POLITIET
POLITIDIREKTORATET

PST
POLITIETS SIKKERHETSTJENESTE

Nasjonal risikovurdering

Hvitvasking og terrorfinansiering 2020

Innhold

1. Innledning

Nasjonal risikovurdering hvitvasking og terrorfinansiering (National Risk Assessment - NRA) er en nasjonal, tverretatlig risikovurdering som beskriver de største truslene, sårbarhetene og risikoene innen hvitvasking og terrorfinansiering.

For å implementere anbefaling 1 fra Financial Action Task Force (FATF) og artikkel 7 i EUs fjerde hvitvaskingsdirektiv skal Norge utarbeide risikovurderinger av hvitvasking og terrorfinansiering. En oppdatert samlet nasjonal risikovurdering av hvitvasking og terrorfinansiering er et godt utgangspunkt for forståelse og erkjennelse av risikoene vi møter i Norge, og for å møte disse risikoene på en effektiv og virkningsfull måte. Dette arbeidet er også viktig for å sørge for at Norge etterlever sine internasjonale forpliktelser på området. Nasjonalt er dette arbeidet forankret ved regjeringsbeslutning, og det er bestemt at risikovurderingen skal oppdateres hvert andre år.

Norge har de beste forutsetningene til å forebygge, avdekke og sanksjonere forbrytelser forbundet med hvitvasking og terrorfinansiering. Gjennom sterk tilslutning til internasjonalt regelverk, en stabil og gjennomsiktig økonomi, uavhengige institusjoner, lav korrupsjon og en høy grad av finansiell inkludering er alle elementer for et effektivt system til stede. Likevel viser så vel evalueringer, trusselvurderinger og andre kilder at det er reelle og alvorlige trusler i Norge, og at det er rom for ytterligere forbedringer av Norges systemer.

NRA 2020 skal også være grunnlaget for risikodempende tiltak på alle nivåer både i privat og offentlig sektor. Den bør brukes i den risikobaserte tilnærmingen til bekjempelse og forebygging av hvitvasking, for eksempel ved utvikling av regelverk og veiledning, prioritering av ressursbruk, utvelgelse av tilsynssubjekter eller åpning av straffesaker, samt til videre analyser. NRA kan benyttes som basis for å videreutvikle mer detaljerte risikoanalyser for egen sektor.

Risikovurderingen må ses i sammenheng med regjeringens *Strategi for bekjempelse av hvitvasking, finansiering av terror og finansiering av spredning av masseødeleggelsesvåpen.* Formålet med strategidokumentet er å sikre koordineringen av den samlede nasjonale innsatsen mot hvitvasking, finansiering av terror og finansiering av spredning av masseødeleggelsesvåpen ved å gjennomføre nye tiltak. Målet er at tiltakene i strategien skal gi de berørte etatene de nødvendige føringene og metodene for dette arbeidet.

NRA 2020 er utarbeidet på oppdrag fra Justis- og beredskapsdepartementet. Politidirektoratet (POD) og Politiets sikkerhetstjeneste (PST) har i fellesskap ansvaret for å utgi NRA2020. ØKOKRIM har utarbeidet risikovurderingen for hvitvasking, mens Politiets Sikkerhetstjeneste (PST) har utarbeidet risikovurderingen for terrorfinansiering. Ved utarbeidelsen er det innhentet informasjon og vurderinger fra en rekke aktører i politi- og påtalemyndigheten, kontrolletater, tilsyn og privat sektor.

Denne nasjonale risikovurderingen for bekjempelse av hvitvasking og terrorfinansiering (NRA 2020) er Norges fjerde samlede risikovurdering av trusler, sårbarheter og risikoer for hvitvasking og terrorfinansiering.

2. Hovedfunn

2.1. De største risikoene innen hvitvasking

- COVID-19 har ført til noen nye kriminalitetsutfordringer, som utnyttelse av støtteordninger og den statlige lånegarantiordningen, samt økt smugling av høyt skattede varer.
- Kriminalitet som utføres eller tilrettelegges for digitalt er en økende trussel og medfører et større omfang av grensekryssende kriminalitet. På grunn av pandemien er flere mennesker i en sårbar situasjon, og det er økt bruk av hjemmekontor. Dette øker risikoen for at bedragerier utført og tilrettelagt digitalt vil lykkes.
- Bruk av kryptovaluta for å hvitvaske utbytte fra kriminalitet vurderes å ha høy risiko, særlig knyttet til uregistrerte vekslere. Men også de registrerte vekslerne har betydelig risiko for å bli benyttet til hvitvasking.
- Det knyttes særlig høy risiko til aktører innen arbeidslivskriminalitet, som i tillegg til å hvitvaske egen profittgenererende kriminalitet tilrettelegger for hvitvasking av utbytte fra narkotikakriminalitet i sin næringsvirksomhet.
- Grensekryssende varehandel som fremgangsmåte for hvitvasking er lite omtalt i tidligere NRA-er. Risikoen vurderes å være moderat, men omfanget er ikke kjent.
- Banker og agenter for utenlandske betalingsforetak har den største risikoen for å bli utnyttet til hvitvasking.
- Eiendomsmeglingsbransjen er vurdert til å ha høyere risiko for å bli benyttet til hvitvasking nå enn i 2018. Det samme er revisorer og regnskapsførere.

Matrise risikovurdering rapporteringspliktige sektorer

	Risiko
Banker	Høy
Agenter for utenlandske betalingsforetak	Høy
Betalingsforetak	Betydelig
Kreditt- og finansieringsforetak	Betydelig
Eiendomsmeglere	Betydelig
E-pengeforetak	Betydelig
Veksling og oppbevaring av virtuelle valuta	Betydelig
Regnskapsførere	Moderat
Revisorer	Moderat
Verdipapirforetak	Moderat
Forsikringsforetak og forsikringsformidlere	Moderat
Advokater	Moderat
Innenlandske spillselskap	Lav

Matrise risikovurdering modus hvitvasking

	Risiko
Kryptovaluta	Høy
Nye betalingstjenester	Høy
Næringsvirksomhet	Høy
Utenlandske spillselskaper	Betydelig
Norge som transittland	Betydelig
Eiendomsmarkedet	Betydelig
Plassering i utlandet	Moderat
Grensekryssende varehandel	Moderat
Utførsel av kontanter	Moderat
Verdigjenstander	Moderat
Muldyr	Moderat
Profesjonelle tilretteleggere	Moderat

2.2. De største risikoene innen terrorfinansiering

- Trusselnivået i Norge er MODERAT. Dette gjelder både trusselen fra ekstrem islamisme og høyre-ekstremisme.
- Gjentatte handlinger som oppfattes som krenkelser av islam medfører økt potensial for radikalisering og forsøk på terror. Handlingene kan lede til radikalisering også utenfor Norge og kan derfor utløse terror mot Norge fra aktører i utlandet.
- Militant islamisme og høyreekstremisme kopierer hverandre, og det er sannsynlig at de i framtiden også vil gi næring til hverandre.
- ISILs tap av territorium har ført til en endret strategi, hvor fokuset nå er å bygge opp organisasjonen i flere deler av verden.
- Hjemvendte fremmedkrigere til Vesten, hvor enkelte soner fengselsstraff, vil i løpet av få år være løslatt og utgjøre en ytterligere trussel.

Flere av sårbarhetene og risikoene for hvitvasking som blir presentert i NRA 2020 gjelder også for terrorfinansiering. Dette gjelder i stor grad fordekte transaksjoner, der enten avsender og/eller mottaker er fordekt eller anonymisert og sporbarheten i transaksjonen minimal. Dette gjelder spesielt transaksjoner som foretas via følgende:

- Uregistrerte betalingsforetak og betalingsforetak som ikke etterlever hvitvaskingslovens krav eller rapporterer til Valutaregisteret.
- Virtuell valuta, hvor aktørene etterlater seg elektroniske spor som det kreves oppdatert kunnskap og analyseverktøy for å avdekke.
- Frivillig sektor, hvor enkelte aktører i liten grad registrerer seg og dermed unngår kontroll og rapportering. Små frivillige organisasjoner som i hovedsak driver med innsamling av penger til konfliktområder.
- Pengeinnsamling via sosiale medier til krypterte aktører og virtuell valuta.

3. Risikovurdering hvitvasking

3.1. Metodikk

Internasjonale regelverk som Norge er tilsluttet stiller visse krav til prosessen og analysen for å vurdere risiko for hvitvasking og terrorfinansiering. NRA 2020 er utarbeidet i tråd med Norges internasjonale forpliktelser på dette området og i henhold til de kravene og anbefalingene som stilles gjennom EUs fjerde og femte hvitvaskingsdirektiv, samt gjennom FATF-rekommandasjon nr. 1. Kravene og anbefalingene er operasjonalisert i FATF Guidance, National Money Laundering and Terrorist Financing Risk Assessment (februar 2013).

ØKOKRIM har også utarbeidet risikovurderingen av hvitvasking i henhold til rammer og prinsipper beskrevet i Politiets etterretningsdoktrine.

Det prioriterte etterretningsbehovet ble angitt til: *«Hva er risikoen relatert til hvitvasking i Norge og til at midler som er utbytte fra kriminalitet i Norge hvitvaskes i utlandet?»*

Trusselvurderingen av utbyttegenererende kriminalitet er utarbeidet på bakgrunn av politiets samlede etterretningsproduksjon på området.

Vurderingen av fremtidig utvikling av truslene vil alltid inneholde en grad av usikkerhet. For å håndtere dette på en standardisert og strukturert måte er det benyttet sannsynlighetsord (se tabell). Sannsynlighetsord angis i kursiv i teksten.

Nasjonal standard	Beskrivelse	NATO standard
Meget sannsynlig	Det er meget god grunn til å forvente …	Highly likely (〉90 %)
Sannsynlig	Det er grunn til å forvente …	Likely (60–90 %)
Mulig	Det er like sannsynlig som usannsynlig …	Even chance (40–60 %)
Lite sannsynlig	Det er liten grunn til å forvente …	Unlikely (10–40 %)
Svært lite sannsynlig	Det er svært liten grunn til å forvente …	Highly unlikely 〈10 %

Nasjonal standard for sannsynlighetsord (2018).

3.2. Definisjoner

Hvitvasking defineres i straffeloven § 337. For hvitvasking straffes den som

a. yter bistand til å sikre utbyttet av en straffbar handling for en annen ved for eksempel å innkreve, oppbevare, skjule, transportere, sende, overføre, konvertere, avhende, pantsette eller investere det, eller
b. gjennom konvertering eller overføring av formuesgoder eller på annen måte skjuler eller tilslører hvor utbyttet av en straffbar handling han selv har begått, befinner seg, stammer fra, hvem som har rådigheten over det, dets bevegelser, eller rettigheter som er knyttet til det.

Likestilt med utbyttet er gjenstand, fordring eller tjeneste som trer i stedet for det.

Trusler defineres som en person, et objekt, grupper av personer eller aktiviteter som potensielt kan skade staten, samfunnet og økonomien. I snever forstand kan man si at trusler utnytter sårbarheter ved hjelp av bestemte moduser. Dette inkluderer kriminelle og deres fasilitatorer som utfører hvitvaskingsaktiviteter. Den utvidede definisjonen av trusler ser på omfanget av utbyttet som genereres fra kriminelle handlinger i ett land (intern trussel) og innførsel fra utlandet (ekstern trussel), samt moduser og trender som kjennetegner trusselaktørene.

Sårbarheter er innretninger og mangler ved eksempelvis vårt kontrollsystem og vår kriminalitetsbekjempelse, som kan bli utnyttet av trusselaktører, og derigjennom bidra til kriminalitet. I risikovurderingen av sektorer forstås sårbarheter som karakteristika ved sektorer, finansielle produkter eller bestemte typer tjenester som er attraktive i en hvitvaskingssammenheng. Svakheter og hull i det overordnede anti-hvitvaskings-systemet på nasjonalt nivå kan også utgjøre en sårbarhet for sektorer. Dette kan omfatte alt fra innebygde sårbarheter i infrastrukturen i bekjempelsen av hvitvasking, til mangelfull MT-rapportering og dårlig ID-kontroll hos de rapporteringspliktige. Videre kan det være svakheter ved lovverket og fraværende reguleringer som forhindrer forebygging av hvitvasking.

Konsekvenser refererer til skaden hvitvasking og terrorfinansiering kan påføre, og inkluderer effekten av primærkriminaliteten og terrorvirksomhet på finanssystemer og -institusjoner, økonomien og samfunnet. Størrelsen på verdiene som hvitvaskes er en vesentlig del av skaden.

Risikoen for at en sektor er særlig utsatt for hvitvasking er avhengig av trusselen mot sektoren, sektorens sårbarhet for trusselen og konsekvensene av hvitvaskingen i sektoren.

3.3. Tverretatlighet

Tverretatlighet i oppdraget med å utarbeide en nasjonal risikovurdering er sikret gjennom å innhente informasjon fra alle aktører i regimet. De som svarte var tre politidistrikter, Kripos, Finanstilsynet, Tilsynsrådet for advokatvirksomhet, Lotteritilsynet, Finans Norge, Skatteetaten, Tolletaten, Enheten for Finansiell Etterretning (EFE), Advokatforeningen, Norsk tipping, Revisorforeningen, Økonomiforbundet, Regnskap Norge, Finansieringsselskapenes forening, Forex Bank, Western Union, DNB og Nordea. Vi retter en stor takk til disse for deres bidrag.

3.4. Datagrunnlag

Til utarbeidelsen av trusselvurderingen har ØKOKRIM brukt politiets informasjon. Til resten av risikovurderingen består datagrunnlaget av utarbeidede rapporter og analyser fra både politiet, tilsyns- og kontrollorganer samt private aktører, samt internasjonale trussel og risikovurdering som EUs supranasjonale risikovurdering. I tillegg gir informasjonen som ble hentet inn aktørenes vurderinger av trusler, sårbarheter de ser fra sitt ståsted og eksempler de måtte ha på hvitvasking.

3.5. Risikomodell for å vurdere hvitvasking

Risikovurderingen av hvitvasking gjøres ved hjelp av en modell utviklet av ØKOKRIM[1]. Modellen tar utgangspunkt i veilederen til FATF og følger deres retningslinjer.[2]

Modellen benytter indikatorer for trussel, sårbarhet og konsekvenser for å vurdere den totale risikoen i sektoren. Modellen kan benyttes til å vurdere både hvitvaskingsrisikoen knyttet til modus og sektorer.

Indikatorer for trussel:
- Omfang/antall trusselaktører
- Aktørens kapasitet når det gjelder å benytte sektoren
- Utbytte relatert til trusselaktørene
- Utsatthet for internasjonale pengestrømmer

Indikatorer for sårbarhet ved vurdering av hvitvaskingsrisiko i sektorer:
- Iboende egenskaper ved sektoren og eksponering for risiko
- Juridisk rammeverk/reguleringer
- Forståelse av ansvaret for hvitvaskingsarbeid og fokus på compliance og rapportering i sektoren, inkludert systemer
- Kontroll med sektoren

Indikatorer for sårbarheter ved vurdering av hvitvaskingsmodus:
- Tilgjengelighet
- Anonymitet
- Kontroll/oppdagelsesrisiko
- Sannsynlighet for straffeforfølgelse

Indikatorer for vurdering av konsekvenser:
- Direkte konsekvenser
- Langsiktige konsekvenser

Risikomatrise			
4	8	12	16
3	6	9	12
2	3	6	8
1	2	3	4

Farge	Risikonivå
	Høy
	Betydelig
	Moderat
	Lav

Indikatorene vurderes fra 1 til 4 (lav, moderat, betydelig og høy). Nivået på trussel, sårbarhet og konsekvenser fastsettes ved å beregne et gjennomsnitt av indikatorene innenfor hver kategori.

For å beregne risiko beregnes først «justert trusselnivå», hvor den opprinnelige trusselen justeres for sårbarhetsnivået, som er en indikator på hvor bra anti-hvitvaskingssystemet er til å forhindre at utbyttet blir hvitvasket. Justeringen gjøres ved å justere ned trusselnivået etter følgende nøkkel, basert på score relatert til sårbarhetsnivå: høy (0 %), betydelig (25 %), moderat (50 %) og lav (75 %).

Risikonivået finnes ved å multiplisere det justerte trusselnivået med konsekvensnivået.

[1] ØKOKRIM, «Modell risikovurdering hvitvasking i sektorer», 2020.
[2] Financial Action Task Force (FATF), «National Money Laundering and Terrorist Financing Risk Assessment», 2013.

3.6. Trusselbildet for hvitvasking

3.6.1. Norsk økonomi

Norge er et av de rikeste landene i verden og hadde i 2019 et prisnivåjustert bruttonasjonalprodukt per innbygger 57 prosent over gjennomsnittet i de 27 EU-landene.[3] Et karakteristisk trekk ved det norske samfunnet er også den relativt jevne fordelingen av inntekt og den store middelklassen. Det gjør Norge til et utsatt land for bedragerier rettet mot privatpersoner og et attraktivt land for arbeidsinnvandring.

Norge har ikke strukturell og gjennomgripende korrupsjon, men fra 2018 til 2019 falt Norge fra tredje- til sjuendeplass på Transparency Internationals korrupsjonsindeks. Det kan tolkes som at den norske befolkningen oppfatter at forekomsten av korrupsjon i offentlig sektor er mer utbredt nå enn tidligere.[4]

En klar trend på 2000-tallet har vært arbeidsinnvandring fra land i Europa med svakere økonomisk utvikling enn i Norge og en påfølgende utnyttelse av mange av disse arbeiderne i det norske arbeidsmarkedet.

Norsk økonomi er preget av store internasjonale bedrifter og tette bånd til utlandet – mange av de største norske bedriftene har også etablert seg i utviklingsland. Dette øker trusselen for alvorlig økonomisk kriminalitet som korrupsjon og skatte- og avgiftsunndragelser. Prispress og konkurranse fra lavkostland bidrar også til at bedrifter tar snarveier og begår alvorlig miljøkriminalitet, som ved ulovlig avfallshåndtering.

Oslo Børs har stor handel innenfor nisjemarkeder og er i dag verdens nest største innenfor shipping, og verdens største når det gjelder sjømat.[5] Norske banker nyter også stor tillit internasjonalt. Dette er strukturer som kan utnyttes til alvorlig kriminalitet, som overføring av bestikkelsespenger, finansiering av terror, hvitvasking av utbytte fra alvorlig kriminalitet, samt tradisjonell verdipapirkriminalitet.

Norsk økonomi er i større grad digitalisert enn mange andre økonomier internasjonalt.[6] Kriminelle benytter likevel kontanter. Kontantbruk kan særlig knyttes til drift av virksomhet med stor kontantomsetning, som kamuflerer hallikvirksomhet, svart arbeid, omsetning av ulovlige varer (som narkotika) og bedrageri.

3.6.1.1. Utviklingen under koronapandemien og forventinger til utviklingen fremover

Tiltakene for å begrense smitten under koronapandemien førte til børsfall og økonomiske utfordringer i land verden over, og i Norge forventes en kraftig nedgang i produksjonen i 2020.[7] En verdireduksjon i boligmarkedet[8] og at mange, både privatpersoner og virksomheter, vil få utfordringer med blant annet å betjene stor gjeld er sannsynlig. Det ventes også langvarige negative virkninger på sysselsettingen og produksjonsnivået i økonomien, som kan vare i mange år.[9]

---

[3] SSB, «BNP per innbygger, prisnivåjustert», 2019.

[4] Transparency International korrupsjonsindeks 2019 viser at Danmark og New Zealand ble rangert som nr. 1, etterfulgt av Finland på en 2. plass, og Singapore, Sverige og Sveits på delt 3. plass. Indeksen baserer seg på folks oppfatninger av korrupsjon i offentlig sektor.

[5] Oslo Børs, «Energi, shipping og sjømat», 2020.

[6] EUROPOL, «Why is Cash still king? », 2015.

[7] IMF, «World Economic Outlook April 2020», 2020.

[8] Finansavisen, «Økonomer er mer negative til boligmarkedet», 2020.

[9] Dagens Næringsliv, «Regjeringens ekspertgruppe: Dette vil ulike korona-scenarioer ha å si for norsk økonomi de neste ti årene», 2020.

Deler av næringslivet har blitt hardt rammet, og mange virksomheter i Norge opplever nå bortfall av inntekter og anstrengt likviditet. På kort sikt får tiltakene særlig alvorlige konsekvenser for tjenesteytende næringer og turistnæringen, og for virksomheter som hadde anstrengt økonomi før pandemien.[10] Også norsk eksport har blitt redusert.[11]

Arbeidsledigheten i Norge er betydelig høyere enn før pandemien. Det er særlig alvorlig at mange unge i yrker med lav utdanning rammes. Dette er personer som kan ha lettere for å bli langtidsledige.

Norge er likevel et av landene i verden som har de beste forutsetningene for å kunne kompensere næringslivet for bortfallet i inntekter. Statens pensjonsfond utland har blitt – og vil fortsatt bli – benyttet til å redde mange virksomheter fra konkurs. Mange andre land har dårligere forutsetninger for å støtte næringslivet, og mange av våre handelspartnere vil sannsynligvis oppleve en større økonomisk krise enn det vi vil oppleve i Norge.[12]

Selv med en forventet nedgang i den økonomiske veksten fremover vil norsk økonomi gjøre det bra relativt til økonomien i mange andre land. Som et land med stor grad av økonomisk og politisk stabilitet vil Norge forbli et attraktivt land å plassere verdier for utenlandske aktører. Også midler av ulovlig opprinnelse kan forventes å bli kanalisert til Norge.

3.6.2. Næringsstruktur og kriminalitet innen viktige sektorer

3.6.2.1. Olje- & gassektoren

Oljesektoren er den dominerende næringen i Norge i dag og utgjorde i 2019 48 prosent av vareeksporten. Oljesektoren er imidlertid preget av et fåtall store aktører og er strengt regulert og kontrollert, noe som antas å begrense mulighetene for økonomisk kriminalitet. Korrupsjon kan derimot være en utfordring når de samme selskapene opererer utenlands.[13]

Oljeinvesteringer er kapitalintensive, og det er store verdier på kontraktene som inngås. Kontraktstørrelser kan i seg selv øke risikoen for korrupsjon ved at betydelige summer enklere kan kamufleres gjennom forhøyede kontrakter, noe Petrobras-skandalen vitner om.

En studie utført av konsulentselskapet EY fant at olje- og gassnæringen i Storbritannia var representert i de fleste sluttførte rettsforfølgelser for bestikkelser og korrupsjon i perioden 2008–2012, hvorav det som regel involverte betalinger til utlandet.[14] Flere norske selskaper opererer i land med høy korrupsjonsrisiko. Norske selskaper står også i fare for å pådra seg ansvar for bestikkelser eller korrupte aktiviteter begått av partnere eller tredjeparter som opptrer på deres vegne.

Petroleumsnæringen i Norge er også interessant for utenlandske investorer. Reelt eierskap kan skjules i nominee-kontoer, gjerne fra banker i Sveits eller Luxembourg, med lite innsyn. Dette gjør det vanskelig å få oversikt over pengestrømmer og å avsløre skatteunndragelser, innsidehandel og hvitvasking.

---

10 Dagens Næringsliv, «Snart 200.000 koronapermitterte: - Vi skal klore oss fast», 2020.

11 SSB, «Rekordstort handelsunderskudd», 2020.

12 Menon Economics, «Effekt av Korona på norsk eksportrettet næringsliv», 33/2020.

13 EY, «Managing bribery and corruption risks in the oil and gas industry», 2014.

14 EY, «Managing bribery and corruption risks in the oil and gas industry», 2014.

3.6.2.2. Fiskeri og havbruksnæringen

Fiskeeksport er den største eksportnæringen utenom olje og har opplevd en enorm vekst de seneste årene. Sektoren eksporterte i 2019 for 104 milliarder kroner, tilsvarende 22 prosent av fastlandseksporten. Havbruksnæringen har blitt viktig for kyst-Norge og produserer nå for langt mer enn de tradisjonelle fiskeriene. Fra havbruksnæringen var samlet skattebidrag 7,9 milliarder kroner, mens nærmere 8 milliarder kroner kom fra underleverandørene.

Fiske- og sjømatindustrien kan være et utsatt område for kriminalitet, ved at produksjonskjeden åpner for muligheter til å utføre forskjellige typer kriminalitet, og siden oppdagelsesrisikoen tradisjonelt har vært lav.

Fiskerisektoren er sårbar for flere typer kriminalitet. Ved eksport av fisk kan fiktiv fakturering, feilaktig prising og bruk av uriktige dokumenter legge grunnlaget for å kamuflere grov økonomisk kriminalitet, herunder skattesvik, regnskapsovertredelser og bedrageri, i tillegg til overfiske. Store deler av norsk eksport av sjømat går også til land som har strukturelle korrupsjonsproblemer, og som rangeres langt nede på Transparency Internationals korrupsjonsindeks.

Fiskerinæringen er også et eksempel på en næring hvor forholdene ligger til rette for multikriminalitet. Det forekommer utnyttelse av arbeidstagere innen fiskerinæringen. Mange arbeidere formidles fra selskaper i lavkostland, for eksempel fra Øst-Europa og de baltiske landene. Flere av disse virksomhetene opptrer ikke i henhold til norsk regelverk.

3.6.2.3. Eiendomsutvikling, bygg og anlegg

Eiendomsmarkedet er et kapitalintensivt marked der store beløp flyttes. Det er derfor egnet for hvitvasking av utbytte fra kriminalitet.[15] Det norske eiendomsmarkedet har over lengre tid hatt en høy prisstigning som har gitt god gevinst ved investeringer, og det har vært høy aktivitet innenfor nybygging. Det forekommer også manipulasjon av eiendomsverdier, ved at eiendommer som selges kort tid etter å ha blitt kjøpt har steget unormalt mye i verdi. Tilgangen til svart arbeidskraft for bygging og rehabilitering av eiendom i Norge er god og muliggjør økt profitt.

Eiendomsutvikling og bygg- og anleggsbransjen er preget av store prosjekter og hard konkurranse, der pris ofte er utslagsgivende for hvem som vinner oppdrag. Dette gjør næringene sårbare for særlig a-krimaktører, som blant annet kutter lønnskostnader og/eller unnlater å betale lovpålagte skatter og avgifter for å vinne anbud.

[15] Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», 2019.

3.6.3. Utbyttegenererende kriminalitet i Norge

Antall registrerte anmeldelser i Norge er redusert med nærmere 12 prosent de siste fem årene. Det er særlig anmeldelser av narkotikalovbrudd og vinning som har blitt redusert. Sistnevnte skyldes i stor grad en omkategorisering av alminnelig bedrageri fra vinning til økonomisk kriminalitet. Følgelig har også anmeldt økonomisk kriminalitet økt betraktelig.

Omfanget av utbytte som hvitvaskes i Norge hvert år er ikke kjent, men det genereres årlig store summer fra kriminalitet i Norge. Det føres også store summer fra kriminell virksomhet i utlandet inn til Norge.

Det har over flere år vært et kriminalpolitisk mål å sikre verdier og inndra utbytte fra profittmotivert kriminalitet for å hindre at kriminalitet lønner seg. I 2019 ble det i Norge idømt inndragning på 185,4 millioner kroner. Det er langt lavere enn inndragningspotensialet til utbytte fra kriminalitet som reelt sett hvitvaskes. For hasj alene ble det i 2019 beslaglagt et kvantum som i verdi utgjør om lag 274 millioner kroner etter salg.

3.6.3.1. Kriminalitet som genererer utbytte til aktører innen arbeidslivskriminalitet

Arbeidslivskriminalitet har alvorlige konkurransevridende konsekvenser for norsk næringsliv. I flere sektorer utkonkurreres lovlydige virksomheter av virksomheter som ikke overholder norske lover og regler som over tid er opparbeidet for å sikre arbeidstakers rettigheter. Arbeidstakerne som utnyttes blir underbetalt eller arbeider uregistrert, slik at de mister velferdsretter som forsikring, sykepenger og dagpenger. De risikerer å skade seg eller dø under arbeid eller innkvartering fordi arbeidsgiver ikke overholder HMS-bestemmelser.

Skatt- og avgiftsunndragelser medfører årlig svært store tap for den norske stat, noe som indirekte kan føre til eksempelvis mindre velferdsmidler til befolkningen og høyere skatter.

Kostnadsbesparelser i form av underbetaling, svart arbeid og manglende HMS-tiltak, samt bedrageri av det offentlige, genererer utbyttet i arbeidslivskriminalitet. Det er altså statens inntektstap og arbeidstakeres opparbeidede rettigheter som utgjør a-krimaktørers profitt. Utbyttet kan både genereres og hvitvaskes ved misbruk av systemer og mekanismer i arbeidslivet, blant annet ved bruk av fiktiv fakturering.

3.6.3.1.1. Skatteunndragelser – svart arbeid

Med svart arbeid menes arbeid som utføres uten at det betales lovpålagte skatter og avgifter. Dette foregår ved å gi uriktige opplysninger eller å unnlate å gi opplysninger om omsetning og lønn.[16] Svart arbeid er ofte kontantbasert. Det antas også å være store mørketall knyttet til svart arbeid.

Svart arbeid er et samfunnsproblem ved at store summer unndras fra fellesskapet og bidrar til konkurransevridning. Skatteetaten anslo i 2015 at staten tapte 12 milliarder kroner direkte knyttet til unndragelse av skatter og avgifter.[17]

Antall anmeldte skattesvik har gått ned fra 1315 i 2016 til 763 i 2019, tilsvarende 42 prosent.[18] Antall nordmenn som svarer at de kjøper svart arbeid i undersøkelser har også gått ned. Dette skyldes trolig at etterspørselen etter svart arbeid er redusert i det norske samfunnet. Fremdeles svarer imidlertid

16 ØKOKRIM, «Skattekriminalitet», 2017.

17 Dagens Næringsliv, «Slik jakter politiet personer som benytter svart arbeid», 2018.

18 SSB, «Anmeldte lovbrudd og ofre, tabell 08484», 2020.

10 prosent av virksomhetsledere at det i enkelte tilfeller kan aksepteres at en virksomhet bevisst unndrar skatt og avgift. De fleste av disse arbeider innen bransjer som preges av arbeidslivskriminalitet.[19]

Pandemien har ført til økt etterspørsel i bransjer identifisert som sårbare for skatte- og avgiftskriminalitet. Samtidig forventes arbeidsledigheten å holde seg høyere enn før koronapandemien.

Det er derfor *sannsynlig* at det vil bli en økning av arbeidsgivere som benytter svart arbeid, og dermed at utbytte fra skatteunndragelser vil øke fremover. Økningen forventes å komme innen bransjer med stort innslag av arbeidslivskriminalitet, som varetransport og bygg- og anleggstjenester.

3.6.3.1.2. Utnyttelse av utenlandske arbeidstakere

Enkelte aktører i bransjer med lave krav til utdannelse rekrutterer bevisst utenlandske arbeidstakere for å minimere lønn og lovpålagte kostnader forbundet med ansattes helse, miljø og sikkerhet. Arbeidsgiverne er både norske og utenlandske, særlig øst-europeiske. Utnyttelsen fordekkes ofte i en kjede av underleverandører, eller ved at utlendingen oppfordres til å arbeide i et enkeltpersonforetak med mindre velferdsrettigheter.

Rekruttering av utenlandsk arbeidskraft har blitt lukrativt, og falske arbeidskontrakter legitimerer innreise til Norge for å omgå reiserestriksjoner.

Det er *sannsynlig* med en økt og grovere utnyttelse av arbeidstakere som følge av større konkurranse om kunder og anskaffelser som medvirker til at arbeidsgivere presses til å holde kostnader på et minimum. Dette vil *meget sannsynlig* øke utbyttet fra utnyttelse av utenlandske arbeidstakere.

3.6.3.1.3. MVA-bedrageri

Merverdiavgift (mva) er skatt på innenlands forbruk, omsetning og anskaffelse av varer og tjenester har som formål å skaffe inntekter til staten. Merverdiavgift er estimert til å gi Norge 310 milliarder kroner i inntekter i 2019, hvilket utgjør omtrent en femtedel av de samlede skatte- og avgiftsinntektene.[20]

MVA-bedrageri er en hovedkilde til profitt innen arbeidslivskriminalitet. Bedrageriene utføres ofte ved bruk av fiktiv fakturering eller ved utholdt[21] omsetning. Formålet ved begge fremgangsmåtene er å unndra skatt og avgift og frigjøre kontanter til svart avlønning, uten at det fremkommer av regnskapet. Momsunndragelser ved innførsel av varer som byggevarer, biler og bildeler gir utgiftsbesparelser for a-krimaktører.

A-krimsenteret i Oslo har funnet at 20 prosent av foretakene som ble kontrollert i varebilsegmentet og 38 prosent av kontrollerte virksomheter i bilpleien i Oslo underrapporterer omsetning til skattemyndighetene.[22] 25 kontrollerte underleverandører innen varetransportbransjen i Oslo var skyldig 21 millioner kroner i hovedsakelig merverdiavgift.

Det er *meget sannsynlig* at særlig aktører innen arbeidslivskriminalitet vil benytte både fiktiv fakturering og utholdt omsetning for å unndra merverdiavgift.

---

19 Samfunnsøkonomisk analyse, «Eksterne faktorer – Arbeidslivskriminalitet og arbeidsinnvandring», Rapport 2/2019.

20 Finansdepartementet, «Proposisjon til Stortinget 1 LS (2018-2019)», 2018.

21 Det er omsetning (salgs-/driftsinntekter) som ikke er tatt inn i regnskapet for bedriften, og ikke tatt med som grunnlag for beregning av merverdiavgift og/eller grunnlag for skatteberegning (dvs. helt svart).

22 A-krimsenteret i Oslo og Akershus, «Arbeidslivskriminalitet i transportbransjen – varebilsegmentet», 2019.

3.6.3.2. Kriminalitet som genererer utbytte til næringslivsaktører

Kriminalitet begått av næringslivsaktører genererer årlig store utbytter som hvitvaskes. Utbyttene genereres på bekostning av miljøet, forsvarlig forvaltning av naturressurser og dyrevelferd samt økosystemet. Både slike kostnadsbesparelser og tilfeller av korrupsjon er konkurransevridende. Matkriminalitet kan være helseskadelig, og konkurskriminalitet kan ha konsekvenser for en viktig hjørnesten i vårt økonomiske system – kredittgivning til næringslivet og tillit mellom kredittgiver og næringslivsaktører.

Støtteordninger som er iverksatt som følge av COVID-19 har vist seg å bli utnyttet av både organiserte kriminelle og næringslivsaktører som ikke tidligere er knyttet til straffbare forhold. Dette gjelder spesielt lønnskompensasjonsordningen og misbruk av statlig lånegarantiordning.

3.6.3.2.1. Korrupsjon

Det har de seneste årene blitt avslørt flere alvorlige korrupsjonssaker innenfor kommunale etater som plan- og bygg, samt saker knyttet til offentlige anskaffelser. OECD anser anskaffelser som ett av de viktigste risikoområdene for korrupsjon internasjonalt.[23] Korrupsjon i offentlig sektor kan svekke tilliten til lokale styrings-organer og kan gi kriminelle tilgang til kommunale oppdrag. Norske kommuner er sårbare for korrupsjon og korrupsjonsfaren er særlig til stede der privat sektor møter offentlig sektor.

Det er *meget sannsynlig* at korrupsjon i lokalforvaltningen, særlig rettet mot utbyggingsprosjekter og anskaffelser, vil fortsette å være en trussel. Korrupsjonsfaren vil avhenge av kommunenes egeninnsats i eget antikorrupsjonsarbeid, graden av gode varslingskanaler, kontrollutvalg og solid varslervern.

Store deler av norsk eksport, inkludert oljesektoren, går til land som har strukturelle korrupsjonsproblemer.[24] Det gjør næringer eksponert for korrupsjon. Bestikkelser kan for eksempel være en forutsetning for å komme i posisjon til å bli tildelt kontrakter i korrupsjonsutsatte land.[25]

Erfaringer fra tidligere saker viser at bestikkelser kan generere svært stort utbytte til de kriminelle aktørene.

Mange private selskaper vil bli hardt presset økonomisk som følge av pandemien. Det er *sannsynlig* at dette vil øke incentivene til bruk av ulovlige midler, som bestikkelser, for å vinne kontrakter og anbud. Det er videre *sannsynlig* at norske virksomheter som eksporterer varer til korrupsjonsutsatte land, eller etablerer seg i utlandet, vil bli involvert i korrupsjon i utlandet. Det er *meget sannsynlig* at utbyttet fra korrupsjon vil fortsette å være betydelig.

3.6.3.2.2. Matkriminalitet

Matkriminalitet beskriver avvik i matproduksjonskjeden som oppstår som følge av bevisst bedrageri av forbrukeren eller en annen virksomhet og som begås for å oppnå økonomisk gevinst. Kriminalitet i matproduksjonskjeden kan være tilknyttet organiserte kriminelle organisasjoner.[26]

Det anslås at 19 prosent av mat- og drikkevarene i Norge er svindlet med, sammenlignet med verdensgjennomsnittet som er på 25 prosent. Fisk anses som en av de mest svindelutsatte varene. Manipuleringen av fisk skjer i mye større grad enn manipulering av kjøtt.[27] Ut fra 200 studier fra 55 land antas det

---

23 Nærings- og fiskeridepartementet, «Melding til Stortinget, 22 (2018–2019), 'Smartere innkjøp – effektive og profesjonelle offentlige anskaffelser'», 2019.

24 Mer enn 1 milliard eksporteres til land i Vest- og Sentral-Afrika, mer enn 12 milliarder til Øst-Europa og Sentral-Asia.

25 ØKOKRIM, «Trusselvurdering 2020», 2020.

26 EUROPOL, «EU Serious and organised crime threat assessment (SOCTA) 2013», 2013.

27 Labolytic, «Hvor utbredt er egentlig matsvindel i Norge?».

at ca. 20 prosent av all fisk hos detaljist og catering er feilmerket. Det er misledende merking og svindel med fiskearter som er den største trusselen, som at fisk med lav kvalitet eller mindre attraktive fiskearter selges som mer kostbare og eksklusive arter, eller at lavkvalitet råvare blir blandet inn i høykvalitetsråvare og fremstilt som høykvalitet.[28] Det kan være betydelig fortjeneste når volumene er store.

Det er *meget sannsynlig* at økt globalisering vil føre til økt trussel for matsvindel og feilmerking av produkter. Det er også *meget sannsynlig* at feilaktig merking vil generere store summer i utbytte for aktørene som setter denne typen kriminalitet i system. Feilaktig og spekulativ merking av produkter kan svekke forbrukerens tillit til bransjer nasjonalt og tilliten til viktige eksportnæringer i utlandet.

3.6.3.2.3. Konkurskriminalitet

Likviditetsmangel er ofte driveren for konkurskriminalitet. Historisk følges finanskriser av omfattende saker med konkurskriminalitet. Enron-saken i USA, Finance Credit-saken i Norge og bankkollapsen på Island ved tidligere finanskriser er eksempler på dette.

Store virksomheter tappes ofte urettmessig for aktiva mens de fortsatt eksisterer, ved eksempelvis salg av eiendeler til underpris eller plassering av aktiva i andre foretak. I forkant av konkurser begås det også ofte bedrageri mot kredittinstitusjoner og investorer for urettmessig å tilføre driftskapital til en virksomhet som ikke lenger har livets rett. Konkurs benyttes også som et redskap for å begå eller skjule annen økonomisk kriminalitet. Konkursryttere som gjentagende utnytter selskaper og slår dem konkurs utgjør en vesentlig samfunnstrussel.

Det er *sannsynlig* at det vil bli en økning i antall bedrifter som går konkurs på grunn av pålagte restriksjoner i forbindelse med COVID-19 og den økonomiske nedgangstiden. Det er også *sannsynlig* at muligheten til betalingsutsettelse vil medføre at en del konkurser blir forskjøvet til 2021.

Det er *meget sannsynlig* at redusert oppdagelsesrisiko vil føre til at flere kriminelle utnytter situasjonen og begår konkurskriminalitet, og dermed til at utbyttet fra konkurskriminalitet vil øke. Det er også *meget sannsynlig* at kriminelle aktører vil benytte muligheten til å få betalingsutsettelse for å holde liv i virksomheter lenger, og på den måten vil få mer utbetalt enn de har rett på, eller bygge seg opp store restanser.

3.6.3.2.4. Fiskerikriminalitet

Fiskerinæringen er globalisert med en kompleks og lite oversiktlig produksjons- og verdikjede. Varer, arbeidstagere og penger krysser Norges grenser i stadig større volum. Fisk og fiskevarer er Norges nest største eksportmarked til en verdi av 104 milliarder kroner i 2019.[29] Aktørgalleriet i fiskerinæringen består av alt fra små enkeltpersonforetak, til store globaliserte konsern som rår over flere ledd i verdikjeden med betydelig geografisk spredning.

Det er sannsynlig at det ved eksport av fisk foregår fiktiv fakturering, feilaktig prising og bruk av uriktige dokumenter. Dette er handlinger som tilrettelegger for og kamuflerer grov økonomisk kriminalitet, herunder skattesvik, regnskapsovertredelser og bedrageri, i tillegg til overfiske.[30]

Det er *meget sannsynlig* at kvotefiskerne vil fortsette med omfattende ulovlig fiske som mottakene vil bidra til å kamuflere ved hjelp av underrapportering av uttaket av fiskeriressurser i Norge.

---

28 Food and Agricultural Organization of the United States, «Overview of food fraud in the fisheries sector», 2018.

29 Statistisk sentralbyrå, «Fiskeeksporten passerte 100 milliard kroner i 2019», 2020.

30 ØKOKRIM, «Trusselvurdering 2020», 2020.

Norske fiskeriressurser tiltrekker seg også useriøse aktører med koblinger til utlandet. Aktørene tilegner seg norske ressurser på ulovlig vis, som ved turistfiske, men utfordrer også norsk jurisdiksjonsutøvelse over norske ressurser, slik man har sett i krabbefisket.[31]

Det er *meget sannsynlig* at fiskerne vil fortsette med betydelig ulovlig uttak av kongekrabbe. Ulovlig uttak av kongekrabbe gir grunnlag for senere svart omsetning, samt skatteunndragelser og brudd på matloven og tolloven. Det er *meget sannsynlig* at utbyttet fra denne typen fiskerikriminalitet vil være stort i årene fremover.

3.6.3.2.5. Ulovlig avfallshåndtering

Enhver bedrift i Norge som slipper ut noe som helst til luft, avløp og vann, eller som håndterer farlige kjemikalier inn og ut av bedriften og kan ha risiko for akuttutslipp eller grunnforurensning og farlig avfall, skal kunne fremvise en tillatelse, samt dokumentasjon på forholdene. Det er også forbudt å kaste eller plassere avfall i naturen.

Det norske avfallsregelverket er strengt, og avfall har ofte en negativ verdi fordi det er kostbart å behandle det forsvarlig etter regelverket. Systemet med såkalt omvendt økonomi[32] gjør at aktørene kan øke profitten betydelig ved ikke å etterleve regelverket. Ulovlig håndtering av avfall kan være billigere enn lovlig behandling av avfall på et avfallsanlegg.

Det er avslørt flere store saker innen ulovlig avfallshåndtering, særlig ved avfallsanlegg. Ulovlig avfallshåndtering gjennomføres hovedsakelig av avfallsanlegg med tillatelse til drift fra miljømyndighetene. Så lenge profittmotivasjonen består, er det *sannsynlig* at ulovlig avfallshåndtering vil fortsette å være en trussel. Det er *sannsynlig* at denne typen ulovlig virksomhet vil generere betydelig utbytte til aktørene.

3.6.3.2.6. Marin forsøpling

Marin forsøpling[33] er en av de største miljøutfordringene vi har, og omfanget er økende. Plast utgjør ca. 80 prosent av søppelet i havet. Over tid kan plasten brytes ned til mikroplast, som kan påvirke hele det marine økosystemet.[34] Hoveddelen av plastavfallet i sjøen i Norge og rundt Svalbard kommer fra lokale utslipp – nesten 50 prosent av avfallet på norske strender stammer fra norsk skips- og fiskerinæring.[35,36]

Fiskeutstyr, som garn og teiner, mistes i hovedsak som følge av påvirkninger fra vær og vind, og ved at det hekter seg fast. Aktiv dumping av utrangert fiskeutstyr forekommer i mindre grad i dag enn tidligere, men det skjer likevel fortsatt. Det observeres også større mengder avkapp av tau og not som trolig stammer fra mindre reparasjoner av fiskeutstyr, som ikke blir håndtert på en god nok måte.[37]

---

31 Store norske leksikon, «Senatorsaken», 30. april 2019.

32 Det vil si at den som tar imot avfall får fullt ut betalt når avfallet er mottatt.

33 Vi følger her Miljødirektoratet som definerer marin forsøpling som alt fast materiale fra menneskelig aktivitet som er forlatt eller på annen måte havner i det marine miljø. Marin forsøpling inkluderer avfall fra landbaserte kilder som er fraktet til havet med vassdrag, avløp eller vind. Marin forsøpling kan bestå av plast, trevirke, metall, glass, gummi, tekstiler, papir, etc. Definisjonen inkluderer ikke avfall i væskeform, som mineralsk eller vegetabilsk olje, parafin og andre kjemikalier. Biologisk nedbrytbart avfall fra fiskerinæringen og akvakultur omfattes heller ikke av definisjonen (Lozano et al. 2009).

34 Miljødirektoratet, «Kunnskap om marin forsøpling i Norge 2014», Rapport M-265/2014.

35 NRK, «Ingen i Norge har ansvar for søpla til havs», 2018.

36 Miljødirektoratet, «Kunnskap om marin forsøpling i Norge 2014», Rapport M-265/2014:22.

37 Miljødirektoratet, «Overordnet vurdering av kilder og tiltak mot marin forsøpling», 2016.

Også skipstrafikken bidrar til marin forsøpling – en FN-rapport viser at så mye som 80 prosent av søppelet i de nordlige havområdene stammer fra skipsfart.[38]

Det er *sannsynlig* at økt trafikk av fartøy og fortsatt høy fiskeriaktivitet langs kysten vil utgjøre en høy trussel for marin forsøpling og dumping av plast i havet. Manglende håndtering av avfall vil generere ulovlig utbytte til aktørene.

3.6.3.3. Kriminalitet som genererer utbytte til internasjonale kriminelle aktører

Trusselbildet preges av økt globalisering. Nasjonale grenser har fått mindre betydning på mange områder. Norske borgere handler på utenlandske nettsteder, og betalingen gjennomføres ofte 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. Grensekryssende virksomhet blir mer utbredt, og finansielle transaksjoner går raskere. Med økt globalisering og integrering av økonomier følger utfordringer med grensekryssende kriminalitet og grensekryssende aktører.[39]

Bedrageri er en form for grensekryssende kriminalitet som fører til store økonomiske tap for både personer og næringslivsaktører i Norge. Personer som utsettes for bedrageri, det være seg som privatperson eller som ansatt, opplever det også som traumatiserende, og det påvirker tilliten til andre mennesker og næringslivet negativt. Bedrageri som medfører tap av sensitiv informasjon kan også medføre stor skade for den personlige integritet og blottlegge systemsvakheter og forretningshemmeligheter i næringslivet, så vel som personlige data lagret av både offentlige etater og næringsliv.

3.6.3.3.1. Bedrageri

Økt digitalisering har ført til en økning i digital kriminalitet, inkludert bedragerier i Norge. Antall anmeldte bedragerier totalt i Norge økte med 36 prosent fra 2009 til 2018.[40] Like fullt er det store mørketall på omfang av bedrageri og økonomisk tap.

Bedragerier utføres ofte av organiserte kriminelle grupperinger i utlandet, hvilket vanskeliggjør etterforsking av saker og sporing av transaksjoner. Risikoen for å bli avslørt og straffeforfulgt er liten. Aktørene fremstår som meget tilpasningsdyktige, velger ofre bevisst og utnytter menneskelige feil og/eller sårbarheter i datasystemer.

Også norske aktører kan knyttes til bedragerier, eksempelvis til såkalte Olga-bedragerier mot eldre og eiendomsinvesteringsbedrageri.

Modus	Kjent tap i 2018 i mill. NOK[41]	Kjent tap i 2019 i mill.NOK[42]
Direktørbedrageri	34	188
Fakturabedrageri	8,7	138,5
Kortbedrageri	148	190
Investeringsbedrageri	101	111
Eiendomsinvesteringsbedrageri	92	99

38 UNEP, «Marine plastic debris and micro plastics sources of macro and micro plastics», 2016.
39 ØKOKRIM, «Trusselvurdering 2020», 2020.
40 NTAES, «Bedrageri mot næringslivet», 2019.
41 Finanstilsynet, «Risiko og sårbarhetsanalyse for 2018», 2019.
42 Finanstilsynet, «Risiko og sårbarhetsanalyse for 2020», 2020.

I 2019 var det i Norge størst økonomisk tap knyttet til direktørsvindel og fakturabedrageri ved endring av mottakerkonto. Sosial manipulering er en essensiell del av bedrageriet. Utbyttet fra kortbedrageri har vært stabilt høyt over flere år. Økt netthandel, raske sømløse betalingsmuligheter og innføringen av betalingsdirektivet PSD2 øker de kriminelles handlingsrom.[43,44] Transaksjoner stanses sjelden i tide, sporing av utbytte vanskeliggjøres og tredjepartsaktørers tilgang til kunders lønnskonto er sårbarheter som kan utnyttes.

Det er *meget sannsynlig* at kriminelle aktører vil øke forsøk på faktura- og direktørbedrageri rettet mot norske virksomheter. Dette ses i sammenheng med at det er høy profitt og lav oppdagelsesrisiko. Dette er også en type kriminalitet som har økt de siste årene. Utbyttet vil avhenge av hvor mange som blir bedratt og hvilke virksomheter som blir lurt. Det er *meget sannsynlig* at utbyttet vil fluktuere fra år til år, men ha en økende trend fordi bedragerne evner å endre modus etter hvert som metodene blir offentlig kjent.

Også antall forsøk på investeringsbedrageri har økt de siste årene. I 2019 ble 725 kunder i DNB utsatt for forsøk på investeringsbedrageri – en markant økning fra 469 fornærmede i 2018.[45] Privatpersoner eller foretak forledes til å investere i prosjekter eller produkter som er verdiløse eller ikke-eksisterende.[46]

En variant av investeringsbedrageri er ulovlige pyramidespill der verving av investorer sikrer ny kapital, men hvor pengene flyttes til bedragerne på toppen av pyramiden. De fleste pyramidespill gjennomføres av internasjonale selskaper registrert i utlandet, og med utenlandske bankkontoer. Lotteritilsynet har avdekket at nordmenn i løpet av få år har betalt minst 500 millioner kroner til Lyoness alene. 150 000 nordmenn antas å være, eller ha vært, deltagere i selskapet.

Under koronapandemien har det vært en økning i investeringsbedrageri, spesielt via falske handelsplattformer. Det er *meget sannsynlig* at investeringsbedrageri vil fortsette å øke, både knyttet til kryptovaluta og falske handelsplattformer, og at dette særlig vil ramme eldre Det er derfor *meget sannsynlig* at utbyttet ved investeringsbedrageri også vil øke. Det er videre *meget sannsynlig* at det vil dukke opp nye pyramidespill i Norge.

3.6.3.3.2. Narkotikakriminalitet

2019 ble det registrert 23 413 narkotikasaker[47] i Norge. Dette er en nedgang på 25 prosent fra 2014.[48] Antallet registrerte narkotikalovbrudd reflekterer i stor grad politiets og tollvesenets ressurstilgang og prioriteringer.

Å anslå verdien av det norske narkotikamarkedet er vanskelig, men det omsettes for store verdier, hovedsakelig i kontanter. Utbytte som genereres ved omsetning av narkotika hvitvaskes og reinvesteres i både kriminell og legal virksomhet, eller sendes til utlandet. Noen ganger plasseres de i skatteparadis. Omsetningen innenlands er ofte kontantbasert og kamufleres via strømenn og kriminelle i næringsliv og eiendom, samt restaurant- og utelivsbransjen.

Digitale markedsplasser tilrettelegger også for krypterte og anonyme kjøp som vanskeliggjør sporing av transaksjoner.

Det er *meget sannsynlig* at omsetning av narkotika vil fortsette å være en av de kriminelle nettverkenes primærkilder til profitt. Det er *sannsynlig* at narkotikaomsetningen på internett og via sosiale medier vil

43 Cifas, «Fraudscape», 2019.
44 EUROPOL, «Internet organised crime threat assessment (IOCTA) 2018», 2019.
45 DNB, «Annual Fraud report 2019», 2020.
46 NTAES, «Bedrageri mot næringslivet», 2019:41.
47 Statistikken inneholder både toll- og politibeslag av narkotika.
48 Kripos, «Narkotika- og dopingstatistikk 2019», 2020.

øke fremover, og også utbyttet knyttet til denne typen omsetning. Det er *sannsynlig* at flere transaksjoner ved kjøp på digitale markedsplasser krypteres for å sikre anonymitet.

3.6.3.3.3. Menneskesmugling og menneskehandel

EUROPOL estimerer inntekten fra menneskesmugling til å være mellom 300-5000 EUR per person. De anser bruken av kontanter og hawala-virksomhet som en økende utfordring ved menneskesmugling.[49] Menneskehandel[50] ansees for å være blant de tre største ulovlige markedene globalt, sammen med våpen- og narkotikakriminalitet. Utbyttet anslås til å være på om lag 150 milliarder USD på verdensbasis i 2018.[51]

Det avdekkes få saker vedrørende menneskehandel og menneskesmugling i Norge,[52] men det registreres en økning i andel saker som omhandler menneskehandel til tvangsarbeid.[53]

Sammenholdt med informasjon om at utenlandske ansatte ofte utnyttes i arbeidslivskriminalitet er det *sannsynlig* at omfanget av menneskehandel i Norge er høyere enn hva som er registrert.

Politiet anser den største utfordringen med menneskesmugling til Norge å være menneskesmugling med utnytting til arbeid som formål. Det vil fortsatt være stor etterspørsel etter arbeidskraft i arbeidsintensive yrker.

Det er derfor *meget sannsynlig* at organiserte kriminelle vil smugle mennesker til Norge med formål om utnytting til arbeid og prostitusjon i årene som kommer.

I Norge blir utbytte fra menneskehandel sjelden identifisert, det er derfor vanskelig å anslå omfanget av utbytte fra menneskehandel og hvordan dette hvitvaskes. Selv om vi ikke vet omfanget av utbyttet, vil det *meget sannsynlig* være snakk om betydelige summer i årene fremover.

3.6.3.3.4. Kjøp av seksuelle overgrep

Gjerningspersoner i Norge bestiller overgrep, som strømmes via kommunikasjonstjenester med chatte- og videofunksjon. Politiet mottar stadig flere rapporter om nordmenn som foretar mistenkelige transaksjoner som kan knyttes til direkteoverførte overgrep. Antallet norske statsborgere som overfører penger til kjente tilretteleggere er langt høyere enn antall personer som anmeldes for slike overgrep. Dette indikerer at omfanget av direkteoverførte overgrep er høyere enn anmeldelsestallene tilsier. Overførslene går til land som er relativt fattige, hvor mennesker er særlig utsatt for utnyttelse.

Det er *mulig* at flere personer med en seksuell interesse for barn vil bestille direkteoverførte overgrep, ettersom det i kommende år vil være vanskelig å reise for å begå fysiske overgrep mot barn. Dette vil i så fall gjøre at kriminelle aktører i utlandet vil få økt utbytte ved salg av direkteoverførte overgrep.

---

49 EUROPOL, «EMSC 3rd Annual activity report – 2018», 2019.

50 Ved menneskehandel tvinges, utnyttes eller forledes en person med formål om økonomisk profitt. Utnyttelsen kan bestå i prostitusjon eller andre seksuelle ytelser, arbeid eller tjenester ved bruk av vold, trusler eller misbruk av sårbar situasjon eller annen utilbørlig atferd. Menneskehandel omfatter også live-streaming av seksuelle overgrep mot barn, samt å tvinge, utnytte eller forlede mennesker til å tigge eller begå kriminalitet.

51 FATF, «Financial flows from human trafficking», 2018.

52 Menneskesmugling rammes av utlendingsloven og innebærer å hjelpe en migrant med ulovlig innreise eller opphold i landet. Det forutsettes at migranten har samtykket til smuglingen. Menneskesmugling som lovbrudd opphører ved ankomst til destinasjonsstedet. Migranten settes i gjeld til menneskesmuglerne og må betale tilbake gjennom ulovlig arbeid eller annen kriminalitet.

53 KOM, «Rapport fra Koordineringsenheten for ofre for menneskehandel 2018», 2019:35.

Betalingsmetodene varierer og tilpasses kontinuerlig for å redusere sporbarheten. Det betales relativt små summer for dette, mellom 50 og 1000 kroner. Over tid kan det imidlertid bli store beløp. Vi har kjennskap til personer som over noen år har overført opptil en million kroner på det som fremstår å være kjøp av seksuelle overgrep.

Det er enkelt å overføre penger til overgripere i andre land ved overføring direkte fra norsk konto, ved oppmøte hos en, eller via betalingsformidlere på internett, hvor avsender betaler med visa-/kredittkort. Dette kan gjøre transaksjonene vanskeligere å avdekke.

3.6.3.3.5. Ulovlig eksport av EE-avfall

Det er estimert at ca. 400 000 tonn ulovlig utrangerte elektriske og elektroniske produkter (EE-avfall), blir eksportert ut av Europa hvert år udokumentert.[54,55] Miljødirektoratet estimerer at 4 000 til 10 000 tonn EE-avfall kommer på avveie fra mottak i Norge hvert år.

EE-avfall inneholder verdifulle komponenter med høy omsetningsverdi. Tyveri av komponenter fører til store tap for gjenvinningsforetakene i Norge og kan generere stort utbytte for de kriminelle aktørene når det selges i utlandet.

Tyveri av EE-avfall knyttes til aktører fra Øst-Europa. De har videreformidlet avfallet til grupper som eksporterer det ut av landet, ofte i kontainere. Avfallet har i mange tilfeller havnet i land i Afrika, som Ghana og Nigeria, men også i Asia. Eksporten av brukte produkter til Vest-Afrika har vært stabil i løpet av koronapandemien, men det har vært en nedgang i den deklarerte eksporten av EE-produkter. I sommer har imidlertid flere varebiler, kjørt av aktører fra Øst-Europa, blitt stanset på vei ut av landet med udeklarert EE-avfall.

Økt velstand i større deler av verden antas å gi økt etterspørsel etter elektroniske produkter og EE-avfall. Det er *sannsynlig* at omfanget av tyveri og ulovlig eksport av EE-avfall vil vedvare og at kriminelle aktører vil få betydelig utbytte fra slik ulovlig eksport og salg. Det er *sannsynlig* at aktører fra Øst-Europa har endret mo- dus til å transportere EE-avfallet ulovlig ut av landet udeklarert i varebiler, istedenfor å benytte eksportører til å frakte det ut i kontainere.

3.6.3.3.6. Ulovlig handel med illegale varer

Det internasjonale illegale markedet for handel med truede arter er stort, og det innføres også ulovlige arter og ulovlige kunst- og kulturgjenstander til Norge. Organiserte kriminelle grupper som står bak slik ulovlig handel retter sin oppmerksomhet mot dyr og planter av stor økonomisk verdi og opererer gjennom komplekse, globale kriminelle nettverk. Utenlandske aktører som kommer til Norge og stjeler og eksporterer fugleegg er en vedvarende utfordring.

Det er et økende problem med ulovlig omsetning på internett av kosttilskudd, nye matprodukter og andre produkter. EUROPOL og INTERPOL har avdekket at det er organiserte kriminelle aktører som står bak mange av disse nettstedene.[56] Omsetningen er en enkel kanal for hvitvasking av penger fra andre kriminelle aktiviteter. Mange land sliter med å avdekke hvem står bak slike nettsteder, og dermed er det enkelt å slippe unna kontroll og sanksjoner.

Det er *meget sannsynlig* at den ulovlige handelen med illegale varer vil vedvare og generere betydelig utbytte til kriminelle aktører. Netthandelen har økt kraftig under koronapandemien. Det er *meget sannsynlig* at denne endringen hos forbrukerne vil vedvare også etter koronapandemien. Det er videre *meget*

---

54 CWIT-project, «Countering WEEE Illegal Trade Summary Report», 2015.

55 Det er estimert at 1,3 millioner tonn udokumentert elektronikk blir eksportert ut av Europa hvert år, og 30 prosent av dette antas å være ulovlig EE-avfall.

56 EUROPOL, «EU Serious and organised crime threat assessment (SOCTA) 2017», 2017.

sannsynlig at kriminelle aktører vil utnytte dette, og at omsetning av illegale varer på nett som vil generere ulovlig utbytte og hvitvasking gjennom slike nettsteder vil øke.

3.6.3.3.7. Smugling av varer

Det ligger et stort potensialt for urettmessig gevinst gjennom bevisst feildeklarering av tollverdi, feilkategorisering av varer og opprinnelse, samt underdeklarering av vekt eller volum. Økonomisk kriminalitet på dette området medfører først og fremst økonomisk tap for staten, men også ulike konkurransevilkår med tap for andre næringslivsaktører.

Ulike grupperinger, blant annet enkelte aktører fra Øst-Europa, utnytter lovlige virksomheter som skallfirmaer for å smugle alkohol og tobakk. En rekke ulike smuglervarer, som tobakk, alkohol, narkotiske stoffer og tabletter samt mat- og byggevarer, omsettes av aktører som også begår arbeidslivskriminalitet.

Reduserte muligheter til grensehandel under koronakrisen har sannsynligvis gitt høyere etterspørsel etter billig alkohol, kjøttvarer og sukkervarer (godteri og brus). Samtidig har restriksjonene på reiser over grensen gjort småsmugling med privatbil vanskelig. Dette skaper et marked som kan utnyttes av kriminelle, herunder a-krimaktører, ved å organisere smugling av etterspurte varer med andre varebærere. Blant annet sesongarbeidere kan bli utnyttet.

Handel på internett er økende. Dette er et mindre regulert marked, og potensialet for toll- og momsunndragelser er økende.

Det er *sannsynlig* at smugling av varer vil fortsette å være en trussel og generere utbytte som hvitvaskes. Det er *meget sannsynlig* at organiserte kriminelle aktører i større grad vil benytte legale virksomheter for å kamuflere og hvitvaske utbytte fra smugling. Det er videre *meget sannsynlig* at toll- og momsunndragelsene ved handel på internett, og dermed utbyttet knyttet til dette, vil øke i årene fremover.

3.6.4. Utbytte fra utlandet

Det hvitvaskes også utbytte i Norge som kommer fra primærkriminalitet begått i utlandet. Dette påvirker den totale hvitvaskingsrisikoen i Norge.

Utenlandske aktører har større mulighet til å skjule reelt eierskap, blant annet ved hjelp av klientkontoer. Det kan være en utfordring for norske banker å få innsikt i hvem reell eier i utlandet er, noe som kan føre til at norske banker benyttes til å hvitvaske midler fra kriminell virksomhet i utlandet. Erfaring fra sakene vedrørende baltiske banker viser også at det er utfordrende å avdekke mistenkelige transaksjoner, spesielt i bedriftsmarkedet, hvis man ikke har fagsystem som gjør det mulig å benytte regler/alarmer.

En måte for utenlandske aktører å legitimere pengestrømmer på er å bruke norske finansinstitusjoner til å gjennomføre transaksjoner. Informasjon fra de rapporteringspliktige indikerer at Norge benyttes som transittland.

Kontoer i norske banker benyttes også til muldyr-/oppsamlingskontoer for norske og utenlandske kriminelle i forbindelse med bedrageri, hovedsakelig nettbank- og såkalt direktørbedrageri. De fleste muldyrkontoer er imidlertid utenlandske, og midler føres fra norske bedrageriofre til de utenlandske oppsamlingskontoene.

Det er *sannsynlig* at Norge vil være et attraktivt land å hvitvaske midler både i og gjennom også i fremtiden. Sårbarhetene med hensyn til reelt eierskap består fremdeles, og det er fortsatt mangelfull kundekontroll og høy risiko knyttet til flere produkter innen bedriftsmarkedet. Det er *meget sannsynlig* at det årlig vil gå store summer utbytte til og gjennom Norge.

3.6.5. Særlige risikomoduser hvitvasking

For at kriminelle aktører skal kunne ta i bruk utbytte fra kriminell virksomhet som legale midler, utføres aktiviteter med formål å tilsløre utbyttets opprinnelse – hvitvasking. Hvitvasking kjennetegnes også ved at utbytte fra en straffbar handling introduseres i lovlig økonomi, og dermed fremstår som legitim.[57] I dette kapitlet presenteres særlig alvorlige moduser som kriminelle benytter for å hvitvaske utbytte.

De tre modusene med høyest risiko for hvitvasking er bruk av kryptovaluta og nyere betalingstjenester, samt hvitvasking gjennom næringsvirksomhet.

Matrise risikovurdering, moduser hvitvasking

	Trusselnivå	Sårbarhetsnivå	Konskvensnivå	Risiko
Hvitvaskingsmoduser som er grensekryssende eller digitale				
Kryptovaluta				Høy
Nye betalingstjenester				Høy
Utenlandske spillselskaper				Betydelig
Norge som transittland				Betydelig
Plassering i utlandet				Moderat
Grensekryssende varehandel				Moderat
Hvitvaskingsmoduser som benyttes i norge				
Næringsvirksomhet				Høy
Eiendomsmarkedet				Betydelig
Utførsel av kontanter				Moderat
Verdigjenstander				Moderat
Aktører som bidrar i hvitvaskingsoperasjoner				
Muldyr				Moderat
Profesjonelle tilretteleggere				Moderat

3.6.5.1. Kriminelle aktører benytter kryptovaluta

Kryptovaluta er en stadig mer utbredt metode for hvitvasking og benyttes som betalingsmiddel i omsetning av illegale varer, og i transaksjoner som følge av bedrageri og løsepengevirus. Kryptovaluta og vekslere av virtuell valuta omtales nærmere under sektorer pkt. 4.8.13.

Anonymiteten ved kryptoadresser og tilsløringen av partene i transaksjonen ved bruk av uregistrerte kryptovekslere, gjør det *meget sannsynlig* at slike vekslere vil benyttes til hvitvasking. Risikoen for at kryptovaluta og uregistrerte vekslere skal bli brukt til hvitvasking av midler, vurderes å være høy.

[57] Justis- og beredskapsdepartementet, «Nasjonal Strategi for bekjempelse av hvitvasking, finansiering av terror og finansiering av spredning av masseødeleggelsesvåpen», 2016.

3.6.5.2. Kriminelle aktører benytter nye betalingstjenester

Med nye betalingstjenester siktes det til applikasjoner og internettbaserte programmer som benyttes til å gjennomføre pengetransaksjoner, men som ikke er en nettbank.[58] Dette er tjenester som foregår utenfor det tradisjonelle banksystemet hvor det kan gjennomføres kortbetaling, veksling og pengeoverføringer nasjonalt og internasjonalt. De tilbyr økt anonymitet og raskere overføringer til en lav pris. Estimater tilsier at 39 millioner mennesker globalt benytter såkalt neo-banking.[59]

ØKOKRIM har kjennskap til flere personer som har gjennomført mistenkelige transaksjoner via nye betalingstjenester. Formålet har ofte vært oppgjør mellom kriminelle for kjøp og salg av illegale varer som eksempelvis narkotika, men slike betalingstjenester benyttes også av pengemuldyr til hvitvasking og terrorfinansiering.

På grunn av anonymiteten og de raske internasjonale overføringene er det *sannsynlig* at nye digitale betalingstjenester vil bli benyttet av kriminelle som ønsker å hvitvaske utbytte. Risikoen for at nye betalingstjenester vil benyttes til hvitvasking av utbytte fra straffbare forhold vurderes å være høy.

3.6.5.3. Kriminelle aktører bruker utenlandske spillselskaper for å hvitvaske utbytte

Det har vokst frem et stort uregulert marked av utenlandske pengespill som kasino, poker, oddsspill og bingo på nettet. Det er ulovlig for utenlandske spillselskaper å tilby eller markedsføre spillene i Norge, og norske banker og andre betalingstjenester i Norge har ikke lov til å formidle innsats og utbetaling i pengespill som tilbys av pengespillselskaper uten tillatelse i Norge.[60]

Det foreligger informasjon om at aktører innen narkotikaomsetning og mc-miljø mottar beløp fra ulike utenlandske spillselskaper.

Kriminelle overfører utbytte fra straffbare handlinger via en betalingsformidlingstjeneste til en utenlandsk spillekonto. På denne måten tilsløres reell avsender og mottaker av transaksjonen, og banker, finansinstitusjoner og betalingsformidlingsforetak forledes til å gjennomføre transaksjoner som i utgangspunktet er forbudte. Utbyttet kan brukes til å spille, men kan også bare oppbevares på spillekontoen før det overføres videre.[61]

Underslag, selvvask og dokumentforfalskning

En 45 år gammel mann er i tingretten dømt til fengsel i fire år og seks måneder for blant annet grovt underslag, grov selvvasking og dokumentforfalskning.

Etterforskningen avdekket at det var laget et forfalsket avtaledokument angående et vannprosjekt i Afrika, og at utbetalinger til dette ble lagt til grunn for bokføringen i selskapet. Beløpene som er opplistet i den falske avtalen og bokført som overført til dette selskapet samsvarer i det vesentlige med beløp som er overført fra organisasjonens konto til ulike spillselskaper.

Kilde: Dom fra Gulating lagmannsrett 3.12.2019.

Uavhengig av om utbyttet genererer gevinst eller har vært urørt, vil flytting og endring av form på utbyttet være hvitvaskingshandlinger.

58 ØKOKRIM, «Trusselvurdering 2020», 2020.
59 Business Insider, «The global neobanks report», 2019.
60 Lotteri- og stiftelsestilsynet, «Pengespill på nett», 2020.
61 NTAES, «Vouchers og betalingsformidlingstjenester – effektiviserer netthandel, tilslører kriminalitet», 2018.

Utenlandske spillselskapers manglende kundekontroll og ikke-eksisterende beløpsgrenser, i kombinasjon med betalingsformidleres tilsløring av transaksjonskjeden, gjør det *sannsynlig* at kriminelle aktører vil benytte utenlandske spillselskaper til hvitvasking. Risikoen for at utenlandske spillselskaper skal bli brukt til hvitvasking av midler, vurderes å være betydelig.

3.6.5.4. Utenlandske kriminelle aktører benytter Norge som transittland

En måte for utenlandske aktører å legitimere pengestrømmer på er å bruke norske finansinstitusjoner til å gjennomføre transaksjoner. I Norge er det flere titalls tusen norske bankkontoer som innehas av utenlandske selskaper.

Det er ofte utenlandske virksomheter som benytter seg av bedriftskontoer i norske banker som gjennomstrømningskontoer. Men vi har også informasjon om privatpersoner som bruker sine konter som gjennomstrømningskontoer.

Norske kontoer brukes som transaksjonskontoer for store beløp. Midlene føres relativt raskt ut igjen til andre kontoer. Ved å foreta transaksjoner gjennom skallselskaper i skatteparadis tilsløres opphavet til pengestrømmene ytterligere.[62]

I dokumentlekkasjen FinCEN files fremkommer det at amerikanske banker har varslet om at en milliard norske kroner har blitt sluset gjennom ulike DNB-kontoer. Det mistenkes at pengene kan knyttes til hvitvasking, korrupsjon og terrorfinansiering.[63]

Det er *meget sannsynlig* at norske banker benyttes som gjennomstrømmingskontoer for både utenlandske personer og selskaper som ønsker å tilsløre opphav og mottaker av transaksjoner knyttet til hvitvasking og annen profittmotivert kriminalitet. Det er *sannsynlig* at norske finansinstitusjoner vil fortsette å være attraktive for å legitimere illegale pengestrømmer, samt at kriminelt utbytte fra utlandet vil havne i Norge. Risikoen for at kriminelle aktører og virksomheter vil benytte norske banker til gjennomstrømming av midler knyttet til hvitvasking og annen kriminalitet vurderes å være betydelig.

3.6.5.5. Kriminelle aktører plasserer utbytte i utlandet

Utbytte fra kriminell virksomhet i Norge kan plasseres i og hvitvaskes via utlandet. Hvitvasking av eget skattesvik ved hjelp av tilslørende utenlandstransaksjoner forekommer i flere ulike typer saker, i mange bransjer og med skattytere i ulike aldre. Forskning viser imidlertid at det er de aller mest velstående skattyterne som har størst sannsynlighet for å skjule verdier i skatteparadiser, og at denne gruppen eier 50 prosent av verdiene som holdes der.[64]

Det har vært en økning i pågangen av nye skatteytere som ønsker å benytte ordningen med frivillig retting. I 2018 var det 575 nye saker. Samme år ble 845 saker ferdigbehandlet. Disse utgjorde til sammen 6,3 milliarder kroner i formue, og 279 millioner kroner i inntekt.[65] Metodene for å omgå initiativene blir mer komplekse og innebærer økt bruk av strukturer hvor eierskapet tilsløres. Profesjonelle mellommenn

62 NRK, «DNB brukte fleire år på å stenge omstridte kontoer», 2019.

63 Aftenposten, «Derfor er dokumentlekkasjen til FinCEN files viktig», 2020.

64 Alstadsæter Annette; Johannesen, Niels & Zucman, Gabriel, «Tax Evasion and Inequality», 2018:2.

65 Skatteetaten, «Uoppgitte formuer for 6 milliarder kroner meldt inn til Skatteetaten», 2019.

spiller en sentral rolle ved opprettelse av slike strukturer.[66] Nordmenn kjøper også eiendom i utlandet, enten ved å benytte profesjonelle rådgivere i Norge, eller ved å benytte utenlandske selskaper med skjult eierskap, der eier og innehaver i realiteten er norsk skattyter bosatt i Norge.

Når midler skal tas tilbake til Norge, kan dette gjøres ved å opprette fiktive lån, og ved at lån i Norge nedbetales med skjult inntekt/formue i utlandet. Dersom midlene benyttes til forbruk, gjøres det ofte med utenlandske bankkort i Norge.

Grensekryssende transaksjoner fremstår i dag som vesentlig mer hyppige enn bare for noen år tilbake. Tilgjengeligheten av tilbydere av finansielle tjenester på internett og via ulike applikasjoner har økt. Internasjonalisering og økt virksomhet på tvers av landegrensene betyr samtidig at stadig flere har inntekt eller formue i utlandet.

Oppgjør på utenlandsk depotkonto

Oppgjør for tjenester utført i utlandet med mistanke om korrupsjon ble gitt i aksjer på en utenlandsk depotkonto.

Midlene ble dels hvitvasket og skjult ved at de sto på konto i Sveits. Noe av midlene ble benyttet i Norge ved kjøp av varer/tjenester betalt med utenlandsk kredittkort knyttet til kontoen i den sveitsiske banken. Midler ble også overført til et annet norsk selskaps bedriftskonto. Denne kontoen ble disponert av den kriminelle eller hans nærstående.

Det er *sannsynlig* at bedre informasjonstilgang gjennom nye multilaterale og bilaterale skatteutvekslingsavtaler, og økt internasjonalt samarbeid mellom kontrollorganer og politimyndigheter vil bidra til å redusere mulighetene for hvitvasking. Risikoen for at penger skal bli plassert i utlandet som del av en hvitvaskingsoperasjon vurderes likevel å være betydelig.

3.6.5.6. Kriminelle aktører benytter grensekryssende handel til å hvitvaske utbytte

Verdenshandelen med varer utgjorde omtrent 143 000 milliarder kroner i 2017.[67] Myndigheter har reelt sett bare mulighet til å kontrollere små andeler av dette enorme volumet. Når varer og penger i tillegg krysser landegrenser vanskeliggjøres sporing og kontroll ytterligere.

Ved handelsbasert hvitvasking flyttes utbyttet fra kriminalitet ved bruk av handelstransaksjoner. Det foregår ved å underslå eller overrapportere pris, kvantitet eller kvalitet ved import eller eksport.[68] Det er altså en form for over- eller underfakturering av varers reelle verdi og oppgitt verdi (fakturabeløp). Handelsbasert hvitvask-ing forutsetter ofte et samarbeid mellom eksportør og importør.

Attraktive varer for handelsbasert hvitvasking er varer som er vanskelig å vurdere verdien av, som eksempelvis gullvarer, smykker, kunst og samlegjenstander. Fisk og byggevarer er også attraktive varer for handelsbasert hvitvasking i Norge.

Tolletaten og skattemyndighetene i Norge avdekker flere saker med over- og underfakturering årlig. Transaksjonene kan overføres på en slik måte at det tilsløres hvem pengene kommer fra, som for eksempel betaling med kryptovaluta eller overførsel via mellommann, eller at det utstedes kreditnota.

---

66 De Groen & Willem Pieter, «Role of advisors and intermediaries in the schemes revealed in the Panama Papers, European Parliament Economic and Monetary Affairs, Study for the PANA-Committee», 2017.

67 World Trade Organization (WTO), «World Trade Statistical Review», 2018.

68 FATF, «Trade-based money laundering», 2006.

Eksportprodukter kan benyttes til å hvitvaske midler ved at lovlige varer kjøpes med utbytte fra kriminalitet, slik at selve pengeutbyttet ikke må krysse landegrensene. Denne modusen er observert brukt av nigerianske mellommenn som benytter kontanter fra narkotikasalg eller bedrageri til å kjøpe tørrfisk som eksporteres til Nigeria.

Norsk fiskerinæring eksporterte fisk og fiskevarer til en verdi av 104 milliarder kroner i 2019.[69] Det er kjent at selgere og kjøpere går sammen om å unndra skatt og hvitvaske penger ved hjelp av kreditnotaer. Selger eksporterer fisk til kjøper i et annet land, og når fisken mottas hevder kjøper at deler av partiet er av dårlig kvalitet. Kjøper ber om en kreditnota for partiet og at deler av beløpet overføres til en konto i en sekretessejurisdiksjon. Beløpet kan kanaliseres tilbake til både selger og kjøper. Både selger og kjøper kan på denne måten oppgi mindre inntekter til myndighetene enn de reelt sett har. Utbyttet kamufleres ved falsk kreditnota og i sekretessejurisdiksjoner.

Grunnet den omfangsrike grensekryssende handelen i verden er det *meget sannsynlig* at handelsbasert hvitvasking forekommer i et større omfang enn det som er registrert i Norge. Risikoen for at handelsbasert hvitvasking skal bli brukt til hvitvasking av midler vurderes å være moderat.

3.6.5.7. Kriminelle aktører hvitvasker utbytte gjennom næringsvirksomhet

Plassering av utbytte i næringsvirksomhet gir mulighet til å anskaffe «hvit» inntekt/utbytte som kan legitimere forbruk og investeringer. Dette gjør kriminelle aktører enten ved å investere i eller sluse penger gjennom legalt næringsliv, eller ved å starte eget foretak.

Narkotikaomsetning genererer mye kontanter og skaper et behov for å hvitvaske midlene. Utbytte fra narkotikavirksomhet investeres i etablering av næringsvirksomheter og blandes sammen med inntekt fra næringsdrift, betaling for løpende driftskostnader eller bankoverføring til andre butikker eller enkeltpersoner. En fremtredende modus er fiktiv fakturering ved bruk av underleverandører som mellomledd. Penger videresendes til nytt foretak eller uttaksledd. Kontanter fra narkotikaomsetning kan også benyttes til svart avlønning.

Eierforhold og roller i flere virksomheter gjør det lettere å kamuflere pengetransaksjoner mellom partene, slik at ulovlig ervervede verdier kan føres inn i næringslivet. Aktører i næringslivet som både begår skatte- og avgiftsunndragelser eller arbeidslivskriminalitet, i tillegg til at de tilrettelegger for hvitvasking av utbytte fra narkotikakriminalitet, utgjør en særskilt stor trussel.

Det er *meget sannsynlig* at hvitvasking gjennom næringsvirksomhet vil fortsette å være en egnet form for å sikre inntekt til kriminelle nettverk og aktører. Risikoen for at næringsvirksomhet skal bli brukt til hvitvasking av midler vurderes å være høy.

3.6.5.8. Kriminelle aktører hvitvasker utbytte via eiendomsmarkedet

Eiendomsmarkedet er et kapitalintensivt marked der store beløp flyttes. I Norge har det vært en betydelig verdiøkning i boligmarkedet de siste tjue årene. Det er derfor egnet for hvitvasking av utbytte fra kriminalitet.[70]

---

69 Statistisk sentralbyrå, «Fiskeeksporten passerte 100 milliard kroner i 2019», 2020.

70 Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», 2019.

Eiendomsmarkedet benyttes av aktører innen arbeidslivskriminalitet, narkotikakriminalitet og økonomisk kriminalitet til å hvitvaske midler. De investerer både i privatboliger og i næringsbygg, i Norge og i utlandet.[71] Det benyttes ofte stråpersoner og stråselskaper når utbytte fra kriminalitet investeres i eiendom. Både under kjøpsprosessen og i offentlige registre tilsløres midlenes opphav og reell eier på denne måten.

Moduser for å hvitvaske midler i eiendomsmarkedet inkluderer kontant betaling av utbedringer og oppussing med utbytte fra kriminell aktivitet. Denne typen oppgraderinger utføres gjerne svart. En annen fremgangsmåte er manipulasjon av eiendomsverdier. Eiendommer stiger raskt i verdi og omsettes igjen uten å ha vært lagt ut på det åpne markedet, gjerne kort tid etter at de ble kjøpt. Profesjonelle aktører, som meglere og advokater, kan medvirke med fiktive verdivurderinger og tilrettelegge for såkalt svingdørsalg, hvor samme eiendom omsettes hyppig og gjerne med unormal prissetting.

Det er *sannsynlig* at eiendom som er kjøpt eller rehabilitert med utbytte fra kriminalitet leies ut til både private og offentlig aktører, noe som gir et skinn av legitimitet. Det er *sannsynlig* at omsetning av kontrakter på kjøp av prospektive prosjekter brukes for å hvitvaske midler, samtidig som skatt unndras. Risikoen for at eiendomsmarkedet skal bli brukt til hvitvasking av midler vurderes å være betydelig.

3.6.5.9. Kriminelle aktører fører kontanter ut av Norge

Kriminelle nettverk frakter kontanter utenlands, gjerne ved bruk av pengekurer. I 2019 ble det deklarert inn om lag 11 milliarder kroner mer enn det ble deklarert ut av Norge. Det tilsvarende tallet for 2020 var ved utgangen av oktober rundt 4,5 milliarder. Dette tilsier at restriksjoner knyttet til COVID-19-pandemien har redusert både ut- og innførselen av kontanter fra Norge.[72] Utførsel av kontanter kan knyttes til miljøer som allerede har et system for logistikk og smugling.

Det er *sannsynlig* at flere valutabeslag på utreise er knyttet til arbeidslivskriminalitet.

Store summer overføres årlig fra Norge til utlandet, blant annet ved bruk av betalingsformidling og hawala.[73] Pengene ender ofte i konflikt- og krigsområder, og i randsonen av slike områder. Overførslene gjøres ofte av personer med utenlandsk opprinnelse. Noen av dem er godt kjent av politiet, med forbindelser til narkotika, vold og radikalisering. Selv om de fleste av transaksjonene trolig er midler av legal opprinnelse som går til familie, er det i flere tilfeller mistenkelige forhold knyttet til både den som overfører og den som mottar pengene.[74]

Bankenes endrede praksis, som gjør det vanskeligere å overføre penger fra flere kunder som én transaksjon til utlandet, gjør det *sannsynlig* at flere betalingsformidlere vil benytte fysisk utførsel av kontanter. Utførsel av kontanter og hawala-virksomhet har høy iboende risiko for hvitvasking. Risikoen for at utførsel av kontanter skal bli brukt til hvitvasking av midler vurderes å være moderat.

---

71 NTAES, «Situasjonsbeskrivelse – Arbeidslivskriminalitet 2019», 2020.

72 Deklareringer over 25 000 kroner fra både virksomheter og privatpersoner.

73 Hawala er et ukonvensjonelt system for betaling og pengeoverføringer over landegrenser, som oftest anvendes når betalingsmottakerne bor i land uten normalt fungerende bankvesen. Det fungerer som et alternativ til bankvesenet og er basert på tillit.
ØKOKRIM, «Trusselvurdering 2020», 2020.

3.6.5.10. Kriminelle aktører benytter verdigjenstander for å hvitvaske utbytte

Kriminalitet som generer profitt i kontanter skaper et behov for å hvitvaske pengene uten å tiltrekke seg oppmerksomhet fra kontrollmyndigheter. En velkjent fremgangsmåte for å avhende seg med en betydelig kontantbeholdning er å kjøpe ulike verdigjenstander som kunst, kostbare klokker, klær og kjøretøy. Ved videresalg av gjenstandene fremstår oppgjøret som legal inntekt.

Politiet har kunnskap om aktører som hvitvasker utbytte fra straffbare handlinger ved å overføre større beløp via flere personer og foretak for så å kjøpe kunst. Dagens Næringsliv har i en artikkel om kunstoppbevaringen i DHL Excel Fine Art sitt lager på Kalbakken rettet mistanke om at det omsettes kunst ulovlig, og at det således benyttes til hvitvasking.[75] Lageret oppbevarer kunst for milliarder av kroner, og kundelisten er hemmelig. Enkelte kunstverk lagres i navnet til advokater.[76]

Konvertering av kontanter til kostbare forbruksgjenstander som klokker, biler og kunst er en kjent form for hvitvasking innen gjengmiljøer som omsetter narkotika, mc-miljøet og hos aktører som begår økonomisk kriminalitet. Gjenstandene er lett omsettelige og kan benyttes som oppgjørsmiddel ved en senere anledning. Spesielt klokker egner seg godt for utførsel til utlandet.

Det er *meget sannsynlig* at enkelte aktører som driver med kjøp/salg av klokker og kunst gjør dette for å hvitvaske egne og andres penger. Risikoen for at verdigjenstander skal bli brukt til hvitvasking av midler vurderes å være moderat.

3.6.5.11. Kriminelle aktører benytter muldyr for å overføre utbytte

Med pengemuldyr menes de som mottar penger fra én person og overfører dem videre til en annen, enten digitalt eller som kontanter, mot betaling.[77] Dette kan være både av frivillig og ufrivillig art, de kan både forstå og ikke forstå at man hjelper kriminelle og er medskyldig i eventuelle straffelovsbrudd.[78]

Det er i hovedsak tre grupper som lar seg bruke som pengemuldyr. Den første er unge mennesker som gjør dette i bytte mot penger eller luksusvarer. Mange av de forstår antagelig ikke alvoret i handlingen. Den andre gruppen er eldre som er alene. Disse forstår gjerne ikke at de utnyttes. Den tredje gruppen er personer med økonomiske problemer som er mer tilbøyelige til å takke ja til «lettjente penger».[79]

Bruk av muldyr er et økende problem i mange land, og det rapporteres også om en økning i Norge i 2020.[80] Britiske CIFAS skriver at det i 2018 ble rapportert 40 000 saker hvor man mistenkte at bankkontoer ble misbrukt for å bistå kriminelle. Dette var en økning på 26 prosent fra 2017.[81] Omfanget i Norge er ikke kjent.[82]

Ofre for sosial manipulering og kjærlighetsbedrageri blir også i enkelte tilfeller forledet til å stille sin bankkonto til disposisjon for pengeoverføringer og bidrar dermed til å skjule overføringer av midler som stammer fra ulovlig virksomhet.[83,84]

---

75 Dagens Næringsliv, «Kunstlagerets konfidensielle "show room"», 2019.
76 Dagens Næringsliv, «Toll, Skattekrim og Kemneren aksjonerte mot kunstlager», 2019.
77 ØKOKRIM, «Hvitvasking gjennom pengemuldyr», 2019.
78 CIFAS, «Fraudscape», 2019:10.
79 ØKOKRIM, «Hvitvasking gjennom pengemuldyr», 2019.
80 «DNB advarer: Oppdager flere som hvitvasker penger for fiktive selskaper», 2020.
81 CIFAS, «Fraudscape», 2019:10.
82 ØKOKRIM, «Hvitvasking gjennom pengemuldyr», 2019.
83 Finanstilsynet, «Risiko og sårbarhetsanalyse (ROS) 2018», 2019:19.
84 DNB, «Trusselvurdering 2020», 2020.

Det er sterk vekst internasjonalt, og det anses derfor som *mulig* at både antall transaksjoner via pengemuldyr, og totalsummen som blir overført, vil øke fremover. Risikoen for at muldyr skal bli brukt til hvitvasking av midler vurderes å være moderat.

3.6.5.12. Kriminelle aktører bruker advokaters klientkonto for å kamuflere utbytte og hvitvaske midler

Det er uvisst i hvilket omfang kriminelle benytter advokater til hvitvasking, men i løpet av de siste 15 årene er flere advokater dømt for å ha medvirket til hvitvasking av utbytte ved å stille klientkonto til disposisjon for kriminelle.[85]

Å benytte advokaters klientkonto ved transaksjoner gir høy legitimitet. Transaksjoner og opplysninger om hvem midlene tilhører, er også til dels beskyttet av advokatenes taushetsplikt og hindrer utenforstående innsyn. Advokaters klientkonto er derfor særlig egnet for å skjule og tilsløre midlers opprinnelse og eierskap.

Det foreligger informasjon om at klientkontoer benyttes som rene gjennomstrømmingskontoer for å skjule utbytte fra straffbare handlinger. Kriminelle aktører benytter også klientkontoer som bankkonto når de unndrar beskatning med bistand av advokat.

Bruken av profesjonelle aktører som advokater vanskeliggjør politiets og kontrolletaters arbeid ved å fordekke kriminaliteten. De bidrar til at kriminelle lykkes med hvitvasking av utbyttet og sikrer kriminelle nettverks videre eksistens. Folks tillit til profesjoner og rettstaten undergraves.

Det er *meget sannsynlig* at kriminelle aktører forsøke å bruke advokaters klientkontoer til å hvitvaske utbytte. Risikoen for at advokaters klientkontoer vil benyttes til hvitvasking av midler vurderes å være moderat.

[85] Borgarting lagmannsrett dom av 2. april 2013 (12-107624AST-BORG/01), Oslo tingrett 14. august 2013 – 12-197822MED-OTIR/08, Borgarting lagmannsrett dom av 8. juli 2015 (14-181913AST-BORG/02), Borgarting lagmannsrett dom av 27. april 2017 (16-019686AST-BORG/03).

3.7. Overordnede sårbarheter for hvitvasking

Kravene til etterlevelse av hvitvaskingsreglementet har økt på mange områder. Det har utvidet ansvars- og arbeidsbyrden for rapporteringspliktige og tilsynsorganer. Disse kravene krever både kompetanseheving hos aktører som er forpliktet til å implementere hvitvaskingsloven, samt tilstrekkelige ressurser øremerket kampen mot hvitvasking.

Hvitvaskingsregelverket skal styrkes ytterligere i årene fremover. Cyberkriminalitet og miljøkriminalitet er inntatt som lovbrudd i det sjette hvitvaskingsdirektivet. Det innebærer at ansatte i rapporteringspliktig virksomhet må opplæres i å avdekke og håndtere utbytte fra nye typer kriminalitet.

3.7.1. Utfordringer med nasjonalt kunnskapsgrunnlag, kompetanse og nasjonal koordinering

Informasjonsbehovet knyttet til hvitvasking er fortsatt stort. Det utarbeides interne trussel- og risikoanalyser på ulike nivåer, men de deles i liten grad.

Det er også en sårbarhet at det ikke i tilstrekkelig grad utarbeides statistikk over utbytte i straffesaker. Dermed er det ikke mulig å få en god oversikt over utbytte som genereres innenfor de enkelte kriminalitetsområder. Mangelen på kunnskap er en utfordring både i myndighetenes utforming av tiltak og i de rapporteringspliktiges arbeid med å identifisere mistenkelige transaksjoner.

For at politiet skal bli bedre på å identifisere og avdekke indikasjoner på hvitvasking, kreves det både bedre kunnskap og opplæring. Ytterligere satsing på å bygge robuste fagmiljøer for å etterforske og iretteføre saker som springer ut av meldingssystemet etter hvitvaskingsloven er helt nødvendig for å redusere denne systemsårbarheten.

Nasjonal koordinering av innsatsen er avgjørende for et velfungerende regime mot hvitvasking. Den overordnede koordineringen og målrettingen av den nasjonale innsatsen skal ivaretas av Kontaktforumet. Det vil imidlertid ta noe tid før Kontaktforumet når sitt potensial som nasjonal koordineringsmekanisme.

3.7.2. Svakheter i det internasjonale samarbeidet

Hvitvasking er grensekryssende kriminalitet. Effektiv bekjempelse av slik kriminalitet fordrer samarbeid med andre lands myndigheter. Norske myndigheter har over tid utviklet og engasjert seg aktivt i internasjonalt rettslig og politioperativt samarbeid. Etterforskning av grensekryssende kriminalitet er likevel ressurskrevende og en utfordring for politiet.

Det har blitt lettere å innhente informasjon etter inngåelse av bistandsavtaler med de fleste land.[86] Skatteutvekslingsavtaler (TIEA) gir Skatteetaten raskere og bedre tilgang til informasjon fra utlandet. Ved etterforskning av grensekryssende hvitvasking erfares det imidlertid at myndighetene i noen land yter lite eller ingen bistand, eller at samarbeidet er omstendelig, med tidkrevende prosesser. Kriminelle som plasserer utbytte fra straffbare handlinger, eller tilslører midlers opprinnelse, søker gjerne nettopp til land preget av strengt hemmelighold og lite samarbeidsvillige myndigheter.

[86] Norge har inngått skatteavtaler med cirka 100 land. De fleste bilaterale skatteavtalene tar utgangspunkt i føringer fra OECD eller FN.

3.7.3. Svakheter i tilsynsvirksomhet

Tilsynet som føres med de rapporteringspliktiges arbeid på hvitvaskingsområdet skal sikre at kriminelle ikke kan misbruke finansielle tjenester for å sikre utbytte.

Det er tre offentlige aktører som fører tilsyn med rapporteringspliktige i Norge – Finanstilsynet, Tilsynsrådet for advokatvirksomhet og Lotteritilsynet.

I Finanstilsynets strategi for 2019–2022 er kriminalitetsbekjempelse ett av seks prioriterte mål. I 2019 ble det opprettet en egen seksjon for anti-hvitvasking og betalingsforetak, noe som blant annet har medført økt tilsynsvirksomhet på hvitvaskingsområdet, samt en rekke nye veiledningsdokumenter. FATFs evalueringsrapport publisert sent i 2019 konkluderer med at tilsynet fremdeles har forbedringspunkter, herunder at det bør føres flere tilsyn med banker og betalingsforetak. Finanstilsynet har utstedt overtredelsesgebyr for brudd på hvitvaskingsloven til en rekke banker, eiendomsmeglere samt én revisor siden 2018. FATFs anbefaling om bruk av overtredelsesgebyr ved avdekking av alvorlige mangler i etterlevelsen av hvitvaskingsloven ble likevel ikke vurdert som fullstendig gjennomført fordi gebyrene ble ilagt foretakene etter rapporteringsfristen til FATFs oppfølgingsevaluering i 2019.[87]

Arbeidet til Tilsynsrådet for advokatvirksomhet har vært preget av uklarheter rundt hvitvaskingsloven og rekkevidden av særskilte unntak fra rapporteringsplikten når det gjelder anti-hvitvaskingsarbeid. Finansdepartementet ga Tilsynsrådet medhold i deres forståelse, noe som innebærer at advokatenes rapporteringsplikt representerer et klart unntak fra advokatens lovbestemte taushetsplikt. Advokatenes taushetsplikt har vært gjenstand for diskusjon, herunder hvor langt den rekker og hvem den egentlig er ment å beskytte.

Hvitvaskingslovens anvendelsesområde ble utvidet til også å omfatte tilbydere av spilltjenester, som medførte at Lotteritilsynet siden 2018 har utvidet sitt tilsynsmandat.

De rapporteringspliktiges forståelse av hvitvaskingsregelverket er ulikt, og kunnskapsnivået om hvordan deres virksomhet kan bli utnyttet til hvitvasking varierer. I bingobransjen fremstår nivået som lavt. Det er imidlertid mange aktører som trenger veiledning og oppfølging.

Jevnt over er tilsynsorganene presset fra flere kanter og besitter ikke tilstrekkelige ressurser til å ha en tilsynsaktivitet i tråd med krav og forutsetninger fra for eksempel FATF, EBA og IMF. Det er også en sårbarhet at man har noen internasjonale aktører innen betalingsformidling som det i praksis ikke blir ført tilsyn med.

3.7.4. Manglende transparens om reelle rettighetshavere

Mye av den alvorlige økonomiske kriminaliteten kamufleres ved at lovbryterne gjennomfører transaksjoner og organiserer eierskap på en ikke-transparent måte. Et sentralt element i hvitvaskingsregelverket er gjennomføringen av kundekontroll ved etablering av kundeforhold. Når kunden er et selskap skal identiteten til reelle rettighetshavere også bekreftes, noe som kan være utfordrende for foretak med kompleks eierstruktur, herunder oppkjøpsfond som eier store nasjonale og internasjonale virksomheter. Hvordan bankene foretar denne kontrollen varierer.[88]

Finanstilsynet erfarer at de rapporteringspliktige er mer opptatt av identifisering av reelle rettighetshavere enn tidligere. Finans Norge har gjennomført mange kunde- og ID-kontroll-kurs de siste årene.

---

87 Financial Action Task Force (FATF), «5th Year Follow-Up Assessment Report of Norway», 2019.

88 ØKOKRIM, «Trusselvurdering 2015–2016», 2016.

Finanstilsynet har imidlertid konstatert at det fortsatt er mangler i kontrollen av rettighetshavere for foretak med kompleks eierstruktur.

I tråd med EUs fjerde hvitvaskingsdirektiv er det planlagt å ferdigstille et nasjonalt register over reelle rettighetshavere i begynnelsen av 2021. Foretak skal selv rapportere inn informasjon, og registeret skal bli et hjelpemiddel for rapporteringspliktige i arbeidet med å identifisere reelle rettighetshavere.[89] Regelverket knyttet til reelle rettighetshavere oppfattes imidlertid fremdeles som komplisert, særlig når det gjelder faktisk innflytelse og ikke bare eierandel. Basert på erfaringer fra arbeidsgiver- og arbeidstakerregisteret forventes det at etterlevelsen blir begrenset. Det er også overlatt til rapporteringspliktige å vurdere og verifisere informasjonen, noe som sår tvil om kvalitetssikringen av registeret.[90]

3.7.5. Asymmetri i ressursfordeling i regimet

Ansvars- og arbeidsbyrden for rapporteringspliktige og tilsynsorganer har økt. Mange av de store rapporteringspliktige har derfor etablert store avdelinger som arbeider med anti-hvitvaskingsarbeid, og antallet MT-rapporter øker årlig. Privat sektor har påpekt at det er utfordring at etatene som skal motta og agere på rapportene ikke er oppbemannet i samme takt. FATFs oppfølgingsevaluering fra 2019 anbefaler også at EFE utvider sin funksjon for strategisk analyse.[91]

3.7.6. Forbedringspotensial i bruken av finansiell etterretning

Et grunnleggende element i den samlede innsatsen mot hvitvasking er at finansiell etterretning blir analysert, og at resultatet av disse analysene blir videreformidlet til politiet, som benytter den i politiets øvrige etterretningsproduksjon, etterforskning og inndragning.

Kvaliteten på informasjon som mottas fra rapporteringspliktige påvirker potensialet for EFEs produkter og den videre oppfølgingen overfor politi eller kontrollmyndigheter. Det er en sårbarhet at det, på tross av en bedring i mange rapporter, fortsatt er varierende kvalitet og generelt svak kvalitet på MT-rapportene fra noen av de rapporteringspliktige. Sårbarheten i MT-rapporteringen ligger fremdeles vel så mye i hva som ikke rapporteres til EFE, som i innholdet i det som faktisk rapporteres.

Det har vist seg vanskelig å måle om informasjonen fra EFE, som blir formidlet som etterretningsinformasjon, blir brukt av politiet. Som et tiltak i den sammenheng har riksadvokaten utarbeidet en instruks for politiets bruk av informasjon fra EFE som fortsatt er i startfasen.[92] Ny funksjonalitet som gjør rapporteringen fra distriktene til EFE enklere må på plass, slik at politiets bruk av finansiell etterretning og oppfølging av straffesaker blir målbart.

Det registrerte antallet hvitvaskingssaker har vært lavt over tid. I mange tilfeller må komplekse saker avgrenses i etterforskningssporet av hensyn til effektivitet og ressursforhold. Dette kan medføre at etterforskningen ofte velger å fokusere på primærforbrytelsen, og ikke utvides til å involvere hvitvaskingsaktørene.

---

89 Regjeringen, «Proposisjon til Stortinget 117 S (2019-2020), Tilleggsbevilgninger og omprioriteringer i statsbudsjettet 2020», 2020:159.

90 ØKOKRIM, «Hvitvaskingskonferansen», 2019.

91 Financial Action Task Force (FATF), «5th Year Follow-Up Assessment Report of Norway», 2019.

92 ØKOKRIM, «Instruks om bruk av informasjon fra ØKOKRIM, enhet for finansiell etterretning (EFE) i politidistriktene», 15. februar 2017.

En annen årsak kan være mangel på kunnskap om finansiell etterforskning og om hvordan ulovlige pengestrømmer og hvitvasking foregår i Norge. Ettersom sakene krever noe økonomisk etterforskning og særskilt kompetanse, kan det finnes en oppfatning om at dette er saker som bør behandles av særskilte enheter i politiet, og ikke i den ordinære straffesaksporteføljen.

3.7.7. Økt bruk av teknologiske systemer

Det eksisterer flere anti-hvitvaskings- og compliance-program som identifiserer risikokunder og er forankret i hvitvaskingsreglementet. Samtidig som FinTech[93] har sine fordeler, skaper den økte bruken av teknologi nye sårbarheter for hvitvasking.[94] FinTech kan legge til rette for blant annet raske og anonyme transaksjoner med liten grad av ansikt-til-ansikt-relasjoner i finansiell sektor. Dersom innovasjon av nye produkter og tjenester ikke i tilstrekkelig grad tar hensyn til krav om kundetiltak og transaksjonsovervåkning, utgjør dette en sårbarhet for hvitvasking. Det forventes at bruken av digitale tjenester vil øke i en digital økonomi.[95] Påliteligheten til elektroniske systemer kan undergraves av for eksempel datatap som følge av uautorisert tilgang. Kriminelle aktører kan også misbruke digitale systemer ved for eksempelvis å bruke falske identiteter.[96]

PSD2, EUs reviderte betalingstjenestedirektiv, har bidratt til å øke tempoet innenfor finansteknologi i Norge. Ved innføringen av betalingsdirektivet PSD2 i 2018 ble finansinstitusjoner pålagt å tillate tredjepartsaktører tilgang til deres kunders lønnskonto etter samtykke. Direktivet gjør bankkundenes informasjon lettere tilgjengelig for leverandører som ønsker å utvikle nye tjenester som bygger på bankenes data og infrastruktur. Finanstilsynet vurderer ikke at de nye tjenestene, betalingsfullmektig og opplysningsfullmektig, i seg selv er tjenester som utgjør noen signifikant hvitvaskingsrisiko. Politiet anser imidlertid PSD2 og tredjeparter som en sårbarhet ved bedragerier.

---

93 FinTech (finansteknologi) er et paraplybegrep på innovative teknologier som skal forbedre eller erstatte dagens produkt- og tjenestetilbud innen bank- og finansnæringen.

94 Finanstilsynet, «Fintech og regulatorisk sandkasse», 2020.

95 European Commission, «Report from the commission to the European parliament and the council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities», 2019.

96 Financial Action Task Force (FATF), «Guidance on Digital Identity», 2020.

3.8. Risiko for hvitvasking i rapporteringspliktige sektorer

Antall innsendte rapporter om mistenkelige forhold (MT-rapporter) har økt betydelig de siste årene. Totalt sett mottok ØKOKRIM 11 500 MT-rapporter i 2019, en økning på 145 prosent i perioden 2015–2019. Banker og betalingsformidlingsaktører har formidlet høyest antall MT-rapporter. Den generelle økningen antas å ha sammenheng med høyere oppmerksomhet rundt viktigheten av etterlevelse av hvitvaskingsregelverket og implementering av en mer risikobasert tilnærming blant de rapporteringspliktige. Myndighetene har intensivert tilsynsarbeidet og oppfølgingen av de rapporteringspliktige sektorene. Finanstilsynet har også ilagt overtredelsesgebyr, som sannsynligvis har satt presedens og sendt tydelige signaler om konsekvensene ved brudd på den nye hvitvaskingsloven.

EFE opplever at de større aktørene med godt fagmiljø som rapporterer mange mistenkelige forhold innen hver sektor generelt har bedre rutiner og forståelse for både anti-hvitvaskingsregelverk og risikobildet. Både Finanstilsynet og EFE opplever likevel at risikoforståelse og kvalitet på rutiner og tiltak er sterkt varierende mellom aktører som for øvrig er sammenliknbare. Rapporteringspliktige som rapporterer hyppig har generelt bedre kvalitet på MT-rapportene enn rapporteringspliktige som rapporterer sjeldnere.

Risikovurderingen viser at banker og agenter for utenlandske betalingsforetak har den største risikoen for å bli utnyttet til hvitvasking. Betalingsforetak, kreditt- og finansieringsforetak, eiendomsmeglere, e-pengeforetak samt vekslere og oppbevaringstjenester for virtuell valuta har også en betydelig risiko for å bli utnyttet til hvitvasking.

Matrise risikovurdering rapporteringspliktige sektorer

	Trusselnivå	Sårbarhetsnivå	Konskvensnivå	Risiko
Banker				Høy
Agenter for utenlandske betalingsforetak				Høy
Betalingsforetak				Betydelig
Kreditt- og finansieringsforetak				Betydelig
Eiendomsmeglere				Betydelig
E-pengeforetak				Betydelig
Veksling og oppbevaring av virtuell valuta				Betydelig
Regnskapsførere				Moderat
Revisorer				Moderat
Verdipapirforetak				Moderat
Forsikringsforetak og forsikringsformidlere				Moderat
Advokater				Moderat
Innenlandske spillselskap				Lav

3.8.1. Banker

Banker tar imot innskudd og andre tilbakebetalingspliktige midler fra allmennheten, yter kreditt og stiller garantier for egen regning. De tilbyr også betalingstjenester, og vil på grunn av dette være inngangspunktet for det meste av utbyttet fra kriminalitet som plasseres i finanssystemet. Andre rapporteringspliktige vil også bruke banksystemet for å gjennomføre betalinger i sin virksomhet. Norske banker varierer i størrelse, og også i tjeneste- og produktspekter og eksponering for hvitvaskingsrisiko. I 2019 ble det meldt inn 7959 MT-rapporter fra banksektoren. Det er en prosentvis økning i rapportering på 10 prosent fra 2018–2019 og en økning på 61 prosent fra perioden 2015–2019. Den største andelen av MT-rapportene kommer fra de store bankene, mens mindre banker med færre kunder sender færre MT-rapporter.

Trusler
Både plassering og flytting av midler i banker utgjør en trussel for hvitvasking. Hvor avansert hvitvaskingsmodus de kriminelle bruker vil variere med beløpsstørrelsen, egenskaper og kontrolltiltak knyttet til produktene eller tjenestene som brukes til plassering eller flytting av midlene.

En utbredt modus er overføring av utbytte ved banktransaksjoner innenlands og utenlands. Midlenes opprinnelse kan bli tilslørt via et nett av strømenn ved å overføre midler til kontoer i ulike finansinstitusjoner, eksempelvis ved å utnytte sårbare personer og personer som låner ut identiteten sin mot en andel av utbyttet. Tilbakebetaling av illegalt utbytte tilslørt som falske lån til bakmannsapparatet er også en kjent hvitvaskingsmodus. Bruk av falsk ID og falske dokumenter vanskeliggjør bankenes anti-hvitvaskingsarbeid.

EU-kommisjonens overnasjonale risikovurdering (SNRA) peker på at den iboende risikoen for hvitvasking er høyere for tjenester rettet mot bedriftsmarkedet enn i personmarkedet, fordi både transaksjoner og forhold knyttet til reell rettighetshaver er mer komplekse enn i privatmarkedet.[97] Det er en trussel at norske kontoer benyttes som uttakskontoer og gjennomstrømmingskontoer av både norske og utenlandske aktører. Økte overføringer til kryptovekslere eller betalingsformidlere medfører også en forhøyet risiko og vanskeliggjør kontroll. Det har vært tilfeller hvor større banker er blitt misbrukt til profesjonell hvitvasking fra utenlandske aktører, der hvitvaskeren ikke har et kundeforhold hos banken, men eksempelvis benytter et norsk selskap som mellomledd.

Private banking er en samlebetegnelse for konsepter hvor banken tilbyr pakkeløsninger av spesialtilpassede banktjenester for velstående kunder, slik som brukskonto, lån og investerings- og skatterådgivning. SNRA-en vurderer at kombinasjonen av sofistikerte produkter og rådgivningstjenester gjør risikoen for misbruk høy.[98]

Aktører som utnytter støtteordninger knyttet til COVID-19 overfører ofte midlene til bankkontoer. Også utbytte fra bedrageri går i mange tilfeller via bankkontoer.

Sårbarheter
Bankenes etterlevelse av hvitvaskingsregelverket varierer. Risikovurderinger skal ligge til grunn for bankenes tiltak og rutiner på hvitvaskingsområdet. I mange tilfeller er de imidlertid lite utfyllende og gir etter Finanstilsynets oppfatning ikke en korrekt vurdering av den konkrete banks hvitvaskingsrisiko.[99]

---

97 U-kommisjonens overnasjonale risikovurdering 2019, s. 54.

98 uropean Commission, «Report from the commission to the European parliament and the council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities», 2019:57.

99 Finanstilsynet, «Vedtak om overtredelsesgebyr – Åfjord Sparebank», 18. jun. 2020.

Finanstilsynet erfarer videre at bankenes rutiner i enkelte tilfeller er mangelfulle eller ikke etterlever kravene. Det sees særlig at rutinene ikke tar utgangspunkt i risikovurderingene, og at de i begrenset grad faktisk veileder de ansatte i konkret oppgaveutførelse. Finanstilsynet erfarer at de største bankene og filialene i for liten grad innhenter og bekrefter informasjon om reelle rettighetshavere, noe som resulterer i mangelfulle risikovurderinger og risikoklassifiseringer av kunder og feilslåtte kundetiltak, for eksempel mot selskaper med komplekse eierstrukturer og kunder som bruker skatteparadis.

EFE ser en utvikling der store banker har økt innsatsen på anti-hvitvasking, særlig i implementeringen av kontrollmekanismer. Dette medfører imidlertid at enkelte kriminelle flytter sitt kundeforhold til mindre banker.

Finanstilsynets erfaring er at bankenes transaksjonsovervåkningssystemer og bruken av dem har forbedringspotensial. De rapporteringspliktige kjenner ikke til, eller benytter ikke, all funksjonalitet. Finanstilsynet erfarer også at bankene ikke bruker tilstrekkelige ressurser til å sette regler tilpasset egen virksomhet og risiko i systemene. Det er krevende å utvikle gode regler for systemene. Tilsynet har også funnet eksempler på mindre banker som ikke lagrer informasjon om undersøkelser og vurderinger som danner grunnlag for MT-rapporter eller alarmer i transaksjonsovervåkning som er blitt lukket.[100] I kombinasjon med en ofte noe lavere fagkompetanse på hvitvasking hos mindre banker, samt underrapportering av mistenkelige forhold, er det grunn til å tro at enkelte banker ikke evner å identifisere alle forhold som bør undersøkes og rapporteres.

Overføring fra utlandet

3 millioner i utbytte fra bedragerier i utlandet er overført fra utlandet, til mottakers konto i Norge, før det i løpet av to dager er ført videre til flere andre privatkontoer og videre til kjøp av kryptovaluta hos flere ulike forhandlere. Det er benyttet falsk dokumentasjon for opprinnelsen til midlene (salg ev eiendom i utlandet), og minst en av kontohaverne i Norge er utsatt for ID-tyveri. Dette ble oppdaget da vedkommende sperret sin konto.

Overtredelsesgebyrer til tre banker for brudd på hvitvaskingsloven

Finanstilsynet ila tre overtredelsesgebyr til norske banker for brudd på bestemmelser i hvitvaskingsloven i 2019. Komplett Bank, Santander Consumer Bank og Hønefoss Sparebank fikk hhv. 18, 9 og 1,5 MNOK i gebyr. Bakgrunnen for ileggelse av gebyrene var alvorlige mangler knyttet til risikovurderinger, rutiner på hvitvaskingsområdet transaksjonsovervåkning, løpende kundetiltak og rapportering av mistenkelige transaksjoner til Økokrim.

Risiko

Totalt vurderes risikoen for at banker utnyttes til hvitvasking for å være høy. De mest vanlige produktene innen personmarkedet og bedriftsmarkedet antas å være mest utsatt for hvitvasking på grunn av antallet kunder med tilgang til tjenesten og at de er enkle å bruke. Enkeltinnskudd av kontanter anses fremdeles å ha høy risiko for hvitvasking, men volumet av transaksjoner er ikke lenger så store.

Mer avanserte bankprodukter i bedriftsmarkedet kan anvendes i tilsløringsfasen hvis kriminelle først får tilgang til dem gjennom for eksempel strømenn eller selskapsstrukturer. I bedriftsmarkedet er trade finance-produkter til utenlandske virksomheter et produkt med høy risiko. Det skyldes dels mangelfull identifisering av reelle rettighetshavere, grunnet ikke-transparente eierskapsstrukturer og betydelige summer.

[100] Finanstilsynet 18.06.20, Vedtak om overtredelsesgebyr.

3.8.2. Agenter av utenlandske betalingsforetak

De største aktørene i det norske betalingsoverføringsmarkedet er agenter for utenlandske betalingsforetak som opererer i Norge på grunnlag av konsesjon fra sitt hjemland. Western Union, Moneygram og Ria er de utenlandske betalingsforetakene med flest agenter i Norge. Agentene er som regel mindre foretak, særlig kiosker, dagligvarebutikker og reisebyrå.

Trusler
Agenter av utenlandske betalingsforetak benyttes ofte for å overføre utbytte av kriminalitet til høyrisikoland. De benyttes også i forbindelse med bedragerisaker på sosiale medier. Penger overføres da til en konto i en norsk bank som innehas av en utenlandsk betalingsformidler med konsesjon. Midlene føres deretter sannsynligvis ut av landet.

Sårbarheter
De utenlandske betalingsforetakenes oppfølging av forpliktelsene etter hvitvaskingsloven oppfattes ikke som tilstrekkelig. De baserer seg i stor grad på bruken av transaksjonsovervåkingssystemer. Bruken av disse kombineres sjelden med manuelle kundetiltak utført av agentene. Manglene i utførelsen av kundetiltak både sentralt i betalingsforetakene og hos agentene gjør dem ekstra sårbare for hvitvasking.[101]

Utførsel av kontanter

En norsk statsborger ankom Gardermoen høsten 2019 for utreise til Dubai. Personen la frem utfylt skjema for deklarering av 14 millioner NOK på vegne av et betalingsforetak som hadde konsesjon fra Finanstilsynet. Koffertene tilhørende personen inneholdt utelukkende norske sedler. Ved ankomst Dubai ventet representant fra samarbeidsforetak som mottok koffertene med pengene. NOK ble deretter konvertert til USD og fraktet videre til Somalia.

Til sammen transporterte personen fem ganger i løpet av én måned, for samme foretak, penger i størrelsesorden fra 6 millioner NOK til 14 millioner NOK.

Tilsynsmyndighetene i landet hvor det utenlandske betalingsforetaket har konsesjon har ansvaret for kontroll med etterlevelsen på hvitvaskingsområdet. Finanstilsynet erfarer at enkelte hjemlandsmyndigheter ikke foretar selvstendige vurderinger av om en agent bør avregistreres. Bekymringsmelding fra vertslandet videreformidles til betalingsforetaket, og foretaket avgjør hvorvidt melding om avregistrering skal sendes. Agenter av utenlandske foretak har en stor kontantandel i sin omsetning. Enkelte av foretakenes utfordringer med å skaffe kundeforhold i banker gjør at de benytter seg av pengetransporter for å frakte kontanter til utlandet. Dette medfører redusert kontroll med pengene, siden de enkeltstående transaksjonene ikke blir registrert i valutaregisteret, og at informasjon om avsender og mottaker forblir uregistrert.

Risiko
Risikoen knyttet til hvitvasking for agenter av utenlandske betalingsforetak anses som høy, da en vesentlig andel av transaksjonene betales med kontanter hvor midlenes opprinnelse er ukjent. Midlene sendes i stor grad til sluttdestinasjoner som anses som høyrisikoland. Sektoren har store sårbarheter knyttet til kundekontroll. Når et foretak er agent for flere betalingsforetak, øker risikoen for sammenblanding av midler, som vil bidra til å gjøre identifisering av midler mer utfordrende.

[101] Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», juli 2019:10-11.

3.8.3. Betalingsforetak

Betalingsforetak kan tilby betalingstjenester, herunder innskudd og uttak av kontanter fra konto, gjennomføring av betalingstransaksjoner, utstedelse av betalingsinstrument, pengeoverføringer og så videre. Betalingsforetak med norsk konsesjon får enten innvilget full eller begrenset tillatelse. Femten foretak har full betalingsforetakskonsesjon, ni foretak har begrenset konsesjon for betalingsformidling.[102] Enkelte norske betalingsforetak er etablert for å understøtte andre tjenester, eksempelvis låneformidlings- eller e-pengeforetak, eller inkasso. Disse aktørene er få og omsetter for mindre beløp.

Trusler

Betalingsforetak benyttes ofte for å overføre store beløp ut av landet. I noen tilfeller kamufleres opphavet til kontantutbytte fra kriminalitet som pengeinnsamling. For å unngå sporbarhet forekommer feilrapportering av fødselsnumre og registrering av transaksjoner på fiktive eller misbrukte identiteter.

Norske betalingsforetak og agenter av betalingsforetak benytter utenlandske betalingsformidlere som et tilslørende ledd for gjennomføring av transaksjoner til utlandet.

Sårbarheter

Finanstilsynet har ved tilsyn funnet at betalingsforetaks etterlevelse av hvitvaskingsregelverket er mangelfull og utdatert, og at interne kontrollrutiner ikke overholdes i praksis.

Enkelte betalingsforetak overfører transaksjoner til samarbeidspartnere i utlandet i bulk. Den utenlandske samarbeidspartneren splitter opp beløpene og videresender dem til sluttmottagerne. Noen banker har nå lagt begrensninger på praksisen med bulktransaksjoner. «Straksbetalinger» er også en sårbarhet, fordi det muliggjør pengeoverføringer så raskt at det blir utfordrende å stanse, undersøke og rapportere mistenkelige transaksjoner i henhold til regelverket.

Tilbakekall av betalings-foretaket TTCs konsesjon

Finanstilsynets anti-hvitvaskingstilsyn avdekket blant annet at foretaket ikke hadde en foretaksspesifikk risikovurdering, utdaterte og utilstrekkelige anti-hvitvaskingsrutiner og at det ikke overholdt undersøkelses- og rapporteringsplikten.

Foretaket hadde dessuten gjennomført en rekke transaksjoner ved hjelp av misbrukte identiteter, noe Finanstilsynet mente belyste foretakets svært mangelfulle internkontroll. Fordi foretaket hadde blitt nektet å gjennomføre bulktransaksjoner av sin bankforbindelse, fraktet dessuten foretaket midlene fysisk i og ut av Norge på en uforsvarlig måte, noe Finanstilsynet anså som brudd på forsvarlighetskravet i finansforetaksloven.

Foretaket har klaget inn tilbakekallet til Finansdepartementet. Saken er dermed ikke avgjort.

Risiko

Risikoen for hvitvasking gjennom betalingsforetak vurderes totalt som betydelig. Den utbredte bruken av kontanter og utilstrekkelige kundetiltak øker risikoen.

[102] Bille Finance AS, Capital Express Yaseen, Gele Money Transfer, BMT Norway Mohammadi, Humbul AS, IMT Consulting AS, Lex FInans AS, Nordic Finance AS og Taran Express Money Transfer AS.

3.8.4. Kredittforetak og finansieringsforetak

Kredittforetak og finansieringsforetak rommer ulike forretningsmodeller og har ulike risikoer og sårbarheter knyttet til hvitvasking. Kredittforetakene kjennetegnes ved at de kan finansiere sin virksomhet ved å motta andre tilbakebetalingspliktige midler enn innskudd og yte kreditt og stille garantier for egen regning. 23 av de totalt 32 selskapene med kredittforetakskonsesjon er såkalte boligkredittforetak, hvor bankene har flyttet hele eller deler av sin boliglånsvirksomhet. Tillatelse til å drive virksomhet som finansieringsforetak kan omfatte blant annet leasing, factoring, valutavirksomhet og annen finansieringsvirksomhet.

Trusler

Kredittforetak og finansieringsforetak kan brukes til å hvitvaske midler gjennom nedbetaling av lån, leasingforpliktelser eller fakturaer med bruk av utbytte fra straffbare forhold. Unormal nedbetaling av ulike typer lån eller øvrige forpliktelser er imidlertid moduser som rapporteringspliktige er godt kjent med og som kan fanges opp av transaksjons- og porteføljeovervåkning.

Overføring fra utlandet

Det ble foretatt overføringer til en norsk kunde fra to shippingselskap. Selskap 1 var registrert i et skatteparadis i Karibia. Overføringene ble gjennomført av et selskap fra et øst-europeisk land som er bøtelagt grunnet manglede etterlevelse av hvitvaskingsregelverket. Selskap 2 er registrert på Kypros med eiere som har roller i over 600 ulike selskap.

Kredittforetak kan også benyttes til å overføre midler mellom flere foretak og personer. Høyrisikokunder har høye og mange innbetalinger som på kort tid tas ut av kontoen igjen. Bruken av virtuelle valutaer og muldyr er moduser som benyttes for å kamuflere hvitvaskingen. I mange tilfeller overføres penger innenlands direkte til kunders kontoer eller via en betalingsformidler ut av landet.

Et norsk finansieringsforetak leverte i juli 2020 inn sin konsesjon på bakgrunn av at det hadde levert utenlandsk valuta for en verdi av 500 millioner DKK til en rekke danske vekslingskontor. Vekslingskontorene ble etterforsket av dansk politi for hvitvasking og heleri i stor skala. Foretaket etterlevde blant annet ikke krav til kundekontroll, løpende oppfølging, undersøkelser og rapportering i forbindelse med kundeforholdene med vekslingskontorene.[103]

Sårbarheter

Kredittkort er særlig sårbart for å misbrukes til hvitvasking siden det kan benyttes på tvers av landegrenser.

Risiko

Risikoen knyttet til kredittforetak og finansieringsforetak vurderes som betydelig. Det er imidlertid store variasjoner i risiko blant finansieringsforetakene siden produktene er av ulik art. Manglende kontroll med at selskapet som har kjøpt varen i realiteten er selskapet som betaler for varen, øker risikoen for hvitvasking. Finanstilsynet vurderer at tre av finansieringsforetakene driver valutavirksomhet hvor risikoen for hvitvasking er høy.

[103] Finanstilsynet, «Endelig tilsynsrapport – Loomis Foreign Exchange AS», 7. juli 2020.

3.8.5. Eiendomsmeglere

Eiendomsmeglere, eiendomsmeglingsforetak samt rettshjelpere og advokater som driver eiendomsmeglingsvirksomhet omfattes av hvitvaskingsregelverket. Eiendomsmeglingsforetak og advokater som driver eiendomsmegling formidlet i 2019 rundt 167 000 eiendommer, til en verdi av i overkant av 616 milliarder kroner. Per august 2020 var det 527 foretak (med totalt 624 avdelinger) med tillatelse til å drive eiendomsmeglingsvirksomhet. I tillegg har Finanstilsynet tilsynsansvar for 898 advokater som har stilt sikkerhet for å drive eiendomsmeglingsvirksomhet, tre rettshjelpere som oppfyller vilkår for eiendomsmeglingsvirksomhet samt 6069 eiendomsmeglere og jurister med tillatelse til å være ansvarlig megler. Det er en betydelig økning i rapporter om mistenkelige forhold. Antallet har økt fra 45 i 2015 til 880 i 2019.

Trusler

Fast eiendom er kapitalintensiv, og hvitvasking av store beløp kan gjennomføres i én operasjon. Store illegale beløp kan investeres i fast eiendom, og deretter re-investeres og integreres i den legale økonomien med relativt liten risiko for tap ved senere salg eller utleie av eiendommen. Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) legger for eksempel til grunn at halvparten av nettverkene knyttet til arbeidslivskriminalitet i Norge investerer kriminelt utbytte i fast eiendom. I andre tilfeller er eiendommen ervervet med legale midler, men renoveres med illegale midler og svart arbeid. Ved salg eller utleie av eiendommen utført av en megler hvitvaskes det ulovlige utbyttet.

Det foregår også såkalt «svingdørssalg», der eiendomsverdier manipuleres og eiendommer omsettes hyppig med ubegrunnet verdiøkning. Det kan også oppføres at deler av kjøpesummen består av inventar og utstyr som er vanskelig å prise. Ulovlig utbytte plasseres i fast eiendom gjennom stråmenn eller lovlige selskaper, noe som vanskeliggjør identifiseringen av reelle rettighetshavere.[104] Bud og avtaler som går utenom megler, oppgjør som gjennomføres med kun egenkapital, endring av eierforhold etter kontraktsinngåelse, overføringer fra utlandet, salg før visning og salg etter at kjøper har tatt direkte kontakt med selger er indikatorer på at eiendommer benyttes til å hvitvaske utbytte.

Bruk av blanco-skjøter

Privatpersoner kjøper eiendom, og overdragelsen foretas ved bruk av blanco-skjøter, dvs. at kjøpers navn ikke registreres på skjøte, kun i bakenforliggende avtaler.

Hensikten til kjøper er å renovere eiendommen og selge den videre med fortjeneste, uten at vedkommende er registrert i offentlige registre. Det vil kun være opprinnelig selger og ny kjøper som er registrert i Eiendomsregisteret.

I mange tilfeller kommer oppgjøret til selger fra andre personer/selskaper enn kjøper.

Det er også registrert at samme person har kjøpt mange eiendommer i løpet av kort tid, fordelt på ulike meglere, og i noen tilfeller fremstår det som organisert ved at flere personer samarbeider om finansieringen, «private lån» eller at oppussingsarbeidet gjennomføres av dem selv eller er uregistrert.

Utferdigelse av verdivurderinger kan også være en tjeneste som benyttes av kriminelle for å hvitvaske illegale midler.

ØKOKRIM har vurdert at det er økt trussel for at kriminelle aktører vil søke å plassere midler i eiendomsmarkedet på grunn av koronapandemien.

[104] Finanstilsynet, «Veiledning til etterlevelse av hvitvaskingsregelverket i eiendomsmeglingsvirksomhet», 2019.

Sårbarheter
Finanstilsynet har siden 2016 gjennomført 84 tilsyn hvor eiendomsmeglingsvirksomhetenes anti-hvitvaskingsarbeid er undersøkt, og hvor en rekke svakheter er avdekket. Etter det Finanstilsynet erfarer, har de fleste eiendomsmeglingsforetak nå etablert et anti-hvitvaskingssystem. Advokatmeglerne har i noen grad etablert et anti-hvitvaskingssystem.

Finanstilsynet har avdekket mange svakheter i virksomhetenes etterlevelse av hvitvaskingsregelverket. Det er manglende sammenheng mellom risikovurderingen og de rutinene som er etablert. Ofte er ikke virksomhetens hvitvaskingsrisiko vurdert eller analysert, risikovurderingen er svært mangelfull eller ikke tilpasset den faktiske virksomheten. Virksomhetenes rutiner er ofte svært mangelfulle. Det avdekkes eksempelvis mangler knyttet til grunnleggende kundetiltak, som innhenting av informasjon om formålet med transaksjonen, midlenes opprinnelse, hvem som betaler og mottar kjøpesum og reelle rettighetshavere. Det henger trolig sammen med at opplæring av hvitvaskingsansvarlig og ansatte ikke er gjennomført, eller er begrenset til opplæring i utfylling av kontrollpunkter i meglersystem og gjennomføring av identitetskontroll. Dette medfører manglende kunnskap om hvitvaskingsmoduser og evne til å avdekke indikasjoner på mistenkelige transaksjoner.

Rutiner for å kontrollere egen etterlevelse er få og mangelfulle. Bruk av meglersystemer sikrer ikke at det foreligger reelle vurderinger av risiko ved kunder og transaksjoner før det merkes av i systemet at kontroller er foretatt. Stikkprøvekontroller viser dessuten at tiltakene omtalt i rutinene i noen grad heller ikke gjennomføres.

Som ledd i anti-hvitvaskingsarbeidet gjennomførte Finanstilsynet i november/desember 2018 tematilsyn hos ni eiendomsmeglingsforetak – åtte næringsmeglingsforetak og ett boligmeglingsforetak. Hos sju av foretakene ble det avdekket så alvorlige brudd på hvitvaskingsregelverket at Finanstilsynet besluttet å ilegge disse overtredelsesgebyr.

Risiko
Totalt sett anses hvitvaskingsrisikoen for eiendomsmeglere å være betydelig. Risikoen er særlig knyttet opp til virksomhetens klientkonto. Risikoen for hvitvasking knyttet til ordinære salgsmeglingsoppdrag for bolig- og fritidseiendom anses å være lavere. Risikoen er større i tilfeller hvor eiendomsmeglere eller advokater som tilbyr eiendomsmeglingsoppdrag kun bistår med oppgjør, siden oppgjørsmegleren har mangelfull kjennskap til innholdet i avtalen, partene og salgsobjektet. Ved megling av rehabiliteringsprosjekter, nyboligprosjekter samt næringseiendommer er også risikoen vurdert som høyere.

Advokatmeglere vurderes å ha en generelt høyere risiko for hvitvasking og lavere sannsynlighet for å avdekke mistenkelige forhold. De har ofte rene oppgjørsoppdrag – også for boliger under oppføring, der de driver en begrenset virksomhet i et mindre foretak uten rammeverk i form av risikostyring og internkontroll eller innspill fra andre advokater. Og dersom det er etablert et anti-hvitvaskingssystem, er dette ofte ikke innrettet med tanke på eiendomsmeglingsvirksomheten.

3.8.6. E-pengeforetak

Med elektroniske penger («e-penger») menes en elektronisk lagret pengeverdi, som eksempelvis forhåndsbetalte kort, vouchers og e-lommebok. Forhåndsbetalte kort kan være personlige (identifisert kortholder) eller upersonlige (anonym kortholder). Vouchers minner om forhåndsbetalte kort, men er som regel en kode lagret på et elektronisk medium som har global rekkevidde. En e-lommebok er i all hovedsak en digital e-pengekonto, som består av ett eller flere betalingsinstrumenter, som eksempelvis Skrill, Apple Pay og Paypal. Flere e-pengeforetak har avtaler med kortselskaper som Visa og Mastercard for å sikre aksept av brukersteder. E-pengeforetak kan ha distributører som innløser og distribuerer e-penger på vegne av foretaket. EFE mottok totalt 25 MT-rapporter fra ett e-pengeforetak i 2019.

Trusler
E-lommebøker er særlig egnet til å flytte ulovlig ervervet utbytte til utlandet med begrenset sporbarhet, siden tjenesten er lett tilgjengelig på nett og kan benyttes i et stort utvalg av både norske og utenlandske brukersteder. Forhåndsbetalte kort og vouchers kan kjøpes anonymt med kontanter og er begrenset til relativt små beløp per kjøp. Det foretas ingen kundetiltak for denne typen kjøp, noe som utgjør en trussel i hvitvaskingssammenheng.[105] Politi- og kontrolletatene ser at flere kriminelle miljøer benytter seg av forhåndsbetalte kort fra utenlandske foretak for å hvitvaske utbytte.

Personer som betaler for overgrepsmateriale og live-streaming av seksuelle overgrep på nett benytter ofte internettbaserte betalingstjenester. En økning i kjøp av seksuelle overgrep på nett kan øke trusselen knyttet til bruk av e-pengeforetak.

Sårbarheter
De nyere betalingstjenestene som leveres av e-pengeforetak krever ofte ingen personopplysninger ved opprettelse av kundeforhold, og mange av tjenestetilbyderne er ikke rapporteringspliktige til norske myndigheter. Det er enkelt å bruke mellommenn og andres identitet. Ved innbetalinger og overføringer tydeliggjøres det heller ikke hvem som er avsender eller mottaker og hva transaksjonen omhandler.

Norske anonyme e-penger som tilegnes med kontanter og uten kundekontroll er begrenset til små beløp. Utenlandske anonyme og forhåndsbetalte kort har en vesentlig høyere beløpsgrense, noe som vil være attraktivt dersom brukeren ønsker å være anonym og skjule pengenes opphav.

Finanstilsynet erfarer at norske e-pengeforetak er bevisste på at det er unntak for kundekontroll for e-pengetjenester. Dette utnyttes av foretak som driver andre tjenester. I enkelte tilfeller har betalingstjenester blitt oppgitt som e-pengetjenester, og kundekontroll har ikke blitt foretatt.

Risiko
Risikoen vurderes som betydelig for bruken av e-pengeforetak i hvitvaskingssammenheng, når det angår norske forhåndsbetalte kort med lave beløpsgrenser. For utenlandske forhåndsbetalte kort er risikoen høyere, grunnet minimale restriksjoner på beløpsgrenser og trenden med økt etterspørsel fra Norge.

[105] Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», juli 2019:11-12.

3.8.7. Vekslingsplattformer og oppbevaringstjenester for virtuell valuta

Før rapporteringsplikten for vekslings- og oppbevaringstjenester trådte i kraft 15. oktober 2018 var det 10–15 mer eller mindre seriøse tilbydere i Norge. Kun et fåtall av de rundt 20 søkerne oppfylte kravene til registrering hos Finanstilsynet da registreringsplikten ble kunngjort. Per 25. mai 2020 er det hos Finanstilsynet registrert ni tilbydere av oppbevaring og veksling av virtuell valuta, som alle tilbyr krypterte virtuelle valutaer. Den 11. oktober 2019 innførte Finansdepartementet egnethetskrav etter hvitvaskingsregelverket for slike tilbydere.

Trusler

ØKOKRIM har observert tre ulike metoder der kriminelle benytter kryptert virtuell valuta (kryptovaluta) i et forsøk på å hvitvaske illegalt utbytte. Den første innebærer at kriminelle mottar en bankoverføring av ulovlig ervervede midler og ønsker å veksle den offisielle valutaen om til kryptovaluta, for deretter å sende utbyttet utenlands. Eventuelt veksles kryptovaluta som er utbytte fra en kriminell handling om til en offisiell valuta. Den andre metoden baserer seg på at et bedragerioffer veksler egen offisiell valuta til kryptovaluta, og sender dette til den kriminelle, eventuelt får veksleren til å gjøre dette.[106] Den tredje og siste metoden innebærer at kriminelle får kontroll over nettbanken til offeret og overfører penger derifra til seg selv via veksleren ved å utgi seg for å være offeret. Fellesnevneren er at det er vanskelig for veksleren å vite den offisielle valutaens opphav, eller om den som ønsker å veksle er et bedragerioffer. En økning i digital kriminalitet vil sannsynligvis gi økt trussel for at krypterte virtuelle valutaer blir brukt til hvitvasking.

Overførsler av utbytte fra bedrageri

Utbytte fra bedrageri på minst seks millioner kroner er fordelt ved overførsel til ti kontoer i fire banker, videreført til ytterligere kontoer før store deler av verdiene er overført til fem forskjellig forhandlere av kryptovaluta. Det er grunn til å anta at flere av bankkontoene er opprettet ved bruk av andre personers ID.

Transaksjonene er gjennomført i løpet av få dager, og kryptovaluta er ført videre til nye «wallets» – hvor mottaker ikke er kjent.

Sårbarheter

Det er en sårbarhet at regelverket er nytt og ikke implementert i hele EU. Vekslere av kryptovaluta er primært aktører med lite erfaring som mangler innarbeidede rutiner for rapportering av mistenkelige forhold. Flere av de registrerte vekslerne er små foretak med begrensede ressurser og kompetanse til å utføre kundekontroll. Det er en iboende sårbarhet at virtuell valuta er et digitalt og grensekryssende produkt, hvor vekslinger går raskt. Virtuelle valutaer som er anonyme eller delvis identifiserbare og mikset med andre valutaer vanskeliggjør sporbarheten på blokkjeden.

Risiko

Rapporteringspliktige tjenester med virtuell valuta vurderes å ha en betydelig risiko for hvitvasking.

[106] Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», juli 2019:21-22.

3.8.8. Regnskapsførere

Regnskapsførerbransjen omfatter 20–30 større regnskapsførervirksomheter og -grupperinger, men domineres av mindre virksomheter med få ansatte, herunder enkeltpersonforetak. Om lag 93 prosent av regnskapsførervirksomhetene har færre enn ti ansatte. [107] Det ble innrapportert 58 MT-rapporter fra regnskapsførere i 2019.

Trusler
Autoriserte regnskapsførere kan benyttes til å skape legitimitet for et foretak eller en person. Hvitvaskingsrisikoen er knyttet til regnskapsførerens evne til å forhindre eller avdekke hvorvidt oppdragsgiver er involvert i hvitvasking. Det krever mye erfaring og god kjennskap til en kunde før man gjenkjenner et transaksjonsmønster som indikerer hvitvasking. Regnskapsførere kan bli delaktig i hvitvasking ved oppdrag der regnskapsfører har fullmakt til å utføre betalinger på vegne av kunde og betaler eksempelvis fiktive fakturaer. Det har også forekommet at regnskapsførere har utarbeidet fiktive arbeidskontrakter og leiekontrakter. Virksomheter som benyttes til utnyttelse av COVID-19 støtteordninger øker trusselen.

Sårbarheter
Erfaring viser gjennomgående mangelfull kunnskap og oppmerksomhet rundt ulike trusler, særlig inngående kjennskap til at oppdragsgivere i enkelte bransjer kan utgjøre en trussel. Bransjen selv mener det er en sårbarhet at det eksisterende hvitvaskingsregelverket oppfattes som utfordrende og ikke som et tilstrekkelig verktøy for å opparbeide seg denne nødvendige kompetansen.

Bransjen peker også på at verifisering av opplysninger, særlig for utenlandske selskaper og statsborgere, er en utfordring. Det nasjonale eierskapsregisteret er heller ikke en tilstrekkelig kilde til å få oversikt over reelle rettighetshavere. Finanstilsynet peker også på manglende utarbeidelse av rutiner, retningslinjer og utpeking av hvitvaskingsansvarlig i foretakene.

Regnskapsførerforetak tilbyr også rådgivningstjenester, og det er ofte ved leveringen av slike tjenester at foretakene utnyttes som ledd i hvitvasking, særlig i forbindelse med skatte- og selskapsrådgivning.

Risiko
Risikoen forbundet med hvitvasking knyttes til regnskapsførerens evne til å forhindre eller avdekke at oppdragsgiver er involvert i hvitvasking og vurderes å være moderat. Det krever erfaring og kjennskap til en kunde før man gjenkjenner et transaksjonsmønster som indikerer hvitvasking. Nye kundeoppdrag innebærer derfor større risiko for å ikke oppdage hvitvasking. Mindre regnskapsførervirksomheter er mer utsatt for involvering i hvitvaskingsoperasjoner sammenlignet med større virksomheter. Større regnskapsvirksomheter har imidlertid større sjanse for å bli involvert i grensekryssende hvitvaskingsoperasjoner.[108] Når regnskapsførere opptrer i rollen som rådgiver, vurderes risikoen å være høyere.

[107] Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», juli 2019:48.
[108] Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», juli 2019:48.

3.8.9. Revisorer

Det følger av revisorloven § 1-2 at revisor er allmennhetens tillitsperson ved revisjon av revisjonspliktiges årsregnskap. Revisjonsbransjen er dominert av fem store revisjonsnettverk, som til sammen har en markedsandel på nærmere 70 prosent målt etter revisjonshonorar. I 2019 var det 12 revisjonsselskaper som hadde foretak av allmenn interesse, eksempelvis børsnoterte selskaper, banker og forsikringsselskaper, som revisjonsklienter. I 2019 ble det formidlet 45 MT-rapporter fra revisorer.

Trusler
Godkjente revisorer kan bli benyttet til å skape legitimitet for et foretak. Revisorer kan tilrettelegge for at kunden på egenhånd eller i samarbeid med andre hvitvasker ulovlig utbytte. Fiktiv fakturering, skatte- og avgiftsunndragelse, arbeidslivskriminalitet samt tilsløring av reelle rettighetshavere og midlenes opprinnelses gjennom kompliserte selskapsstrukturer er moduser som er mye brukt for hvitvasking gjennom revisorer. Transaksjonen oppgis da som en ordinær post i oppdragsgivers regnskap. Virksomheter som benyttes i utnyttelse av COVID-19-støtteordninger øker trusselen.

Flere av tilsynsenhetene er tilknyttet internasjonale nettverk og har mange internasjonale oppdrag. Dette øker trusselen for å bli brukt som ledd i hvitvasking. Tilsyn har avdekket manglende kundetiltak utført overfor flere oppdragsgivere med internasjonal tilknytning.

Sårbarheter
Revisors gjennomgang skjer normalt etter at eventuelle hvitvaskingstransaksjoner har funnet sted. Det kan medføre at det er vanskeligere å avdekke ulovlige forhold.

Det er utarbeidet dokumentmaler av bransjeforeningen for å bidra til etterlevelse av hvitvaskingsregelverket. Det meldes imidlertid om vesentlige mangler ved tilpassing av slike maler til den enkelte virksomhet, og særlig for risikovurdering og rutiner. I tillegg synes det å være generelt liten oppmerksomhet rundt hvitvaskingslovgivningen og mangelfull kunnskap om at oppdragsgivere i enkelte bransjer kan utgjøre en trussel.

Enkelte revisorer anser at mer automatiserte transaksjoner/betalinger, også over landegrensene, på noen måter kan gjøre det lettere å gjennomføre hvitvasking. Samtidig blir transaksjonene mer sporbare i disse systemene, noe som kan gjøre hvitvasking vanskeligere.

Revisjonsselskaper tilbyr også rådgivningstjenester, og det er ofte ved levering av slike tjenester at foretakene utnyttes som ledd i hvitvasking, særlig i forbindelse med skatte- og selskapsrådgivning.

Risiko
Risikoen for hvitvasking vurderes som moderat. Liten grad av aktsomhet fra revisor kan imidlertid føre til at tillit etableres til virksomheter som er involvert i hvitvasking. Mindre revisjonsvirksomheter er generelt mer utsatt for å bli utnyttet til hvitvasking sammenlignet med større virksomheter, som er del av et nettverk og kjennetegnes av høy profesjonalitet. Større revisjonsvirksomheter som inngår i et internasjonalt nettverk er derimot utsatt for å bli involvert i multinasjonale hvitvaskingsoperasjoner.

3.8.10. Verdipapirforetak

Verdipapirforetak opptrer som mellommenn i verdipapirmarkedet og tilbyr investeringstjenester knyttet til finansielle instrumenter etter tillatelse fra Finanstilsynet. Verdipapirforetakene har en svært sentral rolle i annenhåndshandelen med finansielle instrumenter (fondsmegling) og ved tilrettelegging av emisjoner i førstehåndsmarkedet (corporate-virksomhet). Verdipapirforetakene tilbyr også investeringsrådgivning, analysevirksomhet og garantistillelse for fulltegning av emisjoner, og de driver også aktiv forvaltning av investorers portefølje på individuell basis og etter investors fullmakt. I juni 2020 var det 227 norske verdipapirforetak med konsesjon fra Finanstilsynet.

Trusler
Det eksisterer få observasjoner av hvitvasking på verdipapirområdet.

Det kan genereres ulovlige midler gjennom verdipapirmarkedet, eksempelvis gjennom markedsmisbruk, innsidehandel eller bedrageri.[109] Verdipapir kan også benyttes til å hvitvaske midler ved at aksjer handles med utbytte fra en straffbar handling. Aksjene selges senere, og beløpet overføres til en aksje- eller lønnskonto.

Eierskap til aksjer kan også overføres som betaling for ulovlige tjenester. Meglerhus kan bli bedt om å overføre et gitt antall aksjer i et selskap til en ny eier med instruksjon om at oppgjør har funnet sted. Når ny eier selger aksjene, er de hvitvasket. Det kan også være at det omsettes andeler i rene skallselskaper med hensikt om hvitvasking, innsidehandel, markedsmanipulasjon eller annen verdipapirsvindel.

Utenlandske investeringer

Et verdipapirforetak har opplyst at en av deres meglere mottok informasjon om at en kunde ønsket å plassere deler av sin formue, nærmere 10 millioner kroner, i norske verdipapirer. Kunden opplyste i meglersamtalen at det er en fordel om handelen ble registrert på VPS-kontoen tilhørende hans samboers selskap, siden han selv ikke har offisiell norsk adresse og heller ikke ønsker å ha norsk konto. Formuen var plassert på kontoer i Sveits og «karibiske øyer» tilhørende ulike stiftelser hvor det ikke er klart hvem som er reelle rettighetshavere, men det fremgår at ovennevnte person har kontroll på kontoene. Det er ikke kjent hvordan formuen er etablert.

Sårbarheter
Tilsyn med verdipapirforetak, forvaltningsselskaper og AIF-forvaltere har avdekket forhold som muliggjør hvitvasking og forhold der det burde vært rapportert mistanke om hvitvasking. Det har også blitt avdekket manglende bevissthet om regelverk, svake risikovurderinger og mangelfullt rutineverk, samt manglende eller mangelfull dokumentasjon på kontroller.

Risiko
Risikoen for hvitvasking vurderes som moderat for verdipapirforetak. Uregulerte markedsplasser er imidlertid eksponert for høyere hvitvaskingsrisiko enn regulerte, særlig der eierskapet i unoterte aksjer er registrert hos utsteder eller hos foretak som ikke er en verdipapirsentral.

[109] Financial Action Task Force (FATF), «Guidance for a risk-based approach for the securities sector», 2018:24.

3.8.11. Forsikringsforetak og forsikringsformidlere

Forsikringsforetak er som regel livsforsikringsforetak, skadeforsikringsforetak eller kredittforsikringsforetak. Skadeforsikring omfattes ikke av EUs hvitvaskingsdirektiv, og det anses dermed ikke som et risikoområde i forhold til hvitvasking i EU-sammenheng. Hvitvaskingsforskriften gir for øvrig unntak fra krav om kundetiltak ved tegning av skadeforsikringspoliser, reiseforsikringspoliser og kredittforsikringspoliser. Hvitvaskingsloven omfatter ikke pensjonskasser. Forsikringsformidlere, hhv. forsikringsagenter og forsikringsmeglere, er aktører som enten selger forsikringer på vegne av forsikringsselskapene, eller som skal forhandle forsikringsavtaler på vegne av kundene. Antallet rapporter om mistenkelige transaksjoner fra forsikringsselskaper har vist en klar økning fra 2014. Fra 2018 til 2019 ble antallet rapporter omtrent doblet, fra 108 rapporter i 2018 til mer enn 259 rapporter i 2019. Det er et fåtall av de store selskapene som rapporterer mest.

Trusler

For å foreta hvitvasking gjennom et forsikringsforetak må kunden innbetale premie til foretaket, og foretaket må foreta utbetaling til kunden eller en tredjemann. Innbetaling av premie på normal måte med midler som er utbytte fra straffbare handlinger vil være hvitvasking. Ved tjenestepensjon vil betaling av premie med ulovlig ervervede midler kunne være en «effektiv» måte å hvitvaske midler på.

Falske fakturaer

Et dataselskap meldte fra om innbrudd, og et krav om forsikringsutbetaling for datautstyr for 1 056 000 kr ble dokumentert med fakturaer fra et annet firma. Utredningen viste at fakturaene var falske, og at datautstyret opprinnelig var tyvegods.

I livsforsikring er det i mange tilfeller ikke kun risikopremie som innbetales, men også innbetalinger til sparing/investering. Dette er midler som skal komme til utbetaling på et senere tidspunkt. Det er særlig individuelle livsforsikringsavtaler som kan ha en noe forhøyet grad av hvitvaskingsrisiko.

Forsikringsforetak kan også utnyttes til hvitvasking ved bruk av «feilinnbetaling» av forsikringspremie, med etterfølgende tilbakebetaling av midlene, og ved at det tegnes forsikring på objekter som er kjøpt med utbytte fra en straffbar handling. Når det utbetales erstatning for skade på det forsikrede objektet, innebærer forsikringsutbetalingen at objektet hvitvaskes.

Sårbarheter

Tilsyn har i liten grad avdekket hvitvasking eller forhold der det burde vært rapportert mistanke om hvitvasking. Imidlertid er det funnet mangler ved risikovurderinger, rutiner og etterlevelse, slik at det trolig er forhold som ikke er blitt oppdaget.

Risiko

Det er samlet sett moderat risiko knyttet til hvitvasking i forsikringsbransjen. Individuelle livsforsikringsavtaler med stort innslag av spare-/investeringselement har en noe høyere risiko for hvitvasking på grunn av muligheten til å innbetale store beløp og fleksibiliteten i forbindelse med uttak.[110] Skadeforsikring har lav risiko. Når forsikring omsettes via mellomledd, øker risikoen fordi det kan medføre en ansvarspulverisering, hvor forsikringsformidleren kan anta at forsikringsselskapet utfører kundetiltakene og vice versa. En økende grad av sammenblanding av ulovlig og lovlig virksomhet vil også medføre økt risiko for at ulovlige midler kan benyttes til betaling av forsikringspremie.

[110] Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», juli 2019:8-9.

3.8.12. Advokater

Advokater er rapporteringspliktige når de på vegne av klient utfører finansielle transaksjoner, bistår ved planlegging eller utføring av transaksjoner for en klient i forbindelse med kjøp og salg av fast eiendom eller virksomhet, forvaltning av en klients penger, verdipapir eller andre aktiva. De er også rapporteringspliktige ved åpning eller forvaltning av bank- eller verdipapirkonto, fremskaffelse av nødvendig kapital til opprettelse, drift eller ledelse av selskap, og ved opprettelse, drift eller ledelse av selskap, fond eller lignende juridisk person eller formuesmasse, herunder utenlandsk trust eller tilsvarende juridisk arrangement. Advokater er også rapporteringspliktige når de opptrer som bostyrere (med unntak for ved konkurs).[111] Per 31. desember 2019 var 8200 personer registrert som praktiserende advokater.

Trusler

Advokatstanden nyter generelt høy tillit i samfunnet, og bruken av advokat til å foreta transaksjoner gir høy legitimitet. Advokaters klientkonto kan bli misbrukt til å hvitvaske midler. Internasjonale erfaringer viser at fiktive lån settes opp for å muliggjøre finansielle transaksjoner til og fra klienters kontoer, noe som bidrar til legitimeringen av ulovlige midler.

Sårbarheter

Bruk av advokaters klientkonto er ikke underlagt særskilt regulering når det gjelder hvilke typer transaksjoner advokaten kan bistå med. I tillegg er det svært vanlig å benytte en samlekonto, noe som vanskeliggjør identifiseringen av midlene dersom advokaten ikke har kontroll på innbetalinger og utbetalinger, samt hvem som er reell avsender og mottaker av slike midler.

Bruk av klientkonto

Advokaten bisto en person som hadde flyttet til utlandet for å unngå å betale skattegjeld med omsetning av kunst. Advokaten kunne ikke fremlegge dokumentasjon på at det var noen spesiell grunn til å benytte advokatens klientkonto som oppgjørskonto i forbindelse med kunsthandelen. Advokaten burde ha forstått at klientens behov for bistand hadde som formål å skjule den økonomiske virksomheten knyttet til kunsthandelen. Advokaten hadde i tillegg benyttet sin klientkonto som «bankkonto» for klienten og dermed holdt midler utenfor innsyn og kontroll for andre aktører.

Tilsynsrådet erfarer at flere mellomstore, små og nyetablerte advokatforetak ikke har rutiner tilpasset en reell risikoforståelse. I store og mellomstore advokatforetak har det vært tegn til holdningsendringer, men ved tilsynsbesøk er det tidvis blitt observert at det legges en for snever forståelse av hvitvaskingslovens anvendelsesområde til grunn.[112] Det er også blitt avdekket mangelfulle internkontrollrutiner.

Risiko

Risikoen for hvitvasking knyttet til advokater er vurdert å være moderat. Risikoen er større for advokater som har en høy andel transaksjoner til og fra klientkonto, og der advokaten har mangelfull kunnskap om bakgrunnen for en transaksjon, for eksempel der advokatens bistand er begrenset til å motta eller videreformidle et oppgjør. Uklarheter vedrørende hvitvaskingslovens rekkevidde leder også til svakere rutiner og økt hvitvaskingsrisiko.

[111] Bostyrere i konkurs er ikke omfattet av ny hvitvaskingslov, men er underlagt en rapporteringsplikt etter konkursloven § 122 a.

[112] Hvitvaskingsloven § 4 (2) c.

3.8.13. Innenlandske selskaper som tilbyr spilltjenester

Alle som arrangerer spill som krever tillatelse etter lotteriloven, pengespilloven eller totalisatorloven er omfattet av hvitvaskingsregelverket. Det er bare Norsk Tipping, Norsk Rikstoto og enkelte av de store landsdekkende lotteriene som kan tilby regulerte pengespill på nett fra Norge.

Trusler

Den vanligste modusen knyttet til hvitvasking gjennom norske spill er innskudd – enten kontant eller via overføring i kiosk – på kundens spillekonto, som deretter overføres til bankkonto uten vesentlig spillaktivitet. Illegalt utbytte kan tilsløres ved å gjennomføre en rekke kontantinnskudd hos flere forskjellige kommisjonærer. Forhåndsbetalte kort benyttes også som betalingsmiddel ved innsats/innskudd. Kontoutskriften viser ordinær gevinstutbetaling.

Kjøp av spillkvitteringer for å legitimere midlers opphav er også en kjent modus for hvitvasking i bingobransjen.

Hvitvasking i bingovirksomhet

Bingovirksomheter gir særlig handlingsrom til hvitvasking av kontantutbytte. En bingovirksomhet kan knyttes til kriminelle aktører. Bingovirksomheten har trolig hvitvasket utbytte fra kriminelle handlinger via bingospill, og ved at spillkort har blitt brukt til dette formålet. Pengeoverførsler viser at penger kanaliseres ut av bingovirksomheten til tilknyttede foretak i annen bransje.

Sportsspill og terminalspill er særlig utsatt for å bli brukt til hvitvasking på grunn av den høye gevinstandelen. Ved sportsspill kan også resultat manipuleres, noe etterforskning av større kampfiksingssaker i Europa har vist. Risiko for hvitvasking foreligger også ved bruk av lånte eller falske identiteter, og falske eller stjålne debetkort, ved registrering av spillekonto som kan benyttes til for eksempel oppbevaring av kriminelt utbytte.

Sårbarheter

Ved bruk av kontanter er det vanskelig å spore midlenes opprinnelse. Enkeltbeløpene er også gjerne små, og kommisjonærer har begrenset kompetanse og kapasitet til å avsløre hvitvasking.

Lotteritilsynet har gjennom sine tilsyn avdekket at aktører ikke har hatt tilstrekkelig gode risikovurderinger for å forebygge og avdekke hvitvasking. Mange risikovurderinger er generiske og tar ikke høyde for geografiske forhold, kunder og andre spesifikke risikoer. I flere kontrollerte bingovirksomheter hadde de ansatte ikke fått nødvendig opplæring.

Risiko

Risikoen for hvitvasking via innenlandske spillselskaper vurderes som lav. Risikoen vurderes imidlertid å være høyere for bingobransjen i og med at bingobransjen har en relativ stor kontantomsetning og kontanthåndtering, man kan spille anonymt og spillterminaler kan teoretisk sett manipuleres til å omgå regulatoriske krav. Dette øker risikoen for hvitvasking.

4. Risikovurdering terrorfinansiering

4.1. Oppbygning og metode

I terrorfinansieringsdelen av NRA 2020 er mye av oppbygningen lik de foregående publikasjonene når det gjelder struktur og inndeling av kapitler.

Det internasjonale og deretter det norske trusselbildet for terrorisme blir først presentert. Deretter blir de ulike truslene og sårbarhetene omtalt.

PST har arrangert møter og mottatt både skriftlige og muntlige innspill fra privat og offentlig sektor. Dette gjelder spesielt innspill til sårbarheter de ulike aktørene ser og erfarer. Sårbarhetene som blir presentert har i hovedsak vært omtalt i tidligere utgaver av NRA. Likevel er det mindre endringer og mer utfyllende informasjon i denne utgaven.

Noen av sårbarhetene som presenteres er også sammenfallende med sårbarheter innen hvitvasking. For å unngå gjentagelser vil vi henvise til aktuelle kapitler i den delen av NRA som omhandler hvitvasking.

4.2. Definisjon terrorfinansiering

Terrorfinansiering defineres i straffeloven § 135. For terrorfinansiering straffes den som rettsstridig yter, mottar, sender, fremskaffer eller samler inn penger eller andre formuesgoder med hensikt eller viten om at midlene helt eller delvis skal brukes

a. til å utføre en handling som nevnt i §§ 131, 134 eller §§ 137 til 144,
b. av en person eller gruppe som har til formål å begå handlinger som nevnt i § 131, § 134 eller §§ 137 til 144, når personen eller gruppen har tatt skritt for å realisere formålet med ulovlige midler,
c. av et foretak som noen som nevnt i bokstav b eier eller har kontroll over, eller
d. av et foretak eller en person som handler på vegne av eller på instruks fra noen som nevnt i bokstav b.

På samme måte straffes den som stiller banktjenester eller andre finansielle tjenester til rådighet for personer eller foretak som nevnt i første ledd bokstav b, c eller d. Straffeloven § 136 a rammer også elementer av terrorfinansiering: «(...) den som (...) yter økonomisk eller annen materiell støtte til en terrororganisasjon (...)».

4.3. Bakgrunn – terrorfinansiering

I de foregående NRA-er har finansiering av ekstrem islamisme og terrorisme blitt mest vektlagt når det gjelder terrorfinansiering. PST vil nå vektlegge at terrortrusselen er like sannsynlig fra høyreekstremistiske miljøer som fra ekstreme islamistiske miljøer. Dette er i tråd med det trusselbildet som er meddelt i PSTs årlige trusselvurdering. Selv om terrortrusselen fra ekstreme islamistiske og høyreekstremistiske miljøer vurderes som like stor i Norge, vil finansieringen ha ulikt modus. Faren og konsekvensene for terrorfinansiering er ulik i de ulike miljøene.

Terroraktivitet er en særlig alvorlig form for kriminalitet, fordi den truer borgernes grunnleggende trygghet og frihet. Det er derfor av stor betydning med tiltak som rammer både potensielle terrorister og

deres støttespillere og aktive sympatisører. Klarer man å forebygge og forhindre tilførselen av midler til terroraktivitet, kan man også hindre terrorangrep.[113]

Finansiell eller materiell støtte til terror er etter norsk rett et selvstendig lovbrudd og defineres som en terrorrelatert handling. Straffebudene rammer ulike former for finansiering og støtte av terrorvirksomhet i og utenfor Norge, som finansiering av konkrete terrorhandlinger og støtte til terrororganisasjoner eller enkeltterrorister (se vedlegg 1 og 2).

I følge FN og FATF er organisert kriminalitet en viktig finansieringskilde for terror-, milits- og opprørsgrupper som truer regional og internasjonal sikkerhet. Som eksempel har ISIL finansiert sin terror gjennom ulovlig salg av olje og kulturskatter, kidnapping for løsepenger, skattlegging, smugling og plyndring.

Når det gjelder fremmedkrigere som har reist fra Norge til ISIL-kontrollerte områder, erfarer PST at de i stor grad har vært selvfinansierte. De har brukt egne midler til å betale reise, klær og utstyr i forkant av utreisen. Egne midler har vært inntekt, enten lønnsinntekt eller sosiale ytelser, salg av egne eiendeler og verdigjenstander samt penger fra familie. Men det har også i tillegg forekommet misbruk av kredittkort, lån og stipender.

4.4. Trusselbildet

Alle trusselvurderinger er beheftet med usikkerhet, og trusselbildet påvirkes av mange faktorer. Uforutsigbarhet og usikkerhet knyttet til potensielle enkelthendelser og mer langsiktige negative utviklingstrekk i Vesten gjør at vi kan erfare raske endringer.

Denne NRA er skrevet i en tid da koronaviruset har sterk innvirkning på verdens samfunnsstrukturer, sikkerhet og økonomi. Da regjeringen besluttet å stenge Norge 12. mars 2020, var det få som kunne forutse dette bare noen uker tidligere. Vi blir derfor minnet på at store omveltninger og usikkerheter kan ramme landet vårt og innbyggerne våre svært raskt.

Terrorfinansieringstrusselen sees i sammenheng med den generelle terrortrusselen, og det gjelder trussel både fra ekstrem islamisme (IX) og høyreradikal ekstremisme (HX). Med det som bakteppe er det viktig å klargjøre det nåværende trusselbildet.

4.4.1. Internasjonal terrorisme[114]

ISIL har i løpet av 2019 mistet sin øverste leder og siste rest av sin territorielle kontroll, propagandaapparatet har blitt redusert og en stor andel av organisasjonens medlemmer, inkludert fremmedkrigerne, har blitt drept eller tatt til fange. Selv om organisasjonen er svekket, er det sannsynlig at terrortrusselen fra ISIL mot Vesten på lengre sikt vil øke, og at organisasjonen vil fortsette å representere den største internasjonale terrortrusselen mot Vesten. Det er tre grunner til dette:

For det første har ISIL endret sin strategi og økt sitt fokus på å bygge seg opp i flere deler av verden.
For det andre har ISIL vært godt forberedt på tapet av det såkalte kalifatet i Syria og Irak.
For det tredje har stormaktsrivaliseringen i regionen gitt ISIL nytt spillerom.

---

[113] Regjeringens strategi for bekjempelse av hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen, juni 2020.

[114] Innholdet i dette kapittelet er i hovedsak hentet fra: FOKUS 2020, Etterretningstjenestens vurderinger av aktuelle sikkerhetsutfordringer.

ISIL har sannsynligvis flere tusen aktive medlemmer i Syria og Irak, og økonomien er tilstrekkelig robust til at de kan videreføre opprørsstrategien i lang tid framover. Selv om ISIL ikke lenger har de store inntektene fra olje og skatteinnkreving som under det såkalte kalifatet, har organisasjonen heller ikke utgiftene som driften av en stat medfører. I tillegg har organisasjonen i høy grad lyktes med å opprettholde sine internasjonale finansieringsnettverk.

Ingen annen konflikt i moderne tid har mobilisert et så høyt antall militante islamister i Europa som Syria-krigen. Over 5000 europeiske fremmedkrigere har reist til Syria og Irak, og av disse har over 1500 returnert. Mange av dem har kamperfaring, noe som betyr økt voldskapasitet, et internasjonalt nettverk som gjerne strekker seg på tvers av landegrenser og en styrket ideologisk overbevisning som kan føre til at de vil radikalisere andre når de vender hjem. Radikalisering og nettverksdannelser i fengsler representerer en særlig utfordring.

Fremmedkrigere

Av de returnerte fremmedkrigerne fra Syria og Irak som har vært straffeforfulgt fremstår de fleste å fortsatt ha en ekstrem islamistisk overbevisning. Flere av disse har vært og er aktive som radikalisatorer i fengsel.

Fremmedkrigere som per september 2020 er fengslet vil være ute innen februar 2024. Returnerte fremmedkrigere er viktige i trusselbildet fordi de, sammenliknet med ekstreme islamister som ikke har vært på jihadreise, har status og troverdighet som kan komme til nytte i fremtiden i eventuelle forsøk på å radikalisere andre, i pengeinnsamling og i terrorplanlegging. På den måten kan de påvirke det fremtidige trusselbildet.

Flere tusen fremmedkrigere er ikke gjort rede for. Mange har sannsynligvis blitt drept i kampanjen mot ISIL og vil aldri bli identifisert. Et mindretall er fortsatt i live og på frifot, og noen vil ha returnert uoppdaget til Vesten eller forflyttet seg til nye konfliktområder. Enkelte er igjen i Syria og Irak. Trusselen fra gjenværende fremmedkrigere i Syria og Irak mot Vesten er begrenset. Nå som ISIL ikke lenger har territoriell kontroll, er fremmedkrigernes handlingsrom og bevegelsesfrihet innskrenket. De utgjør primært en trussel gjennom kontakt med meningsfeller i Vesten og kompetanseoverføring til disse miljøene.

Også andre terrororganisasjoner har endret strategi. Dette er mest tydelig hos al- Qaida, som også utnytter stormaktsrivaliseringen til å bygge allianser og rekruttere. Al-Qaida har gode vekstvilkår globalt og har nå en større medlemsmasse enn noen gang tidligere. Koblingene mellom lokale og globale grupperinger i de ulike organisasjonene skaper et mer sammensatt trusselbilde, samtidig som rivaliseringen blant stormaktene gjør det mindre sannsynlig at stater vil enes om hvordan internasjonal terrorisme skal bekjempes.

Midtøsten vil altså fortsatt være den mest framtredende arenaen for ISIL, men terrororganisasjonen får stadig flere tilhengere og grupperinger i Kaukasus, Sør-Asia og Afrika. I Nord-Afrika er ISIL mest aktiv i Libya og Egypt. I Vest-Afrika er det mest aktivitet i Tsjad, Niger, Nigeria og Mali. I Øst- og Sentral-Afrika styrker ISIL seg i den demokratiske republikken Kongo og Mosambik.

I Øst-Afrika, på Afrikas Horn, har terrororganisasjonen al-Shabaab fortsatt en solid forankring.

Parallelt med det såkalte kalifatets framvekst og fall har Vesten blitt mer polarisert.

De militante islamistiske miljøene i Europa har fått sin egen dynamikk basert på brede internasjonale kontaktnettverk. Disse nettverkene vil sannsynligvis utgjøre den største terrortrusselen fra militante islamister mot Europa i årene som kommer. Samtidig er det en økende oppslutning om høyrepopulistiske partier, en økning i høyreekstrem retorikk og høyreekstrem terrorisme rettet mot muslimske deler av samfunnet. Høyreekstremisme er i økende grad et internasjonalt fenomen, og bidrar til et mer sammensatt og utfordrende trusselbilde i Vesten.

I Europa er det en økende oppslutning om høyrepopulistiske partier og en økning i høyreekstrem retorikk og høyreekstrem terrorisme rettet mot muslimske deler av samfunnet.

Flere høyreekstremistiske terrorangrep har funnet sted det siste året både i USA og Europa, og også i Norge, mot Al-Noor-moskeen i Bærum. De høyreekstreme angrepene har for det meste vært planlagt og gjennomført av enkeltpersoner. Gjerningspersonene har ofte vært inspirert av tidligere angrep i andre land, og de har vært aktive i internasjonale nettfora.

Høyreekstremisme er i økende grad et transnasjonalt fenomen, både når det gjelder radikalisering på nett og i form av konkret organisasjonsbygging. En av faktorene som gjør dagens høyreekstremisme mer transnasjonal, er at den ikke begrenser seg til en ideologi som fokuserer på nasjonalstaten. Det er flere nyanser av høyreekstrem ideologi som vil kunne virke samlende på tvers av landegrenser og skape grunnlag for internasjonalisering. Den høyreekstreme Siege-ideologien vil kunne utgjøre en særskilt utfordring i årene som kommer.

> Militant islamisme og høyreekstremisme kopierer hverandre, og det er sannsynlig at de i framtiden også vil gi næring til hverandre». FOKUS 2020.

En potensiell arena for å skape samhold og knytte bånd mellom høyreekstreme elementer i Europa er konflikten i Ukraina, der flere høyreekstreme har sluttet seg til Azov-bataljonen, en organisasjon som slåss på den pro-ukrainske siden i konflikten. Denne konflikten kan bli sentral for høyreekstreme, særlig som en arena for å tilegne seg ferdigheter som kan brukes til å planlegge og gjennomføre terroroperasjoner. I tillegg gir sosiale medier og elektronisk kommunikasjon gode forutsetninger for at også de høyreekstreme miljøene kan danne fungerende internasjonale nettverk og terrorceller, på linje med de islamistiske terrornettverkene i Europa.

4.4.2. Terrorfinansiering fra og i Norge[115]

Det overordnede terrortrusselnivået i Norge er MODERAT, og dette gjelder trusselen både fra ekstrem islamisme og høyreekstremisme.

4.4.2.1. Ekstrem islamisme – IX:

Det vurderes som mulig at ekstreme islamister vil forsøke å gjennomføre terrorhandlinger i Norge i det kommende året.

Det er få personer som støtter ekstrem islamisme, og få radikalisatorer er aktive – dermed forventes et vedvarende begrenset omfang av radikalisering i 2020. Det er lite aktivitet blant radikaliserte personer, og ingen organisasjoner fremmer ekstrem islamistisk ideologi i det offentlige fysiske rom. Den aktiviteten som foregår, finner sted på religiøse arenaer, i fengsler og på internett. Aktiviteten på internett foregår gjerne kryptert og anonymt. Dette betyr at trusler er vanskeligere å oppdage, men også at færre eksponeres for propaganda og radikaliseringsvirksomhet.

Forventningen om fortsatt lav aktivitet blant ekstreme islamister i Norge skyldes at de i flere år har manglet en kampsak. Samtidig har ISIL-tilhengere vist resignasjon over kalifatets gradvise svekkelse og fall. Økt aktivitet, radikalisering og vold kan imidlertid utløses av handlinger som oppfattes som krenkelser av islam. I tillegg kan norske militære bidrag i muslimske land, videre utvikling av ISIL i Syria samt tematikk

[115] Innholdet i dette kapittelet er i hovedsak hentet fra PSTs nasjonale trusselvurdering for 2020.

knyttet til retur av fremmedkrigere skape reaksjoner og utløse radikalisering.

Gjentatte handlinger som oppfattes som krenkelser av islam vil øke potensialet for radikalisering til ekstrem islamisme. Dette skyldes at også moderate muslimer oppfatter budskapet som krenkende. Geografisk nærhet til krenkelsen er ikke avgjørende for hvor vi vil se radikalisering og voldelige motreaksjoner, fordi bilder og filmer av slike hendelser spres raskt på internett.

Eventuelle nye krenkelser i Norge vil spres på internett og i utenlandske medier. Det er sannsynlig at gjentatte krenkelser vil skape stadig sterkere reaksjoner og protester. Koranskjendinger i andre europeiske land vil forsterke effekten i Norge. Gjentatte handlinger som oppfattes som krenkelser av islam har potensial til å endre Norges posisjon i fiendebildet til ekstreme islamister utenfor Norge og utløse angrepsplanlegging i utlandet rettet mot Norge.

I det kommende året vil utviklingen i ISIL-sympatiserende nettverk i Europa være utslagsgivende for det norske trusselbildet. Aldri før har en ekstrem islamistisk terrororganisasjon hatt så mange sympatisører i Europa. Det er sannsynlig at de mange fremmedkrigerne og terrordømte som løslates de nærmeste årene vil danne fysiske og digitale nettverk. Det er sannsynlig at slike nettverk vil radikalisere, oppfordre til terror og drive faktisk angrepsplanlegging på tvers av landegrenser.

Nettverkene i Europa vil påvirke trusselbildet i Norge i de tilfellene der ekstremister i Norge har bånd til terrorplanleggere som inspirerer, veileder eller samarbeider. Det er også mulig at en eventuell økning i antall terroraksjoner eller omfanget av terroraksjoner i andre europeiske land kan inspirere norske islamister til å agere i Norge.

Al-Qaida vil fortsatt motiveres av det de tolker som Vestens krig mot muslimer og kampen for et fremtidig kalifat. De har intensjon om og kapasitet til å ramme Europa. Organisasjonen vurderes imidlertid ikke å utgjøre en like stor trussel som ISIL. I tillegg er det relevant for trusselbildet at det også finnes ekstremister i Norge som først og fremst er engasjert i regionale konflikter i Asia og Afrika, og som ikke har noen intensjon om å angripe mål i Norge. Disse iverksetter imidlertid pengeinnsamlinger og andre støtteaktiviteter herfra.

Høyesterett avsa endelig dom i straffesak 4. september 2018 mot en person for deltagelse, rekruttering, materiell og finansiell støtte til en terrororganisasjon. Personen var leder i et ekstremistisk nettverk, og Høyesterett la, i likhet med lagmannsretten, til grunn at han hadde operert som «rådgiver, organisator, fasilitator, mellommann og portåpner, spesielt med sikte på å hjelpe fremmedkrigere fram til ISIL og mens de oppholdt seg i Syria under ISILs kommando. Han har i den forbindelse hatt kontakt med en rekke land, herunder Storbritannia, Danmark, Sverige, Tyrkia og Syria.»

Den finansielle støtten bestod av flere pengeoverføringer på til sammen ca. NOK 30 000 via kontaktpersoner i Tyrkia, som videre skulle gå til en person han visste var aktiv deltager i ISIL. Straffen for de samlede forholdene ble satt til fengsel i ni år. De økonomiske overtredelsene ble vurdert til i overkant av ett års fengsel.

I Oslo tingretts dom av 1. mars 2019 ble en person dømt til to år og ni måneders fengsel samt inndragning av 27 000 kroner for ulike former for deltagelse og forsøk på å reise til ISIL i Syria, jf. straffeloven § 136 a, og finansiering av terrorvirksomhet, jf. § 135.

Finansieringen skjedde på fire ulike tidspunkt i 2016 og 2017. Beløpene var ikke høye, det største enkeltbeløpet var 150 amerikanske dollar.

Personen ble også utvist fra Norge og må forlate landet etter endt soning.

4.4.2.2. Høyreekstremisme – HX

Det vurderes som mulig at høyreekstremister vil forsøke å gjennomføre terrorhandlinger i Norge i det kommende året.

Det siste året har høyreekstremismen blitt mer grensekryssende når det gjelder nettverk og ideologi. I flere av de høyreekstremistiske miljøene ser vi forbindelser til våre naboland og andre land i Europa.

> Ytre høyre er en samlebetegnelse for både høyreekstreme og høyreradikale ideologier, herunder anti-islam/kulturnasjonalisme, entopluralisme, fascisme og raserevolusjonisme. Høyreekstremisme impliserer aksept for vold som virkemiddel for å skape politisk endring.

Høyreekstreme viser i økende grad vilje til å bruke terror for å nå sine mål.

Høyreekstremisme er i økende grad et transnasjonalt fenomen, både når det gjelder radikalisering på nett og i form av konkret organisasjonsbygging. Ukraina-konflikten er en potensiell arena for å skape samhold og knytte bånd mellom høyreekstreme elementer i Europa.

Blant de nynazistiske gruppene i Norge er det Den nordiske motstandsbevegelsen (DNM) som har fått størst eksponering i offentligheten de siste årene. DNM har som mål å avskaffe demokratiet og etablere en nordisk, nynazistisk stat. Dette målet har svært liten støtte i det norske samfunnet. DNM forventes fortsatt å være en liten organisasjon og ikke øke i antall medlemmer og sympatisører i 2020.

Innvandrings- og islamfiendtlige organisasjoner og bevegelser har fremdeles få medlemmer og forventes fortsatt å samle få tilhengere under offentlige markeringer. En viktig årsak til dette er lav innvandring til Norge. Disse miljøene vil imidlertid fortsette å spre sitt budskap. Det omfatter blant annet et ønske om forbud mot islam og et ønske om utsendelse av ikke-vestlige innvandrere. I tillegg står konspirasjoner om muslimsk og jødisk maktovertagelse av Europa og Norge sentralt for enkelte.

For øvrig har den islam- og innvandrerfiendtlige organisasjonen Stopp islamiseringen av Norge (SIAN) gjennomført og planlegger flere markeringer i ulike byer og tettsteder i Norge i 2020. SIANs mål med markeringene er å vise befolkningen at religionen islam er uforenelig med det norske samfunnet, blant annet gjennom å framprovosere voldelige reaksjoner fra muslimer. Dette gjøres primært gjennom muntlige taler, men også ved bruk av plakater, klesplagg, flagg og skjending av Koranen.

SIANs markeringer har fått mye oppmerksomhet og har medført ordensforstyrrelser initiert av motdemonstranter. Det er flere forhold ved markeringene som kan påvirke trusselen fra de ulike ekstreme miljøene og bidra til en negativ utvikling.

Internett er en viktig arena for spredning av terroroppfordrende, høyreekstrem propaganda. I likhet med andre ekstremister bruker høyreekstreme i økende grad krypterte kommunikasjonsplattformer og lukkede fora for å dele propaganda og kommunisere. Videre bidrar den lukkede kommunikasjonsformen til at motstemmer ikke høres eller blir gitt spillerom.

4.4.2.3. Venstreekstremisme

I PSTs nasjonale trusselvurdering for 2020 vurderes det som svært lite sannsynlig at venstreekstreme vil forsøke å gjennomføre terrorhandlinger i Norge det kommende året. Samtidig forventes det at de vil fortsette å bruke vold mot sine meningsmotstandere, fortrinnsvis i forbindelse med demonstrasjoner. De venstreekstreme miljøene i Norge er små og består av et fåtall ekstreme grupper, og det er lite sannsynlig at disse vil vokse i det kommende året. For øvrig har deler av miljøene blitt mer aktive og voldelige de

siste årene. Dette har ført til en økning i politisk motiverte voldshandlinger mot politiske meningsmotstandere, da særlig høyreekstreme og de innvandrings- og islamfiendtlige miljøene. Det er sannsynlig at venstreekstreme vil fortsette å kartlegge, sjikanere og forsøke å begå voldshandlinger mot disse.

Norske venstreekstreme har kontakt med venstreekstreme i andre land. Gjennom denne kontakten knyttes norske venstreekstreme til miljøer som har en lavere terskel for voldsbruk. Det er mulig at dette vil kunne radikalisere miljøene her hjemme til økt voldsutøvelse mot meningsmotstandere.

4.5. Sårbarheter – risiko

Å avdekke og hindre transaksjoner som skal støtte terrorisme, er en stor utfordring. Ofte er slike transaksjoner fordekt og nesten umulig å spore, særlig når det benyttes ikke-rapporteringspliktige aktører. Da forblir ofte avsender og/eller mottaker skjult.

4.5.1. Banker

Rapporteringspliktige foretak synes å ha enkelte utfordringer knyttet til avdekking og bekjempelse av terrorfinansiering. En utfordring synes å være tilpassing av risikoforståelse og tiltak når risikobildet endres, eksempelvis utvikling av nye scenarier for å fange opp terrorfinansiering gjennom høyreekstreme grupperinger.

Finanstilsynet erfarer at kunnskapen og bevisstheten hos bankene om terrorfinansiering er varierende. Faktorer som bankenes størrelse, antall kunder, sammensetningen av kundemasse, kompleksitet i tjeneste- og produkttilbud samt internasjonal eksponering påvirker risikoen for misbruk til terrorfinansieringsformål.

I bankenes risikovurdering på hvitvaskingsområdet er det et krav at terrorfinansiering vurderes selvstendig, og at det foreligger gode rutiner for håndtering av dette. Finanstilsynet erfarer at enkelte mindre og mellomstore banker ikke i tilstrekkelig grad inntar risikoen for terrorfinansiering i sin etterlevelse av hvitvaskingsloven. Finanstilsynet har også observert at større banker etterlever kravet om at terrorfinansiering risikovurderes, men at etterlevelsen utover dette varierer. Når bankene har liten bevissthet om problematikken på overordnet plan, ei heller ingen terrorfinansieringsscenarier i transaksjonsovervåkningssystemene og ingen rutiner for å håndtere dette, så er forutsetningene for å avdekke konkrete terrorfinansieringsforhold svake.

Risikoen er at transaksjoner som skulle vært stoppet basert på sanksjonsregimet blir gjennomført og går til kriminalitet.

Antall meldinger fra de rapporteringspliktige i henhold til hvitvaskingsloven om mistenkelige transaksjoner med mistanke om terrorfinansiering har de siste årene vært ganske stabilt, med en liten nedgang i antallet de siste par årene. Dette kan skyldes at krigen i Syria og Irak har stilnet, og at fokuset på finansiering av fremmedkrigere ikke er så stort.

Trusselbildet er stadig i endring, og det er derfor viktig at finansinstitusjonene har oppdaterte indikatorlister på terrorfinansiering i sitt overvåkingssystem for transaksjoner. Dialog og kunnskapsdeling med politiet er derfor svært viktig for å oppnå god etterlevelse.

En av flere indikatorer på en mistenkelig transaksjon knyttet til terrorfinansiering kan være at pengene går til konfliktområder. Slik trusselbildet ser ut nå, med mange hjemvendte fremmedkrigere i Europa og fremmedkrigere som er ferdige med soning og er ute i samfunnet igjen, er det viktig å ikke ha for stor

oppmerksomhet rettet mot destinasjonen pengene går til. Penger til terrorisme trenger ikke kun å gå til konfliktområder. Det kan bli for snevert, og dermed kan en gå glipp av en slik transaksjon som burde vært meldt. Som tidligere påpekt har ISIL og AQ etablert seg med celler i mange land, og med sympatisører i enda flere land.

Også HX-miljøene har et internasjonalt nettverk, med grensekryssende transaksjoner. Det kan være utfordrende å avdekke disse transaksjonene, for det er ikke åpenbart at pengene går til kjente konfliktområder.

4.5.2. Sanksjonsforskrifter

De rapporteringspliktige har krav og rutiner for å sikre at de internasjonale vedtatte sanksjons- og tiltaksforskriftene følges. Banker kjøper inn systemer for screening mot de ulike sanksjonslistene. Finanstilsynets erfaring er at systemene som benyttes genererer en stor grad av feiltreff, noe som øker risikoen for at bankene ikke reagerer på adekvat måte når treffene er korrekte, og at undersøkelser for å avkrefte feiltreffene medfører unødvendig ressursbruk.

En annen sårbarhet knyttet til terrorfinansieringstrusselen og sanksjonslister, og som påpekes av EU-kommisjonens overnasjonale risikovurdering (SNRA), er at sanksjonsscreening kun fanger opp kjente individer og grupper, mens risikoen for terrorfinansiering ofte kan knyttes til personer som ikke er fanget opp av sanksjonsregimet. Det er derfor av stor betydning for bekjempelsen av terrorfinansiering at de rapporteringspliktige har flere systemer for å avdekke terrorfinansiering.

4.5.3. Betalingsforetak med konsesjon og agenter for EØS-registrerte betalingsforetak

De større betalingsforetakene har sanntidsregler og annen transaksjonsovervåkning som skal avdekke terrorfinansiering og finansiering av fremmedkrigere. Det gjøres også noe overvåkning av åpne kilder. Flere av betalingsforetakene spesialiserer seg på overføringer til høyrisikoland som gjerne også er konfliktsoner med liten eller ingen bankinfrastruktur.

Det er Finanstilsynets oppfatning at både de norske betalingsforetakene og agentene for de større utenlandske betalingsoverføringsnettverkenes gjennomføring av kundetiltak ikke etterlever hvitvaskingslovens krav.

De fleste agenter av EØS-registrerte betalingsforetak har agentvirksomheten som bigeskjeft. De er avhengige av opplæring og oppfølging fra selskapene de representerer for å følge opp de norske kravene. Det er også en sårbarhet at agentene ikke har forutsetninger til å kjenne kundene når deres gjennomføring av transaksjoner i stor grad skjer på drop in-basis.

Kombinasjonen av mangelfulle kundetiltak og pengetransaksjoner til konfliktområder gjør risikoen for at slike tjenester blir brukt til terrorfinansiering høy.

Enkelte norske og utenlandske betalingsforetak benytter seg av pengetransport for å frakte kontanter ut av landet. Bakgrunnen for dette er at enkelte betalingsagenter har vanskeligheter med å opprette konto i norske banker for videreføring av pengene.

Når norske og utenlandske betalingsforetak frakter kontanter ut av Norge via pengetransportører, kan det innebære at myndighetenes kontroll med pengenes opprinnelse og mottaker minsker. Det er også

risiko for at summen som faktisk føres ut av landet er større enn den som blir oppgitt til fraktselskapet, fordi det er mangelfull kontroll av summene som blir oppgitt.

Se Økokrims omtale i kapittel 3.8.2. og 3.8.3.

4.5.4. Uregistrerte betalingsforetak

Det er en sårbarhet at uregistrerte betalingsforetak sender penger til og fra Norge, fordi disse aktørene representerer en særlig stor risiko for finansiering av hvitvasking og terror. Det forekommer at organisasjoner registrerer seg som en frivillig organisasjon (NPO), men i hovedsak driver med betalingsformidling. De misbruker da NPO-ordningens integritet og driver forretningsvirksomhet. Organisasjonene har da hverken konsesjon fra Finanstilsynet eller agentavtale med et EØS-registrert betalingsforetak, og de rapporterer ikke transaksjonene til Valutaregisteret eller sender meldinger om mistenkelige transaksjoner til Enheten for finansiell etterretning. Det gjør at den opprinnelige avsenderen og den endelige mottakeren forblir ukjent for myndighetene, og det igjen kan være en metode for å hvitvaske penger eller finansiere terrorisme.

En ser også at enkeltpersoner opererer som betalingsformidlere. I begge tilfeller trenger aktørene en bankkonto, og det blir derfor viktig at bankene kjenner sine kunder godt og har varslingssystemer som fanger opp aktørens ulovlige aktivitet.

4.5.5. Virtuell valuta

I årene som kommer vil internett fortsatt være en viktig arena for spredning av terroroppfordrende propaganda. Digitale nettverk setter soloaktører i en sosial kontekst. Dette vil bidra til radikalisering og terrorplanlegging, som også har innvirkning på finansiering.

Med dagens digitale løsninger og globale samhandling over internett er det viktig og utfordrende å holde oversikt og kontroll over selskaper som tilbyr finansielle tjenester i Norge. Ulike nyere betalingstjenester etterlater seg elektroniske spor som det kreves kunnskap om og analyseverktøy for å avdekke. [116]

Vekslere og oppbevaringstjenester av virtuell valuta er nå underlagt hvitvaskingsregelverket. Det er positivt, ettersom det stilles krav for å øke kunnskapen om terrorfinansieringstrusler ved bruk av vekslings- eller oppbevaringstjenester. Ettersom bransjen er relativt ny, og tidligere uregulert, er det svært sprikende kompetanse hos aktørene. Det vil trolig ta noe tid før bransjen er tilstrekkelig moden for å ha de rette mekanismene på plass for å bekjempe hvitvasking og terrorfinansiering på en tilstrekkelig måte.

Virtuell valuta er et digitalt og grensekryssende produkt, der tjenestetilbyderen ikke har en tydelig tilknytning til ett enkelt land, kombinert med at vekslere og oppbevaringstjenester av virtuell valuta vurderes å ha en høy iboende risiko for hvitvasking og terrorfinansiering.

Det er en risiko for at kriminelle aktører søker seg til tjenestetilbydere som ikke er underlagt registreringsplikt av Finanstilsynet.

Se Økokrims omtale i kapittel 3.8.7.

[116] Regjeringens strategi for bekjempelse av hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen, juni 2020.

4.5.6. E-pengeforetak

Det handles for betydelige beløp i Norge med forhåndsbetalte anonyme betalingskort fra utlandet. Slike kort skjuler hvem som bruker kortet, informasjonen begrenser seg til beløp og utsteder. Slike kort kan være egnet for å hvitvaske penger, men kortene kan også finansiere terrorisme.

Se Økokrims omtale i kapittel 3.8.6.

4.5.7. Frivillig sektor (NPO) og pengeinnsamling

> Pengeinnsamling er tillatt for alle uten å registrere seg. Dermed blir giveres aktsomhet svært viktig.

Pengeinnsamling i Norge er ikke lovregulert, og alle kan drive pengeinnsamling, enten som organisasjon eller privatperson. Det er ingen krav til registrering eller underretting. Ved for eksempel naturkatastrofer og akutte humanitære kriser, hvor mange ønsker å gi penger og bidra til hjelp, kan useriøse aktører se muligheter til underslag eller finansiering av terrorisme. Dette er en sårbarhet og krever givers aktsomhet.

Innsamling av penger via sosiale medier kan i enkelte tilfeller tilsløre den opprinnelige giveren. Flere kjente utenlandske og norske ekstremistiske organisasjoner og miljøer ber om finansiell støtte på sosiale medier. Ofte blir det oppgitt ønske om innbetalinger via ulike, gjerne krypterte, betalingsplattformer.

Hvert år blir betydelige pengesummer sendt ut av landet av frivillige organisasjoner (NPO), med det formål å støtte veldedig virksomhet. I enkelte tilfeller kan giver bli forledet til å tro at pengene går til humanitære formål, mens de i realiteten går til kriminelle.

Målet er å hindre at NPO-sektoren mottar eller samler inn penger og flytter de med det formål å finansiere terrorisme. Dette er også viktig fra et annet perspektiv, nemlig å bevare NPO-sektorens integritet.

Financial Action Task Force (FATF) har utarbeidet en egen anbefaling med veiledende retningslinjer for å forhindre at NPO-sektoren blir utnyttet til å finansiere terrorisme. Denne anbefalingen er gjort ettersom det internasjonale samfunnet har erfart at NPO-vsektoren ble og blir utnyttet til dette. EU-kommisjonens overnasjonale risikovurdering for hvitvasking og terrorfinansiering fra juli 2019 tar også opp problemstillingen.

PST har utarbeidet en ugradert temarapport kalt «Risiko for at frivillig sektor kan finansiere terrorisme» på oppdrag fra Justis- og beredskapsdepartementet. Under arbeidet med denne rapporten og i kontakt med Frivillighet Norge (paraplyorganisasjon for NPO) og Innsamlingskontrollen kom det fram at de ikke erfarte at NPO-er ble brukt til å finansiere terrorisme. Det de derimot erfarte var at enkelte NPO-er ble utsatt for bedrageri, og at betrodde enkeltpersoner i organisasjoner hadde begått bedrageri av penger, gjerne innsamlede midler. Noen organisasjoner var også etablert i den hensikt å drive pengeinnsamling til veldedige formål, men i stedet for å gi pengene til dette beholdt nøkkelpersonene pengene selv. Deres erfaring kan settes i sammenheng med at de NPO-ene som de er i kontakt med og representerer i mindre grad er en trussel for terrorfinansiering, fordi de er registrert i flere registre og underlagt mer rapportering.

Mye av kontrollen av NPO-sektoren er frivillig, og det er en sammenheng mellom i hvor stor grad en NPO er registrert, hvilke incentivordninger den har og hvor godt den blir kontrollert. Det er de NPO-ene som i liten grad registrerer seg som utgjør størst risiko for at pengene går til kriminelle formål, herunder finansiering av terrorisme.

FATFs anbefaling nr. 8 lyder slik:

Non-profit organisations (NPOs):

Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse, including:

(a) By terrorist organisations posing as legitimate entities;

(b) By exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and

(c) By concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

NPO refers to a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".

På det øverste nivået, med forhøyet risiko, er det små uregistrerte organisasjoner og private innsamlingsinitiativ. Nedover i pyramiden øker kontrollmekanismene parallelt med at de forskjellige registreringsinstansene blir flere og mer omfattende. Risikoen reduseres lengre ned i pyramiden.

Indikatorlisten viser de ulike typene registreringer, og det kan si noe om graden av ekstern kontroll og vilje til å underkaste seg dette. Når det gjelder drift og innsamling, er det faktorer som omtale i media og i åpne kilder samt erfaring og resultater fra innsamlingsvirksomhet som kan avdekke viktig informasjon, dessuten at en undersøker, i den grad det er mulig, kulturell tilknytning, tilstedeværelse i mottakerlandet og åpenhet for å gi informasjon om driften.

En kan også undersøke om giverne, privatpersoner og andre organisasjoner kan knyttes til terrorisme.

Et kontrollpunkt kan også være å undersøke om sluttmottaker av de innsamlede midlene er omhandlet i media på en positiv eller negativ måte. Dersom sluttmottaker befinner seg i et konfliktområde – begås det terrorisme der?

En skal skille mellom generelle og saksorienterte organisasjoner og lete etter uregelmessigheter. Som eksempel kan nevnes:

- En saksorientert organisasjon donerer til urelatert sak.
- En generelt fokusert organisasjon inkluderer nye områder, for eksempel: En nødhjelpsorganisasjon sender penger til område uten katastrofe.[117]

Indikatorliste - Risiko for terrorfinansiering gjennom NPO		
Indikatorer	**Ja**	**Nei**
Registrering av NPO		
Er NPO registrert i Frivillighetsregisteret		
Er NPO registrert hos Frivillighet Norge eller Innsamlingskontrollen		
Har NPO momsfradragsordning og/eller Skattefradragsordning		
Drift og innsamling		
Er NPO, ledelse eller kontaktpersoner negativt omtalt i media		
Er det kontantuttak fra den norske bankkontoen på de innsamlede midlene		
Har NPO drevet innsamling eller veldedig arbeid før med godt resultat		
Er det åpenhet rundt disponeringen av de innsamlede midlene		
Har NPO tilstedeværelse eller knytning til mottakerlandet		
Har innsamlerne tilhørighet til områdene som er målet for innsamlingen		
Mottaker		
Er mottakerne for de innsamlede midlene omhandlet negativt i media		
Er innsamlingen knyttet til konfliktområder hvor det begås terrorisme		
Dersom en saksorientert NPO donerer til urelatert sak		
Dersom midler går til konfliktområde, er mottaker en anerkjent motpart		
Høy risiko		
Lav risiko		

[117] PST: Temarapport – Risiko for at frivillig sektor kan finansiere terrorisme.

5. Vedlegg – Norges antihvitvaskings- og terrorfinansieringsregime

5.1. Internasjonalt rammeverk

5.1.1. Financial Action Task Force (FATF)

FATF er et mellomstatlig samarbeidsorgan som ble etablert i 1989 av G7-gruppen. FATF er en selvstendig enhet, men mandatet og oppgavene har en sterk tilknytning til G20 og beslutninger som blir fattet på ministermøtene.

Mandatet til FATF fastsettes på ministernivå av medlemslandene. Formålet er å fastsette standarder og sikre implementering av rettslige og operative tiltak for å bekjempe hvitvasking og finansiering av terror. FATF består av 37 medlemsland, 2 regionale organisasjoner, 9 assosierte medlemsgrupper og 23 observatører (som Egmont Group, Verdensbanken, EUROPOL, FN og Eurojust). Formålet med FATF er å få til en enhetlig internasjonal tilnærming til bekjempelsen av hvitvasking og finansiering av terror. FATF har fastsatt 40 anbefalinger som er en internasjonal standard for bekjempelsen av hvitvasking og finansiering av terror. I tillegg er det fastsatt kriterier for å måle om medlemslandene har implementert anbefalingene, og om de gir de forventede resultatene, slik som antall analyser for finansiell etterretning, straffesaker, inndragning, med mer.

FATFs 40 anbefalinger[118] og krav til nasjonal etterlevelse av standardene (Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems)[119] er grunnlaget for regimet mot hvitvasking og terrorfinansiering i Norge. FATF legger til grunn at medlemslandene skal ha en risikobasert tilnærming til hvitvasking og finansiering av terror. Basert på de identifiserte risikoene skal det utarbeides en nasjonal policy på området, og det skal være mekanismer på plass som ivaretar kravet om implementering, ressursallokering og samarbeid mellom berørte aktører.[120] Den nasjonale risikovurderingen for hvitvasking og terrorfinans er en del av dette.

5.1.2. EUs hvitvaskingsdirektiv

Europaparlamentets- og rådsdirektiv (EU) 2017/849 om tiltak for å beskytte det finansielle system mot hvitvasking og terrorfinansiering ble vedtatt 20. mai 2015. Direktivet er EUs fjerde hvitvaskingsdirektiv. Gjennomføringsfrist i medlemsstatene i EU var 26. juni 2017. Direktivet ble tatt inn i EØS-avtalen i desember 2018.

Fjerde hvitvaskingsdirektiv ble foreslått endret av EU-kommisjonen i 2016, og det ble oppnådd enighet mellom organene i EU i desember 2017. Endringsdirektivet ble formelt vedtatt i mai 2018 og er til vurdering for innlemmelse i EØS-avtalen. Innlemmelse av direktivkravene i EØS-avtalen vil innebære endring i det norske anti-hvitvaskings- og terrorfinansieringsregelverket. Disse endringene er i all hovedsak allerede gjennomført.

---

118 Financial Action Task Force (FATF), «The FATF Recommendations; International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation», 2012.

119 Financial Action Task Force (FATF), «Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems», februar 2013.

120 Anbefaling 1 og 2.

5.1.3. FN

FNs sikkerhetsråds resolusjoner (UNSCR) gir også føringer. Særlig relevant her er UNSCR 2253, UNSCR 1267 og UNSCR 1373, som fastsetter og styrker regimet for sanksjoner mot terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen.

5.1.4. The Egmont Group

The Egmont Group er en internasjonal sammenslutning for enheter for finansiell etterretning (Financial Intelligence Units (FIU-er)). 164 FIU-er fra hele verden er medlemmer i Egmont. Enheten for finansiell etterretning i ØKOKRIM (EFE)[121] er Norges FIU og ble medlem av Egmont i 1995. Det er et kriterium i FATF at medlemslandenes FIU skal være medlem i Egmont. Kriteriene for medlemskap fastsettes ved FATFs anbefalinger, Egmonts Charter og Principles for Information Exchange between FIUs. De to sistnevnte er bindende for EFE.

FATF og Egmont Group jobber også for å utvikle et nærmere samarbeid for å sikre at FIU-enes operative erfaringer og kompetanse skal nyttiggjøres bedre i det internasjonale samarbeidet, herunder ved FATFs evalueringer, rapporter om strategisk analyse og policydiskusjoner.

5.2. Nasjonal lovgivning

5.2.1. Lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven) med forskrifter

Gjeldende hvitvaskingsregelverk fremgår av lov 1. juni 2018 om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven) og forskrift 14. september 2018 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften).

Hvitvaskingslovens formål er å forebygge og avdekke hvitvasking og terrorfinansiering, jf. § 1. Loven angir i § 4 hvem som er rapporteringspliktige, og i §§ 9 flg. gis regler om kundetiltak og løpende oppfølgning. Dersom rapporteringspliktige avdekker forhold som kan indikere at midler har tilknytning til hvitvasking eller terrorfinansiering, skal det foretas nærmere undersøkelser, jf. § 25. Dersom det etter de nærmere undersøkelsene er forhold som gir grunnlag for mistanke om hvitvasking eller terrorfinansiering, skal rapporteringspliktige oversende opplysninger om forholdene til ØKOKRIM ved Enheten for finansiell etterretning, jf. § 26. Mistenkelige transaksjoner skal som hovedregel ikke gjennomføres før ØKOKRIM er underrettet, jf. § 27. ØKOKRIM har da muligheten til i særlige tilfeller å gi pålegg om at transaksjonen ikke skal gjennomføres.

I hvitvaskingsforskriften er det gitt nærmere regler om kundetiltak og løpende oppfølging av kunden (kapittel 4), undersøkelse og rapportering (kapittel 5) samt behandling av personopplysninger og andre opplysninger (kapittel 6).

5.2.2. Straffelovens bestemmelser om hvitvasking

Hvitvasking er straffsanksjonert i straffeloven §§ 337 (simpel hvitvasking), 338 (grov hvitvasking), 339 (mindre hvitvasking), 340 (uaktsom hvitvasking) og 341 (forbund om hvitvasking). En endring i forhold til reglene i straffeloven av 1902 er at medvirkning til hvitvasking nå er straffbart. Bortsett fra en nedjuste-

[121] EFE er nærmere beskrevet under pkt. 5.3.

ring av strafferammen ble det ikke foretatt realitetsendringer i forhold til straffeloven av 1902. Innholdet i bestemmelsen er nærmere omhandlet i Ot.prp. nr. 53 (2005–2006) om lov om endringer i straffeloven 1902 og utleveringsloven (gjennomføring av FN-konvensjonen mot korrupsjon).

Straffeloven §§ 337 *første ledd bokstav a* inneholder gjerningsbeskrivelsen for hvitvasking av utbytte som en bistandshandling til andre og erstatter straffeloven 1902 § 317 første ledd annet alternativ. *Første ledd bokstav b* gjør det straffbart å hvitvaske utbytte fra egne straffbare handlinger (selvvask) og viderefører straffeloven 1902 § 317 annet ledd. *Annet ledd* retter seg mot hvitvasking av surrogater og viderefører straffeloven 1902 § 317 første ledd tredje punktum. *Tredje ledd* viderefører straffeloven 1902 § 317 tredje ledd om at hvitvaskeren kan straffes, selv om den som begikk primærlovbruddet var utilregnelig eller mindreårig. *Fjerde ledd* angir strafferammen og bestemmer at hvitvasking kan straffes med bot eller fengsel inntil to år. Dette er en nedjustering i forhold til straffeloven 1902 § 317. Begrunnelsen er at strafferammen skal gi et mer realistisk bilde av straffutmålingspraksis i dag, og det er ikke meningen at hvitvasking skal bedømmes mindre alvorlig enn i dag.

5.2.3. Straffelovens bestemmelser om terrorfinansiering

Terrorfinansiering er straffesanksjonert i straffeloven §§ 135 og 136 a. Nevnte paragrafer gjennomfører FNs terrorfinansieringskonvensjon artikkel 4 bokstav a, jf. artikkel 2 og FNs sikkerhetsråds resolusjon 1373 (2001) OP 1 (b) og (d) med flere. Bestemmelsene rammer det å samle inn og fremskaffe penger eller andre økonomiske midler til terrorhandlinger eller til noen som begår slike handlinger.

Straffeloven § 135 rammer både den som «yter» eller «mottar», og den som passivt tar imot penger som er samlet inn av andre, for så å gi dem videre til støtte til en terrorhandling eller til noen som begår slike handlinger. Bestemmelsen omfatter også den som «sender» – sørger for at midlene overføres til andre – i tillegg til den som «fremskaffer eller samler inn», altså mellommenn som skaffer til veie økonomiske midler ved innsamlinger eller lignende.

Det er ikke et krav at det ved oversendelse er klart hvilken terrorhandling midlene skal finansiere, eller at midlene alene er tilstrekkelige til å finansiere terrorhandlinger. Bestemmelsen rammer også den som fremskaffer eller samler inn midler som delvis skal finansiere terrorhandlinger. Det trenger heller ikke være den tiltenkte bruken, men om mottageren er en person eller enhet som begår eller forsøker å begå terrorhandlinger, som kan danne grunnlag for straff. Det kan dermed være straffbart å gi økonomisk støtte til slike personer eller organisasjoner, selv om støtten er tiltenkt personens eller organisasjonens eventuelle lovlige virksomhet.

Bestemmelsen rammer også den som stiller finansielle tjenester til rådighet for terrorister eller terrorgrupper, for foretak som eies eller kontrolleres av terrorister eller terrorgrupper, eller for noen som handler på vegne av eller på instruks fra disse. Med «finansielle tjenester» forstås blant annet ulike banktjenester – som betalingstjenester, lån og kreditter – og ulike typer rådgivning og investeringstjenester etter verdipapirhandelloven.

Straffeloven § 135 omfatter altså alle elementer av finansiell støtte, men antas å være mest anvendelig ved finansiering i form av penger eller formuesgoder av en viss størrelse. For tilfeller av støtte i form av mindre pengebeløp, eller for eksempel anskaffelse av utstyr, kan straffeloven § 136 a komme til anvendelse.

Straffeloven § 136 a tilsvarer straffeloven 1902 § 147 d. Den rammer etter sin ordlyd «(…) den som danner, deltar i, rekrutterer eller yter økonomisk eller annen materiell støtte til en terrororganisasjon (…)». Materiell støtte kan være for eksempel i form av å levere utstyr til en fremmedkriger.

5.2.4. Båndlegging av formuesgoder og finansielle sanksjoner – frysforpliktelser

FNs sikkerhetsrådsresolusjon 1373 om frys- og listeføringsforpliktelser er gjennomført i norsk rett ved bestemmelser i politiloven § 17 g om båndlegging (frys) av midler tilhørende personer som med god grunn mistenkes for overtredelse av eller forsøk på overtredelse av straffeloven §§ 131, 133, 134, 135, 136 eller 136 a.

FNs sikkerhetsrådsresolusjon 1267 om finansielle sanksjoner er implementert i norsk rett gjennom forskrift 22. desember 1999 nr. 1374 om sanksjoner mot al-Qaida og forskrift 8. november 2013 nr. 1294 om sanksjoner mot Taliban. Når det gjelder restriktive tiltak vedtatt av Rådet for den europeiske union, gjennomføres disse i norsk rett med hjemmel i lov 27. april 2001 nr. 14 om iverksetjing av internasjonale, ikkje-militære tiltak i form avbrot eller avgrensing av økonomisk eller anna samkvem med tredjestater eller rørsler.

Utenriksdepartementet og Finanstilsynet har utgitt en veiledning om båndlegging av formuesgoder og finansielle sanksjoner/restriktive tiltak. Veilederen gir en beskrivelse av relevante lovbestemmelser og retningslinjer for gjennomføring av FNs og EUs frysforpliktelser.

5.3. Regimets aktører og koordinering

5.3.1. De rapporteringspliktige

I henhold til hvitvaskingsloven (2018) § 4 er følgende juridiske personer rapporteringspliktige:

- bank
- kredittforetak
- finansieringsforetak
- Norges Bank
- e-pengeforetak
- foretak som driver valutavirksomhet
- betalingsforetak og andre som har rett til å yte betalingstjenester
- verdipapirforetak
- forvaltningsselskap for verdipapirfond
- forsikringsforetak
- foretak som driver forsikringsformidling som ikke er gjenforsikringsmegling
- verdipapirsentraler, i tilfeller der verdipapirsentralen ikke benytter ekstern kontofører som er rapporteringspliktig. For kontohavere og utstedere som har ekstern kontofører som er rapporteringspliktig, er det kontoføreren som er rapporteringspliktig
- foretak som driver depotvirksomhet
- forvalter av alternative investeringsfond
- låneformidlingsforetak

Loven gjelder også for følgende juridiske og fysiske personer i utøvelsen av deres yrke:

- statsautoriserte og registrerte revisorer, godkjente revisjonsselskaper og revisorer som er ansvarlig for revisjon av regnskap for kommune, fylkeskommune eller kommunalt eller fylkeskommunalt foretak. Tilbyr personer eller foretak som nevnt i første punktum virksomhetstjenester, er de uansett underlagt loven på dette grunnlaget.

- autoriserte regnskapsførere og autoriserte regnskapsførerselskaper. Tilbyr personer eller foretak som nevnt i første punktum virksomhetstjenester, er de uansett underlagt loven på dette grunnlaget.
- advokater og andre som ervervsmessig eller stadig yter selvstendig rettshjelp, når de på klientens vegne utfører finansiell transaksjon eller en transaksjon som gjelder fast eiendom, eller når de bistår ved planlegging eller utføring av transaksjon for klient i forbindelse med
    - kjøp og salg av fast eiendom eller virksomhet
    - forvaltning av en klients penger, verdipapir eller andre aktiva
    - åpning eller forvaltning av bank- eller verdipapirkonto
    - fremskaffelse av nødvendig kapital til opprettelse, drift eller ledelse av selskap
    - opprettelse, drift eller ledelse av selskap, fond eller en lignende juridisk person eller formuesmasse, herunder utenlandsk trust eller tilsvarende juridisk arrangement
- eiendomsmeglere og eiendomsmeglingsforetak
- tilbydere av virksomhetstjenester
- personer med begrenset tillatelse til å yte betalingstjenester
- tilbydere av spilltjeneste

Forhandlere av gjenstander er ikke rapporteringspliktige og kan ikke motta vederlag i kontanter på 40 000 kroner eller mer eller tilsvarende beløp i utenlandsk valuta. Skattekontoret fører kontroll med at dette blir overholdt, jf. § 5.

Tilbydere av vekslingstjenester mellom virtuell valuta og offisiell valuta, og oppbevaringstjenester for virtuell valuta, omfattes av gruppen rapporteringspliktige, jf. § 1-3 i forskrift til hvitvaskingsloven.

5.3.2. Enheten for finansiell etterretning

Enheten for finansiell etterretning (EFE) er den avdelingen i ØKOKRIM som behandler rapportene om mistenkelige transaksjoner som sendes inn av de rapporteringspliktige. EFE har i motsetning til straffesaksteamene i ØKOKRIM ikke etterforskning eller straffesaksarbeid som primære oppgaver, men er Norges nasjonale enhet for finansiell etterretning (Financial Intelligence Unit (FIU)), og er å betrakte som en etterretningsenhet med nasjonalt ansvar.

EFE er opprettet på bakgrunn av FATF-anbefalingene, som pålegger medlemslandene å etablere nasjonale FIU-er for mottak, analyse og videreformidling av finansiell informasjon knyttet til mulig hvitvasking og finansiering av terror.

EFEs hovedoppgaver er å motta rapporter om mistenkelige transaksjoner (MT-rapporter) fra rapporteringspliktige etter hvitvaskingsloven, å analysere informasjonen og å videreformidle informasjon til rett instans. Opplysningene EFE mottar behandles og videreformidles i tråd med politiregisterloven og forskriftens bestemmelser. EFE kan formidle informasjon i form av etterretningsrapporter, informasjon i politiets etterretningssystem, anmeldelser, politirapporter i eksisterende straffesaker, strategiske rapporter, årsrapporter og i form av publisering på hvitvasking.no, foredrag ved ulike studier ved Politihøgskolen samt foredrag for politidistrikter der det har vært behov eller etterspurt. Mottagerne av etterretningsinformasjon er i all hovedsak politiet, inkludert PST, forvaltningsorganer med kontrolloppgaver samt andre lands FIU-er. I tillegg formidles det informasjon til privat sektor. Dette gjelder særlig formidling av moduser og trender til de rapporteringspliktige. På bakgrunn av initiativ fra Egmont Group og FATF har EFE på lik linje med andre FIU-er formidlet informasjon om fenomenet fremmedkrigere med mer til privat sektor. Formålet med dette er å sette dem best mulig i stand til å identifisere transaksjoner som har tilknytning til finansiering av terror.

EFE er et nasjonalt kompetansesenter for spørsmål relatert til hvitvasking og terrorfinansiering. EFE følger med på kriminalitetsutviklingen blant annet gjennom deltagelse i aktuelle internasjonale fora, som

FATF, Egmont Group og INTERPOL, og holder løpende kontakt med samarbeidspartnere og spesielt de rapporteringspliktige, for å bidra til kompetanse- og metodeutvikling.

Det nasjonale regimet mot hvitvasking og finansiering av terror skal som bemerket innledningsvis være risikobasert. Med bakgrunn i dette, og i tråd med det særskilte internasjonale fokuset som er på finansiering av terror, har EFE dreid mye av sin aktivitet mot dette feltet. Dette er spesielt synlig i innsatsen på operativ analyse. Mye av samarbeidet på operativt nivå har skjedd ved deltagelse i nasjonale samarbeidsprosjekter med terrorfinansiering som en av flere moduser. Dette har vist seg å være en fornuftig og effektiv måte å få delt informasjon på. Samarbeidet med PST er særlig viktig i denne sammenhengen.

5.3.3. Finanstilsynet

Det følger av lov 7. desember 1956 nr. 1 om tilsynet for kredittinstitusjoner, forsikringsselskaper og verdipapirhandel mv. (finanstilsynsloven) § 1 at Finanstilsynet skal føre tilsyn med en rekke foretak og personer. Flere av disse foretakene og personene er rapporteringspliktige etter hvitvaskingsloven, herunder tilbydere av virksomhetstjenester (siden 1. juli 2017).

Det følger av finanstilsynsloven § 3 at tilsynet skal påse at foretak det har tilsyn med virker på hensiktsmessig og betryggende måte «i samsvar med lov og bestemmelser gitt i medhold av lov». Det fremgår videre av samme bestemmelse at foretakene plikter å gi alle opplysninger som tilsynet måtte kreve og å la tilsynet få innsyn i og i tilfelle få utlevert dokumenter, protokoller, regnskapsopplysninger og annet tilgjengelig materiale.

Finanstilsynet gjennomfører hvitvaskingstilsyn både som særskilte tematilsyn og som en del av det ordinære tilsynet med de rapporteringspliktige. Tilsynsvirksomheten er innrettet mot at interne rutiner faktisk beskriver institusjonens gjennomføring av regelverket – hvordan lovbestemmelsene er operasjonalisert i foretakenes virksomhet – og at interne retningslinjer faktisk etterleves.

Finanstilsynet kan gi rapporteringspliktige foretak under tilsyn pålegg om retting der de ikke etterlever sine forpliktelser etter hvitvaskingsregelverket. Pålegg kan knyttes til endringer i rutiner eller organisering. Ved alvorlige overtredelser av foretakenes lovpålagte plikter kan Finanstilsynet tilbakekalle institusjonens konsesjon.

I ny hvitvaskingslov er tilsynsmyndighetene gitt hjemler til å ilegge flere typer forvaltningstiltak og administrative sanksjoner, slik som ledelseskarantene og overtredelsesgebyr.

5.3.4. Tilsynsrådet for advokatvirksomhet

Det følger videre av lov 13. august 1915 nr. 5 (domstolloven) § 225 første ledd at Tilsynsrådet for advokatvirksomhet fører tilsyn med advokater. Tilsynsrådet har adgang til å meddele irettesettelser og advarsler, og dersom det mener at det bør treffes vedtak om tilbakekall av advokatbevilling, kan det fremme slikt forslag overfor Advokatbevillingsnemnden. I hvitvaskingsloven (2018) er tilsynsmyndighetene gitt hjemler til å ilegge flere typer forvaltningstiltak og administrative sanksjoner, slik som ledelseskarantene og overtredelsesgebyr.

5.3.5. Skatteetaten

Skatteetaten har fått i oppgave å kontrollere at forhandlere av gjenstander ikke mottar 40 000 kr eller mer i kontanter. Kontroll som nevnt foran kan gjennomføres i forbindelse med etatens øvrige kontroller av

relevante kontrollobjekter (forhandlere av gjenstander). Skatteetaten er ikke tilsynsmyndighet tilsvarende Finanstilsynet og Lotteritilsynet, og det blir lagt til grunn at kontrollomfanget skal balanseres mot etatens øvrige kontrollvirksomhet basert på vurderinger av risiko og vesentlighet.

5.3.6. Lotteri- og stiftelsestilsynet

Tilbydere av spilltjenester er en ny gruppe rapporteringspliktige i ny hvitvaskingslov, som derfor ikke tidligere har vært underlagt tilsyn etter hvitvaskingsregelverket. Etter ny hvitvaskingslov skal tilsynet utføres av Lotteri- og stiftelsestilsynet.

5.3.7. Politiets sikkerhetstjeneste

Politiets sikkerhetstjeneste (PST) skal forhindre at terror og terrorfinansiering foregår i og fra Norge. I tillegg skal PST avverge at Norge utnyttes som transittland for penger til terrorformål. PST er direkte underlagt Justis- og beredskapsdepartementet (sideordnet med Politidirektoratet) og er en del av den norske politietaten.

PST skal opprette forebyggende sak når det innledes undersøkelser med sikte på å bekrefte eller avkrefte at noen forbereder et straffbart forhold innenfor PSTs ansvarsområde etter politiloven § 17 b. Forebyggende saker om terror og terrorfinansiering kan avsluttes eller håndteres med mottiltak i det forebyggende sporet. I enkelte tilfeller fører undersøkelser i forebyggende øyemed til at det etableres en mistanke, jf. straffeprosessloven § 224, som begrunner etablering av en etterforskning i straffeprosessuell forstand. PST har ansvar for etterforskning av avvergende terror- og terrorfinansieringssaker.

Som nasjonal sikkerhetstjeneste har PST et nært samarbeid med mange etater, institusjoner og andre aktører i Norge. Med de viktigste samarbeidspartnerne er det et formalisert samarbeid, og med andre er det samarbeid og kontakt ved behov. Etterretningstjenesten og PST har etablert et Felles kontraterrorsenter for analyser.

PST har et utstrakt samarbeid med andre lands politimyndigheter og sikkerhets- og etterretningstjenester. I tillegg er PST medlem av flere internasjonale samarbeidsfora, blant annet Club of Bern, Counter Terrorism Group (CTG), NATO CIC (Civilian Intelligence Committee) og PWGT (Police Working Group on Terrorism). Dette omfattende internasjonale nettverket er avgjørende for å forebygge alvorlig kriminalitet mot norske interesser.

PST driver omfattende opplæring og foredragsvirksomhet om bekjempelse av finansiering av terror og masseødeleggelsesvåpen for både offentlig sektor og private aktører, spesielt finansnæringen.

5.3.8. Politiet

Politiet består av PST, Politidirektoratet, tolv politidistrikter, særorganene Kripos, ØKOKRIM, Politiets utlendingsenhet, Utrykningspolitiet og Politihøgskolen. Politidistriktene og særorganene er administrativt og faglig underlagt Politidirektoratet,[122] mens riksadvokaten har ansvaret for den overordnede faglige ledelsen av straffesaksbehandlingen i politiet. Politiet startet gjennomføringen av nærpolitireformen i 2016. Reformen innebærer struktur- og organisasjonsendringer i politidistriktene, og antall politidistrikter ble redusert fra 27 til 12.

[122] PST er direkte underlagt Justis- og beredskapsdepartementet.

Fra 2005 har alle politidistrikter vært pålagt å opprette egne økoteam, som har et særskilt ansvar for å bekjempe økonomisk kriminalitet. Økoteamene er bemannet med politi, jurister og revisorer, og den tverrfaglige kompetansen skal gjøre økoteamene i stand til å behandle større økonomiske straffesaker. Økoteamene skal som hovedregel være samlokalisert og skjermet fra andre oppgaver. Manglende kapasitet er en av hovedutfordringene for politiet og for økoteamene. Nærpolitireformen skal sikre mer robuste fagmiljøer med større kapasitet og økt kompetanse til å etterforske økonomisk kriminalitet. De fleste sakene innen økonomisk kriminalitet, herunder hvitvasking, etterforskes i politidistriktene.

Økt fokus på terror har ført til at politiet har økt sin innsats mot, og prioritering av, arbeid mot terror og terrorfinansiering.

5.3.9. Tolletaten

Tolletaten beskytter samfunnet mot ulovlige og restriksjonsbelagte varer og sikrer statens inntekter gjennom riktige grunnlag for toll og avgifter. Gjennom dette bidrar etaten til å beskytte bedrifter og arbeidsplasser mot konkurranse fra uærlige aktører.

Fra 1. oktober 2020 består Tolletaten av tolldirektør med to staber og seks divisjoner med nasjonalt ansvar, hvorav grensedivisjonen og vareførselsdivisjonen er de to største. Tolletaten bidrar til etterlevelse av toll- og vareførselsreglene samt regelverkene til en rekke andre statlige etater, herunder blant annet regelverk for skatter og avgifter, valuta, narkotika, alkohol, tobakk, legemidler, våpen, farlige stoffer, næringsmidler, dyr, miljø, avfall og immaterielle rettigheter.

Tolletaten håndhever regelen om at medbragt valuta ut over grensebeløpet skal deklareres. Tolletaten kan ved avdekking av brudd på deklareringsplikten ilegge et administrativt overtredelsesgebyr på 20 prosent av beløpet eller anmelde forholdet hvis det mistenkes at valutaen stammer fra utbytte av straffbare handlinger, hvitvasking eller lignende. Ved anmeldelse tilbakeholdes hele beløpet, og saken overføres politiet for vurdering, forelegg, videre etterforskning og dom. Tolletaten rapporterer saker jevnlig til EFE.

Tolletaten sørger også for at alle deklarerte beløp som bringes inn eller ut av landet registreres i Valutaregisteret som fysiske transaksjoner.

5.3.10. Overordnet koordinering og samarbeid mellom aktørene i regimet

Et særtrekk ved det nasjonale arbeidet mot hvitvasking og finansiering av terror er at det er tverretatlig og tverrfaglig. Det innebærer at det ikke er en enkelt etat eller organ som sitter med eneansvaret for arbeidet, men at det er summen av alle de ansvarlige etaters innsats som er avgjørende. Dette illustreres særlig ved FATFs Effectiveness-kriterier, hvor samhandling og flyt av informasjon er grunnleggende faktorer for en effektfull nasjonal innsats. I forlengelsen av dette er det ikke eksistensen av innsatsen alene som skal evalueres. Det avgjørende er til syvende og sist de resultatene man klarer å frembringe gjennom samarbeidet. Måleparametere for dette er blant annet antall dommer for hvitvasking og finansiering av terror og dommer og forelegg for inndragning.

Sammenhengen i systemet kan illustreres ved at tilsynsmyndighetene må føre et risikobasert tilsyn for å fange opp mangler i effektiviteten i de rapporteringspliktiges preventive systemer, deretter at de rapporteringspliktige fanger opp de mistenkelige transaksjonene og rapporterer disse til EFE. EFE må ha tilgang til de nødvendige kildene og være i stand til å utføre operative og strategiske analyser, som så formidles til politiet. Det som formidles må være av en slik kvalitet og ha et innhold som gjør at det kan benyttes i politiets videre arbeid med å bekjempe kriminalitet og å sikre midler. Politiet må ha den kompetansen

som trengs for å utnytte den informasjonen som blir formidlet. Tilsvarende synergier er til stede for flere deler av den nasjonale innsatsen, herunder også for finansiering av terror.

Det er særlig to faktorer som er av avgjørende betydning for en vellykket nasjonal innsats: at det er en overordnet styring og målretting av arbeidet fra toppen og ned, og at alle aktører har en risikobasert tilnærming til sine oppgaver.

For å sikre en koordinert innsats og god samhandling mellom etatene i kampen mot hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen er det nedsatt et tverretatlig kontaktforum. Kontaktforumet består av representanter for

- Justis- og beredskapsdepartementet
- Finansdepartementet
- Utenriksdepartementet
- Finanstilsynet
- Politidirektoratet
- Politiets sikkerhetstjeneste (PST)
- Riksadvokatembetet
- Skattedirektoratet
- Tolldirektoratet
- ØKOKRIM

Kontaktforum ledes av Justis- og beredskapsdepartementet. Lederen for Norges delegasjon til Financial Action Task Force (FATF) deltar fast i møtene.

Etter tema og behov, og minst én gang pr. år, skal representanter for følgende etater inviteres i møtene:

- Tilsynsrådet for advokatvirksomhet
- Lotteritilsynet
- Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES)
- Politihøgskolen

Øvrige departementer eller etater inviteres etter behov.

Privat sektor skal involveres i arbeidet:

- Finans Norge, som representant for den største gruppen rapporteringspliktige foretak etter hvitvaskingsloven, møter som fast observatør ved relevante dagsordenspunkter.
- Øvrig privat sektor skal konsulteres gjennom deltakelse i relevante prosesser.

Sekretariatsansvaret går på rundgang mellom ØKOKRIM, Finanstilsynet og POD. Finanstilsynet skal nå ha denne oppgaven i to år.

5.3.11. Utviklingstrekk – samarbeid og informasjonsdeling

Samarbeid mellom offentlige etater og næringsliv er en forutsetning for å lykkes. Nasjonal innsats blir best og gir størst resultat hvis alle aktører virker mot samme mål. Informasjon må deles. Eksempler på dette kan være AMK-regionskontorene, NTAES og andre samarbeidsfora.

Et gjennomgående trekk på området for finansiering av terror er et utstrakt samarbeid og samordning av arbeidet i FATF og Egmont Group. Dette berører både internasjonal policyutvikling og kunnskapsdeling om trender og moduser for finansiering av terror. Forholdet til privat sektor og viktigheten av et nært samarbeid med denne er særlig vektlagt. Viktigheten av samarbeid og informasjonsdeling mellom landene, mellom landenes myndigheter og mellom myndigheter og privat sektor er også understreket av FNs sikkerhetsråd.

På det nasjonale nivået har PST og EFE et tett samarbeid om terrorfinansieringsarbeidet og samarbeider om planlegging og gjennomføring av kurs og foredrag til finansnæringen. Samarbeidet mellom EFE og politiet har økt på terrorfinansieringsområdet. I tillegg har Finanstilsynet og EFE et løpende samarbeid både på operativt og strategisk nivå. Finanstilsynet har også utstrakt kontakt med de rapporteringspliktige og de relevante næringsorganisasjonene.