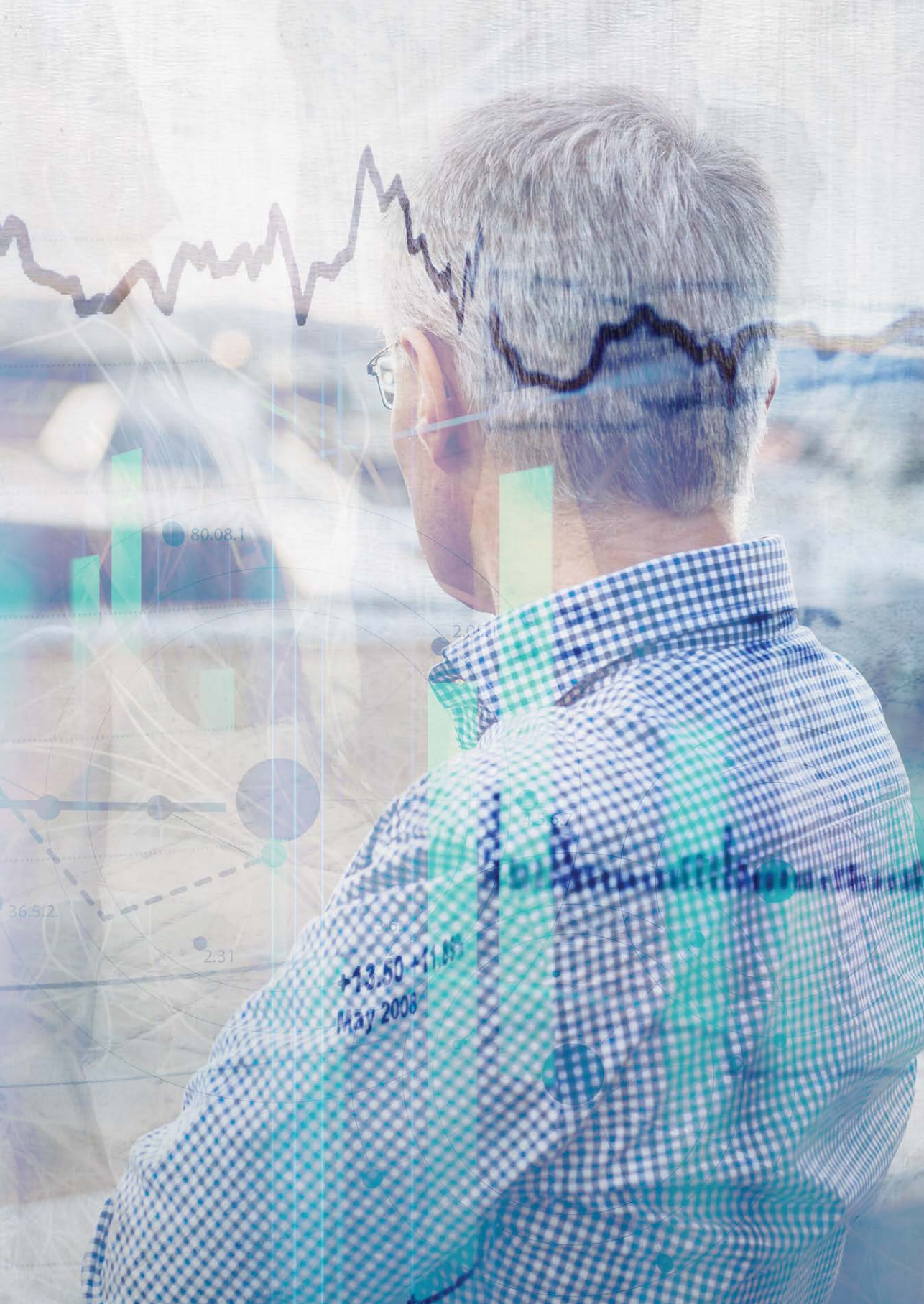
ØKOKRIM

Trusselvurdering
2018


80.08.1
36.5.72.
2.31
+13.50 +1.05
May 2008

Forord

Vi ser siden forrige trusselvurdering en tydeligere tendens til at digitaliseringen gjør det stadig enklere å drive massebedragerier – norske bedrifter og privatpersoner er attraktive mål for utenlandske bedragere. Digitaliseringen og globaliseringen preger også trusselbildet i resten av vårt ansvarsområde. Dette gir politiet og myndighetene nye utfordringer og stiller høyere krav til tverretatlig samarbeid.

I denne trusselvurderingen beskriver vi de største truslene innen ØKOKRIMs ansvarsområde. Det overordnede trusselbildet har vært relativt stabilt siden 2015. På noen områder ser vi få, men svært alvorlige, tilfeller av lovbrudd. Andre kriminalitetsformer vurderes å være store trusler fordi det er mange lovbrudd. Her er ikke hvert lovbrudd nødvendigvis så alvorlig, men det står ofte organiserte kriminelle bak.

Politiets straffesaksarbeid vil fremdeles være viktig i kriminalitetsbekjempelsen innen vårt ansvarsområde. Men innenfor mange av kriminalitetstruslene ligger det et stort potensiale for forebygging – ikke minst i samarbeid med næringslivet.

Vurderingene i denne trusselvurderingen blir førende for prioriteringer av vår innsats. Trusselvurderingen vil forhåpentligvis også bli benyttet ved prioriteringer i andre politi- og påtaleenheter.

Kampen mot kriminalitet er tverretatlig og internasjonal. I prosessen med utarbeidelse av trusselvurderingen har vi innhentet informasjon fra politidistriktene, aktuelle kontrollorganer og søsterorganisasjoner i andre land. Vi takker for bidragene.

Hovedpunkter

- Dreiningen fra fysisk til digital kriminalitet vil fortsette. Dette vil gi politiet både nye muligheter, og utfordringer, i årene fremover.
- Innen arbeidslivskriminalitet har misbruk av foretak blitt en større del av trusselbildet. Merverdiavgiftsbedrageri utført med fiktiv fakturering fortsetter å være en av hovedkildene til profitt. Det vil bli mer utfordrende for potensielle kunder å avsløre arbeidslivskriminalitet når virksomhetene i økende grad fremstår lovlydige.
- Skatte- og avgiftskriminalitet vil fortsatt være den største trusselen innen tradisjonell økonomisk kriminalitet. Det har blitt enklere å anvende sekretessestrukturer i skatteparadis, og det avdekkes oftere mistanke om skattesvik begått av norske statsborgere, som har meldt utflytting fra Norge, men som oppholder seg i Norge så store deler av året at de er skattepliktige hit for hele sin inntekt og formue. Økt informasjonsutveksling mellom land forventes å føre til avdekking av flere slike saker.
- Korrupsjonsrisikoen knyttet til lokal forvaltning, ikke minst kommunal plan- og byggesaksbehandling, har blitt klarere. Dette kan bidra til annen kriminalitet, også arbeidslivskriminalitet.
- Norske bedrifter er utsatt for ulike typer bedragerier, og vil fortsatt være attraktive mål for utenlandske bedragere. Forebygging og stans av transaksjoner er viktige strategier for å håndtere denne trusselen.
- Omvendt økonomi innen avfallshåndtering gir stort potensiale for profitt ved å ikke etterleve regelverket. Trusselen for forurensingskriminalitet, inkludert akutte hendelser, vil fremdeles være stor.
- Det er betydelige økonomiske incentiver for lovbrudd i fiske- og akvakulturnæringene. Det er sannsynlig at betydelige mengder fisk vil bli oppdrettet og fisket ulovlig og omsatt svart.
- Kriminelle vil i økende grad ta i bruk nyere betalingstjenester og digital valuta for å hvitvaske penger.
- Terrortrusselen i Norge knyttes til enkle angrep som krever få ressurser. Det vil være en utfordring at de ofte er snakk om små beløp som overføres i forbindelse med finansiering av terror.

Main findings

- The shift from physical to digital crime will continue. This will, in the coming years, present the police with both new possibilities, and challenges.
- Abuse of business structures has become more prominent in work-related crime. VAT-fraud by production of fictive invoices continue to be one of the main sources to profit. It will become more challenging for potential customers to discover work-related crime, as the businesses increasingly present themselves as law abiding.
- Tax crime will continue to be the largest threat within traditional economic crime. It has become easier to use secrecy structures in tax havens. Norwegian citizens who reportedly moved abroad but spend enough time here to be liable for taxation in Norway of all their income and wealth, are also more frequently discovered. Increased information exchange between countries is expected to result in the uncovering of more of these cases.
- The corruption risk in the local administration, particularly in relation to planning and building applications in the municipalities, has become clearer. This can contribute to other crime, including work-related crime.
- Norwegian businesses are prone to different types of fraud, and will continue to be attractive targets for foreign fraudsters. Preventive measures and stopping transactions will be important strategies to handle this treat.
- Reverse economy within waste handling means that there is a large potential for profit if businesses do not comply with regulations. The threat of pollution crime, including acute incidents, will continue to be high.
- There are significant economic incentives for crime in the fisheries and within aquaculture. It is likely that significant amounts of fish will be raised and fished illegally and sold illicitly.
- Criminals will increasingly start using new payment services and digital currencies to launder money.
- Simple attacks that demand few resources is the main terror threat in Norway. Usually only small amounts of money are needed to finance such attacks. This will be a challenge.

En digital og grenseløs økonomi

To viktige utviklingstrekk har særlig stor påvirkning på norsk økonomi, og vil i tiden fremover fortsatt ha stor påvirkning på truslene innen økonomisk kriminalitet og miljøkriminalitet – digitalisering og globalisering.

Norsk økonomi har blitt digital. Dette gjelder på de fleste områder, som handel, betaling og sosialt samkvem. Også stadig flere samfunnsfunksjoner blir digitale[1], og norske borgere tar i bruk nye teknologiske løsninger hvis de oppfattes som nyttige.

Som resten av befolkningen, benytter kriminelle i større grad digitale betalingsplattformer.[2] Et eksempel er Vipps brukt ved oppgjør mellom kriminelle. Krypterte digitale valutaer[3], kryptovaluta[4], er også, gitt sin natur og måten de blir omsatt på, godt egnet til å finansiere kriminell aktivitet og bli brukt til hvitvasking.[5] En studie viser at omtrent en fjerdedel av brukerne, og nesten halvparten av transaksjonene med Bitcoin, kunne kobles til ulovligheter, og estimerer at illegal aktivitet for omtrent 72 milliarder dollar hvert år betales via Bitcoin.[6] Fremover vil kriminelle sannsynligvis velge andre kryptovalutaer som er mindre sporbare enn Bitcoin.[7]

Samtidig har verden på mange måter blitt grenseløs. Norske borgere handler på utenlandske nettsteder. Betalingen gjennomføres ved hjelp av utenlandske betalingstjenester. Norske bedrifter etablerer seg i utlandet, og utenlandske bedrifter konkurrerer om anbud i Norge på like vilkår som norske bedrifter. Grenseoverskridende virksomhet, og transaksjoner, fremstår i dag som langt mer hyppige enn bare for noen år tilbake.

Digitalisering og globalisering har preget økonomien lenge, men utviklingen går nå stadig raskere, og vil ha stor innvirkning på norsk økonomi og næringsliv.

1. NorSIS, «Trusler og trender 2017–18», 2017.
2. Digitale betalingsplattformer brukes om apper, og internettbaserte programmer som kan brukes til å overføre transaksjoner, ikke nettbank. De kan være tilknyttet både tradisjonell bankvirksomhet, og nyere betalingstjenester.
3. Digital/virtuell valuta er en samlebetegnelse for ulike internettbaserte valutaer. Digitale valuter er ikke utstedt, eller garantert, av en sentralbank, men er akseptert som et betalingsmiddel og kan overføres, lagres, og handles elektronisk.
4. Kryptovaluta er digital valuta som bruker kryptografi for å sikre transaksjoner (NTAES, «Kryptovaluta», NTAES Tema, nr. 1, 2018).
5. Justis- og beredskapsdepartementet (JD), «Nasjonal risikovurdering Hvitvasking og terrorfinansiering i Norge» (NRA), 2016.
6. Sean Foley, Jonathan R. Karlsen, Talis J. Putnins, «Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?», januar 2018. Beregninger basert på et utvalg fra april 2017, og aggregert til årlig aktivitet.
7. Chainalysis, «The Changing Nature of Cryptocrime», January 2018.

Nytt trusselbilde utfordrer politi- og påtalemyndigheten

Også kriminaliteten har blitt digital og grenseløs. De fysiske vinningslovbruddene var i 2017 redusert med 40,4 prosent i forhold til i 2013. Dette har ført til en nedgang i den totale anmeldte kriminaliteten – den digitale kriminaliteten anmeldes i liten grad. Dreiningen fra fysisk til digital kriminalitet forventes å fortsette.

Hele verden er de kriminelles arbeidsplass. I den globale økonomien foregår eksempelvis verdipapirhandel i et internasjonalt marked. Man kan sitte i ett land, handle finansielle instrumenter notert i et annet, og ha bankforbindelse i et tredje. Kartellvirksomhet og prissamarbeid er også en type kriminalitet som ofte er grensekryssende. Og en stor andel av bedragerier i Norge begås av kriminelle fra utlandet.

Mulighetene til å gripe inn gjennom straffehåndhevelse er tradisjonelt knyttet til hvert lands territorium. Godt internasjonalt samarbeid mellom myndigheter i ulike land er i dag avgjørende for å avdekke og forfølge en stor andel av den alvorlige økonomiske kriminaliteten, men det er fortsatt utfordrende å kommunisere raskt og effektivt med noen av de berørte jurisdiksjonene.

Samtlige nyere betalingstjenester[8] er mer sporbare enn kontanter. Økt digitalisering av økonomien gir derfor politiet nye muligheter for å finne spor. Erfaring viser imidlertid at dette er utfordrende for politiet, og nyere betalingstjenester er mer krevende å spore enn tradisjonelle bankoverføringer. Når transaksjoner sendes til, eller fra, nyere betalingstjenester, som Paypal og Worldpay, er det ofte betalingstjenestens navn som fremkommer som mottaker, eller avsender, på kontoutskriften og i valutaregisteret. Reell mottaker og avsender av transaksjonen fremkommer ikke.[9]

Selskaper som leverer digitale tjenester, sitter på store mengder data, men det kan være utfordrende for politiet å få tilgang: Selskapene ligger ofte i utlandet, og enkelte selskaper samarbeider i liten grad med myndighetene. Økt bruk av tjenesteutsetting og lagringstjenester gjør også at man må forholde seg til flere selskaper for å få data utlevert. Samtidig gir selskapenes store datamengder muligheter for politiet, selv om det er begrensinger på bruken av de i norsk rettsvesen. Eksempler på det, er de siste årenes lekkasjer, som Panama Papers (2016), og dataene fra markedsplassen Silk Road.

Det er viktig at politiets innsats innrettes mot en ny digital og global hverdag for å unngå at det etableres lovløse områder innen vårt samfunn og vår økonomi.

8. Her benyttes FATF sin definisjon: «Nyere betalingstjenester anses å være nye og innovative betalingsprodukter og tjenester som tilbyr et alternativ til tradisjonelle finansielle tjenester. Nye betalingstjenester inkluderer en rekke produkter og tjenester som involverer nye måter å initiere betalinger på, eller utvide, rekkevidden til tradisjonell elektronisk handel, samt produkter som ikke baserer seg på tradisjonelle systemer for å overføre en verdi mellom enkeltpersoner eller organisasjoner.» Definisjonen avgrenses mot tradisjonelle finansielle tjenester, som banktjenester, som tilbys på nye plattformer (FATF, «Guidance for a risk-based approach», 2013).
9. NTAES, «Vouchers og betalingsformidlingstjenester – effektiviserer netthandel, tilslører kriminalitet», NTAES Tema, nr. 2, 2018. Reell mottaker og avsender kan imidlertid avdekkes.


ITI

Arbeidslivskriminalitet er i Regjeringens strategi mot arbeidslivskriminalitet (januar 2015) definert som: *«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.»*[10]

Arbeidslivskriminalitet

Profittmotivert multikriminalitet i arbeidsintensive bransjer, og særlig i bransjer med høy andel ufaglært arbeidskraft, har i løpet av de siste knappe ti årene blitt en stor trussel i alle de skandinaviske landene.

I Danmark benyttes ofte komplekse selskapsstrukturer med dekkselskaper og stråmenn for å få utbyttet kanalisert til utlandet, eller utbetalt.[11] I Sverige fremheves offentlige anskaffelsesprosesser som særlig utsatt for å bli utnyttet av organiserte kriminelle.[12] Og i Finland har den økonomiske kriminaliteten i økende grad internasjonale tilknytninger, og knyttes til organisert kriminalitet.[13]

Utfordringen med at kriminelle utnytter legale virksomheter, fremheves også av OECD.[14] Også den tradisjonelle italienske mafiaen har ekspandert til ellers lovlige virksomheter, og allerede i 2013 slo EUROPOL fast at italiensk mafia har etablert seg i flere land i Nord-Europa, blant annet i Tyskland, Frankrike og Nederland. Nå mistenkes det at de er involvert i store utbyggingsprosjekter i Norden gjennom underentreprenører.[15]

Det er utfordrende å anslå omfanget av denne kriminaliteten. Samfunnsøkonomisk analyse anslår at omfanget av arbeidslivskriminalitet i 2015 var om lag 28 milliarder kroner, og at omfanget har vært stabilt de siste årene. Av dette utgjorde skatte- og avgiftsunndragelsene om lag 12 milliarder kroner, og skjult verdiskapning rundt 1,2 milliarder kroner.[16]

Ulovlig utnyttelse av arbeidskraft

Et sentralt element i arbeidslivskriminalitet, er å redusere lønnskostnadene og unngå lovpålagte kostnader forbundet med arbeidskraft. Norge har over tid vært en attraktiv destinasjon for arbeidssøkende, med mulighet for økt inntekt og et bedre liv. Utenlandske personer uten lovlig opphold, er særlig utsatt for utnyttelse av kriminelle aktører. I de mest alvorlige sakene rapporteres det om menneskehandel tilknyttet organisert kriminalitet. ID- og dokumentmisbruket ser også ut til å øke.[17]

Utnyttelse av arbeidskraft er særlig en utfordring innen arbeidsintensive bransjer, som bygg- og anlegg, renhold og transportnæringen. Innen frukt- og grøntproduksjonen i landbruket øker utstrakt bruk av utenlandske sesongarbeidere sannsynligheten for arbeidslivskriminalitet. Også utenlandske sjøfolk, særlig på norske fiskefartøy, er sårbare for utnytting.

Merverdiavgiftsbedrageri og fiktiv fakturering

Merverdiavgiftsbedrageri er en av hovedkildene til profitt innen arbeidslivkriminalitet. Merverdiavgiften er, foruten skatt fra personlige skattytere, statens viktigste inntektskilde, og ga i 2017 268 milliarder til statskassen.[18]

En rapport fra EU fra 2015 konkluderte med et mva-gap[19] i EU på omkring 1600 milliarder kroner. Med tilsvarende omfang av unndragelser som i Sverige og Danmark, kan det norske gapet ligge mellom 11,3 og 25,3 milliarder kroner.[20]

Merverdiavgift kreves inn av norske bedrifter på vegne av staten. Dersom bedriftene har betalt mer merverdiavgift enn de har krevd inn, refunderes dette av staten. Det er registrert en økning av antall aktører

som urettmessig fradragsfører merverdiavgift, og dermed får urettmessige utbetalinger fra staten.

Fiktiv fakturering – organisert produksjon av uriktige dokumenter i en virksomhetsstruktur for å få fiktive kjøp og salg til å fremstå som reelle – er sentralt for å begå slike bedragerier. Fiktiv fakturering benyttes også for å kamuflere svart arbeid, tappe selskaper for verdier, svindle staten for skatt og hvitvasking.

Ansvaret for å kreve inn merverdiavgift ved innførsel av varer ble fra januar 2017 flyttet fra myndighetene, til de avgiftspliktige næringsdrivende. Det kan medføre økt trussel for merverdiavgiftsbedrageri og gjøre Norge mer attraktivt for momskaruseller.[21]

Uforsvarlig arbeidsmiljø

Arbeidstilsynets ulykkesstatistikk viser at utenlandske arbeidstakere utgjør en stor andel av de som omkommer på arbeid. I 2016 og 2017 var henholdsvis 40 og 22 prosent av de omkomne utenlandske statsborgere.

Sett i forhold til antall sysselsatte, er det uforholdsmessig mange omkomne utenlandske arbeidstakere. Det kan skyldes at mange utenlandske arbeidstakere er sysselsatt i næringer med høy forekomst av ulykker, og at de har mer risikofylte arbeidsoppgaver. I allmengjorte bransjer avdekkes det ofte arbeidstakere som er utsatt for et dårlig arbeidsmiljø med høy risiko; kjemisk eksponering, farlig arbeid i høyden, lange arbeidsdager og lønn under minstelønn.[22] De ansatte har gjerne en løsere tilknytning til virksomheten, eller har vært ansatt i kort tid. Opplæring og instruksjoner kan også være mangelfull på grunn av språkproblemer. [23]

Det har vært en rekke uønskede hendelser og alvorlige arbeidsulykker knyttet til prosjekt hvor store internasjonale entreprenørbedrifter har vært involvert.

Trygdebedrageri

Trygdebedragerier er også en kilde til profitt innen arbeidslivskriminalitet, og arbeidsgivere og arbeidstakere samarbeider ofte om å bedra det offentlige.

En velkjent metode for trygdebedrageri er arbeidstakere som arbeider svart, samtidig som de får utbetalt ytelser fra NAV. I 2017 anmeldte NAV 1048 personer for trygdebedrageri for til sammen 187 millioner kroner. 954 personer er anmeldt for å ha svindlet med dagpenger og AAP, de fleste for at de har arbeidet og mottatt lønn som er uforenelig med ytelsen

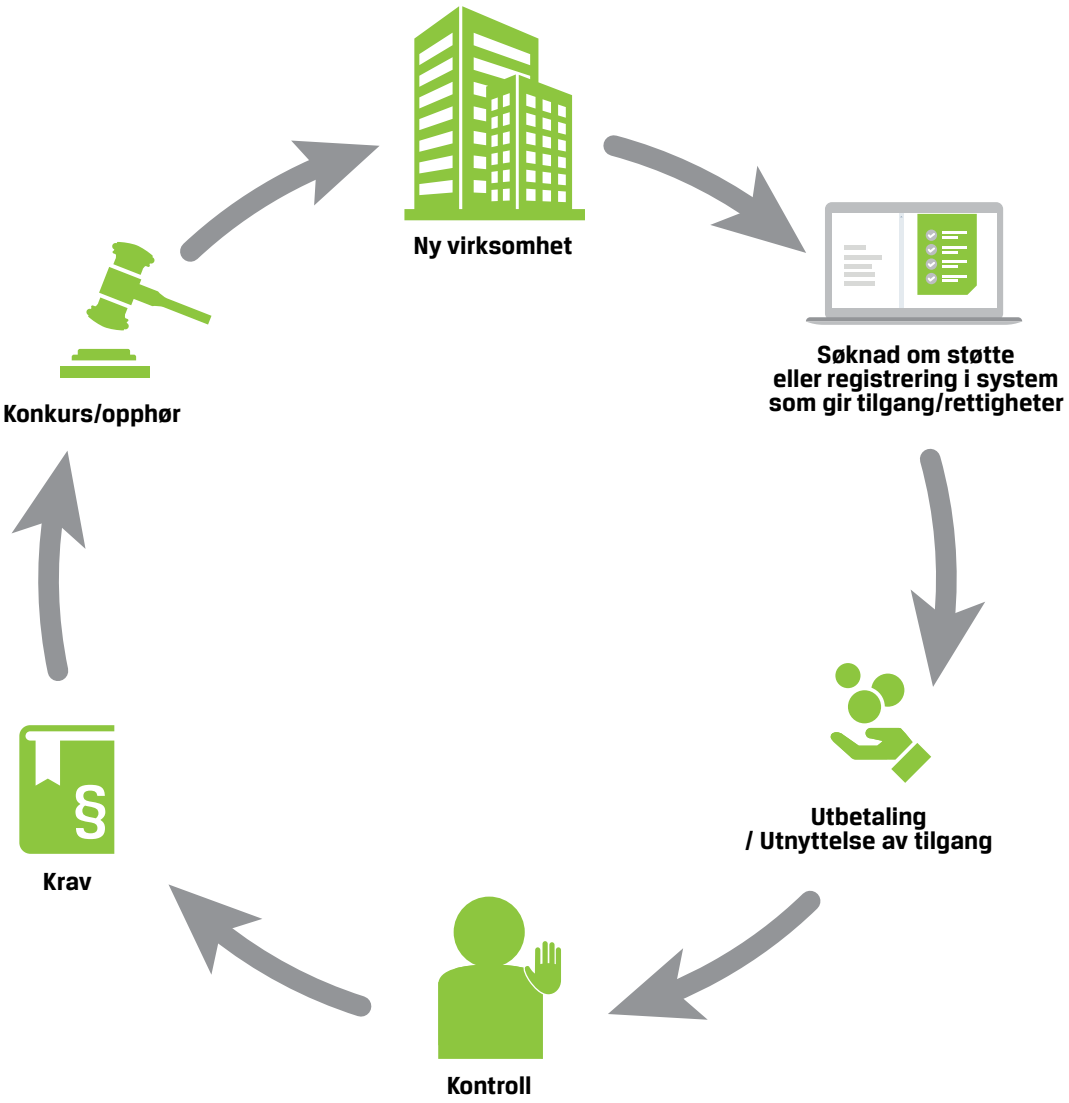
Trygdebedragerier kan også begås ved bruk av fiktive ansettelsesforhold. Bedriften rapporterer da inn lønn, og arbeidsgiveravgift og skatt innbetales. Den fiktivt ansatte opparbeider seg rett til en rekke NAV-ytelser, som dagpenger, sykepenger, uføretrygd og arbeidsavklaringspenger. For bedriften legitimerer slike fiktive ansettelser svart arbeid utført av andre uregistrerte arbeidere, og svart omsetning.

Utnyttelse av selskapsstrukturer

Uklare eier- og ansvarsforhold, og misbruk av foretak, er sentrale elementer i arbeidslivskriminalitet. Legal virksomhet brukes til å gjennomføre og kamuflere kriminaliteten samtidig som utbyttet blir hvitvasket.

Mer komplekse selskapsstrukturer med etablering av selskaper i utlandet, strømenn og skallselskaper er vanlig. Krav fra myndighetene resulterer ofte i hyppig flytting av aktiviteten mellom virksomheter, som illustrert i figur 1, og planlagte konkurser. Dette medfører risiko for konkurskriminalitet. Mangelfull tilgang til informasjon om konkursryttere og deres selskaper vanskeliggjør straffeforfølgelse.

For å oppnå økt fleksibilitet, redusere kostnadene, og unngå arbeidsgiveransvar, benyttes også enkelt-



Figur 1: Virksomhetskarusell

mannsforetak og innleie fra utenlandske bemanningsforetak i en rekke bransjer, noe som igjen gir økt kontrollbehov. I Sverige pekes det på at innvandrere oftere tvinges til å opprette foretak for å få jobb.[24]

Virksomheter prøver nå i større grad å fremstå som lovlydige, gjennom en fin fasade i myndighetenes registre, og rettet mot kunder og leverandører.[25] Det gir mulighet til å utnytte den tillitsbaserte innretningen til offentlig sektor og kontrollorganer, og er en felles utfordring som fremheves i de skandinaviske landene.

Ensidig fokus på pris ved anskaffelser

Store anskaffelser i både næringslivet og det offentlige, skjer som regel i form av anbudskonkurranser. For stor vekting av pris ved anbud, øker risikoen for at virksomheter som drives av arbeidslivskriminelle får oppdrag, da slike aktører har lavere kostnader enn sine lovlydige konkurrenter. Valg av svært lavt prisede anbud medfører et stort press på leverandørene, noe som igjen innebærer en økt trussel for arbeidslivskriminalitet.

Trusselen for arbeidslivskriminalitet er stor innen alle bransjer hvor anbud benyttes for valg av leverandør, også innen salg av for eksempel barnevernstjenester til norske kommuner. Det er observert at kriminelle aktører som tidligere opererte i bygg- og anleggsbransjen har etablert seg her.[26]

Fortsatt trussel

Det har blitt iverksatt mange tiltak for å motvirke sosial dumping og arbeidslivskriminalitet, og innsatsen mot arbeidslivskriminalitet er blitt mer målrettet, organisert og tverretatlig. Aktørene som ønsker å utnytte systemet er imidlertid tilpasningsdyktige. De tilpasser metodene til kontrollmyndighetenes og politiets innsats, og utnytter svakheter i regelverket. Det er fortsatt stor etterspørsel etter, og tilbud av, arbeidstakere som vil jobbe for under normal norsk lønn. Og for potensielle kunder, blir det mer utfordrende å avsløre kriminaliteten når virksomhetene i økende grad fremstår lovlydige. Arbeidslivskriminalitet vil fortsette å være en trussel som utfordrer norsk samfunnsstruktur.

Et skjerpet fokus på enkeltbransjer medfører risiko for at kriminelle kan få handlingsrom til å etablere seg, og drive uforstyrret i andre bransjer.

10. Arbeids- og sosialdepartementet, «Strategi mot arbeidslivskriminalitet», 13.1.2015.
11. [Dansk] Politi, «Nasjonal Strategisk analyse», 2017.
12. NUC, «Myndighetsgemensal lägesbild om organiserad brottslighet 2018-2019», 2017.
13. https://www.vero.fi/en/grey-economy-crime/phenomena/, lest 17.1.2018.
14. OECD, «Shining Light on the Shadow Economy: Opportunities and Threats», 2017.
15. Oslo politidistrikt, «Trender i kriminalitet 2018-2021», 2018.
16. Samfunnsøkonomisk analyse, «Analyse av former, omfang og utvikling av arbeidslivskriminalitet», Rapport nr. 69-2017. Dette er et anslag som er basert på skjult verdiskapning og medianverdier.
17. NTAES, «Situasjonsbeskrivelse 2017. Arbeidslivskriminalitet i Norge», 2017.
18. Skatteetaten, «Årsrapport 2017», 2018.
19. Forskjellen mellom det som skulle vært innbetalt av merverdiavgift til staten, og det som faktisk blir innbetalt.
20. The European Commission, «Study to quantify and analyse the VAT Gap in the EU Member States», 2015 Report, TAXUD/2013/DE/321.
21. Ved momskaruseller (Missing Trader Intra-Community (MTIC) Fraud), blir varer fakturert i en konstruert omsetningskjede for å danne grunnlag for utbetaling av merverdiavgift, før de blir eksportert til et nytt land hvor det samme gjentas. Når den som importerer ikke betaler avgift, og den som eksporterer til utlandet får merverdiavgiften refundert, tappes statskassen. For mer informasjon, se NTAES, Tema – Grensekryssende merverdiavgiftssvindel. Karusellsvindel, nr. 1, 2017.
22. Arbeidstilsynet, NAV, Politiet, Skatteetaten, «Sammen mot kriminalitet i arbeidslivet. Felles årsrapport for styrket innsats mot arbeidslivskriminalitet 2017», 2018.
23. Arbeidstilsynet, «Risiko for arbeidsskadedødsfall i det landbaserte arbeidslivet», KOMPASS Tema, nr. 1, 2018.
24. Ekobrottsmyndigheten, «Ekobrottsmyndighetens lägesbild om ekonomisk brottslighet i Sverige 2016», 2016.
25. NTAES, «Situasjonsbeskrivelse 2017. Arbeidslivskriminalitet i Norge», 2017.
26. Ibid.

Foto: Gorm K. Gaare, EUP Berlin

ØKOKRIMs tradisjonelle definisjon av **økonomisk kriminalitet**, er lovbrudd, ofte profittmotiverte, som begås innenfor rammen av økonomisk virksomhet som i seg selv er lovlig. Ofte dreier det seg om lovbrudd i næringslivsvirksomhet eller offentlig virksomhet. Både politiets statistikk over anmeldte lovbrudd innen «økonomi», og ulike oversikter over økonomisk kriminalitet, omfatter en videre krets av lovbrudd enn de som faller inn under denne definisjonen. Det gjør også denne trusselvurderingen.

Økonomisk kriminalitet

Digitaliseringen og globaliseringen gir nye trusler, samtidig som de gamle fremdeles er der. Skatte- og avgiftskriminalitet, korrupsjon og bedrageri er kriminalitetskategorier av svært ulik karakter, men utgjør i dag de største truslene innen økonomisk kriminalitet. Politidistriktenes saksbilde preges også av andre typer kriminalitet, som konkurskriminalitet og regnskapskriminalitet samt utroskap og underslag.

Konkurskriminalitet anmeldes av bostyrere, og utgjør en stor andel av politidistriktenes saker. Det er en trend at virksomheter opprettes og drives til de tvangsoppløses, og at selskaper endrer registrert adresse like før de blir slått konkurs; For å unngå etterforskning, utnytter aktørene at det er ulik kapasitet i politidistriktene. En stor andel av konkurssakene finner man i bygg- og anleggsbransjen, og konkursgjengangere, som starter ny virksomhet rett etter konkurs, er en utfordring. Ofte etterforskes annen økonomisk kriminalitet, som skatte- og avgiftskriminalitet, trygdebedrageri, samt utroskap og underslag i sammenheng med konkurssaker.

Aktører som har tilgang til klientmidler, begår årlig underslag av betydelige beløp. Ulovlig bruk av innsideinformasjon kan også gi stor profitt. Ansatte i sentrale stillinger i både virksomheter, og hos profesjonelle aktører, kan være attraktive mål for kriminelle på jakt etter informasjon. Aktører som besitter innsideinformasjon, kan også bli utsatt for tyveri av informasjonen ved angrep på datasystemene.

Det kreves kompetanse for å begå økonomisk kriminalitet. Det er derfor fortsatt en trussel at profesjonelle aktører, som regnskapsførere, advokater og takstmenn bistår kriminelle med å tilsløre midlers opprinnelse, hvitvaske midler, gi råd om plassering og skape legitimitet. Ofte uten selv å være klar over det. Dette ser vi innen et bredt spekter av økonomisk kriminalitet, fra arbeidslivskriminalitet til hvitvasking.

Fokuset på, og innsatsen mot arbeidslivskriminalitet har blitt skjerpet. Det kan gi kriminelle økt handlingsrom for å begå annen alvorlig kriminalitet. Det er viktig med fortsatt fokus på den tradisjonelle økonomiske kriminaliteten og miljøkriminaliteten.

Økonomisk kriminalitet

Skatte- og avgiftskriminalitet

Skatte- og avgiftslovbrudd begås av både arbeidstakere og selskaper, og spenner over et vidt spekter av forøvelsesmåter. Av de lovbruddene Skatteetaten avdekker, sanksjoneres de fleste administrativt. Dette gjelder i dag mange saker om svart arbeid. Vi har fokus på de skatte- og avgiftslovbruddene som vurderes som så alvorlige at de anmeldes. I tillegg til de forøvelsesmåtene som beskrives her, er merverdiavgiftsbedrageri ved fiktiv fakturering, som omtales i kapitlet om arbeidslivskriminalitet, en stor trussel.

Det ble i 2017 anmeldt 924[27] forhold innen det som kan klassifiseres som skatte- og avgiftskriminalitet. Litt over 300 forhold ble anmeldt av Skatteetaten etter manglende oppgaver og kontroll. I omfang, og konsekvens, er skatte- og avgiftskriminaliteten fortsatt den største trusselen innen tradisjonell økonomisk kriminalitet.

Unndragelser via skatteparadis[28]

Globalt har husholdninger rundt åtte prosent av sin finansielle formue i skatteparadis. Det antas at det meste av denne formuen unndras beskatning.[29]

Også eiere av norske bedrifter, som den maritime bransjen, benytter seg av skatteparadiser. Slik omgår rederne også en rekke nasjonale og internasjonale reguleringer. Det er nå også en trend at næringsinntekter i små og mellomstore virksomheter kanaliseres til utenlandske konti, og ikke oppgis til beskatning i Norge, gjerne ved hjelp av fiktiv fakturering fra nærstående selskap i skatteparadis. Skatteparadiser benyttes også til å hvitvaske penger.

Tross internasjonale avtaler om utveksling av informasjon, og økt press for åpenhet, øker verdiene som holdes i skatteparadis.[30] Unndragelsesmetodene blir mer komplekse og tilslørte, og det er svært mange utenlandske rådgivere som tilbyr opprettelse av strukturer i skatteparadiser på internett. Langt flere har nå derfor mulighet til å anvende sekretessestrukturer i skatteparadis enn tidligere. OECD er bekymret for at skatteunndragelsene relatert til den grensekryssende økonomien øker.[31] Trusselen for skatteunndragelser via skatteparadis vurderes derfor å være stor.

Urettmessige skatteflyktninger

Skatteplikt avhenger av reelt bosted. Det avdekkes stadig oftere mistanke om skattesvik begått av norske statsborgere, som har meldt utflytting fra Norge, men som oppholder seg i Norge så store deler av året at de er skattepliktige hit for hele sin inntekt og formue.

Etter at det er meldt flytting, kanaliseres inntekter gjerne fra oppdragsgiveren til selskaper i skatteparadis gjennom bankkonti i land hvor det er vanskelig å få tilgang til finansielle opplysninger. I én sak alene, ble det avdekket inntekter på over 130 millioner kroner og formue på 200 millioner kroner, som var unndratt fra beskatning.

Denne typen saker har vært vanskelig å avdekke, men økt informasjonsutveksling mellom land forventes å føre til avdekking av flere slike saker.

Ulovlig skatteplanlegging

En svært stor del av verdenshandelen foregår mellom, og innen, konsern. Multinasjonale selskaper benytter

seg av svakheter i rettsregler, og det faktum at det ikke finnes et multilateralt regelverk for internasjonal beskatning.[32] For å minimere betalt skatt, kombineres dette ofte med en innviklet organisasjonsstruktur med liten grad av gjennomsiktighet, skatteparadis og royalty på eget varemerke,[33] noe Paradise-papers lekkasjen i oktober 2017 viste.[34]

Dette er i seg selv ikke ulovlig, men lekkede dokumenter og forskning har vist at også omfanget av ulovlig skatteplanlegging er stort, og at skallselskaper også blir brukt til kriminell virksomhet, som bedrageri, skatteunndragelse, og å unngå internasjonale sanksjoner. Medieavsløringene de siste årene har satt denne typen internasjonal skatteunndragelse ytterligere på agendaen, og bedrifter med denne typen struktur møtes med mer kritikk i dag enn tidligere.

Strukturen i norsk næringsliv, med mange store internasjonale selskaper, tilsier at internprising, og ulovlig skatteplanlegging, kan føre til store reduksjoner i det norske skattefundamentet. Skatteetaten har

gjennomsnittlig avdekket nærmere 10 milliarder kroner per år i kontroller av internprising.[35]

Flere internasjonale initiativ, som BEPS[36], forsøker å begrense flytting av skattefundamentet til lavkostland. Fortsatt stor utbredelse av internasjonal skatteplanlegging medfører imidlertid at risikoen for ulovlig skatteplanlegging vil vedvare.

Urettmessig bruk av særordninger

Det er betydelig potensiale for unndragelser på områder der skattyterne kan få store utbetalinger fra staten, som ordninger med fradrag for kostnader til forskning og utvikling (skattefunn/kildeskatt), refusjon av skatteverdien av leteutgifter i oljesektoren (leterefusjon) og skatteinsentivordningen.

Samlet fradrag via skattefunnsordningen var ca. 5,7 milliarder kroner i 2017. Over halvparten av 200 selskaper som ble kontrollert av Skatteetaten, ba om urettmessige refusjoner og 60 millioner ble krevd fra selskapene.

I Danmark svindlet organiserte kriminelle i 2015 danske skattemyndigheter for 12,4 milliarder DKR via kildeskatt på aksjer. Samme miljø og gjerningspersoner har også forsøkt å svindle Skatteetaten i Norge.

Det har kun blitt avdekket et fåtall saker med alvorlig svindel i Norge, men trusselen vil være der så lenge ordningene eksisterer.

En global og digital økonomi gir nye trusler

Nye forretningsmodeller og internasjonale plattformer utfordrer skatte- og avgiftssystemet. Det kan være vanskelig å fastslå hva som skaper verdier, hvem som skaper dem og i hvilket land verdiskapningen skjer.

En økende andel av handelen omfatter varer, inkludert digitale varer, som omsettes av aktører på internasjonale nettsteder, og betales via globale nettløsninger. Det gjør overvåking av grunnlaget for beregning av avgifter vanskeligere. Det antas også å redusere aktørenes forhold til at slike varer er avgiftspliktige.

En dreining fra et tradisjonelt nasjonalt bankmarked til et vesentlig mer åpent europeisk og globalt marked for finansielle tjenester, vil også føre til at en mindre andel blir innrapportert direkte til Skatteetaten. En økt del av fremtidens transaksjoner vil derfor falle utenfor Skatteetatens regler, ordninger og systemer for innrapportering og kontroll. Skatteetatens erfaringer viser at det er betydelig lavere etterlevelse på områder med manglende, eller mangelfull, tredjepartsrapportering.

Nye sårbarheter for skatte- og avgiftsinnkrevingen vil sannsynligvis bli utnyttet av de som ønsker å unndra midler fra beskatning og unngå å betale avgifter.

27. Beregnet ut fra «JUS065, antall registrerte anmeldelser» tatt ut 1.1.2018.
28. Folkelig benevning på sekretessestrukturer i stater med lav, eller ingen, beskatning.
29. Skatteetaten, «Utenlandsk skatteunndragelse under lupen», Forskningsnytt, nr. 1, 2014.
30. Zucman, Gabriel, «Taxing across borders: tracking personal wealth and corporate profit», Journal of Economic Perspectives, vol. 28, nr. 4.
31. OECD, «Shining Light on the Shadow Economy: Opportunities and Threats», 2017.
32. Skatteetaten, «Skattlegging over landegrenser», Forskningsnytt, nr. 1, 2014.
33. Skatteetaten, «IKEA og aggressiv skatteplanlegging», Forskningsnytt, nr. 1, 2014.
34. Lekkasje av 13,4 millioner dokumenter fra advokatfirmaet Appleby, som angivelig ble stjålet i et cyberangrep.
35. Kontrollprosenten er under 1 %.
36. BEPS – Base Erosion and Profit Shifting.


Skatteetaten
SKATTEMELDING
for lønnsmottakere, pensjonister mv.
for formues- og inntektsskatt

Økonomisk kriminalitet

Korrupsjon

Transparency International rangerer Norge som et av de land i verden med minst korrupsjon.[37] Undersøkelser indikerer likevel at rundt 10 prosent av bedriftene i Norge kjenner til korrupsjon[38], og i 2017 ble det anmeldt 83 korrupsjonssaker, noe som er en vesentlig økning fra de to foregående årene.[39] Flere av straffesakene om korrupsjon, som har vært ført i Norge, har vært alvorlige, og det har vært vel så mange alvorlige saker i Norge som i andre nordiske land.[40] Korrupsjon er konkurransevridende og spesielt skadelig for tilliten mellom næringslivsaktører og til forvaltningen. Mer utstrakt korrupsjon kan undergrave fundamentet for, og finansieringen av, vårt demokratiske velferdssystem.

Korrupsjon i lokalforvaltning

Det er en risiko for at ansatte tilbys, eller forsøker å skaffe seg, utilbørlige fordeler i forbindelse med eksempelvis anskaffelser og offentligrettslige tillatelser. Straffesaker de siste årene indikerer at det er en særlig korrupsjonsrisiko innen kommunal plan- og byggesaksbehandling.

Folks oppfatning av hva som kan betegnes som korrupsjon, er mer vidtrekkende enn det som følger av straffeloven. ØKOKRIM får jevnlig tips om tilfeller med sammenblanding av profesjonelle roller og private interesser i kommuner, uten at tipsene får et straffe-rettslig etterspill. Dette fordi det som har skjedd – til tross for at det kan fremstå som kritikkverdig – ikke er straffbart. I andre tilfeller etterforskes saken nærmere, men henlegges etter bevisets stilling.

I en undersøkelse i regi av Kommunenes Sentralforbund offentliggjort i februar 2018, svarer så mye som 85 prosent av enhetslederne i kommunesektoren at korrupsjon er «et lite eller svært lite problem».[41] 13 prosent av lederne har i samme undersøkelse svart at de i løpet av det siste året har opplevd press for å favorisere noen. Transparency International sin gjennomgang av korrupsjonsdommer i Norge i perioden 2003–2017 viser at offentlige tjenestemenn var involvert i nær halvparten av alle sakene, hvilket kan indikere at korrupsjonstrusselen i kommunesektoren er større enn sektoren selv oppfatter.[42]

EUROPOL peker på at organiserte kriminelle infiltrerer offentlig og privat sektor, gjennom bestikkelser og annen form for påvirkning for å legge til rette for andre kriminelle aktiviteter.[43] Dette kan også skje i Norge. Korrupsjon innen lokalforvaltningen kan dermed bidra til annen kriminalitet, også arbeidslivskriminalitet.

Korrupsjon ved virksomhet i utlandet

Norge har en internasjonalt rettet økonomi med omfattende eksport til, og forretningsaktivitet i, utlandet. Mange bedrifter driver innen næringer som erfaringsmessig er utsatt for korrupsjon, som olje- og gassektoren, shipping, våpenhandel og telekommunikasjon. Store deler av norsk eksport av sjømat går også til land som rangeres langt nede på Transparency Internasjonal sin korrupsjonsindeks. ØKOKRIM har håndtert store straffesaker med grov korrupsjon innen flere av disse næringene. Særlig gjelder dette ved etablering

i korrupsjonsutsatte land i de fremvoksende markedene i Asia, Sør-Amerika og Afrika.

Bestikkelser skjules gjerne på sofistikerte måter, ved bruk av mellommenn og selskaper i utlandet.[44] Mellommennene opptrer som betalingskanal for flere selskaper, og innbetalingene blir blandet sammen. Det fordekker at pengene fra norske selskaper blir betalt videre til utenlandske beslutningstakere.

Bevisstheten omkring slike korrupsjonsutfordringer har økt, blant annet som en konsekvens av stor oppmerksomhet rundt slike saker. PWCs Global Economic Crime Survey for 2016 indikerer at bruk av bestikkelser og korrupsjon har gått noe ned internasjonalt.[45]

Store norske bedrifters anti-korrupsjonsarbeid og interne anti-korrupsjonsprogrammer, sammen med medias søkelys, har hatt en viktig forebyggende effekt. Risikoen er imidlertid fremdeles stor når virksomheter uten tilstrekkelig anti-korrupsjonstiltak etablerer seg internasjonalt. Dette gjelder særlig mindre virksomheter.

Med fortsatt omfattende norsk næringslivsengasjement i korrupsjonsutsatte land, utgjør korrupsjon knyttet til norske selskapers virksomhet i utlandet fremdeles en stor trussel.

37. På Transparency International sin korrupsjonsindeks i 2017 ble Danmark rangert som nr. 2, Finland, Norge og Sveits som nr. 3, Sverige som nr. 6.

38. Næringslivets Sikkerhetsråds KRISINOs rapport for 2017 viser at 10 % av virksomhetene kjenner til korrupsjon i egen bransje, et tall som har vært stabilt siden 2008.

39. «JUS065», 1.1.2018. I 2016 ble det anmeldt 47 korrupsjonssaker.

40. Mellom mars 2011 og september 2015 ble 39 personer dømt for korrupsjon i Norge. I 29 av sakene ble det idømt inndragning, totalt 36 millioner NOK. I Yara-saken vedtok virksomheten en bot på 270 millioner NOK, samt at 25 millioner ble inndratt som utbytte. I Klaveness-saken vedtok selskapet en bot på 20 millioner NOK, og 12 millioner ble inndratt.

41. Oslo Economic, Kantar TNS og Prof. Tina Søreide, «Status og råd for etikkarbeid i kommunesektoren», OE-rapport nr. 61, 2017.

42. Transparency International Norge, «Korrupsjonsdommer i Norge 2003–2017», 2018.

43. Europol, «Serious and Organised Crime Threat Assessment» (SOCTA), 2017.

44. OECD fant i 2014 at 71 % av avdekkede bestikkelser i internasjonale forretningsforhold ble kanalisert via mellommenn. (OECD, «An analysis of the Crime of Bribery of Foreign Public Officials», 2014).

45. PWC, «Adjusting the Lens on Economic Crime. Preparations brings opportunity back into focus.», Global Economic Crime Survey, 2016. 24 % av de spurte bedriftene svarer nå at de har opplevd bestikkelser og korrupsjon, noe som er en reduksjon på 11 % siden sist undersøkelse.

Foto: Craig Whitehead, Unsplash

Økonomisk kriminalitet

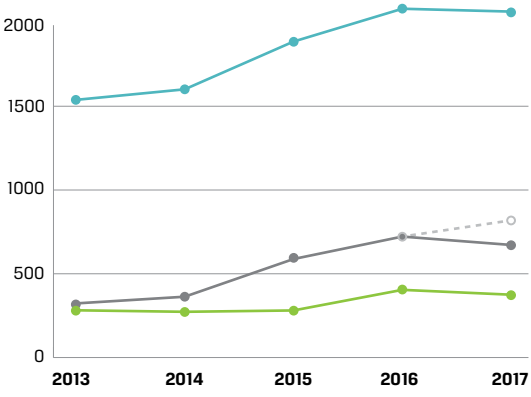
Bedrageri

Bedrageri anmeldes i langt større grad i våre naboland enn her i Norge. I Sverige ble det i 2017 anmeldt 209 000 bedragerier, i Danmark 44 176, mens det i Norge ble anmeldt 19 836 bedragerier. Også sett i forhold til innbyggertallet, ligger anmeldte bedragerier i Sverige langt over anmeldte bedragerier i Danmark og Norge, som figur 2 viser. De lave anmeldelsestallene i Norge knyttes til mørketallsproblematikk. Trusselen vurderes ikke å være mindre.

5 prosent av respondentene i politiets innbyggerundersøkelse svarer at de har blitt utsatt for svindel, eller bedrageri, på internett. Bare 19 prosent svarer at de har anmeldt forholdet. Dette er blant den typen kriminalitet befolkningen synes politiet håndterer dårligst.[46] Dette knyttes til politiets manglende straffeforfølgning av de kriminelle, og at pengene i de fleste tilfellene uansett er tapt. At politiet ikke involveres når næringsliv, offentlig virksomhet, organisasjoner og enkeltpersoner rammes av digitale lovbrudd, representerer en utfordring for rettsstaten.

Norske bedrifter og privatpersoner er attraktive mål for utenlandske bedragere, og trusselen for ulike former for bedrageri er stor. Fremgangsmåtene varierer, bedragerne tilpasser seg og finner nye metoder når gamle ikke lenger fungerer. Bedragerier på internett er typisk pop-up-kriminalitet som spres raskt, har kort varighet, og det er vanskelig å forutse både innholdet og spredningsmønsteret.[47]

Sosial manipulasjon benyttes for å vinne ofrenes tillit, og ofrene utsettes ofte for flere ulike gjerningsmåter.[48] Forebygging i form av informasjon om aktører og deres metoder, samarbeid med næringslivet, og stans av transaksjoner, er viktige strategier for å håndtere denne trusselen. Hvis pengene forlater landet, er vår erfaring at det er vanskelig å få dem tilbake. Summene den enkelte bedrift og privatperson blir svindlet for, kan være store. Bedragerienes alvorlighetsgrad må også ses i sammenheng med at det ofte er organiserte kriminelle grupperinger som står bak.



Figur 2: Anmeldte bedragerier 2010–2017 per 100 000 innbyggere

Norge — Danmark

Sverige — Estimat*

Tall for bedrageri. Sverige: Brottsförebyggande rådet, «Anmälda bedrägerier», tatt ut 18.5.2018. Danmark: Politi, «Nasjonal strategisk analyse», 2017 og oppdatert med 2017-tall fra dansk politi. Norge: «JUS065», tatt ut 1.1.2018. Det totale antallet anmeldelser er vesentlig høyere i Sverige enn i Norge. I 2017 var det totalt 1,51 millioner i Sverige, mot 319 202 i Norge. Statistikken er ikke nødvendigvis direkte sammenlignbar mellom de tre landene.
Tall for innbyggertall. Sverige: SCB, «Befolkningsutredning; födda, döda, in- och utvandring, gifta- og skilda 1749-2017». Danmark: Danmarks statistik, Statistikbanken; «Folketal den 1. kvartalet efter civilstand, alder, køn, område og tid». Norge: SSB, Statistikkbanken; Folkemengde og kvartalsvise endringer.
***** inkludert etterregistreringer.

Bedrageri rettet mot næringslivsaktører

Næringslivet er utsatt for flere typer bedragerier.De antatt største truslene når det gjelder bedragerier rettet mot næringslivet, er for tiden to svært ulike metoder: direktørbedragerier og fakturabedragerier.

Trusselen kan reduseres betraktelig gjennom etablering av gode rutiner i den enkelte virksomhet. De fleste bedrifter og foreninger som er utsatt for CEO-bedragerier, har eksempelvis informasjon om ansatte og deres roller i firmaet fritt tilgjengelig på hjemmesiden.

Direktørbedrageri[49] går ut på at personer som utgir seg for å ha en overordnet stilling, tar kontakt med en underordnet i virksomheten og manipulerer vedkommende til å foreta urettmessige transaksjoner. Gjerne under påskudd av at det dreier seg om en hastebetaling. Bedrifter med hovedkontor eller filialer i utlandet fremstår som særlig utsatt. Bedragerne velger gjerne et tidspunkt hvor sjefen er på reise, og tilnærmer seg ofte nyansatte.

I Norge oppgir 13 prosent av lederne i offentlig eller privat virksomhet at virksomheten deres har blitt utsatt for denne typen bedragerier.[50] Bare i 2016 viser tall rapportert til Bits[51] et tap relatert til direktørbedragerier på nesten 300 millioner kroner.[52] I USA mottok FBI melding om 15 690 tilfeller med et tap på over 675 millioner amerikanske dollar.[53]

Dette er en type bedrageri som kan påføre virksomheter store enkelttap. I april 2016 ble en norsk virksomhet svindlet for en halv milliard kroner. Også flere store europeiske bedrifter har blitt bedratt for svært store beløp: Den belgiske banken Crelan for 700 millioner kroner, og det østerrikske flydelfirmaet FACC Operations for nesten 470 millioner kroner.[54]

Denne typen bedrageri vurderes nå hovedsakelig utført av aktører med tilknytning til Nigeria. Det vil sannsynligvis føre til mindre sofistikerte og mer masseproduserte bedrageriforsøk, samt lavere svindelbeløp. Økt bevissthet hos mange i næringslivet, forventes å føre til at bedragerne retter seg mot såkalte «soft targets» – som festivaler og organisasjoner der de interne rutinene ikke er like godt etablert som i virksomheter ellers.

Fakturabedrageri[55] er en form for massebedrageri, hvor hver enkelt bedrift blir svindlet for mindre beløp, men hvor summene som genereres til bakmennene, blir store.

Fakturabedrageri gjennomføres ved å utstede fakturaer til næringsdrivende for varer eller tjenester de ikke har bestilt, ofte oppføring i kataloger eller på nettsteder som ikke eksisterer, eller som ikke har den verdien som forespeiles. Det har i den senere tid også blitt avdekket bedrageriforsøk knyttet til offentlige godkjennelsesordninger hvor bedragerne utgir seg for å være et offentlig organ, og den bedrageriutsatte blir bedt om å betale et gebyr. Fakturaene kommer gjerne i perioder hvor kontrollen til virksomhetene er mindre, særlig i ferier.

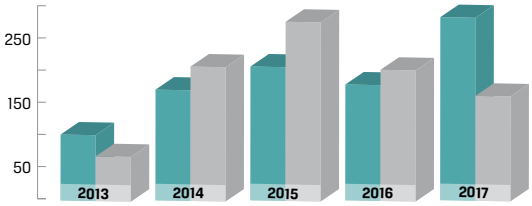
Fakturabedragerier har lenge vært en trussel mot norsk næringsliv. Virke estimerer at årlige bedrageriforsøk fremdeles er i størrelsesorden 2 milliarder NOK.[56]

Et ikke ubetydelig antall av bedriftene som mottar slike fakturaer betaler, enten fordi de ikke fanger opp bedrageriet, eller fordi de anser det som enklere å betale enn å ta bryderiet med å bestride kravet. Sammenlignet med andre land er det relativt enkelt å skaffe kontaktinformasjon til virksomheter i Norge fra offentlige registre. Det er grunn til å tro at omfanget av slike bedragerier rettet mot norske næringslivsaktører fortsatt vil være stort.

HVIS DET VIRKER FOR GODT

TIL Å VÆRE SANT

– ER DET OFTE DET!



Figur 3: Datingbedrageri meddelt ØKOKRIM

Bedratte nordmenn

Mill. NOK sendt ut

Bedrageri rettet mot privatpersoner

God økonomi gjør også norske privatpersoner til attraktive mål for bedragere. Den som utsettes for bedrageri, blir gjerne utsatt for flere typer bedragerier. For eksempel ser vi at personer som har blitt utsatt for datingbedrageri, også har blitt lurt til å investere i binære opsjoner, og til å stille sin bankkonto til disposisjon for pengeoverføringer.

Aksjeinvesteringsbedrageri vurderes å være en vedvarende trussel. Binære opsjoner, hvor investorer vedder på hvilken vei kursen på eksempelvis den underliggende aksjen, varen eller indeksen vil bevege seg, har vært en stor trussel. Investeringsoppleggene som tilbys, er ofte rene bedragerier.[57] Markedsføring, distribusjon og salg av binære opsjoner og CFD-er[58] til ikke-profesjonelle har nå blitt forbudt i EU og Norge. Trusselen for bedragerier via denne typen instrumenter vil da sannsynligvis bli redusert, men de kriminelle forventes å finne nye liknende fremgangsmåter.

Kredittkortbedrageri er en form for massebedrageri med lav risiko og høy profitt. Det er enkelt å få tak i kredittkortinformasjon på nettet. Dette utnyttes i stor skala av organiserte kriminelle i Europa, og over halvparten av de europeiske landene har hatt en økning i saker hvor nettbutikker bedras.[59]

I Danmark er 54 prosent av de anmeldte bedrageriene relatert til misbruk av stjålne kredittkortopplysninger.[60] Også i Norge øker svindelen med kort hvert år.[61] Tapet var i 2016 på 137 millioner kroner.[62]

Datingbedrageri, hvor norske menn og kvinner blir lurt av «kjærester» på nettet til å sende penger ut av Norge, har fremdeles et stort omfang. I 2017 mottok ØKOKRIM henvendelser fra 286 nordmenn som var utsatt for datingbedrageri, og som samlet skal ha overført ca. 150 millioner kroner til utlandet. Mørketallene antas å være store, da mange ikke selv innser, eller vil innrømme, at de er bedratt.

46. POD, «Politiets innbyggerundersøkelse 2017», 2018. Kun 32 % mener politiet håndterer svindel på internett meget, eller ganske, godt.
47. Oslo politidistrikt, «Trender i kriminalitet 2018-2021», 2018.
48. NorSIS, «Trusler og trender 2017-18», 2017.
49. Mange navn benyttes på denne bedragerimetoden, inkludert Chief Executive Officer (CEO)-bedrageri, Business Email Compromise (BEC) og whaling.
50. NSR, «KRISINO 2017», 2017.
51. Bits AS er bank- og finansnæringens infrastrukturselskap.
52. Finanstilsynet, «Risiko- og sårbarhetsanalyse (ROS), 2016», 2017.
53. FBI, «Internet Crime Report», 2017.
54. Aftenposten, «ØKOKRIM advarer mot CEO-svindel», 7. mars 2016.
55. Omtales også som katalogbedrageri.
56. Virke, «Bedragerier og håndteringen av anmeldelser og etterforsking», presentasjon 2017.
57. Mellom 74 og 89 % av kundene taper penger. (Forbruksrådet, «Høringssvar – Forskrift om produktintervensjon vedrørende binære opsjoner og CFD-er», 2018.)
58. Finansielle differenskontrakter.
59. EUROPOL, «Internet Organised Crime Threat Assessment», 2017. Bedragerienе foretas uten fysiske kredittkort.
60. [Dansk] Politi, «National Strategisk analyse», 2017. Beregnet basert på en stikkprøve.
61. Varekjøp på internett uten fysisk kort.
62. Finanstilsynet, «ROS 2016», 2017.

Miljøkriminalitet omfatter kriminalitet innenfor: arbeidsmiljø-, forurensings-, kunst- og kulturminne-, natur-, fiske- og akvakultur samt dyrevelferdskriminalitet. Ofte ses flytende overganger mellom ulike typer miljøkriminalitet, og flere typer overtredelser opptrer ofte sammen. Arbeidsmiljøkriminalitet dekker i år også arbeidslivskriminalitet.

Miljøkriminalitet

Anmeldelsene fra forvaltningsmyndighetene har blitt færre de siste årene. Noe av nedgangen skyldes at flere saker går forvaltningsporet, men ØKOKRIM frykter en utvikling hvor forvaltningen ikke anmelder miljøkriminalitet. Det ble i 2017 anmeldt 3009 lovbrudd innen miljøkriminalitet, med 2174 innen ytre miljø og 835 innen arbeidsmiljø.[63] Politiets statistikk gir imidlertid ikke et helthetlig inntrykk av miljøkriminaliteten i Norge – ØKOKRIMs anslag viser at opp mot 4760 lovbrudd kan falle inn under kategorien.

Mye av den kjente og grove miljøkriminaliteten skjer innenfor rammen av næringsvirksomhet, og er en konsekvens av tiltak for å oppnå økonomisk vinning, eller besparelse av utgifter. Ønske om profitt og stramme økonomiske rammer, kan eksempelvis føre til at naturressurser blir presset til det ytterste, til mangelfullt stell som går ut over dyrehold, og til at det tas uforsvarlig høy risiko når det kommer til fiskehelse og fiskevelferd innen akvakulturnæringen. Profittmotivasjon kan også føre til at verneverdige bygg forfaller, eller rives uten tillatelse.

I politidistriktene består trusselbildet innen miljøkriminalitet også av motorferdsel i utmark, ulovlig avfallshåndtering, ulovlig jakt og fiske, ulovlig importerte kjæledyr, ulovlig metallsøkeraktivitet, tyverier av verdifulle kulturgjenstander, og ulike typer dyremishandling.

Miljøkriminalitet har internasjonale dimensjoner. Illegal handel med både truede arter og kunst- og kulturminner, skjer i et internasjonalt marked. Omfanget av illegal handel med kunst og kulturminner har økt de siste årene. Internasjonale konflikter og mangel på kontroll i områder med mange kulturminner, har ført til økt omsetning, og involvering av organiserte kriminelle.

Kriminalitet mot miljøet rammer ofte fellesgodene mer enn enkeltpersoner, og kan ha globale konsekvenser. Kriminaliteten kommer på toppen av de lovlige inngrepene. Relativt begrensede overtredelser kan derfor få store konsekvenser. Manglende evne til å se konsekvensen og alvorligheten i små overtredelser, bidrar sannsynligvis til å øke trusselen for miljøkriminalitet.

63. POD, «Anmeldt kriminalitet og straffesaksbehandling 2017», Kommenterte STRASAK-tall, 23.1.2018.

Miljøkriminalitet

Forurensingskriminalitet

Ulovlig avfallshåndtering vurderes å være den største trusselen innenfor forurensningskriminalitet. Systemet med såkalt omvendt økonomi[64] gjør at aktørene kan øke profitten betydelig ved ikke å etterleve regelverket i den videre behandlingen av avfallet.

EUROPOL vurderer at kriminelle involvert i ulovlig avfallshåndtering nå opererer i hele kjeden, og benytter legale forretningsstrukturer til å kamuflere sine aktiviteter.[65] Det er en reell risiko at avfall som blir eksportert, ender opp i andre land enn det som er angitt som sluttdestinasjon.

Som en sjøfartsnasjon med lang kystlinje, er trusselen for forurensning fra sjøfarten sentral, inkludert skipsulykker, forurensning fra fartøy med farlig last, samt ulovlige utslipp og dumping av søppel. Både ved akutt forurensning og ved havari av skip, kan kostnadene ved å rydde opp bli store. Det medfører høy risiko for overtredelser, inkludert manglede varsling og iverksettelse av tiltak ved akutt forurensning.

Det er også store profittincentiver hos rederier til å hugge opp skip i fattige land, såkalt «beaching».[66] Skrapprisen er vesentlig høyere i India, Bangladesh og Pakistan, hvor skipene hugges opp på strendene. Det er ulovlig å sende skip ut av Norge til slikt formål. De fleste skipene formidles imidlertid via vrakmeglere – 40 prosent av skipene som ender opp på strendene i Asia, ble importert fra land som spesialiserer seg på omregistrering av skip som skal skrapes.[67] I 2017 ble 16 skip med norske eierinteresser sendt til opphugging på asiatiske strender, noe som er en økning etter flere år med nedgang.[68]

Det er en økning i salget fra utenlandske nettbutikker, som fremstår som norske nettsteder rettet mot norske forbrukere, og mange aktører som importerer varer fra land utenfor EØS-området, har ikke tilfredsstillende internkontroll. Det er også grunn til å tro at det legges frem falske dokumenter ved import av produkter.[69] Det omsettes derfor sannsynligvis produkter som inneholder helse- og miljøfarlige stoffer i strid med krav i produkt- og kjemikalieregelverket, og produkter som ikke overholder krav til faremerking.

64. Det vil si at den som tar imot avfall får fullt ut betalt når avfallet er mottatt.
65. Europol, «SOCTA», 2017.
66. Rederiforbundet definerer beaching som: «resirkulering av skip der det ikke anvendes faste arrangementer for oppsamling og håndtering av farlig og forurensende avfall.»
67. NGO Shipbreaking platform, «2017 Ship dismantling records», 20.2.2018.
68. Flere av skipene ble solgt videre rett før opphugging, andre selskaper hevder opphuggingen skjedde i henhold til Hong-Kong-avtalen.
69. Europol, «SOCTA», 2017.

Foto: Vestfold Interkommunale Brannvesen

Foto: Luke Besley, Unsplash

Miljøkriminalitet

Naturkriminalitet

Den største trusselen innen naturkriminalitet, er relatert til ulovlige, irreversible fysiske naturinngrep og arealendringer, og inkluderer ulovlige byggearbeid. De er hver for seg ofte mindre alvorlige, men kan i sum ha et vesentlig skadepotensiale.

Dette gjelder spesielt dersom arealendringer medfører ødeleggelse av områder som er vernet, eller leveområder for truede arter. I slike tilfeller innebærer inngrepet en trussel mot det biologiske mangfoldet. Slike naturinngrep, og bygge- og anleggsarbeid, kan også medføre skade på automatisk fredete kulturminner. Kontroller med utbygging er tidkrevende, det er lav oppdagelsesrisiko og det utbrer seg en manglende respekt for regelverket. Det bidrar til å øke risikoen for denne typen kriminalitet.

Ulovlig motorferdsel i utmark vurderes å være en vedvarende trussel. Tallet på ATVer har økt sterkt de senere årene, og det er i dag registrert 60 000 ATVer i Norge. Oppdagelsesrisikoen ved ulovlig motorferdsel i utmark, er gjennomgående lav.

Norsk fauna er utsatt for trusler fra mange kanter. Ulovlig jakt er et problem over hele landet. Dette gjelder både ulovlig jakt på rovdyr, og på arter som er truet av utryddelse. Ulovlig innførsel, og spredning, av fremmede organismer i norsk natur, utgjør en stor trussel mot naturmangfoldet. Fremmede arter forårsaker betydelige skader på stedegne arter og naturtyper. I global skala er spredningen av fremmede arter betraktet som en av de største truslene mot naturmangfoldet. De samfunnsøkonomiske kostnadene ved fremmede arter i Norge er i størrelsesorden 1,4–3,9 milliarder kroner per år.[70]

Handel med ville dyr og planter er regulert av det internasjonale CITES-regelverket. Overtredelser av CITES-regelverket representerer en vedvarende trussel mot det biologiske mangfoldet, både i Norge og internasjonalt.

70. Kristin Magnussen, Simen Pedersen og Henrik Lindhjem, «Samfunnsøkonomiske kostnader ved fremmede arter i Norge: Metodeutvikling og noen foreløpige tall», Vista analyse, Rapport nr. 52, 2014.

Miljøkriminalitet

Fiskeri- og akvakulturkriminalitet

Fiskeri- og akvakulturnæringene er internasjonale og møter stor konkurranse. Næringene produserte produkter til en førstehåndsverdi av over 82 milliarder kroner i 2017.[71] Det er mulig å oppnå stor profitt ved å tøye, og bryte, grensene for kvoter og konsesjoner. Det foreligger derfor betydelige økonomiske incentiver for lovbrudd i næringene.

I fiskerinæringen kan betydelig økt profitt oppnås ved å rapportere inn fangsten feil, eller dumpe fisk.[72] Tidligere saker har vist at opptil 45 prosent av fisken i Norge kan bli destruert og dumpet på sjøen.[73] Det er også en stor risiko for uregistrert og ulovlig landing av fisk, og at aktører som fisker ulovlig i Norge lander fisken i andre land. Det er stor aksept for juks – 40 prosent av respondentene i en studie fra Nofima svarer at de oppfatter juks som akseptert. 40 prosent svarer også at de selv jukser, og cirka 60 prosent at de har nær kjennskap til fiskere som underrapporterer.[74]

Verdien av det ulovlige fisket internasjonalt er estimert å være mellom 10 og 23,5 milliarder dollar årlig.[75] Nærmere 95 prosent av fisken fangstet av norske fartøy blir eksportert. Det er en risiko for at eksempelvis opphavsland, mengde og innhold i fiskeprodukter blir deklarert feil, for å unndra toll- og avgifter i mottakerlandet. Feildeklarering og smugling av fisk og fiskeprodukter fra Norge kan også kamuflere overfiske. Aktørene i næringen blir større og kontrollerer stadig flere ledd i verdikjeden både nasjonalt og internasjonalt; flere av aktørene er organisert som konsern med selskaper både i Norge og i utlandet. Kontroll med aktørene er krevende.

Innen oppdrettsnæringen er overproduksjon av fisk den største trusselen. Produksjon av laks og ørret er næringsregulert, og hver konsesjon er begrenset til 780 tonn. Selskapene har rapporteringsplikt til fiskerimyndighetene, og sender hver måned inn sine tall på stående biomasse i hver produksjonsenhet. Produksjon utover lovlig grense blir sjelden rapportert. Manglende rapporteringsplikt i flere ledd i verdikjeden, gjør det mulig å eksportere overproduksjon gjennom lovlige kanaler. Det er derfor sannsynlig at betydelige menger fisk blir fisket og oppdrettet ulovlig i Norge, og omsatt svart.

Produksjon av settefisk er en flaskehals for veksten i oppdrettsnæringen. Med en stadig vekst i næringen, har etterspørselen etter settefisk økt. Fortjenesten ved å bruke mer vann enn det som er tillatt, kan bli stor dersom det fører til at det kan produseres mer smolt.[76] Det er derfor stor sannsynlighet for at settefiskanlegg bruker ulovlig mye vann.

Unnlatt rapportering, og unnlatelse av å iverksette tiltak mot lakselus ved alvorlige sykdomsutbrudd, vurderes også som en alvorlig trussel i fremtiden. Dette får alvorlige dyrevelferdsmessige konsekvenser.

71. Tall fra www.ssb.no/fiskeoppdrett.no/fiskeoppdrett og www.ssb.no/fiskeri. Tall hentet ut 6.6.2018. Førstehåndsverdien er prisen oppdretteren får ved salg av uforedlet eller frossen fisk og summen fiskeren får utbetalt for fangsten.

72. I følge Fiskeridirektoratet kan aktører ved et hal på 500 tonn makrell oppnå en ekstra profitt på anslagsvis 6 millioner NOK ved ulovlig dumping/slipping.

73. Hålogaland langmannsretts dom av 24. april 3013, LH-2012-194001

74. Marianne Svorken og Øystein Hermansen, Urapportert fiske i torskefiskeriene, NOFIMA Rapport nr. 26, 2014.

75. European Parliament, «Illegal, Unreported and Unregulated Fishing: Sanctions in the EU», 2014.

76. I en konkret sak NVE hadde befatning med, hadde anlegget en overkapasitet på 500 000 smolt. Dette tilsvarer en anslått verdi av cirka 150 millioner NOK i omsetning og 8 millioner NOK i fortjeneste.

Foto: Jonas Jacobsson, Unsplash


FIBER
100
KRONE

Hensikten med mange kriminelle handlinger, er å oppnå økonomisk gevinst. For at gjerningspersonen eller andre senere kan ta i bruk de ulovlige midlene som legale midler, utføres aktiviteter med formål å tilsløre utbyttets opprinnelse – hvitvasking. **Hvitvasking** kjennetegnes ved at utbytte fra en straffbar handling introduseres i lovlig økonomi, og dermed fremstår som legitimt.[77]

Hvitvasking

Tilgjengeligheten av tilbydere av finansielle tjenester på internett har økt. Nyere betalingstjenester og digitale valutaer har gjort det enklere å overføre penger kontantfritt, og benyttes stadig oftere til hvitvasking. Dette er en internasjonal trend.[78] Bruk av utenlandske betalingstjenester kan gi større utfordringer med å innhente informasjon om transaksjonene, og å identifisere både pengenes opprinnelse og reelle eier. I 2017 ble det anmeldt 116 hvitvaskingssaker.[79]

Internasjonalt benytter kriminelle fremdeles kontanter i stor skala.[80] Selv om norsk økonomi i større grad er digitalisert, benytter kriminelle i Norge også kontanter, og det føres sannsynligvis store mengder kontanter ulovlig ut av landet: I 2016 ble det deklarert inn 8,5 milliarder kroner mer enn det ble deklarert ut.[81] Utførsel av kontanter kan knyttes til miljøer som allerede har et system for logistikk og smugling. Utbytte i kontanter bringes også ut av landet via aktører som formelt driver annen virksomhet, men som i realiteten driver betalingsformidling. Slike aktører opererer utenfor Finanstilsynets kontroll.

Utbytte fra kriminelle handlinger i Norge kanaliseres også til utlandet ved eksempelvis fiktiv fakturering og kjøp av eiendom i utlandet. Samtidig fører økt virksomhet på tvers av landegrensene til at stadig flere har inntekt eller formue i utlandet. Trusselen for at utbytte av kriminelle handlinger hvitvaskes i utlandet, er derfor fremdeles stor.

Forbruk i Norge av midler som er hvitvasket i utlandet, foregår ofte med utenlandske bankkort. Forhåndsbetalte utenlandske betalingskort benyttes også oftere, noe som ytterligere vanskeliggjør sporing av midlenes ulovlige opphav. Midler tas også tilbake ved hjelp av fiktive lån fra utlandet, og ved at lån i Norge nedbetales med skjult inntekt/formue i utlandet.[82]

Det er en trend at eiendomsmarkedet benyttes for å hvitvaske utbytte. En fremgangsmåte er at utbedringer og oppussingskostnader, som øker eiendommens verdi, betales kontant, med utbytte fra kriminell aktivitet. Andre fremgangsmåter er manipulasjon av eiendomsverdier, svart arbeid, oppgjør med illegale midler, bruk av stråmenn og kompliserte eierforhold. Vi har sett tilfeller av at profesjonelle aktører, som meglere og advokater, medvirker med fiktive verdivurderinger, og tilrettelegger for såkalt svingdørsalg[83].

Mangelen på transparens er en sårbarhet for antihvitvaskingsregimet. Kundekontroll i forhold til norske bankkonti som innehas av utenlandske selskaper er utfordrende, da det kun er oppgitt disponent på en liten andel av norske bankkonti som innehas av utenlandske selskaper. Reelle innehavere bak selskaper i skatteparadiser kan være norske skatteytere og næringsdrivende som skjuler inntekt og formue i utlandet.[84] Trusselen for at norske finansinstitusjoner skal bli brukt som transittsted for å legitimere pengestrømmer, og at utbytte fra kriminalitet begått i utlandet skal bli plassert i Norge, er derfor betydelig.

77. Justis- og beredskapsdepartementet, «Nasjonal Strategi for bekjempelse av hvitvasking, finansiering av terror og finansiering av spredning av masseødeleggelsesvåpen», 2016.
78. Egmont Group, «Emerging Financial Technologies, Money Laundering and Terrorist Financing: A Typology of Virtual Vurrencies», 2018.
79. Beregnet ut fra «JUS065», 1.1.2018.
80. EUROPOL, «Why is Cash still king?», 2015.
81. Beregninger basert på Valutaregisteret.
82. JD, «NRA», 2016.
83. Hyppig salg av samme eiendom med unormal prissetting.
84. ØKOKRIM, «Trusselvurdering 2015–2016», 2015.

Terrorfinansiering[85] skiller seg på flere måter fra hvitvasking og annen kriminalitet. Målet er sjeldent eller aldri profitt. Finansiering av, og støtte til, terrororganisasjoner eller terrorhandlinger, vil ofte være motivert av politiske, ideologiske eller religiøse mål. Til forskjell fra hvitvasking, fokuserer ikke terrorfinansiering på pengenes opprinnelse, men på hva pengene skal brukes til. Finansiell eller materiell støtte til terror er etter norsk rett et selvstendig lovbrudd, og defineres som en terrorrelatert handling.[86]

Terrorfinansiering

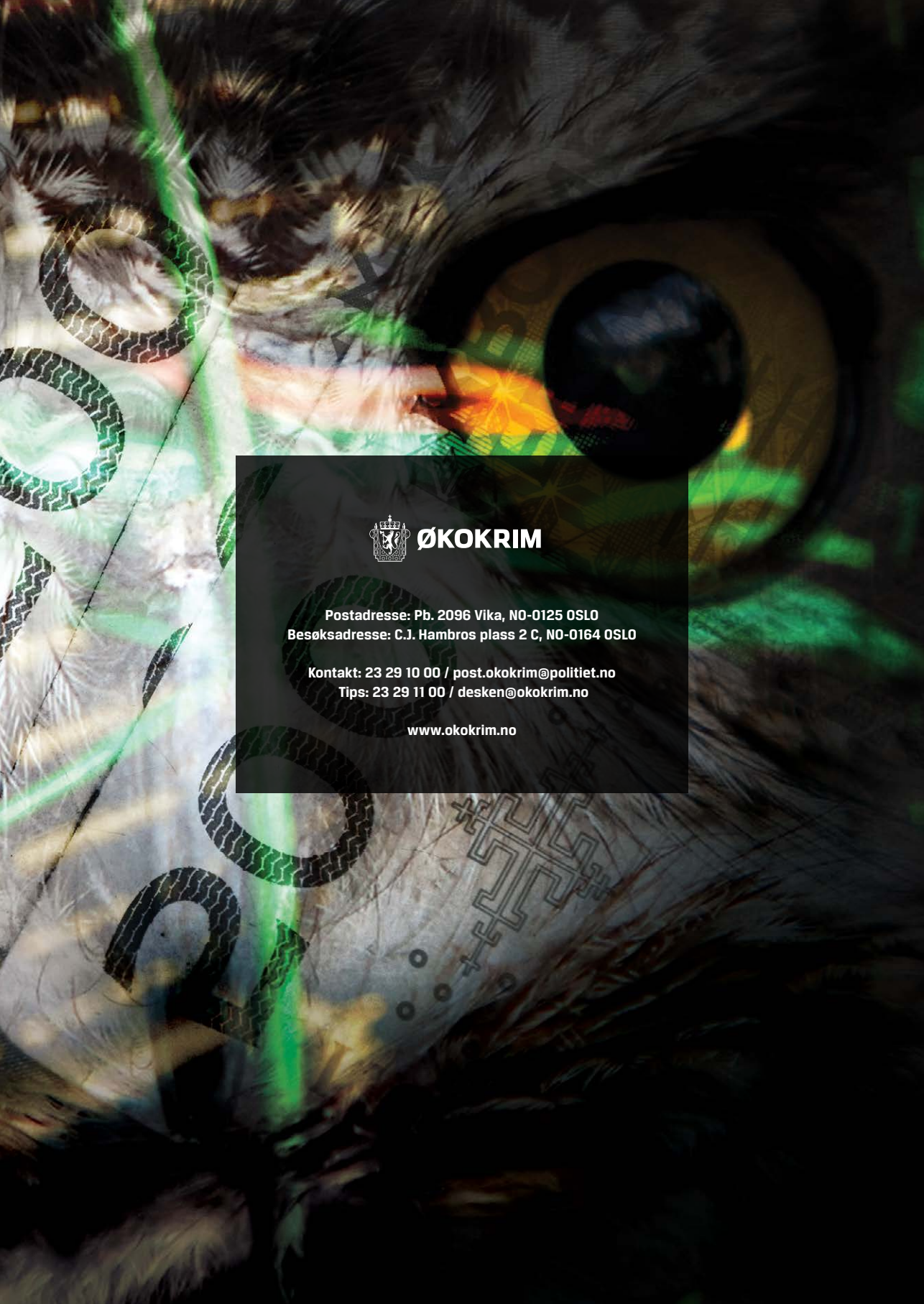
Terrorhandlinger blir ofte finansiert gjennom en kombinasjon av legale inntekter og kriminell virksomhet. Eksempelvis innsamling av penger fordekt som veldedighet, kredittkortbedrageri, og annen kriminalitet. Fremmedkrigere har i stor grad vært selvfinansierte. De bruker egne midler til å betale reise, klær og utstyr i forkant av utreisen. I tillegg forekommer også misbruk av kredittkort og stipender. Vi ser også at lånebedrageri i større grad benyttes for å finansiere fremmedkrigere. Det er en utfordring at det ofte er snakk om små beløp.

Faren for terrorfinansiering må vurderes i forhold til terrortrusselen. Internasjonalt har ISIL mistet sin sentrale posisjon i Syria og Irak. De ekstreme islamistiske miljøene i Norge fremstår også som noe svekket sammenlignet med for noen år siden. ISIL forventes likevel å kunne inspirere tilhengere i Europa til å gjennomføre relativt enkle terrorangrep, og slike inspirerte angrep fremstår som den mest sannsynlige type terrorangrep også i Norge.[87] Angrepene vil primært gjennomføres med enkle midler av personer som allerede er bosatt i Europa.[88] Dette er angrep som krever få ressurser, og det vil være utfordrende å fange opp finansieringen av slike angrep.

Penger overføres ved hjelp av betalingsformidlere, hovedsakelig til konflikt- og krigsområder, og områder i randsonen av slike områder. Frivillige organisasjoner overfører også hvert år betydelige pengesummer til utlandet. Myndighetene har verken kontroll med opprinnelse, eller endelig mottaker. Det er en risiko knyttet til at mindre, frivillige organisasjoner misbrukes til terrorfinansiering. Det er kjent at flere foretak som driver betalingsformidling ikke registrerer seg som det, men velger å registrere seg som frivillige organisasjoner, for å unngå å bli rapporteringspliktig i henhold til hvitvaskingsregimet.[89]

Det er nå ytterst få ekstreme islamister som ønsker eller forsøker å reise til Syria og Irak, og mange fremmedkrigere ventes å bli drept i kamp.[90] Trusselen for finansiering av fremmedkrigere er derfor redusert.

85. Enheten for finansiell etterretning ved ØKOKRIM er mottaker av rapportering om mistenkelige transaksjoner relatert til terrorfinansiering. Rapporteringen er stabil og i tilfeller med kjente objekter holder rapporteringen nå bedre kvalitet enn tidligere.
86. JD, «Nasjonal Strategi», 2016.
87. Politiets sikkerhetstjeneste, «Trusselvurdering 2018», 2018.
88. Etterretningstjenesten, «Fokus 2018», 2018.
89. JD, «NRA», 2016.
90. Etterretningstjenesten, «Fokus 2018», 2018.



ØKOKRIM

Postadresse: Pb. 2096 Vika, NO-0125 OSLO
Besøksadresse: C.J. Hambros plass 2 C, NO-0164 OSLO

Kontakt: 23 29 10 00 / post.okokrim@politiet.no
Tips: 23 29 11 00 / desken@okokrim.no

www.okokrim.no