT-tjenester. For arbeidstakerne gir plattformarbeid en viss fleksibilitet i når og hvor mye de ønsker å jobbe.⁵⁶ Den samme fleksibiliteten gjør imidlertid markedet sårbart for utnyttelse. Der kravene til formell kompetanse er lave, kan allerede utsatte arbeidstakere bli utnyttet.

Dette ser vi i budbransjen. Plattformselskaper benytter i utstrakt grad underleverandører organisert som enkeltpersonforetak (ENK). Små oppstartskostnader gjør det enkelt å etablere slike ENK-er. Plattformselskap unngår på den måten arbeidsgiveravgift, men mister samtidig kontroll over hvem som faktisk utfører leveringsoppdragene bestilt gjennom appen. Dette skaper et handlingsrom for kriminelle aktører.

Siden forrige trusselvurdering har det vært økt oppmerksomhet rundt hvordan personer både utnytter og blir utnyttet i det app-baserte næringslivet, særlig knyttet til matleveringstjenester. Det har

blitt iverksatt en rekke tiltak, men utnyttelsen i næringen fremstår å fortsette. Det er ofte EØS-borgere eller tredjelandsborgere som har opphold i et EØS-land som blir utnyttet. Det er også tilfeller der de samme bilene som frakter mat, også blir benyttet til å frakte prostituerte.⁵⁷

Mye tyder på at mange av arbeidstakerne blir utnyttet av tilretteleggere. Flere er lokket til Norge etter å ha fått forespeilet ordnede forhold både når det gjelder bosted, arbeidstid og lønn. Realiteten er kummerlige boforhold, lange arbeidsdager og krav om å gi fra seg deler av lønnen til en tilrettelegger. I mars 2026 anmeldte et matleveringsbud arbeidsgiveren sin for menneskehandel etter å ha fått hjelp til å komme seg bort fra huset han delte med mange under streng kontroll. Han måtte kjøre på arbeidsgivers bruker, ble tvunget til å jobbe svært lange dager og opplevde trusler.

⁵⁶ FAFO. 2025. *Plattformmediert arbeid i Norge*.

⁵⁷ TV2. 13.05.2026. *Leverte mat - så ble prostituerte kjørt hjem i samme bil*.



Sårbarheter knyttet til kriminelle nettverk i næringslivet

Kapitlet har vist at kriminelle nettverk systematisk skjuler hvem som reelt står bak og utfører arbeidet i en virksomhet, blant annet gjennom strå-selskap, stråpersoner og underleverandørkjeder. Dette er ofte krevende å avdekke, ikke minst fordi aktørene utnytter systemer som i utgangspunktet er bygget på tillit. Nedenfor beskrives tre sentrale sårbarheter som gjør denne utnyttelsen mulig.

Fragmentert forvaltning og manglende helhetstenkning

Kontrollregimene er sektorvise, og forvaltningen mangler en helhetlig risikoforståelse. Ingen enkeltaktør har ansvar for eller oversikt over det samlede risikobildet på tvers av sektorer, slik at aktører kan bevege seg i bransjer og etablere seg der kontrollen er svakest, uten at dette fanges opp. Manglende helhetstenkning innebærer også at forebyggende tiltak i for stor grad rettes inn mot enkeltbransjer eller enkeltsaker, fremfor de mest alvorlige, overordnede sårbarhetene som går på tvers av forvaltningen.

Begrenset informasjonsdeling

Selv der etater har grunn til mistanke om at samme aktør opptrer i flere saker eller sektorer, er det i praksis begrenset adgang til å dele konkrete, taushetsbelagte opplysninger mellom dem. Muligheten til å verifisere opplysninger kan dessuten begrenses av taushetsplikt, manglende

hjemler for informasjonsdeling og svak kultur for deling av informasjon. Dette svekker den enkelte etats mulighet til å vurdere risiko i den enkelte sak, og gjør det krevende å koble sammen enkeltopplysninger som til sammen kunne avdekket multikriminalitet.

Manglende kontroll med hvem som faktisk utfører arbeidet

Bruk av underleverandørkjeder, bemanningsbyråer og enkeltpersonforetak gjør det vanskelig å ha oversikt over hvem som reelt utfører arbeidet bak et oppdrag eller en leveranse. Plattformsselskaper unngår arbeidsgiveransvar ved å benytte personer med enkeltpersonforetak, men mister samtidig kontroll over hvem som faktisk utfører oppdragene som bestilles gjennom appen. Mange bruker dessuten andres kontoer i appen. Dette fører til at noen lar andre gjøre arbeidet for seg og betaler dem mindre enn det som faktisk tjenes gjennom kontoen.



Misbruk av fellesskapets midler

Norge har *offentlige systemer og velferdsordninger* som skal legge til rette for god helse, inntektssikring og omfordeling, og som skal sikre en bærekraftig offentlig sektor. Ordningene forvalter betydelige verdier og bygger i stor grad på tillit mellom myndigheter, næringsliv og innbyggere.

Bedragerier mot offentlige velferdsordninger tapper trolig statskassen for milliardbeløp årlig. Nav anslår feilutbetalinger på minst fem milliarder kroner hvert år.⁵⁸ Ordningene er attraktive fordi de gir økonomisk gevinst med begrenset risiko. For kriminelle nettverk kan de utnyttes systematisk og over tid, og fungere som en stabil inntektskilde.⁵⁹

Unndragelse av skatter og avgifter bidrar også til store inntektstap fra statskassen årlig. Skatteetaten har så langt i 2026 avdekket feilaktige fradrag for over 1,6 milliarder kroner, tilsvarende rundt 350 millioner kroner i skattemessig verdi.⁶⁰

Manipulering av registre og rapportering er sentralt. Uriktige opplysninger, falsk dokumentasjon og fiktive arbeidsforhold legges inn i registre og

danner grunnlag for feil beslutninger eller utbetalinger. Vi forventer at digitale verktøy og kunstig intelligens fremover vil øke kriminelle nettverks kapasitet til å produsere fiktiv dokumentasjon, tilpasse søknader og koordinere aktivitet mellom personer, selskaper og ordninger.

Risikoen er særlig høy der store offentlige beløp gjøres tilgjengelig gjennom nye satsinger, eller der kriminelle aktører får innpass i virksomheter som tilde-ler eller mottar offentlige midler. Dette gjelder også statlige tilskudd, som utgjør omtrent en tredjedel av statsbudsjettets utgifter. Risikoen for økonomiske misligheter vurderes som betydelig, men vanskelig å anslå. I dette kapitlet ser vi nærmere på hvordan enkeltaktører og nettverk misbruker sentrale offentlige systemer og ordninger.

58 NAV.no. *Innsats mot trygdesvindel*. (Anslaget inkluderer både bedrageri og ubevisste feil).

59 Rostami, et.al. 2026. *Svarta siffror – ESO-rapport om den kriminelle økonomiens omfatning*.

60 Skatteetaten. 2026. *Skattemeldingen: Skatteetaten har avdekket store feil og misbruk av fradrag*.

Kriminelle nettverk bedrar offentlige velferdsordninger

I flere tilfeller ser politiet at bedrageri mot offentlige velferdsordninger gjennomføres av kriminelle nettverk, og at utbytte fra bedrageriene utgjør en sentral del av nettverkets økonomi. Utnyttelsen gjennomføres både ved at kriminelle som enkeltpersoner får utbetalt midler de ikke har rettmessig krav på, men også gjennom tilsynelatende legitime organisasjoner og prosjekter. Ved å tilegne seg urettmessige utbetalinger får kriminelle aktører og nettverk tilgang til løpende og tilsynelatende legitime inntekter over tid. Familie- og selskapsstrukturer brukes til å skjule aktivitetene, mens profesjonelle aktører gjør kriminaliteten mer troverdig og vanskeligere å avdekke.

Økokrim har informasjon om at flere aktører fra ulike kriminelle nettverk samarbeider om å utnytte offentlige velferdsordninger via foretak. Ofte foregår bedrageri mot velferdsordninger sammen med arbeidslivskriminalitet, skattekriminalitet, registermanipulasjon, hvitvasking og ulovlig næringsaktivitet. De kriminelle aktørene fremstår å ha god kjennskap til hvordan forvaltningen fungerer og til sårbarheter i regelverkene.

Tilsvarende er avdekket i andre land. I Storbritannia ble fem personer i 2024 dømt i det som britisk påtalemyndighet omtaler som den største straffesaken om trygdebedragerier i England og Wales, etter falske krav på over 53 millioner pund fra den britiske stønadsordningen Universal Credit.⁶¹ Bedrageriet ble gjennomført ved bruk av falske identiteter, forfalsket dokumentasjon og flere bankkontoer som skjulte pengestrømmene. I Minnesota avdekket amerikanske myndigheter i 2022 et bedrageri der falske selskaper og fiktive krav ble benyttet til å få utbetalt nær 250 millioner dollar fra et føderalt barneernæringsprogram under pandemien. Amerikanske myndigheter har omtalt dette som landets største pandemirelaterte bedragerisak.⁶²

Velferdsordningene er særlig sårbare dersom kontroll i hovedsak skjer etter at midlene er utbetalt, eller dersom det er begrenset kapasitet til å undersøke om vedkommende faktisk er uføretrygdet, eller aktivitetene det er søkt om tilskudd for faktisk er gjennomført.

61 Crown Prosecution Service. 2024. *Members of Britain's biggest benefit fraud gang jailed for a combined total of more than 25 years.*

62 United States Attorney's Office, District of Minnesota. 2025. *Federal Jury Finds Feeding Our Future Mastermind and Co-Defendant Guilty in \$250 Million Pandemic Fraud Scheme.*

Misbruk av refusjonsordninger

Refusjonsordninger gjør det mulig for virksomheter å få refusjon, utbetaling eller fradrag fra det offentlige. Ordningene er ofte basert på at aktørene selv rapporterer inn opplysninger og dokumentasjon, mens kontrollene i stor grad skjer i etterkant. Sakene som avdekkes viser et gjennomgående mønster der tillitsbaserte refusjonssystemer utnyttes systematisk for å hente ut midler fra fellesskapet.

SkatteFUNN er en rettighetsbasert skattefradagsordning som skal stimulere til forskning, utvikling og innovasjon i næringslivet. Ordningen administreres av Norges forskningsråd i samarbeid med Skatteetaten, og innebærer at foretak kan få fradrag for en andel av kostnadene i godkjente forsknings- og utviklingskostnader.⁶³ I 2025 utgjorde støtten gjennom SkatteFUNN om lag 3,9 milliarder kroner.⁶⁴

Samme år mottok Økokrim flere anmeldelser knyttet til mulig urettmessig bruk av ordningen. Som del av etterforskningen ble det gjennomført aksjoner på en rekke lokasjoner som ledd i etterforskningen av et sakskompleks der det

er mistanke om grovt skattesvik på inntil 30 millioner kroner og systematisk misbruk av ordningen.⁶⁵ Lovbruddene antas blant annet å være gjennomført ved bruk av fiktive prosjekter, oppblåste kostnader og *rundfakturer* mellom foretak.

Utbetalinger fra det offentlige til helsetjenester utgjør hvert år betydelige beløp. En sentral del av dette systemet forvaltes av Helseøkonomiforvaltningen (Helfo), som håndterer refusjonsordninger

Dom for misbruk av SkatteFUNN

I 2023 ble to personer i Agder tingrett dømt for grovt skattesvik etter å ha gitt uriktige opplysninger om forsknings- og utviklingskostnader gjennom flere selskaper for å oppnå urettmessige utbetalinger via SkatteFUNN. Straffene var fengsel i fire år og seks måneder og to år og tre måneder. Staten ble samtidig tilkjent 12,8 millioner kroner i erstatning.

Kilde: LA-2023-32214 –
UTV-2024-524

63 Forskningsrådet. *SkatteFUNN*.

64 SSB. 2026. *Nærings- og forskningspolitiske virkemidler*.

65 Økokrim. 30.10.2025. *Økokrim har aksjonert flere steder i landet i stor skattesviksak*.

for blant annet leger, tannleger og andre behandlere. Ordningen innebærer at behandlere rapporterer bruk av takstkoder, hvor staten dekker deler av kostnadene.

I 2025 betalte Helfo ut ca. 33,7 millioner kroner i refusjoner til helseaktører. Kontroller har avdekket urettmessige utbetalinger i betydelig omfang. I perioden 2021 til 2024 mistet 53 leger refusjonsretten, og 28 saker ble politianmeldt. Samlet dreier det seg om tilbakebetalingskrav på rundt 314 millioner kroner. Sakene gjelder enkeltleger, men peker på strukturelle sårbarheter i et system som håndterer store offentlige midler. Helfos etterkontroller viser at feilene særlig knytter seg til feil bruk av takstkoder, der kravene ikke kan underbygges gjennom tilstrekkelig dokumentasjon eller medisinsk begrunnelse.⁶⁶

Enkeltsaker illustrerer hvordan dette kan slå ut i praksis. I en dom fra Oslo tingrett i 2023 ble en kiropraktor dømt til ti måneders fengsel for å ha mottatt 1,8 millioner kroner i urettmessige utbetalinger.⁶⁷ I 2025 ble en lege dømt til ett år og, ni måneders fengsel, og samtidig pålagt å betale 2 millioner kroner i erstatning til Helfo.⁶⁸

En større andel av dette ble utbetalt direkte til næringsdrivende helseaktører som skattepliktig næringsinntekt.

Funnene hos Helfo viser at leger som har mottatt utbetalingene, har unnlatt å rapportere disse utbetalingene til skattemyndighetene. Leger sender altså først urettmessig krav til Helfo og mottar penger de ikke har krav på, og deretter unndrar de skatt av samme midler. Dette er et dobbelt misbruk og dobbelt tillitsbrudd.

66 Helfo (2024). *Årsrapport. Funn, erfaringer og resultater fra etterkontroller i 2024.*

67 Dom: 23-118543ENE-TOSL/03.

68 Dom: 24-187061ENE-TNTS/TTRM.

Skatte- og avgiftsunndragelse

Skatte- og avgiftsunndragelse består i å unnlate å gi opplysninger eller å gi uriktige eller ufullstendige opplysninger til norske skattemyndigheter for å kunne oppnå en skattemessig fordel. Sakene spenner fra relativt enkle overtredelser til komplekse former for økonomisk kriminalitet, der legale selskapsstrukturer, registermanipulasjon og profesjonelle tilretteleggere misbrukes for å skjule inntekt eller formue.

Enkelte som begår skatteunndragelse er lite kjent for politiet fra før, mens andre er sentrale aktører i kriminelle nettverk. Flere kriminelle nettverk som er involvert i alvorlig kriminalitet som narkotikavirksomhet, hvitvasking, vold og voldsopdrag, bedrageri og vinningskriminalitet begår også skattekriminalitet. For disse nettverkene inngår skatteunndragelser ofte som ett av flere elementer i en bredere kriminell virksomhet.

De siste årene har Skatteetaten avdekket omfattende misbruk av merverdiavgiftsordningen. Ordningen innebærer at virksomheter krever inn merverdiavgift fra kunder og betaler denne videre til staten, samtidig som de kan kreve fradrag for merverdiavgiften de selv har betalt. Kriminelle aktører videreutvikler etablerte metoder, blant annet ved å

bruke kunstig intelligens til å produsere uriktige eller fiktive skattemeldinger for innrapportering av merverdiavgift. I tillegg brukes selskapsstrukturer der flere selskaper inngår i et oppsett for å få utbetalt uberettiget merverdiavgift. Samtidig skjuler de kriminelle aktørene sin tilknytning til virksomheten ved å benytte en annen identitet.⁶⁹

Internasjonalt regnes merverdiavgiftsvindel som en av de viktigste inntektskildene for organisert økonomisk kriminalitet. Europol peker på at kriminelle nettverk systematisk utnytter merverdiavgiftsordningen gjennom komplekse selskapsstrukturer, fiktive transaksjoner og manipulering av rapporteringssystemer. Et kjent eksempel er såkalte *mva-karuseller*, der varer og fakturaer sendes gjennom flere selskaper i ulike land. Misbruket skjer ved at et selskap unnlater å betale merverdiavgiften til staten, mens et annet selskap krever refusjon for avgift som aldri er innbetalt. Resultatet er at staten både mister avgift som skulle vært betalt, samtidig som det utbetales refusjon av avgift som aldri ble innbetalt. Gjennom flere slike transaksjoner kan store beløp tapes fra statskassen.

69 Nasjonalt tverretattlig analyse- og etterretningssenter (NTAES). 2026. *Risikovurdering arbeidslivs-kriminalitet 2026-2028*.



Foto: Unsplash

Sårbarheter knyttet til misbruk av fellesskapets midler

Kapitlet har vist at kriminelle aktører og nettverk systematisk utnytter offentlige systemer og ordninger for å sikre seg tilsynelatende legitime inntekter, eller unndra seg plikter, ofte ved hjelp av *registermanipulasjon*, fiktiv dokumentasjon og skjulte eierstrukturer. Nedenfor beskrives sentrale sårbarheter som gjør denne utnyttelsen mulig. Felles for disse er at de samme egenskapene som gjør offentlige ordninger tilgjengelige, brukervennlige og effektive, også gjør dem utsatt for utnyttelse.

Høy grad av tillit og selvrapportering

Mange offentlige registre og ordninger bygger i stor grad på at søkere selv oppgir korrekte opplysninger. Offentlige myndigheter må dermed i stor grad legge til grunn opplysninger som i begrenset grad er verifisert. Uriktige opplysninger, falsk dokumentasjon og fiktive arbeidsforhold kan legges inn i registre uten å bli oppdaget, og danne grunnlag for beslutninger, utbetalinger eller skattemessige fordeler.

Manglende kontroll før utbetaling

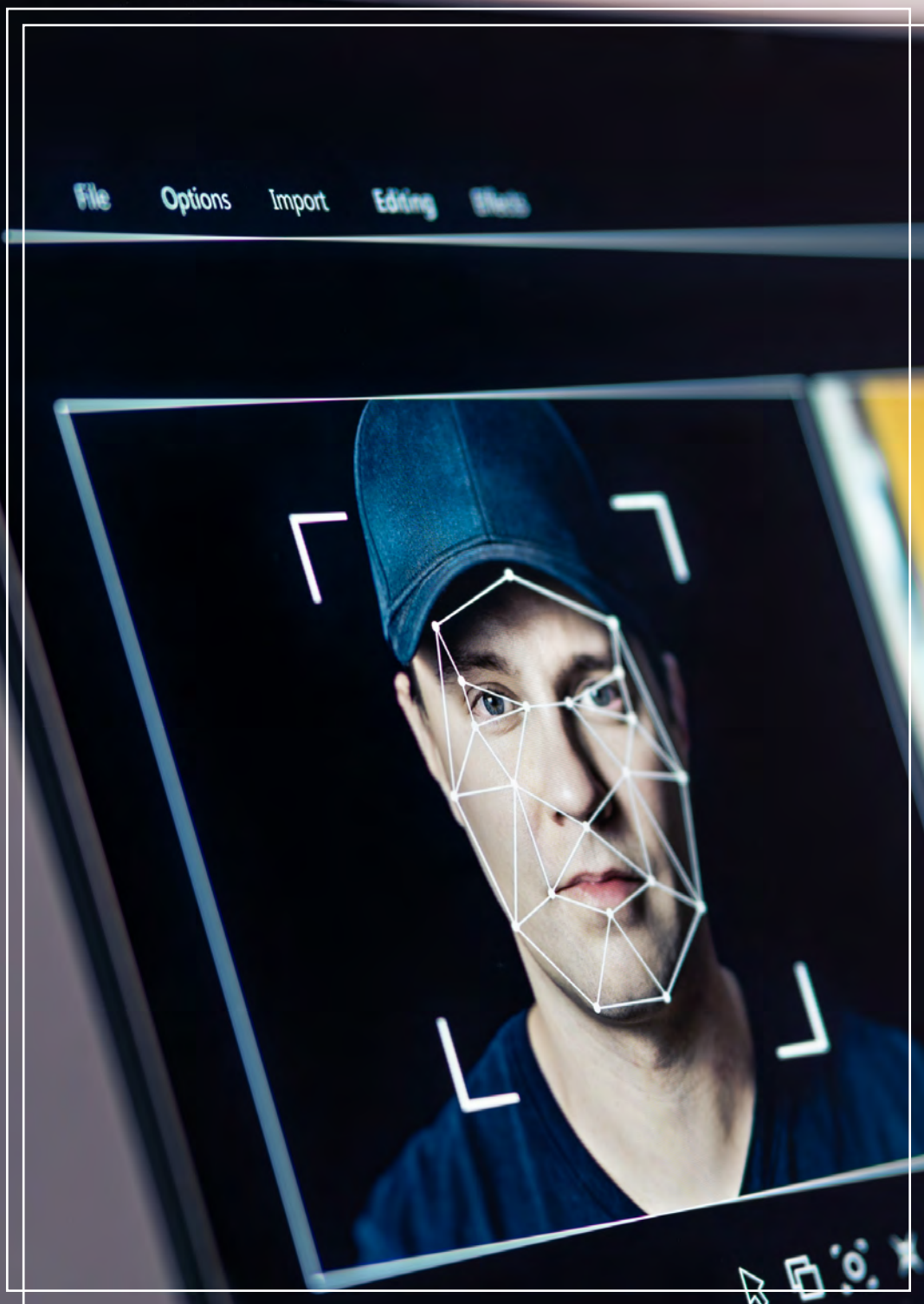
Flere offentlige ordninger er innrettet slik at midlene utbetales først, og kontrollen av om vilkårene faktisk var oppfylt skjer eventuelt i etterkant. Dette følger dels av at brukervennlighet og rask saksbehandling prioriteres når digitale løsninger effektiviseres, uten at det bygges inn tilstrekkelige kontrollmekanismer i samme

prosess.⁷⁰ Jo mer ordningen er innrettet mot kontroll i etterkant fremfor kontroll før utbetaling, jo lengre tid kan gå før misbruk oppdages.

Manglende oversikt og transparens på tvers av ordninger

Når offentlige ordninger mangler oversikt og transparens blir det vanskelig å identifisere overlappende støtte, interessekonflikter eller mønstre av systematisk misbruk på tvers av ordninger. Det finnes ingen samlet oversikt over hvem som mottar midler fra flere ordninger samtidig. Dette gjør seg gjeldende i både tilskuddsforvaltningen og i andre ordninger som forvalter mange parallelle ytelser eller refusjoner. Slike begrensninger svekker også mulighetene for innsyn og etterprøving, både for offentligheten og kontrollmyndighetene.

70 Nasjonalt tverretatlig analyse- og etterretningscenter (NTAES). 2024. *Registermanipulasjon*.



Digitale bedragerier

Bedragerier er det raskest voksende området innen organisert kriminalitet. Europol beskriver dagens situasjon som en «epidemi» der omfang, variasjon og sofistikeringsgrad er uten sidestykke.⁷¹

Digitale bedragerier mot privatpersoner og næringsliv rammer bredt i det norske samfunnet. I 2025 ble det anmeldt over 30 000 fullførte bedragerier, hvorav over 23 000 var digitale. Samtidig er det fremdeles store mørketall. Erfaring fra en av de store bedragerietterforskningene i Økokrim viste at omkring en tredjedel av ofrene anmeldte forholdet. De økonomiske tapene er betydelige, med et estimert årlig samlet utbytte på over 2 milliarder kroner.

Bedragerinettverkene opererer på tvers av landegrenser og samarbeider i Norden. De kan også knyttes til annen kriminalitet, som vold og narkotika, og midler fra bedrageri brukes til å finansiere annen kriminell virksomhet. Økokrim ser også en utvikling der etablerte kriminelle nettverk, tidligere kjent fra andre kriminalitetsområder, gradvis tar i bruk bedrageri som ny inntektskilde. Utbyttet kanaliseres videre inn i den samme

hvitvaskingsøkonomien som beskrives i kapitlet om hvitvasking. Samtidig er bedragerisentre, særlig i Sørøst-Asia, en sentral del av den fremvoksende industrielle kriminaliteten, som beskrevet i kapitlet om industrialisert bedragerivirksomhet.

Lett tilgjengelige digitale tjenester, fra *phishing* til stemme- og ansiktskloning, senker terskelen for avanserte bedragerier og gjør det mulig å ramme mange ofre samtidig. Fremover kan selvgående KI-systemer automatisere hele bedragerikjeder, fra identifisering av ofre til gjennomføring og oppfølging. Det lar bakkennene holde større avstand til handlingene.

I dette kapitlet fremhever vi fire typer bedragerier som først og fremst rammer privatpersoner og foretak. Bedrageriene rammer mange og er estimert å gi kriminelle stort utbytte.

⁷¹ Europol. 2025. *Serious and Organised Crime Threat Assessment (SOCTA) - The Changing DNA of Serious and Organised Crime*.

Investeringsbedrageri

Investeringsbedragerier blir regnet for å være en av de mest utbredte bedrageriformene i verden, og er svært lønnsomme for gjerningspersonene.⁷² Ved investeringsbedrageri blir offeret overtalt til å investere i falske objekter, som kryptovaluta, aksjer og oppstartsforetak. Økokrim har estimert det totale utbyttet fra investeringsbedrageri i Norge i 2025 til 340 millioner kroner.

Investeringsbedrageri er ofte strukturert i tre faser. I **salgsfasen** blir offeret kontaktet og manipulert til å investere. De har ofte selv meldt interesse etter å ha gått inn på en annonse for en investeringsmulighet som lover unormalt høy avkastning. Offentlig kjente profiler og merkevarer misbrukes gjerne i slike annonser. Ofte rekrutteres også av bekjente, ved digitale eller fysiske arrangementer og gjennom sosiale medier.

Tilbakekjøpsfasen inntreffer når offeret ikke lenger vil investere, men ønsker å ta ut utbyttet fra investeringen. Bedragerne forsøker å få offeret til å betale ytterligere i form av ulike avgifter, skatter eller gebyrer under påskudd av at de vil få utbetalt midlene sine og gevinsten like etter. I flere tilfeller har ofre tatt opp lån fra bank eller bekjente i håp om å få frigjort midlene i tilbakekjøpsfasen.

Redningsfasen betegner fasen etter at offeret har gitt opp og anser midlene sine som tapt. Da kan de bli kontaktet av firmaer som utgir seg for å være spesialister på å tilbakeføre tapte midler fra investeringsbedrageri. Denne tjenesten koster også penger, og det er ikke uvanlig at offeret blir kontaktet av flere firma som tilbyr det samme.

Omfattende investeringsbedrageri og hvitvasking

Tre norske menn er tiltalt for grovt bedrageri og grov hvitvasking som del av et kompleks med flere tusen fornærmede i utlandet og over 900 millioner kroner i tap. Ifølge tiltalen ble medlemmene lurt til å tro at de, ved å kjøpe ulike «produktpakker» blant annet bestående av virksomhetens egne kryptovalutaer og aksjer, fikk del i investeringene og overskuddet til en svært lønnsom næringsvirksomhet. I realiteten hadde virksomheten ingen inntjening utenom medlemmenes egne innskudd.

⁷² Interpol. 2024. *Financial Fraud assessment: A global threat boosted by technology*.

Nettbankbedragerier

Nettbankbedrageri er blant de mest alvorlige bedrageriformene målt i økonomisk tap. DNB alene meldte om bedrageriforsøk mot banken for 3,3 milliarder kroner i 2025, på tvers av alle bedrageriformer, hvorav banken klarte å stanse 90 prosent.⁷³ Til tross for at en betydelig andel av forsøkene stanses, blir metodene mer sofistikerte enn før, og antallet forsøk øker markant år for år.

Bedrageriene innledes typisk ved at gjerningspersonen tar kontakt over telefon, SMS eller e-post og utgir seg for å være politi eller bank. Deretter manipuleres ofret til å oppgi BankID, koder eller andre personlige passord som gir tilgang til nettbanken. En tydelig trend i 2025 har vært at gjerningspersonene i tillegg overtaler offeret til selv å installere fjernstyringsprogramvare, slik at de kan styre offerets enhet direkte. Gjerningspersonen logger seg så inn i fornærmedes nettbank og overfører penger, søker om lån eller oppretter konto hos digitale betalingstjenester.

Bedragerne som begår nettbankbedrageri retter seg også mot kryptoverdier, blant annet gjennom såkalte *kryptodrainers* og *phishing*. Programvarer som

benyttes for å få tilgang til midlene er tilgjengelige som *kriminelle handelsvarer*. Denne typen bedrageri kan føre til store tap. I et tilfelle oppga en fornærmet passordet til kryptolommeboken gjennom en lenke han mottok i samtale med det han trodde var kundestøtte. Det førte til at kryptoverdier tilsvarende 4,6 millioner norske kroner ble overført ut av lommeboken hans.

Bedrageri ved bruk av en kombinasjon av digitale og fysiske virkemidler

Gjerningspersoner er villige til å gå langt for å oppnå utbytte. Ved to tilfeller har eldre personer blitt manipulert til å reise og oppholde seg i utlandet, og lidd tap på henholdsvis over 3,5 og 5,5 millioner kroner. Midlene ble tapt gjennom en kombinasjon av bankoverføringer og at gjerningspersonene har benyttet seg av fornærmedes kortinformasjon til å kjøpe smykker og gull i landene de ble tatt med til.

⁷³ DNB. 2026. *Finansiell trygghet: Når virkeligheten utfordres*.

Annonsebedrageri

Annonsebedrageri er bedrageri hvor offeret betaler for en vare eller tjeneste som ikke leveres, eller som avviker vesentlig fra annonsebeskrivelsen. Slike bedragerier foregår ofte på digitale markedsplasser for brukthandel og i «kjøp og salg» – grupper på sosiale medier. Nettsider benyttes også, gjerne ved bruk av .no-domener, slik at de fremstår som seriøse norske foretak. Beløpene per sak er ofte lave, men ettersom dette er bedrageriformen med flest anmeldelser, blir de totale tapsbeløpene betydelige. I 2025 utgjorde det estimerte samlede tapsbeløpet fra annonsebedrageri 127 millioner kroner.

I en betydelig andel av anmeldte annonsebedragerier er gjerningspersonen navngitt og har blitt anmeldt av flere fornærmede som har kjøpt samme vare i en kort tidsperiode mens annonsen er aktiv. I andre saker benyttes falske profiler, eller kaprede profiler fra virkelige personer. Ofte har den kriminelle aktøren fått tak i innloggingsdetaljene og benytter kontoen, uten eierens vitende. Betaling

fra offeret ledes dessuten ofte til en konto som ikke tilhører gjerningspersonen selv, men til et pengemuldyr, slik at det skapes avstand mellom aktøren og det straffbare utbyttet.

Kjente profiler benyttes ofte til å reklamere for produkter som ikke finnes, eller som ikke har de egenskapene det reklameres for. Misbruk av profiler innen helsesektoren er særlig alvorlig. Det er eksempler på at anerkjente fagpersoner har blitt fremstilt i KI-genererte videoer og bilder for å reklamere for udokumenterte helseprodukter, og på deepfake-videoer av leger som blant annet fraråder diabetikere å ta medisinene sine. Stadig mer avansert KI-teknologi bidrar til forbedret kvalitet på slikt falskt innhold, og øker sannsynligheten for at den sosiale manipulasjonen lykkes.⁷⁴

⁷⁴ Kripas. 2026. *Cyberkriminalitet*.

Falsk net jobb

Falsk net jobb representerer en raskt voksende form for bedrageri på verdensbasis.⁷⁵ I Norge ble det først rapportert om denne typen bedrageri i 2023. Siden da har antallet anmeldte saker økt årlig.

Privatpersoner rekrutteres via uoppfordrede meldinger i digitale kommunikasjonskanaler, til det de oppfatter som legitimt arbeid på internett. Enkle digitale handlinger, som å vurdere apper eller like innhold i sosiale medier, presenteres i en profesjonell og tillitsvekkende tone, med løfter om høy inntekt kombinert med fleksibilitet og hjemmearbeid. Kommunikasjonen foregår ofte på norsk, men med et språk som tyder på bruk av oversettelsesverktøy.

Når kontakten er etablert, ledes offeret til en egen digital plattform der oppgavene utføres. Små, reelle utbetalinger i starten etterfølges av stadig mer «lønnsomme» oppgaver som krever at de selv betaler inn penger, som regel i kryptovaluta, eller via *neobanker*.⁷⁶ Presset for å betale raskt for ikke å miste allerede opptjente midler er en gjennomgående metode. Når ofret forsøker å ta ut sine

påståtte inntekter, oppstår som regel «tekniske» eller «administrative hindringer», etterfulgt av gjentatte krav om å betale skatt eller gebyrer for å frigjøre pengene. Dette har klare likhetstrekk med tilbakekjøps- og redningsfasen ved investeringsbedragerier, der ofret lokkes til å betale stadig mer for å få tilgang til midler som i realiteten aldri utbetales. Enkelte ofre kontaktes i etterkant av aktører som hevder å kunne bistå med å få tilbakeført midlene, mot betaling.

Falske net jobber fremstår som en profesjonalisert form for økonomisk kriminalitet som forventes å vedvare i takt med økt digitalisering av arbeidsmarkedet. Den rammer ofte personer som allerede står i en vanskelig økonomisk situasjon.

75 TrendAI. 2025. *Unmasking Task Scams to Prevent Financial Fallout From Fraud*.

76 Federal Trade Commission. 12.12.2024. *Task scams create the illusion of making money*.



Bedrageri har store menneskelige kostnader

Teknologisk utvikling og profesjonalisering av kriminell virksomhet gjør at det blir stadig vanskeligere å skille svindelforsøk fra reelle prosjekter, relasjoner, arbeidsmuligheter og lignende. Likevel sitter mange ofre igjen og føler stor skam etter å ha blitt lurt, noe som fører til at mange ikke søker hjelp, verken fra politiet eller andre institusjoner.

Ofre som har blitt utsatt for bedrageri kan ende opp i svært krevende økonomiske situasjoner. I noen tilfeller har de tapt både bolig og oppsparte midler samt tatt opp betydelige lån. I tillegg kommer de menneskelige kostnadene, der skamfølelse ofte fører til depresjon og isolasjon fra venner og familie. I enkelte tilfeller har ofre for bedrageri tatt sitt eget liv.

Sårbarheter knyttet til digitale bedragerier

Kapitlet har vist at bedragere utnytter systemer som er bygget for å være åpne, globale og raske, snarere enn kontrollerte. Nedenfor beskrives tre sentrale sårbarheter som utnyttes til å begå digitale bedragerier. Disse sårbarhetene knytter seg til manglende verifisering, Norges digitale avhengighet av utlandet, og svak kontroll med domener.

Annonserer på digitale plattformer må ikke verifisere seg

Store digitale plattformer verifiserer i liten grad hvem som står bak annonsekjøp på deres flater. Dette gjelder også annonser for finansielle tjenester. Det gjør det mulig å plassere svindelannonser anonymt, noe som gjør det vanskelig å identifisere hvem som står bak bedrageriene og forebygge aktiviteten.

Norge er avhengig av utenlandske digitale plattformer

Norges digitale suverenitet er begrenset. Norske borgere og foretak bruker primært utenlandske digitale plattformer til kommunikasjon, annonsering og informasjonsformidling. De største teknologiselskapene opererer globalt og er ofte underlagt andre lands jurisdiksjoner og regulatoriske rammeverk. Dette begrenser norske myndigheters mulighet til å stille krav, føre tilsyn og sikre rask oppfølging av skadelig innhold og digitale bedragerier. Avhengighet av

utenlandsk teknologi og sosiale medier svekker Norges påvirkningskraft og gjør landet sårbart for digital manipulering og utnyttelse.

Den nasjonale innsatsen for identifisering og stenging av falske nettsider er begrenset

Norge har begrenset kapasitet til å identifisere og stenge eller blokkere falske nettsider på en effektiv måte. Det gjør det enkelt å bruke falske domener til *phishing* og annen digital svindel. Dette rammer både privatpersoner og virksomheter. Utviklingen innen KI vil trolig forsterke dette problemet.



Foto: Unsplash

Begrepsliste

Arbeidslivskriminalitet er handlinger som bryter med norske lover om lønns- og arbeidsforhold, trygder, skatter og avgifter, gjerne utført organisert, som utnytter arbeidstakere eller virker konkurransevridende og undergraver samfunnsstrukturen.⁷⁷

Blankoskjøte er et skjøte hvor noen felter står åpne for senere utfylling og tinglysing. Det vanligste er at selger underskriver kjøtet og overlater til kjøper å fylle ut resten når kjøper har bestemt seg for hvem som skal bli den permanente kjøperen og hjemmelshaveren til eiendommen.

Kriminalitet som handelsvare (engelsk: Crime-as-a-service, CaaS) er en forretningsmodell hvor kriminelle tilbyr kompetanse, teknologi og informasjon som tjenester eller varer.

Elektronisk ID (eID) er et identitetsbevis som bekrefter ens identitet. Man må ha et norsk identitetsnummer (fødselsnummer eller d-nummer) for å få en elektro-

nisk ID. Det finnes flere typer elektroniske ID-er. De vanligste er MiniID og BankID.

Endemisk korrupsjon er en form for korrupsjon som er så utbredt, dypt rotfestet og integrert i et samfunns sosiale, politiske og økonomiske strukturer at den har blitt en del av den daglige normen.

Falsk net jobb er et svindeltilbud der en person lurer en annen til å tro at de har fått en ekte jobb på internett. Målet til svindleren er å stjele penger, lure offeret til å gjøre ulovlig arbeid, eller stjele personlig informasjon.

Handelsbasert hvitvasking er prosessen der kriminelle flytter verdier og skjuler ulovlig opprinnelse gjennom internasjonale eller nasjonale handelstransaksjoner. Metoden innebærer ofte manipulering av pris, mengde eller kvalitet på varer og tjenester for å overføre penger ulovlig mellom parter.

Hvitvasking innebærer å sikre utbyttet fra en straffbar handling ved å skjule knytning

⁷⁷ Arbeidstilsynet, NAV, Skatteetaten & Politiet. 2022. Felles årsrapport for etatenes innsats mot arbeidslivskriminalitet 2022.

gen til kriminalitet og få utbyttet til å se ut som det er fremskaffet på lovlig måte ved å integrere det i den legale økonomien. Uten mulighet for å hvitvaske utbytte ville motivasjonen for en stor andel av alvorlig profittmotivert kriminalitet forsvinne.

Høynivåkorupsjon er korrupsjon som involverer personer i ledende eller innflytelsesrike posisjoner, for eksempel politikere, ministre, statsledere, ledere i statlige selskaper og andre personer med betydelig beslutningsmyndighet.

Illegal undergrunnsbankvirksomhet (engelsk: underground banking) er et parallelt finanssystem som opererer på siden av det ordinære banksystemet og utenfor bankenes og myndighetenes innsyn.

Innsider benyttes om en som bevisst eller ubevisst tilrettelegger for trusselaktører eller på annen måte skader virksomheten gjennom tilganger og kunnskap personen har fått, nettopp i kraft av å være på innsiden.⁷⁸

Klientkonto er bankkonto der advokater og enkelte andre yrkesgrupper oppbeva-

rer penger som tilhører klienter, adskilt fra egne midler. Den ansvarlige for behandlingen av klientmidler plikter å holde disse adskilt fra egne midler og andre midler som ikke tilhører klienter. Ordningen kan misbrukes til hvitvasking fordi transaksjoner via kontoen er beskyttet av taushetsplikt eller lav innsynsmulighet for tredjeparter, noe som gjør det vanskelig å skille klientens legitime behov fra illegitime.

Konkurskarantene er et tidsbegrenset forbud mot å stifte nye selskaper eller ha ledende roller i næringslivet.

Korrupsjon er misbruk av makt i betrodde stillinger for personlig gevinst. I straffelovens § 387 er korrupsjon definert som det «å kreve, motta eller akseptere, gi eller tilby noen en utilbørlig fordel i anledning av utøvelsen av stilling, verv eller utføringen av oppdrag».

Korrupsjonsmeglere (engelsk: corruption broker) er en type profesjonell tilrettelegger hvis verdi ligger i posisjon og nettverk, ikke fagkompetanse. En korrupsjonsmegler kjenner både den som ønsker å påvirke og den som skal påvirkes, og fungerer som et mellom-

⁷⁸ Nasjonal Sikkerhetsmyndighet (NSM). 2023. *Sikkerhetsfaglig råd - et motstandsdyktig Norge: Innsiderisiko*.

ledd som formidler og skjærer kontakten mellom partene.

Kriminelle nettverk er et samlebegrep på miljøer, gjenger, grupperinger eller sett av individer som er knyttet sammen gjennom kriminalitet. De kriminelle knytningene kan være av både kortvarig og langvarig karakter, involvere alle typer kriminalitet og nettverkene kan ha større eller mindre grad av struktur og organisering.⁷⁹

Krypto-drainer er skadelig programvare eller et skript som brukes til å stjele midler fra en persons digitale kryptolommebok. Verktøyet aktiveres når offeret kobler sin lommebok til en falsk eller kapret nettside og godkjenner en ond-sinnet transaksjon eller tillatelse, hvorpå midlene umiddelbart overføres til angriperens kontroll.

Mva-karusell er en metode for merverdiavgiftsvindell der varer og fakturaer sendes gjennom flere selskaper i ulike land, ved at ett selskap unnlater å betale innkrevd merverdiavgift til staten, mens et annet selskap krever refusjon for avgift som aldri er innbetalt. Resultatet er at staten både mister avgift som skulle

vært betalt, og utbetaler refusjon av avgift som aldri ble innbetalt.

Neobank er finansforetak som kun opererer digitalt, og som gjerne tilbyr banktjenester som sparekonto og kredittkort, uten å ha fysiske filialer.

Offentlige systemer og ordninger

menes i denne rapporten dels ordninger der det offentlige stiller midler til rådighet for enkeltpersoner, virksomheter eller organisasjoner basert på fastsatte vilkår (velferdsordninger, tilskudd, refusjoner), dels obligatoriske systemer for skatt og avgift som virksomheter og innbyggere plikter å forholde seg til. Med misbruk av **offentlige systemer og ordninger** menes tilfeller der noen oppnår en økonomisk fordel eller unndrar seg en plikt ved å gi uriktige opplysninger, fortie relevante forhold eller på en annen måte omgå de fastsatte vilkårene eller reglene. I rapporten omtales slikt misbruk samlet som misbruk av fellesskapets midler.

Phishing (norsk: nettfiske) er en form for svindel der bakmennene forsøker å lure brukeren til selv å oppgi sensitive opplysninger, som passord, PIN-kode eller betalingskortinformasjon. Metoden

⁷⁹ Økokrim. 11.11.2021. *Kriminelle nettverk innen økonomisk-, arbeidslivs-, og miljøkriminalitet*.

baserer seg i stor grad på sosial manipulasjon, ofte ved å utgi seg for å være en pålitelig avsender, som en bank, ansatt i politiet, teknisk support eller en kjent kontakt.

Profesjonelle tilretteleggere er personer som i kraft av sin profesjon og kompetanse medvirker til lovbrudd, eller sørger for at lovbruddene tilsløres.⁸⁰

Proxy-aktører er personer, grupper eller nettverk som utfører handlinger på vegne av en stat uten å være formelt knyttet til den. De kan brukes til å gjennomføre for eksempel sabotasje, påvirkningsoperasjoner eller terrorhandling, slik at statens rolle blir mindre synlig.

Registermanipulasjon er en form for økonomisk kriminalitet der opplysninger i offentlige eller private registre bevisst endres, forfalskes eller manipuleres for å oppnå økonomisk profitt på ulovlig grunnlag, eller annen fordel. Dette kan ramme både velferdsstaten, næringslivet og enkeltpersoner.

Rundfakturering er når flere selskaper sender fakturaer til hverandre for varer eller tjenester som i liten grad, eller ikke i

det hele tatt, er levert. Dette kan brukes for å få det til å se ut som om selskapene har mer aktivitet og inntekter enn de faktisk har, skjule hvordan penger flyttes mellom selskaper, eller unndra skatt og avgifter.

Selvvasking er hvitvasking av egne verdier. Det vil si at en person som selv har tjent penger eller skaffet seg andre verdier, som eiendom, biler eller aksjer, gjennom en kriminell handling, for eksempel skatteunndragelse eller bedrageri, prøver å skjule hvor verdiene kommer fra eller hvem som egentlig eier dem. Dette skiller seg fra vanlig hvitvasking, som handler om å skjule andres kriminelle verdier.

Sanksjonsomgørelser er når man bevisst finner måter å komme rundt sanksjonsreglene på for å skjule hvor varer, penger eller eierskap egentlig kommer fra eller havner.

Skallselskap er et selskap som fungerer som et verktøy for økonomiske transaksjoner uten selv å ha nevneverdige eiendeler eller virksomhet.

Skatteparadis er en jurisdiksjon som tilbyr personer og selskaper fra utlandet

⁸⁰ Økokrim. 18.11.2021. *Profesjonelle aktører som tilretteleggere.*

svært lave skatter og et lovverk med sekretesseregler som begrenser innsyn fra omverdenen.

Stråperson refererer til en person som stiller sitt navn til disposisjon for å skjule den reelle eieren sin tilknytning til en virksomhet eller handling. Hensikten er å skjule kriminelle handlinger.

Stråselskap er firma som opprettes med formål å skjule reell eier eller tilsløre ulovlige aktiviteter. Slike firma har ofte ikke en reell drift, og benyttes gjerne for sanksjonsomgåelse, skatteunndragelser, mva-bedragerier eller hvitvasking av kriminelt utbytte.

Sårbarheter er forhold, innretninger og mangler ved eksempelvis vårt kontrollsystem og vår kriminalitetsbekjempelse, som kan bli utnyttet av trusselaktører, og derigjennom bidra til kriminalitet.

Undergrunnsbanktjenester er finansielle tjenester som leveres systematisk og i stort omfang utenfor den regulerte banksektoren. Eksempler er transport av kontanter, overføringer til andre land og veksling av kontanter og kryptovaluta. Tjenestene er **illegale** når verdiene som formidles stammer fra kriminalitet. **Uformelle verdioverføringssystemer** er en

konkret type av undergrunnsbank. Organiserte nettverk formidler penger eller tilsvarende verdier mellom personer i ulike land, ofte uten at pengene flyttes fysisk. Hawala, hundi og feiqian er eksempler på slike systemer.

Virtuelle IBAN (vIBAN) er kontonumre som ikke er knyttet til en egen fysisk bankkonto, men som viderefører innbetalinger til en felles hovedkonto, ofte i et annet land.

Økonomisk kriminalitet er profittmotiverte, lovstridige handlinger som ofte begås innenfor eller med utspring i en økonomisk virksomhet som i seg selv er – eller gir seg ut for å være – lovlig. Kriminaliteten rammer bredt, fra enkeltpersoner og virksomheter til økonomiske og ideelle samfunnsinteresser og store organisasjoner som finansinstitusjoner eller industriselskaper.

Anbefalt viderelesing

Denne trusselvurderingen bygger på et bredt kunnskapsgrunnlag. Nedenfor følger en oversikt over sentrale rapporter som gir utdypende innsikt i temaene som omtales, og som kan være nyttige for lesere som ønsker å gå dypere inn i enkeltområder.

Europol (2026). Decoding the EU's most threatening criminal networks – Issue 2: The blueprint of criminal opportunism. Undersøker hvordan kriminelle nettverk, som utgjør størst trussel i EU, stadig erstattes av nye, og hva som gjør at kriminaliteten består selv om enkeltaktører forsvinner. <https://www.europol.europa.eu/publication-events/main-reports/blueprint-of-criminal-opportunism>

NTAES (2026). Profittmotiverte lovbrudd i arbeidslivet – Risikovurdering arbeidslivskriminalitet 2026–2028. Vurderer trusler og sårbarheter i arbeidslivskriminalitet og skisserer fremtidsscenarioer frem mot 2028. <https://ntaes.no/no/publikasjoner/risikovurdering-2025-2028/>

Rostami, A., Mondani, H., Mellberg, J. & Roine, J. (2026). Svarta siffror – en ESO-rapport om den kriminella ekonomins omfang. Analyserer omfanget av den kriminelle økonomien i Sverige, og er relevant som sammenligningsgrunnlag siden tilsvarende tall ikke finnes for Norge. https://eso.expertgrupp.se/rapporter/2026_1-svarta-siffror/

Økokrim (2026). Nasjonal risikovurdering hvitvasking 2026. Gir en helhetlig risikovurdering av hvitvasking i Norge, med egne kapitler om blant annet skjult eierskap, stråpersoner, profesjonelle tilretteleggere, og utnyttelse av virksomhetsstrukturer. <https://www.okokrim.no/nasjonal-risikovurdering-2026-hvitvasking-truer-samfunnsstrukturene-i-norge.6748724-549307.html>





ØKOKRIM

Postadresse: Pb. 2096 Vika, NO-0125 Oslo

Besøksadresse: Grenseveien 78, NO-0663 Oslo

Kontakt: 23 29 10 00 / post.okokrim@politiet.no

www.okokrim.no



Financial Intelligence Unit
Norway

Foto: Ki-generert av Økokrim