Hvor langt er nok?

Et kriminologisk blikk på anti-hvitvaskingsarbeidet i finans-sektoren

Kandidat: 129001

Bacheloroppgave i Kriminologi

Institutt for kriminologi og rettssosiologi
Det juridiske fakultetet

UNIVERSITETET I OSLO

Høsten 2021

Innhold

1 Innledning **3**
1.1 Problemstilling 4
1.2 Oppgavens oppbygging og forskningspørsmål 4

2 Bakgrunn **6**
2.1 Tidligere forskning 6
2.2 Kunnskapshull 10

3 Teori **10**
3.1 Overvåkning og sosial kontroll 10
3.2 Sikkerhetisering 11
3.3 Hvitvasking og terrorfinansiering 12

4 Metode **13**
4.1 Informanter og intervjuer 14
4.2 Etiske vurderinger 15
4.3 Ulemper ved valg av metode 16

5 Analyse **16**
5.1 Krav om overvåkning 16
5.2 Definisjoner 21
5.3 Pålegg om mindre overvåkning 25
5.4 Utviklingen av overvåkningen 26
5.5 Meninger 29

6 Diskusjon **35**
6.1 Hvor skal grensen gå? 35

7 Konklusjon **38**

Refferanser **40**

A Intervjuguide **46**

Forord

Forfatteren av denne fordypningsoppgaven i Kriminologi jobber ved siden av studiene (eller kanskje heller studerer ved siden av jobben) i en av Norges største banker og har et arkitektansvar for bygging av overvåkingssystemer for anti-hvitvasking og anti-terrorfinansiering. Problemstillingen i denne oppgaven er sterkt relatert til dette arbeidet.

Det er ikke bare at dette spørsmålet kommer opp i diskusjoner av og til, men det er til tider svært viktig for utviklingen og det fremtidige arbeidet med systemene. Samtidig er den ingen som klart kan si hvor grensene for systemene skal gå. Kravene fra myndighetene fokuserer kun på hva man må gjøre, og ikke på hva som er *«nok»*.

Dette er bakgrunn og motivasjonen for denne oppgaven, et praktisk behov for å finne ut hvor ovennevnte grenser skal og bør gå.

Å skrive oppgaven uten å nevne forfatterens tilknytningen til en av de store bankene i Norge var ikke mulig, siden dette måtte komme opp i avsnittene om rekruttering av informanter og intervjuobjekter, samt de etiske vurderingene rundt dette. Derfor var bruk av anonymitet i oppgaven en utfordring, ettersom enhver som vet hvem forfatteren er, umiddelbart vil kunne knytte ham til denne oppgaven.

Oppgaven er imidlertid skrevet slik at en som ikke allerede kjenner til forfatteren, vil ha utfordringer med å avgjøre nøyaktig hvilken bank forfatteren jobber i.

Det er viktig å avklare at denne oppgaven er skrevet i forfatterens kapasitet som student ved Universitetet i Oslo, og ikke som ansatt i en av Norges største banker. Oppgaven reflekterer ikke banken sitt syn på problematikken som omtales.

Hvor langt er nok?

Et kriminologisk blikk på anti-hvitvaskingsarbeidet i finans-sektoren.

1 Innledning

Vil du tjene penger på kriminalitet, så er hvitvasking essensielt. Det er vanskelig å se for seg vinningsforbrytelser uten noen form for hvitvasking, som ett steg i prosessen til de kriminelle. Hvitvasking er også en aktivitet som er veldig vanskelig å avdekke for politiet.

For å bekjempe hvitvasking og terrorfinansiering er alle som fasiliterer overføringer av verdier i samfunnet[1], som banker, verdipapirforetak, eiendomsmeglere og advokater, pålagt å forebygge, avdekke og rapportere mistanke om hvitvasking og terrorfinansiering. Kravene til dette arbeidet blir også stadig mer omfattende.

Tiltak som kreves gjennomført er omfattende. Det estimeres at det i 2021 vil bli brukt 214 milliarder dollar globalt (LNRS, 2021) på arbeidet. Også i Norge blir det brukt store summer. Norges største bank, DNB, estimerer at de bruker over 1000 årsverk årlig bare på anti-hvitvaskingsarbeid[2] , og i realiteten er det nok mer. Til sammenlikning benyttes det kun 173 årsverk til dette i Økokrim[3].

Arbeidet med å avdekke hvitvasking og terrorfinansiering, ofte forkortet til AML[4] og CTF[5], kan deles opp i tre hovedområder; (1) Sanksjons screening, hvor en ser om en kunde eller part i en transaksjon er på en eller flere sanksjonslister[6]. (2) Know-Your-Customer (KYC) som tar for seg blant annet kundekontroll, risiko klassifisering, oppdatering av kundeinformasjon. (3) Aktivitetsovervåkning, ofte omtalt som Transaksjons Monitoring eller TM. Dette er hovedfokuset for denne oppgaven.

Denne aktivitetsovervåkningen er, som navnet indikerer, en overvåkning av hva kundene

[1] Den fulle listen er ramset opp i Hvitvaskingsloven § 4, og er ganske omfattende.

[2] DNB skriver på sine hjemmesider at de har 400 ansatte som jobber med anti-hvitvasking (DNB, 2021a), men informanter sier at de skal oppdatere dette til 600. Samtidig bruker mange ansatte deler av sin tid på AML-relaterte oppgaver, og da blir estimatet fra informantene *«minst 1000 årsverk»* uten nøyaktige tall.

[3] Oppgitt direkte fra Økokrim ved henvendelse

[4] **A**nti-**M**oney **L**aundering

[5] **C**ombating the **F**inancing of **T**errorism

[6] En sanksjonsliste er en liste med entiteter, som er på en eller annen måte sanksjonert. De vanligste listene for vestlige banker er FN, EU, Storbritannia, og USA (OFAC).

foretar seg. Til å begynne med var dette kun enkel kontroll, men har i senere tid blitt mer avansert med inntoget av ny teknologi, strengere krav, og mer omfattende datainnhenting.

Når både kravene til hva de finansielle institusjonene skal overvåke, og teknologien som blir brukt til dette stadig blir bedre, er det klart at overvåkningstrykket også stadig blir større. Da blir det naturlig også å stille spørsmålet: *Hvor mye er nok?*

1.1 Problemstilling

Når har man gjort nok for å avdekke hvitvasking og terrorfinansiering? Det er en balanse mellom flere interesser; Samfunnet som ønsker å redusere kriminalitet, individets rett til privatliv, og de finansielle institusjoners ønsker om minst mulig bruk av ressurser. Formålet med denne teksten er å belyse sistnevnte område ut fra et kriminologisk perspektiv. Mer presist blir problemstillingen følgende:

Problemstilling Hvor er eller bør den øvre grensen være for hvor mye overvåkning norske banker skal gjennomføre i jakten på hvitvasking og terrorfinansiering?

Omfanget av oppgaven begrenses til å hovedsaklig fokusere på hva banker skal og bør gjøre. Bankene kan ses på som de som har de mest omfattende kravene, og andre, som f.eks. advokater, vil ikke ha samme behov for fullskala overvåkning. Hva som gjelder for banker gjelder også i stor grad for betalingsformidlere. På samme måte begrenses det til norske forhold, for å unngå å gå forlangt inn på temaet om internasjonale reguleringer, selv om dette vil bli inkludert der det er naturlig.

Oppgaven vil heller ikke ta for seg de underliggende kriminelle handlingene, som hvitsnippkriminalitet og årsakene til dette.

1.2 Oppgavens oppbygging og forskningspørsmål

Selv om oppgavens omfang er noe begrenset ved å kun se på norske banker, er det behov for en del forskningsspørmål for å bryte ned problemstillingen ytterligere. Forskningsspørsmålene fokuserer på ulike sider ved den finansielle overvåkningen, og som på hver sin måte belyser problematikken.

Analysen starter i Kapittel 2 med å undersøke tidligere forskning på temaet og kontekstualisere oppgaven, og stiller følgende forskningsspørsmål:

Tidligere forskning Hva er tidligere skrevet om grenser for anti-hvitvasking og anti-terror overvåkning?

Kunnskapshull Hvilke hull er det i forskningen på området, og hva er behovet for mer kunnskap?

Analysen fortsetter så i Kapitel 3 med en gjennomgang av oppgavens teoretiske rammeverk, og Kapittel 4 hvor valg av metode og vurderinger rundt dette blir presentert.

I Kapittel 5 angripes problemstillingen fra fem forskjellige vinkler. Den første av disse vinklene, som belyst i Delkapittel 5.1, er hvilke krav som driver overvåkningen, og hvordan de vil utvikle seg i fremtiden.

Krav til overvåkning Hvilke krav til anti-hvitvasking og anti-terror overvåkning stilles til norske banker i dag, og hvordan vil kravene utvikle seg i fremtiden?

Neste steg, i Delkapittel 5.2, er å se nærmere på definisjonene av hvitvasking og terrorfinansiering. Kravene i lovverket kan forenklet sett komprimeres ned til *«finn hvitvasking og terrorfinansiering»*, men hvordan defineres disse formelt og brukes i praksis?

Definisjoner Hvordan defineres hvitvasking og terrorfinansiering?

Når krav og definisjoner er belyst, går analysen videre i Delkapittel 5.3 ved å prøve å avdekke om noen har gått for langt og har blitt pålagt av myndighetene å redusere overvåkningen. Hvis dette er tilfellet, gir dette en god indikasjon på hvor grensen går eller bør gå.

Pålegg om reduksjon Har noen fått pålegg om å redusere overvåkningen?

Etter å ha undersøkt om noen er blitt pålagt redusere overvåkningen, rettes det i Delkapittel 5.4, fokus mot hvordan den elektroniske overvåkningen har utviklet seg hos bankene. Hvordan har de tekniske kapabilitetene endret seg fra de første kravene kom til der vi er i dag, hvordan fungerer systemene, og hvordan er det sannsynlig at dette kommer til å utvikle seg i fremtiden?

Utvikling av overvåkningen Hvordan har overvåknings kapabilitetene og arbeidet i bankene utviklet seg, og hvordan kommer dette til å se ut i fremtiden?

Undersøkelsen avsluttes i Delkapittel 5.5 ved å spørre hva beslutningstagerne og tilsyn tenker om hvor grensene for anti-hvitvasking- og anti-terror overvåkning bør gå.

Meninger Hva mener personer og organisasjoner med innflytelse om hvor denne øvre grensen bør gå?

Oppgaven retter her spørsmål til tre grupper, tilsyn, beslutningstagere i banker, samt politikere. Til sammen gir svar på disse spørsmål et godt grunnlag for å forsøke å avklare hvor grensen for overvåkning bør gå, samt hvilke utfordringer som ligger i veien for å finne en slik grense, som diskuteres i Kapittel 6. Oppgaven avsluttes så med noen konkluderende tanker og forslag til veien videre i Kapittel 7

2 Bakgrunn

Som nevnt i innledningen, er anti-hvitvasking og anti-terror-finansieringsarbeidet blitt relativt komplisert de siste årene, og omfatter nå nesten alle handlingene en person gjør. Spesielt i Norge, hvor nesten ingen bruker kontanter (Norges Bank, 2020), er dette inngripende.

Overvåkningen dekker ikke bare, slik den gjorde før, større og grensekryssende transaksjoner, men all aktivitet bankkundene har med banken. Denne overvåkningsaktiviteten har ikke unngått søkelyset til den kriminologiske forskningen, selv om dette kanskje ikke er alment kjent.

2.1 Tidligere forskning

Selv om det er publisert mye om overvåkningen, har det fram til nå være få som prøver å klargjøre hvor grensene for overvåkningen skal gå. Felles for mye av det som er publisert rundt AML/CFT overvåkning er at dette fokuserer i stor grad på policy og det store bildet, heller enn å se situasjonen fra et mer detaljert perspektiv, slik målet i denne analysen er.

Hvorfor bryr folk seg ikke?

I artikkelen *«FINANCIAL SURVEILLANCE: Who cares?»* stiller Amicelle & Favarel-Garrigues (2012) seg spørsmålet om hvem det er som faktisk bryr seg om AML/CFT overvåkning. Amicelle & Favarel-Garrigues (2012) finner at finansiell overvåkning ikke genererer på langt nær like mye oppmerksomhet som andre relativt like tiltak, som svartelister, og kommer med tre hypoteser på hva dette skyldes.

Komplisert Den første hypotesen er at problematikken er vanskelig å formulere og kommunisere med massene. Dette gjenspeiles også i denne teksten, hvor bare det å forklare problemstillingen tar stor plass.

Ikke-statlig Den andre hypotesen er at folk ikke er like negative til private overvåkere enn statlige. Her argumenterer Amicelle & Favarel-Garrigues (2012) for at *«Banks are seen as commercial entities and not as the state's right arm»*.

Møter seg selv i døra Den tredje hypotesen er at de som normalt ville kritisert bankene for overvåkningen, er de samme som kritiserer staten for inngripen og de negative sidene ved det finansielle systemet. Amicelle & Favarel-Garrigues (2012) argumenterer med at det vil være vanskelig å forestille seg at den samme gruppen vil argumentere for mer hemmelighetshold for bankene.

Denne mangelen på interesse rundt problematikken viser noen av utfordringene med å finne hvor grensene skal gå. Spesielt kompleksiteten til spørsmålet gjør det vanskelig å holde en god debatt.

Hva driver utviklingen av overvåkningen?

Når det er slik at få bryr seg om denne overvåkningen, hva er det som da driver den fremover? Dette spørsmålet stiller Amicelle (2011) i artikkelen *«Towards a 'new' political anatomy of financial surveillance»*, og ser på dynamikken til finansiell overvåkning og risiko-bassert overvåkning i AML/CFT området. De observerer at det i Storbritannia er en sammenblanding av felles-regulering og felles-produksjon av overvåkning, som utfordrer tradisjonelle skiller mellom institusjonene. Tilsvarende dynamikk kan også finnes i andre land.

De finner at drivkraften bak denne utviklingen er en kombinasjon av tre faktorer; sporbarhet, fokus på risikobaserte tilnærminger, og arbeid mot sømløse felles informasjonsdelingskanaler. Mye av skylden for denne utviklingen, med utvasking av rollefordelingen mellom stat og privat, legger Amicelle (2011) på neoliberal politikk.

Flere andre, som Godefroy et al. (2012), legger mye av forklaringen til en *sikkerhetiseringprosess*, hvor den finansielle kriminaliteten i større og større grad blir et sikkerhetsproblem, som igjen helliggjør sterkere og sterkere midler i jakten på avvik. Spesielt rundt terrorfinansiering er dette tydelig.

Hva er farene med overvåkningen?

Med en slik storskala overvåkning er det flere farer for negative effekter. I artikkelen *«Governance, risk and dataveillance in the war on terror»* ser Amoore & de Goede (2005) på implementasjonen av risikoreduserende tiltak i anti-terror arbeidet, og fokuserer på hvordan denne tilnærmingen flytter mye av risikoen over på minoriteter. Amoore & de Goede (2005) argumenterer at dette fører til marginalisering, samtidig som at effekten på terroroppdagelse er diskutable.

Amoore & de Goede (2005) ser på flere aspekter ved dette arbeidet, deriblant finansiell overvåkning. Her peker Amoore & de Goede (2005) på faren for finansiell ekskludering som den store utfordringen, heller enn den generelle overvåkningsproblematikken slik som blir utforsket i denne oppgaven. Amoore & de Goede (2005) beskriver denne faren for ekskludering både på individnivå, hvor et enkelt individ har utfordringer med å få tilgang til banktjenester, men også hele regioner som får samme typen utforinger med tilgang til det finansielle systemet.

Hva rapporteres - mistanke eller abnormalitet?

Amoore & de Goede (2005) problematiserer også begrepet *mistenkelig transaksjon* og argumenter for at det er langt i fra klart hva som konstituerer *'mistenkelig'* i denne sammenhengen. Dette spørsmålet adresserer Amicelle & Iafolla (2017) i artikkelen *«Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing»* og utforskrer hvordan AML/CFT arbeidet *«produserer mistanke»* gjennom at de finansielle institusjonene har blitt lytteposter for politiet.

Amicelle & Iafolla (2017) beskriver at det blir stadig mer rapportering av *«mistenkelige transaksjoner»*, og denne rapporteringen bygger på en risiko-bassert tilnærming og igjen fører til en vurdering av hva som er normal og unormal atferd. Amicelle & Iafolla (2017) trekker fram tre elementer av dette arbeidet;

Mistanke og abnormalitet Rapportering av mistenkelige transaksjoner basserer seg på en kombinasjon av risiko og hva som er abnormalt, og det er denne abnormaliteten som sier hvor systemene skal lete.

Rapportering bassert på mistanke eller abnormalitet? Det er i praksis uklart om systemene rapporterer på bakgrunn av faktisk mistanke, eller om de rapporterer abnormal adferd.

Fortolkning Om noe er mistenkelig eller ikke er ikke et svart/hvit spørsmål. Det er i høy grad opp til fortolkningen av situasjonen å avgjøre. Dette fører til en utvasking av forskjellen mellom mistenkelig og abnormal adferd.

Amicelle & Iafolla (2017) konkluderer med at denne utvaskingen av forskjellen mellom mistenkelig og abnormal adferd fører til vanskelige politiske spørsmål, blant annet om diskriminering og ekskludering.

Både Amoore & de Goede (2005) og Amicelle & Iafolla (2017) legger her til grunn at grensen for hvor AML/CFT sitt arbeide og overvåkning må gå ett eller annet sted før det oppstår marginalisering av minoriteter og andre negative konsekvenser, uten å diskutere mer om hvor denne grensen skal gå. Amicelle & Iafolla (2017) peker også, implisitt, på at grensen bør gå ved mistenkelig adferd heller enn abnormal adferd.

Forholdet mellom AML/CFT og personvern

Overvåkningens motstykke er personvern, og hvordan forholdet medllom AML/CFT overvåkningen og personvernet diskuterer de Goede (2012) i artikkelen *«The SWIFT Affair and the Global Politics of European Security»*.

de Goede (2012) analyserer implikasjoner av den såkalte *«SWIFT affæren»*[7], når amerikanske myndigheter fikk tilgang til finansielle data for innbyggere i EU. de Goede (2012) bruker dette til å diskuere utfordringene med bruk privatiserte løsninger i sikkerhetsarbeidet.

de Goede (2012) argumenterer hvordan SWIFT affæren viser motsetningen mellom sikkerhet og personvern, og viser at denne saken har latt EU ta rolle som ledere internasjonalt når det gjelder dette. Denne diskusjonen om personvern og sikkerhet problematiserer mange av de elementene som er grunnleggende i AML/CFT overvåkningen, som blant annet om rettigheter blir ivaretatt og overvåket.

Hva de Goede (2012) her tar utgangspunkt i, er at det går en grense for overvåkning gitt av balansen mellom personvern og sikkerhet.

Samarbeidet mellom private entiteter og politiet

Hvem som gjennomfører overvåkningen er også av betydning for hvor grensene for overvåkning skal gå. I dag er mesteparten av den operative overvåkningen gjennomført av bankene med argumentasjon om at det er her det finnes mest kunnskap om dette. Dette samarbeidet mellom bankene og politiet er det flere som problematiserer. Blant annet Favarel-Garrigues et al. (2011) diskuterer dette i artikkelen *«Reluctant partners?: Banks in the fight against money laundering and terrorism financing in France»*.

Favarel-Garrigues et al. (2011) ser på hvordan banker og myndigheter samarbeider om AML/CFT i Frankrike, hvor samarbeidet har økt mye etter 2001, og spesielt for store banker. Banker ansetter tidligere politifolk, og jobber stadig tettere med politiet i saker som trenger finansiell etterretning[8]. Bankene finner seg stadig mer involvert i disse interaksjonene, tvunget av AML/CFT lovgivningen.

Alle aktørene har ulik motivasjon for arbeidet, hvor politiet stort sett ønsker å stoppe kriminalitet, sentralbankene å beskytte det finansielle systemet, og bankene beskytte seg selv mot tap[9].

Her kommer det fram to andre momenter til hvor grensene for AML/CFT overvåkningen skal gå. Disse er hvem som gjennomfører overvåkningen, samt kostnad. Spesielt bankene og den private industrien er, for å underdrive litt, interessert i å miste minst mulig penger på AML/CFT arbeidet.

[7] SWIFT er et International betalingsnettverk nettverk av banker, og er der «alle» internasjonale bankoverføringer blir gjennomført. Skal du overføre penger til en konto i f.eks. Turkmenistan, går nok den overføringen gjennom SWIFT. Innlands-, kort- og en del intereuropeiske betalinger går normalt ikke gjennom SWIFT.

[8] Informantene bekrefter at dette også er tilfellet i de større norske bankene.

[9] Denne artikkelen ble skrevet før praksisen med store bøter kom ordentlig i gang, men man kan bare anta at motivasjonen om å beskytte seg mot tap bare er sterkere, siden en bot også er et «tap».

2.2 Kunnskapshull

Som det er klart av den tidligere forskningen på AML/CFT overvåkningen, er det mye uklarhet på hvor grensen for overvåkning skal gå. Mange kommer innom spørsmålt, som blant annet Amicelle & Iafolla (2017), men få diskuterer det eksplisitt. Dette er kunnskapshullet denne oppgaven sikter å fylle, ved å se på spørsmålet om hvor grensene skal gå totalt sett, heller enn å kun se på ett og ett aspekt.

Hvor disse grensene går og bør gå er ikke bare av akademisk interesse, de har også svært praktiske implikasjoner. Fra et juridisk perspektiv bidrar det til å avgjøre om banker skal få straff for ikke å utføre sin del av overvåkningen, noe som kan være bøter på mange hundre millioner kroner i størrelse. Fra et operasjonelt perspektiv i bankene stilles det ofte spørsmål om *«er dette innenfor»*, både i implementasjonen av nye scenarier, og i utviklingen av nye IT systemer, og svarene er per i dag uklare. Disse og mange andre praktiske vurderinger avhenger av hvor grensene går.

3 Teori

Anti-hvitvasking og anti-terror foregår ikke i et vakuum og det er flere teoretiske rammeverk og begreper som er relevant for denne analysen. I denne analysen er det valgt å bruke en kombinasjon av sosial kontroll, overvåkningstudier, og sikkerhetiserings-perspektiver for å belyse problemstillingen.

Samtidig er det også mye forskning på hvitvasking, terrorfinansiering, og arbeidet med å avdekke de to, og grunnforståelsen av disse er også et viktig grunnlag for denne analysen.

3.1 Overvåkning og sosial kontroll

Overvåkning er handlingen å *«å observere, registrere og/eller lagre informasjon om objekter, fenomener, grupper og/eller individer»* (Løkke, 2018), og *Overvåkningsstudier*, eller *Surveillance studies*, er studien av av denne overvåkningen. Som Kriminologi generelt, er overvåkningstudier et bredt interdisiplinært felt som omfavner de teknologiske, fysiske, og sosiale aspektene, og tett knyttet til studier av sosial kontroll (Ball et al., 2012; Marx, 2015).

Sosial kontroll er *«[...] samfunnets ulike verktøy for å ordne og regulere seg selv, og de systemene og tiltakene som har som mål at mennesker skal oppføre seg innenfor rammene av det vi forstår som konform atferd eller «normal oppførsel».»* (Ugelvik, 2019, s. 13-14).

Et av de mest sentrale begrepene innen overvåkningsstudier og sosial kontroll er begrepet om det *panoptiske*, hvor alt blir sett. Begrepet panoptisk har sitt opphav i Jeremy Benthams ideer om *«panoptikon»*, et fengsel hvor fangene alltid kan bli overvåket, men aldri vet når de

blir sett (Ugelvik, 2019). Bentham mente at denne kontinuerlige følelsen av å bli overvåket presset de innsatte til å følge reglene. Selv om panoptikon var et fengesel, spredte ideen seg til flere andre institusjoner og la en grunnforståelse for at *folk oppfører seg anderledes når de blir sett*, og med AML/CFT overvåkningen, blir alt en bruker penger på, sett.

Et annet sentralt begrep innen overvåkningsstudiene er tanken om *net-widening*, og beskriver hvordan sosial kontroll gradvis utvides til flere og flere steder i samfunnet (Chriss, 2019). I forbindelse med overvåkning blir begrepet stadig mer integrert i flere aspekter av livet. Ett eksempel på *net-widening* er hvordan det stadig blir mer AML/CFT overvåkning i samfunnet.

Hvor mye overvåkning det er i samfunnet, og hvor AML/CFT overvåkningen er en del av dette, diskuteres gjerne i forbindelse med *«The maximum survilance society»*. Norris & Armstrong (2020) beskriver et idealsamfunn med maksimal overvåkning som *«The maximum survilance society»*. Dette idealsamfunnet er en abstrakt ide om hvor langt et samfunn kan gå i overvåkningen, selv om vi ikke er der nå (Ball et al., 2012). Motstykket til *The maximum survilance society* er det såkalte *«minimum survilance society*, hvor det er det er minimalt med overvåkning (Marx, 2015). Vårt samfunn er et sted mellom disse to idealtypene.

Med stadig mer overvåkning og data har ideen om *«predictive policing»*, hvor politiet bruker analytiske verktøy til å forutse hvor kriminalitet kommer til å oppstå, og hvem som kommer til å gjennomføre handlinger, blitt mer relevant (Meijer & Wessels, 2019).

Relaterte begrep til *predictve policing* er *«intelligence led policing»* som beskriver et risikoanalyse-drevet politiarbeid (Ratcliffe, 2016), og det mer generelle *«techno-policing»* som Nogala (1995) beskriver som et stadie hvor politiet fullt ut benytter seg av teknologi.

Mye av AML/CFT arbeidet sentrerer seg rundt risikovurdering av kundene, som i prinsippet prøver å predikere om en kunde har, eller kommer til å gjennomføre hvitvasking eller terrorfinansiering. Grensen mellom predictive policing og denne risikovurderingen blir da ganske liten.

3.2 Sikkerhetisering

Et begrep som er tett knyttet til moderne overvåkning er *Sikkerhetisering*. Buzan et al. (1998) beskriver sikkerhetisering med *«'Security' is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics»* (Buzan et al., 1998, side 23), og beskriver det som overgangen til et sted hvor det er kriminalpolitisk forankring til en sikkerhetspolitisk forankring de kriminalitetsforebyggende tiltakene. Tilsvarende definisjoner brukes også blant annet av Lomell (2012), Hegge (2015) og Kaufmann (2018)

I relasjon til AML/CFT så er arbeidet med anti-terror selve eksemplet på sikkerhetisering.

Ett eksempel på dette er hvordan Godefroy et al. (2012) beskriver anti-terrorfinansieringsarbeidet i franske banker som en sikkerhetiseringsprosess. Men sikkerhetisering er ikke begrenset til bare anti-terror. Anti-hvitvaskingsområdet går også gjennom en sikkerhetiseringsprosess.

3.3 Hvitvasking og terrorfinansiering

Siden begrepet hvitvasking først ble introdusert, har det stadig blitt mer forskning på temaet. Selv om det er mer forskning, domineres den moderne litteraturen på området av mer praktiske og industrirettede publikasjoner. Hva som er publisert kan deles inn i fire forskjellige områder; fenomenene hvitvasking og terrorfinansiering, AML/CFT etterlevelse, og AML/CFT teknologi.

Unger & Van der Linde (2013) beskriver hvitvasking som prosessen å gjøre penger fra kriminelle aktiviteter legitime. Hvitvasking deles normalt opp i tre faser; plassering («*placement*»), hvor midlene innføres i det finansielle systemet, fordekking/tilsløring («*layering*»), hvor koblingen mellom opphavet til pengene tilsløres, og integrasjon («*integration*»), hvor det er skapt et legitimt grunnlag for opphavet til pengene (Rui, 2012; Suszek, 2015).

Freeman (2011) beskriver penger som *livsblodet* til terror-organisasjoner, hvor de rett og slett ikke kan operere uten. Terrorfinansiering er hvor disse pengene kommer fra, og skiller seg fra hvitvasking i stor grad, selv om de tre fasene (plassering, tilsløring, og integrasjon) fremdels er anvendbare.

Terrorfinansiering skiller seg fra hvitvasking ved at opphavet til midlene i stor grad er lovlig[10], og at summene er relativt små[11] Freeman (2011). Terrorfinansiering følger også ofte i mindre grad de etablerte betalingsnettverkene, og bruker ofte andre, uformelle nettverk i stedet, som for eksempel *Hawala*[12]

Et annet område for studier er etterlevelsesindustrien («*the compliance industry*»), som i de siste årene har blitt svært stor. Verhage (2011) beskriver hvordan AML/CFT etterlevelse har endret seg fra å være en sideaktivitet til å nå være en sentral del i arbeidet i bankene, med store avdelinger i hver bank. Et sentralt tema er fremveksten av *AML Etterlevelses ansvarlige* («*AML Compliance Officer*»).

Pettersen & Wainio (2021) beskriver for eksempel hvordan banker og finansforetak reage-

[10] Her er det viktig å merke seg at flere terror organisasjoner også opererer større ulovlige foretak for å tjene penger, slik som for eksempel ulovlig tømmerhogst (Wagner et al., 2020; Boekhout van Solinge, 2008). Disse handlingene har mer tilfelles med hvitvasking, og kan regnes som et hybrid mellom de to.

[11] En informant fortalte at NAV kan anses for å være en av de større kildene til terrorfinansiering i Norge, da flere dømte terrorister har fått støtte fra dem under forberedelser.

[12] Hawala er et alternativt betalingsnettverk med opphav i Asia og er i stor grad basert på tillitt (Jost & Sandhu, 2000).

rer på implementasjonen av hvitvaskingsloven, og kravene som følger med. De peker blant annet på utfordringer med rolleblanding, kommunikasjon og mangel på motivasjon hos bankene, som problemer i forbindelse med den norske implementasjonen.

Å finne hvitvasking og terrorfinansiering har blitt et teknisk problem, for hvordan går man fram for å finne de ulovlige transaksjonene blant milliarder av lovlige? Spesielt innen fagfeltet maskinlæring er det publisert mye de siste årene, som Kute et al. (2021) har beskrevet. Kute et al. (2021) gikk gjennom 198 publikasjoner og fant at de fleste bruke veiledet, og ikke-veiledet maskinlæringsalgoritmer. Denne forskningen sier mye om hvilke kapabiliteter som eksisterer til å finne hvitvasking og terrorfinansiering.

4 Metode

Forskningspørsmålene stilt i Delkapittel 1.2 krever belysning med flere forskjellige metoder. Spørsmålene, lovkrav, og definisjoner krever et dypdykk i både regelverk, praksis, og akademiske tekster. Hvorvidt det har vært pålegg om mindre overvåkning og hva beslutningstagere mener om dette, krever en mer aktiv innhentende tilnærming. Hvordan utviklingen av overvåkningskapabilitenene utfolder seg krever en kombinasjon av analyse av tekster, vurdering av teknologi, samt ekspertenes vurdering på området.

For å møte behovene til hvert av de forskjellige forskningsspørsmålene, ble seks forskjellige metoder vurdert; litteraturanalyse, spørsmål per epost, innsynsbegjæringer, informanter, og intervjuer. Litteraturanalyse, og informanter ble brukt i arbeidet med alle forskningspørsmålene. Spørsmål og innsynsbegjæringer ble sendt ut i forbindelse med spørsmålene om pålegg av mindre overvåkning og meninger. Intervjuer ble kun brukt i forbindelse med spørsmålet om meninger.

Litteraturanalysen ble gjennomført gjennom en kombinasjon av brede og direkte rettede søk, samt analyse av annen tilgjengelig litteratur. Litteraturanalysen er også den metoden som har variert mest i omfang i denne oppgaven, og har blitt brukt i stor grad som supplement til de andre metodene.

I forbindelse med arbeidet om pålegg og meninger ble det sendt ut epost med spørsmål til en rekke forskjellige offentlige aktører, blant annet til Finanstilsynet, Datatilsynet, Økokrim, alle de politiske partiene og stortingsgruppene deres. Valget av aktører det ble sendt spørsmål til utviklet seg underveis i oppgaven, ettersom flere spørsmål kom opp.

Til enhetene omfattet av offentlighetsloven var dette en kombinasjon av innsynsbegjæringer i henhold til offentlighetsloven og spørsmål, mens til andre kun spørsmål. Ved uklarheter i svarene ble oppfølgingspørsmål stilt.

Alle sitater fra intervjuer, informanter, og spørsmål er godkjent med den som er sitert,

hvis personen er sitert ved navn.

4.1 Informanter og intervjuer

AML/CFT området er svært komplisert og vanskelig å få oversikt over, og for å få oversikt ble det i utstrakt grad brukt informanter til å supplementere og skape forståelse for hvordan bransjen fungerer i praksis. Tilsvarende ble intervjuene brukt til å gå litt dypere inn i spørsmålene. I denne oppgaven brukes utrykket *informant* om en som har blitt stilt og har svart på spørsmål om et eller flere tema, og svart på dette. Begrepet *intervjuobjekt* blir brukt om en som er intervjuet i en formell intervju-setting, hvor referat har blitt skrevet.

Rekruttering av informanter og intervjuobjekter er ofte en av de vanskeligere delene av en slik studie (Skilbrei, 2019). I dette tilfelle derimot, var dette ikke en utfordring grunnet forfatterens tilknytning til miljøet. For de som ikke allerede var en del av nettverket til forfatteren, var det kun sendt ut epost med spørsmål om de kunne delta på et intervju eller svare på noen spørsmål. Forøvrig er det ikke brukt noen annen spesiell metode for rekruttering.

Informanter ble valgt på bakgrunn av deres ekspertise på området, og intervjuobjekter ble valgt på bakgrunn av innflytelse i formingen av AML/CFT arbeidet i Norge. Begge grupper er rekruttert bredt blant flere av Norges største banker.

I forbindelse med rekrutteringen av intervjuobjekter ble også et antall medlemmer av stortingets finanskomité kontaktet, ettersom det er de som behandler saker som omhandler hvitvaskingsloven på Stortinget. Det var imidlertid ingen av medlemme som lot seg intervjue grunnet arbeidet med nasjonalbudsjettet, som foregikk i tidsperioden dette var aktuelt.

Gjennomføring av intervjuer

Intervjuene ble gjennomført utelukkende digitalt. Selve intervjuene ble gjennomført som en semi-strukturert, med kun fire spørsmål i intervjuguiden (se Tillegg A). Ettersom intervjuobjektene er normalt svært opptatt, ble intervjuene holdt så korte som mulig og målet var samtale på ca. 30 minutter, selv om et par ble vesentlig lengre. Intervjuene ble ikke tatt opp, og notater ble underskrevet umiddelbart etter intervjuet. Målet med intervjuene var å finne deres mening, ikke banken sin *«offisielle»* stilling.

Intervjuene ble valgt å ikke bli tatt opp av flere grunner, hvor den viktigste var at det ble ansett som lettere å få intervjuobjektene til å snakke fritt når samtalen ikke ble tatt opp. Alle intervjuobjektene uttaler seg i media med noe regelmessighet og en video på avveie kunne slått negativt ut for banken de jobbet for. Det var også et praktisk aspekt ved at intervjuene

ble gjennomført over Teams, og opptak ville være en utfordring[13].

4.2 Etiske vurderinger

Denne oppgaven har to potensielt etisk utfordrende elementer. Den første er at det en intervju/informant undersøkelse, og den andre er at forfatteren har profesjonell rolle i forbindelse med AML/CFT arbeidet.

Intervjuene i denne oppgaven har fokusert på intervjuobjektene sine generelle tanker rundt problemstillingen og relaterte spørsmål i kraft av deres profesjonelle rolle innen området. Det er heller ikke tatt opp noen video eller lagret informasjon annet enn enkle referater, uten noen sensitive eller kontroversielle tema, med navn og tidspunkt fra intervjuene. Det er derfor vurdert at det ikke er behov for søknad til Norsk senter for forskningsdata (NSD) i forbindelse med denne oppgaven. Det er ikke lagret noen liste eller referater vedrørende informanter.

Forfatterens rolle i AML/CFT arbeidet

Forfatterens rolle kan være etisk utfordrende, ettersom han jobber fulltid i en av Norges største banker med utviklingen av IT systemene, systemene som gjennomfører overvåkningen diskutert i denne oppgaven. Gjennom denne stillingen har forfatteren svært god tilgang til informanter, intervjuobjekter, og informasjon om hvordan systemene fungerer i praksis.

Denne rollen har gitt både fordeler og utfordringer i arbeidet med oppgaven. På den positive siden gir det svært god tilgang til ressurser og kunnskap om systemene det skrives om, men på den andre siden skaper det problematikk rundt relasjon til informanter og intervjuobjekter, og taushetsplikten gjennom jobbkontrakten.

Å intervjue og bruke kolleger som informanter, som er gjort til en viss grad i denne oppgaven, kan være en utfordring. For å motvirke eventuelle problemer, har alle spørsmål og diskusjoner vært av en profesjonell karakter, med få eller ingen personlige elementer. Ingen i forfatterens rapporteringslinje (sjefer) er blitt intervjuet. Samtidig er alle fakta, så langt som mulig, kollaborert med offentlige kilder. Alle som er brukt som informanter er blitt orientert om at spørsmålene gjelder en fordypningoppgave i Kriminologi, og om prosessen rundt dette.

Den andre større utfordringen er at forfatteren er underlagt taushetsplikt i forbindelse med arbeidskontrakten, og flere av systemene som er diskutert klassifiseres som sensitive. På bakgrunn av dette har alle fakta som kan være av sensitiv natur, enten vært hentet fra eksterne kilder eller klarert med beslutningstagere internt i banken. Oppgaven er også skrevet

[13] Flesteparten av intervjuene ble gjennomført gjennom en jobb-pc hvor det ikke er mulig å installere opptaksprogramvare.

slik at presis informasjon om sensitive tema ikke har vært nødvendig.

4.3 Ulemper ved valg av metode

Denne oppgaven bruker et bredt sett av metoder for å svare på et bredt sett med spørsmål, noe som i seg selv er en utfordring og kan redusere kvaliteten på den enkelte analysen.

Andre utfordringer med metodevalget er mangelen på kvantitative metoder. Flere av spørsmålene i denne oppgaven ville blitt styrket av kvantitative undersøkelser blant politikere, ansatte i banker, og mannen i gata.

Det er også en svakhet ved utvalget av informanter og intervjuobjekter, ettersom de fleste jobber i samme bransje som forfatteren. Dette kan potensielt føre til ekkokammer problematikk, noe som er forsøkt mitigert ved å innhente intervjuobjekter fra flere banker og institusjoner.

5 Analyse

Hvor grensene skal gå for anti-hvitvasking og anti-terrorfinansierings-overvåkning er et komplisert spørsmål, som krever å bli vurdert fra flere forskjellige perspektiver. Som beskrevet i Delkapittel 1.2, tar denne analysen for seg problemstillingen fra fem ulike vinkler.

5.1 Krav om overvåkning

Det første temaet som belyses i denne analysen er hvilke krav som rettes mot bankene i forbindelse med AML/CFT, hvor kommer de fra, og hvordan de fungerer i praksis. Fokuset blir hvordan disse kravene former overvåkningen, heller enn et juridisk dypdykk, det er allerede dekket i *Hvitvaskningsloven - Lovkommentar* av Rui et al. (2021), som også er en av hovedkildene til jurdiske betraktninger i denne oppgaven.

I Norge er hovedkravet til hva bankene er pålagt å overvåke definert i Hvitvaskingsloven[14]. Hvitvaskingsloven har som formål å *«[...] forebygge og avdekke hvitvasking og terrorfinansiering»* (Finansdepartementet, 2018, § 1.1). Den norske hvitvaskingsloven følger igjen EU sitt anti-hvitvaskingsregelverk, kjent nå som det femte-hvitvaskingsdirektivet[15].

Over kravene både til Norge og EU kan det sies at krevene til *Financial Action Task Force* (FATF) sitter. FATF er et internasjonalt samarbeid for å bekjempe hvitvasking og terrorfinansiering, etablert av G-20 landene. Sentralt i FATF sitt arbeide er det utviklet en liste med 40 anbefalinger for bekjemping av hvitvasking, samt etterlevelse av disse anbefalingene

[14] *Lov om tiltak mot hvitvasking og terrorfinansiering* - Finansdepartementet (2018)
[15] Det sjette-hvitvaskingsdirektivet er for tiden under utredning

(FATF, 2012). Disse anbefalingene er rettet mot statene og anbefaler hvilke lover og reguleringer statene bør gjennomføre. FATF sine anbefalinger stiller ikke krav om et elektronisk overvåkningssystem for AMF/CFT (Rui et al., 2021).

Flere av FATF sine anbefalingene beskrevier hvordan finansielle institusjoner skal samle inn og analysere data på jakt etter hvitvasking. Ett godt eksempel er anbefaling nummer 20, *Reporting of suspicious transactions*, som beskriver rapporteringsplikten:

> *«If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU). »* (FATF, 2012, s. 19)

Anbefalingene til FATF er ganske generelle av natur, men de setter det internasjonale rammeverket for anti-hvitvaskingsarbeidet.

Krav om elektronisk overvåkningssystem

Hvitvaskingsloven § 38 legger krav til at banker *«[...] skal ha elektroniske overvåkningssystemer for å avdekke forhold som kan indikere hvitvasking og terrorfinansiering»* (Finansdepartementet, 2018). Dette lovfestede kravet er spesielt for Norge og er ikke tilstede i hverken FATF sine anbefalinger eller EU sine direktiver (Rui et al., 2021, s. 387). Selv om kravet er særnorsk, så er det De facto standard at alle banker har et elektronisk overvåkningssystemer[16].

Dette særnorske kravet om elektronisk overvåkningssystem har sitt opphav i hvitvaskingsloven fra 2003, hvor det i *Odelstingsproposisjon 72* fremlegger forslag om kravet og finansdepartementet sier seg enig på bakgrunn av effektivitet (Finansdepartementet, 2003b):

> *«Departementet slutter seg til arbeidsgruppens forslag om å pålegge finansinstitusjoner en plikt til å etablere elektroniske overvåkningssystemer. [...] En forutsetning for et slikt pålegg må være at overvåkningen vil være et effektivt middel for å avdekke mistenkelige transaksjoner knyttet til straffbare handlinger. »*
> (Finansdepartementet, 2003b, s. 78)

Det gjøres riktig nok en del forutsetninger om hensiktsmessighet og volum, noe som gjenspeiles i lovens begrensning til finansinstitusjoner.

[16] Selv om det for noen små banker, gjerne som spesialiserer seg i svært rike individer, såkalte *Private Banking* banker, som kan ha et transaksjonsvolum som er lite nok til at alle transaksjoner kan vurderes manuelt.

Krav til det elektronisk overvåkningssystemet

Hvordan det elektroniske overvåkningssystemet skal være utformet sier derimot ikke loven noe om (Rui et al., 2021, Side 389). Dette blir gjort litt tydeligere i *Veilederen til Hvitvaskingsloven* (Finanstilsynet, 2019), hvor Finansdepartementet forklarer sin tolkning av Hvitvaskingsloven, og hva som forventes.

I Veilederen til Hvitvaskingsloven Seksjon *10.3 Elektronisk overvåkingssystem* beskrives kravene Finanstilsynet setter til det elektroniske overvåkningssystemet. Vi tar her for oss de kravene som er relevant for overvåknings-kapabilitetene.

Oppsett Veilederen legger krav om at oppsettet av det elektroniske overvåkningssystemet skal være solid, at feil og mangler oppdages og rettes opp, og at alle avvik skal dokumenteres. Finanstilsynet anser systemet som kritisk, noe som fører til at det omfattes av IKT-forskriften[17].

Regler Veilederen legger krav om at *regler*[18] blir forankret i risikoanalyser og at de er godt dokumentert. Bankene skal også ha *«rutiner for kvalitetssikring og evaluering av effekten av reglene»* (Finanstilsynet, 2019, side 79), og setter krav om at reglene skal justeres ved behov.

Omfang Veilederen sier at *«Transaksjoner fra alle foretakets systemer skal inngå i den elektroniske overvåkningen.»* (Finanstilsynet, 2019, side 79). I en bank som DNB kan dette bety at transaksjoner innhentes fra over hundre forskjellige systemer.

Hva skal man se etter?

Det er to måter å tolke hva bankene skal rapportere, og derfor se etter, basert på kravene i Hvitvaskingsloven[19]. Den første gruppen er det som er dekket av direkte, som hvitvasking, heleri[20], og terrorfinansiering (Rui et al., 2021, s. 64). Den andre gruppen er lovbrudd som er dekket av formålet til loven. Som Rui et al. (2021) argumenterer:

> *«Imidlertid er det slik at hensynet til å bekjempe profittmotivert kriminalitet er en sentral begrunnelse både for at heleri/hvitvasking er kriminalisert, og for at lovbruddene søkes forebygget og avdekket ved hvitvaskingsloven. Hvitvaskingsloven*

[17] IKT-forskriften er forskrift som setter krav til viktige systemer i finansforetak, og skal skal sikre at systemene er sikre og at dokumentasjon ivaretas (Finansdepartementet, 2003a).

[18] Ofte også kalt *scenarioer*, er den analytiske kjernen i overvåkningen. En *regel* er en analytisk kapabilitet som ser etter en type hvitvasking. Det kan være en SQL spørring, en teller, en maskinlærings-algoritme, og mye annet.

[19] Merk at det her fokuseres på hvilke krav som er gitt i Hvitvaskingsloven. Andre krav, som for eksempel for å avdekke pengespill, er ikke tatt med.

[20] Hvitvaskingloven sin definisjon omfatter både hvitvasking og heleri, se Seksjon 5.2.

> *har altså ikke bare som formål å forebygge og avdekke etterfølgende befatning med utbytte fra straffbar handling, men også å forebygge og avdekke de primærlovbrudd som utbyttet stammer fra.»* (Rui et al., 2021, s. 65)

Denne tolkningen av loven gir bankene bred fullmakt til å avdekke profittmotivert kriminalitet, men ikke nødvendigvis pålegg om å gjøre det. Lovtolkningen er noe omstridt blant jurister grunnet den brede fullmakten den gir bankene[21]. Dette gir tre forskjellige grupper lovbrudd sett fra Hvitvaskingsloven:

Direkte dekket Hvitvasking, heleri og terrorfinansiering er direkte dekket av Hvitvaskingsloven. Dette betyr at det er et klart krav at bankene skal av dekke og rapportere denne typen lovbrudd.

Indirekte dekket Profittmotiverte lovbrudd, som skattesvik, ran, tyveri, svindel, og liknende er dekket av det sentrale formålet med loven, og dekkes da gjennom tolkning av forarbeidene. Dette betyr at bankene har lov til, men ikke nødvendigvis plikt til, å avdekke og rapportere profittmotiverte lovbrudd.

Ikke dekket Ikke-profittmotiverte lovbrudd, som voldtekt, pedofili, grooming[22], voldshandlinger og likende er ikke dekket. Dette betyr at bankene ikke er pålagt å følge Hvitvaskingsloven for å se etter denne typen lovbrudd. Siden bankene da ikke er pålagt å lete etter det, har de heller ikke lov til dette grunnet personvernlovgivningen.

Risikobasert Hvitvaskingsloven § 6 sier at AML/CFT arbeidet skal være risiko-basert, noe som i prinsippet betyr at detaljstyringen for hva som skal avdekkes overlates til bankene og deres risikoanalyser (Rui et al., 2021, s. 131-147). Dette, kombinert med lovtolkningen over, gir bankene stort spillerom til selv å prioritere hvilke kriminelle handlinger de skal fokusere på.

Dette er den eneste delen i hvitvaskingslovverket som kan tolkes til å sette en øvre grense for overvåkningen, om enn indirekte. Ved å definere at AML/CFT arbeidet er risikobasert, kreves det i praksis en *kjent risiko* for at bankene skal ha hjemmel til å overvåke etter den. Denne risikoanalysen er derimot i stor grad opp til tolkning, bankenes risikoappetitt, og tilgangen til etterretning.

Den risikobaserte tilnærmingen er hva blant annet Amoore & de Goede (2005) trekker fram som en av farene, og er et område som, sammen med *kontinuerlig forbedring* tankegangen, kan føre til net-widening.

[21] En av informantene fortalte at dette er en pågående diskusjon, og at Finans Norge har bedt finanstilsynet om en klargjøring av dette punktet, og at det mest sannsynlig kommer en revisjon av Veilederen til Hvitvaskingsloven med dette.

[22] Straffeloven § 306. *Avtale om møte for å begå seksuelt overgrep* (Justis- og beredskapsdepartementet, 2005).

Forventninger

Det er som nevnt tidligere ikke bare selve de legale kravene over, som definerer hva som bankene må gjennomføre. Det er flere ting, som enten direkte eller indirekte som følge av loven og forskriftene finanstilsynet, forventer at bankene forholder seg til.

Institusjoner Det er forventet at bankene forholder seg til flere av publikasjonene til FATF. I følge informantene er det slik at det forventes fra myndighetene sin side at *«man skal være kjent med det FATF publiserer og implementere etter det»*, og dette relativt raskt. På denne måten har FATF ofte mer påvirkning over kravene som stilles, enn hva som er det rent legale. Et par gode eksempler her er FATF sine rapporter på Menneskesmugling (FATF, 2018a) og Profesjonell hvitvasking (FATF, 2018b), hvor bankene nå er forventet å ha kapabiliteter på plass for å bekjempe dette.

Det samme gjelder også for blant annet rapporter, veiledninger, og anbefalinger fra flere andre tone-angivende institusjoner, som FN, EU, Interpol, og Europol.

Andre banker Andre banker presser også hverandre til å bli bedre, og dette trykket kan ofte være kraftigere enn hva myndighetene står for. De fleste bankene i verden er tilknyttet SWIFT nettverket, og har såkalte korrespondent banker[23]. Hvitvaskingsloven § 19 første ledd bokstav b sier at bankene skal *«vurdere respondentinstitusjonens tiltak mot hvitvasking og terrorfinansiering»*, (Finansdepartementet, 2018), og andre land har tilsvarende lover.

Dette fører til at hvis en bank ikke tilstrekkelig kan bevise at de gjennomfører AML/CFT arbeid ovenfor andre banker, så kan de miste tilgangen til det internasjonale behandlingsnettverket og viktig valutta. Dette fører blant annet til at de fleste større norske banker gjennomfører sanksjonsscreening ikke bare for de listene norske myndigheter krever, men også for flere andre lister som kreves av banker i andre land.

En av informantene i DNB fortalte om at etter at DNB fikk en bot på 400 millioner kroner i 2021[24], måtte bankens ledere innen AML/CFT området møte flere korrespondentbanker for å forklare boten. Tilsvarende gjøres i alle banker, når en korrespondent har fått bot eller negative tilbakemeldinger fra tilsyn.

[23] En korrespondentbank er, litt forenklet, en bank som banken har avtale med for om å overføre midler til. Dette er nødvendig når en skal overføre penger over landegrenser til land hvor en ikke er knyttet til det lokale oppgjørsnettverket. En overføring blir da gjort til banken sin korrespondent, som har filial i mottaker landet, som overfører pengene videre til destinasjonen. Det kan gjerne være 1-2-3 korrespondentbanker i en overføring.

[24] *Vedtak om overtredelsesgebyr* - 19/12479 - Finanstilsynet (2021)

Utlandet

Hvitvaskingsloven §39 krever at hvis en norsk bank har filial eller datterselskap i et annet land, skal filialen eller datterselskapet følge den lovgivningen som er strengest (Rui et al., 2021, s. 394)

Flere av de større bankene i Norge har filialer i andre land, og må derfor også etterleve lokale anti-hvitvaskingsregler i hvert land. Kravene i andre land, spesielt i land som USA, Storbritannia, og Singapore er ofte strengere enn i Norge. Andre land igjen, slik som Sverige, har likere regelverk og finanstilsyn, og som stoler på det norske finanstilsynet[25].

Regelverkene i utlandet er, mye takket være FATF, ganske like det vi har i Norge. Det er mye de samme lovkravene til rapportering, etterforskning, kundeopplæring, og screening, med lokale variasjoner. Disse lokale variasjonene blir også forsterket av forskjell i tolkning og håndhevelse. En informant fortalte at de hadde utfordringer med det europeiske regelverket, selv om det er et samme felles europeiske regelverket som er implementert i alle landene (det femte hvitvaskingsdirektivet). Problemet lå i at de forskjellige finanstilsynene tolker direktivet forskjellig. En kan derfor ikke bare gjøre det samme i alle land.

Ett annet eksempel på denne forskjellen er kravene til testing av deteksjonssystemene. Veilederen til hvitvaskingsloven sier at *«Foretaket skal ha rutiner for kvalitetssikring og evaluering av effekten av reglene»* (Finanstilsynet, 2019, s. 79). Når tilsynet er på besøk så ser de i all hovedsak på om banken har rutiner som dekker kravene, og lar det bli med det. I USA, mer presist New York, derimot er de mye strengere. Med hjemmel i *504*-regelen[26] holder det ikke bare at en har rutiner, systemene skal testes statistisk (Pleune, 2018). Dette gjelder svært bredt, og kan involverer ende-til-ende validering[27] av alle transaksjoner gjennomført.

Det er altså ikke bare norske krav som definerer hva som er forventet, når en bank skal implementere anti-hvitvaskingskapabiliteter.

5.2 Definisjoner

Hvitvaskingsloven er rettet mot hvitvasking og terrorfinansiering, men hvordan defineres disse begrepene? Disse definisjonene er tett knyttet til hvor grensen for anti-hvitvaskingsarbeidet skal gå. Med en vid definisjon faller alt inn under hvitvasking, med en snever definisjon faller mye gjennom.

[25] Flere av informantene har jobbet tett med etterlevelsesarbeidet i landene nevnt, og kjenner til hvordan tilsynene og regelverkene håndheves internasjonalt.

[26] *New York State Department of Financial Services' Part 504 rule*

[27] ende-til-ende validering er når en trekker ut de samme data fra både starten av en verdikjede, f.eks. betalingssystemene, og fra enden, som f.eks. anti-hvitvaskingssystemet, og validerer at dataene er de samme, og at ting fungerer som det skal.

Definisjon av Hvitvasking

Hvitvasking kan defineres på flere forskjellige måter. Opphavet til begrepet *Hvitvasking* er ofte koblet til Al Capone[28], hvor han brukte vaskerier for å skjule opphavet til pengene (Unger & Van der Linde, 2013). Vi skal her se litt på hvordan selve begrepet Hvitvasking er definert.

Formaldefinisjon Hvitvasking defineres formelt i Norge i Straffeloven §337 bokstav a, som at en *«[...] yter bistand til å sikre utbyttet av en straffbar handling [...]»*, og b, som at en *«skjuler eller tilslører hvor utbyttet av en straffbar handling han selv har begått»* (Justis- og beredskapsdepartementet, 2005). Det spesifiseres også en rekke forskjellige metoder for overførsel og tilsløring av opphav, og kan i stor grad tolkes veldig bredt (Wegner, 2015, side 277-282).

I tillegg til Straffeloven har vi også en definisjon i Hvitvaskingsloven som igjen peker på Straffeloven sin definisjon, men inkluderer i tillegg også definisjonen for Heleri (Finansdepartementet, 2018). Heleri defineres i Straffeloven §332 som *«[...] den som mottar eller skaffer seg eller andre del i utbytte av en straffbar handling.»*. I følge Rui et al. (2021, Side 63) er den norske lovgivningen blant de vidtgående i Europa grunnet denne tilnærmingen.

Veilederen til Hvitvaskingsloven (Finanstilsynet, 2019, side 7) definerer hvitvasking som *«Hvitvasking er all befatning med utbytte fra straffbare handlinger»*.

Internationale definisjoner Det er ikke bare i Norge vi har en definisjon av Hvitvasking. EU deinerer hvitvasking som *«Money laundering is the process by which criminal proceeds are "cleaned", so that their illegal origins are hidden»* på sine nettsider (European Commission, 2021). The Financial Action Task Force (FATF) definerer hvitvasking som *«Money laundering is the processing of these criminal proceeds to disguise their illegal origin»* (FATF, 2015), ganske likt som EU. USA har tilsvarende definisjoner.

Akademiske definisjoner De akademiske definisjonene av Hvitvasking sammenfaller i stor grad med de internasjonale. Unger & Van der Linde (2013) definerer Hvitvasking som *«[...] the disguising of the illicit origin of money [...]*. Andre som Levi (2002) fokuserer mer på hvordan definisjonen av Hvitvasking både varierer i de ulike land, men også hvordan den utvikler seg. Det er varierende hvor stenge og presise definisjoner er, til de svært brede definisjoner. Levi (2002) bruker er en mer folkelig definisjon; *«In essence, it encompasses any concealing of the proceeds of drug trafficking (or other serious crimes) beyond putting the loot visibly on the bed or in one's domestic safe»*.

[28] *Alphonse Gabriel Capone*: Beryktet gangster under forbudstiden i USA, som hovedsaklig opererte i Chicago (Pasley, 2020)

Det er mange definisjoner av hvitvasking, men essensen er at det har med å skjule opphavet til kriminelle midler. En god definisjon er da:

> ***Hvitvasking:*** *Handlingen å skjule eller bidra til å skjule opphavet til midler med kriminelt opphav.*

og det er denne definisjonen som blir brukt videre i denne teksten. Denne definisjonen passer også godt med den norske formaldefinisjonen, selv om definisjonen i Veilederen (Finanstilsynet, 2019) er enda videre.

Definisjon av Terrorfinansiering

Hvitvaskingsloven legger ikke bare krav om at institusjonene skal finne Hvitvasking, men også Terrorfinansiering. Definisjonen av Terrorfinansiering er i stor grad knyttet til definisjonen av terrorisme, uten at vi her skal gå i detalj på dette.

Formaldefinisjon Terrorfinansiering er formelt i Norge definert i Straffeloven §135, som *«[...] rettsstridig yter, mottar, sender, fremskaffer eller samler inn penger eller andre formuesgode [..]»* som brukes til handlinger dekket av Straffeloven §§ 131, 134, 136 b, 137-144, eller kort forklart, til terrorisme (Justis- og beredskapsdepartementet, 2005).

Som for Hvitvasking, henviser Hvitvaskingsloven til Straffeloven sine definisjoner, §§ 135 og 136 b (Finansdepartementet, 2018). Veilederen til Hvitvasking er mer spesifikk i sin definisjon: *«Terrorfinansiering er finansiering av terrorhandlinger, terrororganisasjoner eller individuelle terrorister»* (Finanstilsynet, 2019).

Internationale definisjoner Internasjonalt definer de fleste terrorfinansiering på samme måte som i Norge. FN definerer Terrorfinansiering som *«Terrorist financing encompasses the means and methods used by terrorist organizations to finance their activities.»* (UNODC, 2021). Ett eksempel er Australia sin versjon av vår straffelov, hvor Terrorfinansiering defineres som:

> *(a) the person intentionally:*
> (i) *makes funds available to another person (whether directly or indirectly); or*
> (ii) *collects funds for, or on behalf of, another person (whether directly or indirectly); and*
> *(b) the first-mentioned person is reckless as to whether the other person will use the funds to facilitate or engage in a terrorist act.* (AAG, 1995, Divisjon 103 a)

Selv om definisjonene på terrorfinansiering er ganske lik rundt omkring i verden, er det også

klart at hva som anses som terrorisme, og følgelig hva som dekkes av anti-terrorfinansiering kan variere. Hva som er ansett som terrorisme i USA er ikke terrorisme i Pakistan.

Akademiske definisjoner Det er skrevet mye om terrorfinansiering i litteraturen, men få eksplisitt definerer grensene for hva som er og hva som ikke er dette. To eksempler, Levi (2010) og Freeman (2011) skriver begge i detalj om Terrorfinansiering, men definerer det aldri eksplisitt. Dette er en gjennomgående trend i litteraturen.

Forskjellen i definisjoner av Terrorfinansiering virker å være mindre enn for Hvitvasking. De fleste definisjonene peker på det å bidra til å finansiere terrorhandlinger, enten det er med penger eller handlinger. Dette gir oss følgende definisjon å jobbe med:

> ***Terrorfinansiering:*** *Handlingen å bidra til eller finansiering av terrorhandlinger. eller forberedelser til terrorhandlinger*

hvor selve terrorbegrepet er blir arvet fra lokale eller internasjonale praksiser[29].

Definisjon i praksis

I praksis blir definisjonen av Hvitvasking og definisjonen av Terrorfinansiering brukt om hverandre, som man ofte ser gjøre seg gjeldene i forkortelsen «AML/CTF». I følge flere av informantene så har de som jobber operativt med AML arbeidet ofte med en ganske løs forståelse av definisjonen og ser mer på det som at *«de skal finne kriminalitet»*.

Dette gjør seg også gjeldene i hvordan bankene organiserer overvåkningen. Ofte er den eneste måten en kan skille hvitvasking fra en lovlig transaksjon, er å se på opphavet til midlene, eller andre faktorer om partene eller deres handlingsmønster og aktiviteter. Dette fokuset på omstendighetene rundt transaksjonen heller enn selve overføringen, fører til at spørsmålet ofte blir *«hvilke kriminelle handlinger skal vi se etter?»*. Det er også klart at *«alt»* ikke er et særlig produktivt svar, selv om flere definisjoner hentyder det. Det er rett og slett ikke mulig med de ressursene som er tilgjengelig.

Her har vi altså en begrensning i definisjonen på opphavssiden som stammer fra praktiske begrensninger. Den andre siden er formålet med midlene. Her er det Terrorfinansiering som er er det man formelt ser etter, men igjen blir dette vagt i praksis. Samtidig er det andre formål som man også ser etter, som for eksempel kjøp av seksuelt misbruk av mindreårige i asiatiske land over nettet[30].

[29] Å definere Terrorisme globalt er en vesentlig større oppgave en hva jeg tar for meg i denne teksten.

[30] En type nettovergrep er at en person betaler for at ett mindreåring barn skal bli utsatt for overgrep, og dette strømmes direkte over nettet. Ett eksempel på dette er beskrevet av Bjørgan & Kolseth (2021).

Det er her klart at den praktiske definisjonen nok avviker en del fra de idealiserte nevnt tidligere. En fungerende praktisk definisjon, som også inkorporerer både hvitvasking og terrorfinansiering vil da være:

> ***Praktisk definisjon:*** *Handlingen å skjule opphavet eller formålet til midler hvor enten opphavet og / eller formålet med midlene er ulovlig og hvor de ulovlige handlingene er «viktige nok»*

Her er begrepet *«viktige nok»* sentralt, for hvem avgjør hva som er viktig nok? I praksis er dette en uklar prosess som involverer risikoanalyser, mangelfulle data, juridiske diskusjoner, og mageføelelser.

Et begrep som eksemplifiserer utfordringen med å avgjøre hva som er viktig nok, er den såkalte *VG-testen*[31]. VG-testen går ut på at en prøver å forestille seg hvordan avisen Verdens Gang (VG) ville reagert på det man gjør. For eksempel kan diskusjonen stå på hvorvidt man skal melde en som mistenkes for pedofili til Politiet. Her er situasjonen at en teknisk sett ikke nødvendigvis har hjemmel til å gjøre det, men ved hjelp av VG-testen er det enkelt å se at hvis man ikke melder det til Politiet, er PR konsekvensene vesentlig større enn hvis man rapporterer og ikke skulle ha gjort det.

5.3 Pålegg om mindre overvåkning

I Delkapittel 5.1 og 5.2 har det blitt klart at det er små muligheter i hvitvaskingslovverket til å fastslå at en kan gå for langt i overvåkningen. Dette vil ikke nødvendigvis si at det er umulig, bare veldig vanskelig. Det er også andre regelverk som kan benyttes, uten at dette er noe som blir gått nøyere gjennom i denne oppgaven, som kan pålegge reduksjon i overvåkningen. Ett av disse regelverkene er personvernslovverket. På bakgrunn av dette er det forsøkt å avdekke om noen har blitt pålagt å redusere overvåkningen, hvor hypotesen er at det ikke er det.

Selv om det teoretisk er umulig å bevise at ingen har blitt pålagt å overvåke mindre[32], har det blitt gjort et forsøk på å sannsynliggjøre at det ikke har skjedd. Spørsmål og innsynsbegjæringer har blitt sendt til finanstilsyn og datatilsyn i en rekke land, nettet har blitt søkt systematisk, og det utvidende nettverket er spurt om de har hørt i det minste et rykte om at det har skjedd.

Og svaret er et klart *«nei»*. Ingen av tilsynene har pålagt det, ingen i nettverket har hørt om det, og ingen har skrevet om noen sak på nettet.

[31] Denne testen har flere forskjellige navn i forskjellige miljøer, men går i all hovedsak ut på det samme.

[32] Å bevise at noe ikke har skjedd er ikke mulig. Det en logisk feil kalt *«argumentum ad ignorantiam»*, eller et *«argument fra ignoranse»*, en av de klassiske logiske feilene en kan gjøre.

Dette er en god indikasjon på at dette er ikke et tema på dagsorden blant tilsynene, noe som også ble bekreftet av det norske finanstilsynet direkte.

5.4 Utviklingen av overvåkningen

Metodene og teknologien som brukes i overvåkningen er hele tiden i utvikling, noe som former ikke bare grensene, men også mulighetene for overvåkning. Kartleggingen av denne utviklingen, og tanker om fremtidig utvikling, baserer seg på informanter som har vært en del av utviklingen siden den startet, samt historisk litteratur.

Drivere av utviklingen Informantene beskriver tre hovedfaktorer i utviklingen, selv om alle faktorer er avhengig av hverandre; hvor den første og viktigste er kravet fra myndighetene. Bankene skulle jo, som en av informantene beskrev det, helst ha sluppet å gjøre det, det koster jo penger. Den andre faktoren er tilgjengelighet av teknologi, det som tidligere var umulig er i dag relativt enkelt[33]. Den tredje faktoren en våpenkappløpet mellom overvåket og overvåker, mellom kriminelle og bankene. Hvitvaskere finner alltid nye måter å vaske pengene sine på.

Store beløp og rapportering

Utviklingen starter på mange måter med den amerikanske *«Bank Secrecy Act»* fra 1970, som var den første rettede anti-hvitvaskingsloven i USA (FinCEN, 2021). Den påla banker journalføring av transaksjoner og rapportering av større kontante transaksjoner over 10 000 USD[34]. Fokuset her var å rapportere store overføringer og innskudd. Denne tilnærmingen varte mange år, men ble strammet inn ved flere senere lover. Liknende krav kom også senere til Norge.

Fra et overvåkningsperspektiv var det viktige i denne perioden, at det var ganske snevre krav for hva som skulle rapporteres. Det var ikke en helhetlig overvåkning av kundene sine aktiveteter, bare enkle regler.

Sanksjons screening

Den neste, større endringen i overvåkningen var inntoget av *Sanksjons Screening* på 1990 tallet. Sanksjons Screening foregår på to måter, først undersøkes det om bankens kunder er på en sanksjonsliste, altså en liste over individer eller selskaper som er sanksjonert. Den

[33] En av informantene fortalte om et anti-hvitvaskingsscenarie som på 2000 tallet brukte nesten 24 timer på å kjøre, nå kunne ha kjørt på sekunder eller minutter.

[34] Denne grensen ga opphav til hva som i dag kalles *strukturering* eller *smurfing*, hvor en kriminell setter inn mange beløp like under rapporteringsgrensen for å unngå å bli rapportert.

andre måten er at det før hver transaksjon blir gjennomført, skal alle personer involvert i transaksjonen bli screenet mot sanksjonsliste.

Her har altså overvåkningen utviklet seg videre til også å ta hensyn til personene sin identitet. Dette førte også til enda strengere krav rundt hvilken informasjon som skulle følge med hver transaksjon. Det er fremdeles relativt enkle analyser - *er navn x på liste y?* - men noe større omfang.

Transaksjons monitoring

Når kravene om *Transaksjons Monitorering* kom i 2003 ble overvåkningstrykket kraftig utvidet. Fra kun å se på enten kunder eller transaksjoner uavhengig av hverandre[35], ble det nå krav om at bankene skulle se på helheten. Kravet var og er at bankene skal identifisere *mistenkelige transaksjoner* og rapporetere disse til myndighetene.

Måten denne overvåkningen stort sett fungerer er at en definerer en rekke *scenarier* som er rettet mot en *typologi* av hvitvasking eller kriminalitet. Disse scenarioene blir oftest definert i enten regel-, eller SQL[36]-baserte motorer. Dette er enkle analytiske systemer som har noe begrenset kapasitet, selv om det i teorien er mulig å gjøre svært avanserte analyser med SQL.

Begrensningen i regel-, og SQL baserte systemer ligger ofte i bruken av systemene heller enn i selve teknologien. Selv om scenariene nå overvåker handlingsmønsterene til kundene, så må det fremdeles presist defineres hva en ser etter, noe man ofte ikke helt vet hva er. Dette fører til enorme volum av falske alarmer som må manuelt gjennomgås. Denne utfordringen er, blant annet, bakgrunn for den utvikling som skjer i dag.

Avansert analyse

I de siste årene har det vært en rivende utvikling innen AML med inntoget av mer data og avansert analyse. *Avansert analyse* er en samlebetegnelse for alle analytiske metoder som *'ikke er enkle'*[37], og omfatter tyngre statisktiske modeller som maskinlæring, data-mining, og graf-analyse.

Det er liten tvil om at dette er kommet for å bli, og alle informantene som ble spurt er enige om dette. Utviklingen kan sies å være drevet av stadig sterke krav fra myndighetene, hvor gamle metoder ikke kan dekke behovet, samt ønsket om færre falske alarmer.

For å forstå hva inntoget av ny teknologi betyr for overvåkningstrykket, må selve teknologien forståes. Det er ikke bare "mer overvåkning", det er grunnleggende forskjeller mellom

[35] Dette er en liten forenkling, siden en del AML-tiltak allerede eksisterte.

[36] **S**tructured **Q**uery **L**anguage: Et programmeringsspråk for systematisk uthenting av data fra en database.

[37] Det er ingen god definisjon på hva Avansert Analyse er, men beskrives som helt eller delvis autonome systemer som bruker mer avanserte metoder enn hva som vanligvis finnes innen *Business Intelligence* (foretningsanalyse)

hva som er gjort før og hva som er under utvikling.

Mer data Den kanskje viktigste utviklingen i nyere tid er at det stadig blir mer data tilgjengelig for AML systemene. Der hvor det tidligere bare var begrensede kundedata og transaksjoner, innhenter nå systemene stadig mer informasjon. Denne informasjonen kan være enhetsider[38], offentlige registre, og mye annet. Enkeltvis angir ikke hver av disse dataene så mye, men sammen gir det en stor effekt. Dette er virkelig et sted for summen er større en summen av delene.

Maskinlæring Maskinlæring er egentlig bare avansert statistikk. Maskinlæring deles stort sett opp i *Supervised*, hvor man har nok eksempler på hva man skal finne og trener algoritmene til å finne det, *Unsupervised* hvor algoritmene selv finner potensielle mønster i dataen, og *Reinforcement Learning* hvor algoritmen lærer av sine egne feil. Kute et al. (2021) finner at majoriteten av forskningen inne AML feltet er Supervised og Unsupervised med bare ett tilfelle av Reinforcement Learning.

Maskinlæring har et stort potensiale til å finne den proverbiale nålen i høystakken, som hvitvasking er. Maskinlæring spesialiserer seg på å se mønstre i data, noe som mennesker ikke klarer, og flere har gode resultater. Ett norsk eksempel på bruk av maskinlæring innen AML arbeidet er beskrevet av Jullum et al. (2020), hvor de bruker en såkalt *XG-Boost* algoritme for å finne hvitvasking.

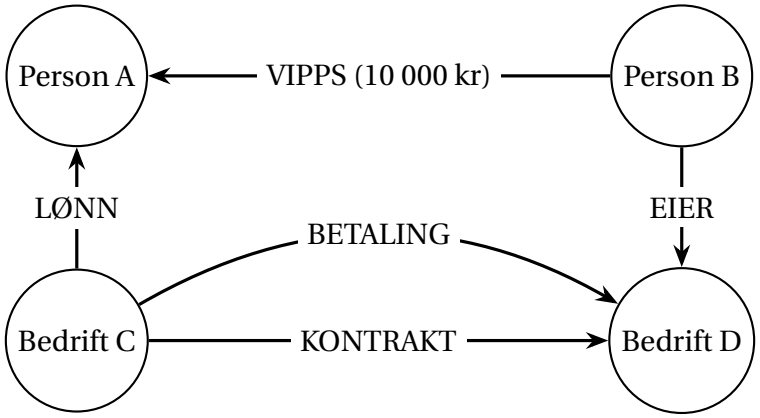
Graf-analyse En graf er en kombinasjon av *noder* og *kanter*, hvor noder kan være personer, eiendeler, bedrifter, og mye annet, mens kanter er relasjonene mellom nodene. Et enkelt eksempel på en graf er vist i Figur 1, hvor det ser ut som at Person B bestikker Person A for at hans selskap (Bedrift D) skal få en kontrakt med Bedrift C. Slik graf analyse, når satt i kombinasjon med de store datamengdene nevnt tidligere gir formidable overvåknings kapabiliteter. Flere, som Li et al. (2020), Dreżewski et al. (2015), og Tiwari et al. (2020) konkluderer med at graf-anslyse er kraftig verktøy for å finne hvitvasking.

DNB (2021b) skriver at de har 2,1 milioner privatkunder og 232 tusen bedriftkunder. Samtidig kan det forventes at de kan identifisere lønnsutbetalinger og vipps overføringer blant transaksjonene til kundene. Med disse data er det enkelt å bygge mesteparten av eksempelet i Figur 1.

Informanter i DNB sier at de jobber med graf-teknologi for å avdekke hvitvasking. Det samme gjør også Europool[39], og det kan forventes at mange andre innen samme område gjør

[38] Omtrentlig en unik identifikator for fra hvilken enhet kunden logget seg inn på nettbanken

[39] Europol har ikke offisielt sagt at de satser på satser graf-systemer, men i en stillingsutlysning fra Mars 2021 skriver de at *«[...] graph databases (e.g. NEO4j, ArrangoDB)»* er ønskelig (Europol, 2021)



Figur 1: Eksempel på en graf. Grafen viser et potensielt tilfelle av korrupsjon. Person A mottar en VIPPS overføring fra Person B, Person A mottar lønn fra Bedrift C, Person B eier Bedrift D, og Bedrift C har gitt en kontrakt til Bedrift D, og betaler for dette. Ingen av disse relasjonene er mistenkelige i seg selv, men når man ser dem i sammenheng blir det mistenkelig.

det samme.

Det er ikke bare i stor-data området hvor grafer er nyttige. Eksempelet i Figur 1 er et eksempel på *graf-visualisering* som blant annet Singh & Best (2019) konkluderer med kan styrke etterforskningen, og er allerede på plass i banker som DNB.

Teknologiske grenser for overvåkningen

Det er ikke bare hvilke lover som gjelder og hvor mange som jobber med overvåkning, som avgjør hvor høyt overvåkningstrykket er. Teknologien som brukes er også svært viktig. Det har helt klart vært en stor utvikling det som i starten var manuelle rapporteringer av store transaksjoner, til i dag hvor avansert analyse og *«stordata»*[40] er tatt i bruk.

Denne utviklingen viser tegn på en stille net-widening effekt, for selv om ingen endrer kravene eller flere jobber med å overvåke, vil overvåkningstykket, på grunn av den stadig forbedre teknologien, øke.

Med stadig forbedret teknologi følger også en økning i den teoretiske øvre grensen for hvor mye overvåkning som er mulig å gjennomføre med de midlene samfunnet setter til rådighet.

5.5 Meninger

Hva beslutningstagere og institusjoner mener om hvor grensene for AML/CFT skal gå er en viktig del spørsmålet stilt i denne oppgaven. Det er denne gruppen som i praksis avgjør i

[40] «Stordata» er datasett som har en størrelse eller kompleksitet som vanskeliggjør tradisjonelle analysemetoder (Dvergsdal & Elster, 2019).

hvilken retning politikken og lovene vil utvikle seg, og hvor grensene går i praksis. Det ble innhentet meninger fra tre forskjellige grupper, tilsynsmyndigheter, banker, og politikere.

Tilsynsmyndigheter

Tilsynsmyndighetene har på papiret kun som oppdrag å føre tilsyn med at de lover og forskrifter som gjelder blir etterlevd. I praksis derimot er tilsynenes tolkninger av lover og regler, og råd i lovprosesser svært viktig. For å få tilsynenes vurdering av hvor den øvre grensen skulle gå, ble det sendt ut til blant annet *Finanstilsynet* (Norge), *Datatilsynet* (Norge), *Økokrim* (Norge), *Monetary Authority of Singapore, Financial Conduct Authority* (Storbritania), og *European Data Protection Supervisor* (EU).

Utvalget av tilsyn ble bestemt på bakgrunn av hvilke tilsyn som er kjent for sin åpenhet og hvilke som har stor påvirkning på den norske utviklingen innen bankvesenet.

Finanstilsyn Finanstilsynene var heller uklare i sine svar på hvor grensen skulle gå, og ingen hadde noen klare grenser. Det mest direkte svaret kom fra det norske finanstilsynet, som skrev at

> *«[...] På bakgrunn av blant annet den varierende risikoen mellom både foretak og ulike rapporteringspliktige er slik sett ikke hensiktsmessig for Finanstilsynet å sette en grense for hvor langt en institusjon går i arbeidet med anti-hvitvasking".[...]»*
>
> (Finanstilsynet, via epost, 11 oktober 2021)

Dette betyr i praksis at de ikke har tatt stilling til det annet enn ved å flytte ansvaret over til bankene, slik at disse selv å avgjøre hvor den øvre grensen for hvor overvåkningen skal gå.

Datatilsyn Datatilsynene viste derimot mer interesse for problemstillingen, selv om ingen hadde helt klare retningslinjer eller vurderinger klare per i dag. Det norske datatilsynet mener at motsetningen mellom de to lovsettene (Hvitvaskingsloven som vil overvåke, og personvernlovgivningen som vil redusere overvåkningen) bør løses på europeisk nivå:

> *«[...] Vi ser at utfordringene knyttet til disse to regelverkene er av en slik karakter at de bør løses på europeisk nivå. Forholdet mellom personvernforordningen og AML-reglene er et aktuelt tema i Personvernrådet (EDPB), uten at det per i dag foreligger noen retningslinjer som gir uttrykk for EDPBs vurdering.»*
>
> (Datatilsynet, via epost, 6 oktober 2021)

Det er ikke bare det norske datatilsynet som finner problemstillingen aktuell. Det europeiske datatilsynet (EDPS) publiserte høsten 2021 en *Opinion* i forbindelse med arbeidet med det

sjette hvitvaskingsdirektivet i EU (EDPS, 2021). EDPS (2021) er generelt bekymret for hvor ekspansive datainnsamlingene og behandlingen i forbindelse med AML/CFT arbeidet er. De retter særlig fokus på grenser for innsamling av data rundt straff og dom, etnisitet og seksualitet, og tilgang til eierskapsregistre. EDPS (2021) stiller seg også kritisk til proporsjonaliteten av de utvidede fullmaktene de forskjellige etterretningsorganisasjonene har til innsyn i databaser og registre.

Hva som virker å være EDPS (2021) sitt hovedfokus er proporsjonaliteten mellom inngrepet i personvern ved overvåkningen og hva de tiltakene er ment å forebygge.

Bankene

Totalt fem beslutningstakere fra tre store banker, som opererer i Norge, ble intervjuet. En rekke informanter ble også stilt de samme spørsmålene utenfor en formel intervjusituasjon.

Få av de intervjuede klarte å definere tydelig hvor de mente at grensen for hva som var greit og hva som ikke var innenfor, men de var i det store og det hele relativt samstemt i sine meninger, selv om det var forskjell hva de fokuserte mest på. En ting alle var helt enige om var at AML/CFT er et område hvor bankene bør samarbeide, heller enn å konkurrere.

Mye av tankene til intervjuobjektene fokuserte på bankens rolle, hva bankene skulle se etter, og hvem som skulle bestemme hva de skulle se etter. Tankene deres kan deles inn i fire grupper, *hva som er bankene sitt ansvar*, *mangel på klare krav*, *mangel på etterretning og tilbakemelding*, og *sentralisering av overvåkningen*.

Bankene sitt ansvar Det som bekymret intervjuobjektene mest, var diskusjonen om bankenes rolle i AML/CFT arbeidet. Slik det er i dag fungerer bankene ikke bare som øyne og ører for politiet, men også for en stor grad som hjerne. Flere av de intervjuede påpekte at i dag gjør bankene allerede for mye, siden terskelen for rapportering skal være lav. Realiteten i de større bankene er at hver enkelt sak som blir rapportert, blir utredet av etterforskere i banken før den blir sendt videre til Økokrim.

Her blir det i følge intervjuobjektene raskt at bankenes rolle blir for stor i overvåkningen. Denne utfordringen mener de setter bankene i en vanskelig rolle. Bankene skal jo være banker, ikke politi. Dette blir også en utfordring i forbindelse med bankenes legitimitet, for få kunder er kjent med hvor mye overvåkning som foregår hos bankene.

Mangel på klare krav Det andre store og gjennomgående punktet, var mangel på klare krav. Her forklarte flere av intervjuobjektene at de i praksis var nødt til å *«gjette»* på hva egentlig finanstilsynet ønsker at de skal gjøre, og hvis de gjør feil, får de bot.

> *«Hva bankene skal finne av kriminalitet er til en viss grad uklart, og vi må i praksis gjette oss til kravene.»* (Bent Richard Eidem, Danske Bank, 3 November 2021)

Denne uklarheten i kravene gjør seg gjeldene i stor grad når det kommer til hva bankene faktisk skal avdekke og se etter. Hvitvasking og terrorfinansiering sier de er ganske rett fram, men hva med andre former for kriminalitet? Hva er det som er innenfor og hva er det som er utenfor? Et annet spørmål er også hvordan de skal prioritere de ressursene de har? Er en underslags-sak viktigere enn ti bedragerisaker? Med klarere krav vil dette bli lettere for bankene å forholde seg til.

Mangel på etterretning og tilbakemelding Når en bank melder noe til Økokrim blir dette et svart hull for bankene. De, som en av informantene beskrev det, kan *«like gjerne kunne kastet det i søppla, for vi får aldri vite om det var en god eller dårlig sak»*. Denne uttalelsen beskriver frustrasjonen til en del av de som jobber med rapportering, hvor de aldri får tilbakemelding fra politiet.

Intervjuobjektene forsto godt hvorfor politiet ikke kan gå rundt å avsløre detaljer om pågående saker, men det gjør allikevel arbeidet med å avsløre hvitvasking og terrorfinansiering lite inspirerende. Noe tilbakemelding får de riktignok, men kun når politiet ber om mer informasjon i forbindelse med en pågående sak, men denne informasjonen kan ikke nødvendigvis deles med personene som utvikler scenarioene som avdekker kriminaliteten. Samtidig er det lite konkret etterretning å få fra politimyndighetene, og de rapportene og publikasjonene som finnes, både nasjonalt og internasjonalt er ofte svært utdaterte[41].

Her stiller flere av intervjuobjektene seg spørsmålet om hvordan de skal kunne gjennomføre en risikobasert tilnærming uten god tilgang til etterretning og tilbakemelding?

Sentralisering av Anti-Hvitvaskingsovervåkning Et tema som kom opp blant flere av intervjuobjektene og informantene, var spørsmålet om sentralisering av overvåkningen for alle bankene i Norge, noe som ble lagt til som eget spørsmål i intervjuguiden (Vedlegg A). En slik sentralisering av AML overvåkningen vil påvirke hvordan denne fremstår, både til det positive og det negative. Motivasjonen for å sentralisere deler av AML arbeidet virker å være delt i fem områder, som også godt illustrerer hvilke utfordringer bankene opplever i dag.

Fragmentering av datagrunnlag En av de store utfordringene for bankene, når de skal finne hvitvasking og terrorfinansiering, er at de ikke ser hele bildet av kunden. Har kunden konto i flere banker er det nesten umulig å avdekke hvitvasking med systemene slik de er i dag.

[41] ACAMS, en av de største sertifiseringssystemene for anti-hvitvaskingsspesialister har i sitt nåværende kursmateriale flere eksempler med bruk av sjekker, enn de har med nettbaserte betalingsformidlere.

Samtidig, peker flere informanter på forskjellen mellom store og små banker. En stor bank har større muligheter til å trene maskinlæringsalgoritmer og lære av tilfeller av hvitvasking. Dette kan føre til at kriminelle trekker mot små banker da de oppfattes som lettere å hvitvaske gjennom.

Analytiske kapabiliteter Tett knyttet til fragmenteringen av datagrunnlaget er de analytiske kapabiliteter. Det koster mye å utvikle nye analyser og små banker har ikke anledning til å ha et team av analytikere slik som større banker. Dette kan også føre til at det blir ulikhet mellom bankene.

Etterretning Mangel på etterretning er et stort problem når de skal finne hvitvasking. En sentralisering vil konsentrere og gi større muligheter til etterretnings-innhenting.

Oversyn I dag er det i praksis veldig lite oversyn over hva de bankene faktisk gjør for overvåkning. Det oversynet som er på plass har hovedsaklig som formål å sørge at de gjennomfører noe overvåkning, uten detaljer. Samtidig er overvåkningen svært omfattende. Sentralisering vil muliggjøre bedre oversyn med denne overvåkningen.

Kostnad Anti-hvitvaskingssystemer er kostbare, og intervjuobjektene mener at det er mulig å spare mye gjennom en sentralisering av overvåkningen.

En slik sentralisering er ikke en ny tanke, og denne typen samarbeid eksisterer på flere andre områder allerede. Flere informanter informerer om at det er en del diskusjon på dette området internasjonalt, i land som Australia og Nederland, uten at dette kan bekreftes av uavhengige kilder.

Hvordan en eventuell sentralisering blir gjennomført vil betydelig påvirke hvordan overvåkningstrykket fra AML/CFT overvåkningen. En kan, med god grunn, stille seg skeptisk til ideen om en slik sentralisering ved å peke på net-widening og veien mot et maximum survilance society. Dette er ikke nødvendigvis tilfellet. En sentralisering vil også potensielt lette oversyn og styring av overvåkningen, begrense tilgang til sensitiv data, og kan organiseres som et samarbeid uavhengig av staten.

Politikere

Den siste og kanskje viktigste gruppene som ble innhentet meninger om grensene til AML arbeidet er de politiske partiene og politikere. Denne undersøkelsen viste seg å være utfordrende da ingen politikere kontaktet hadde anledning til å stille til intervju grunnet arbeidet med nasjonalbudsjett[42].

[42] Politikkerene som ble kontaktet satt alle i Finanskomiteen på stortinget, som mens denne teksten ble skrevet, var fult opptatt med nasjonalbudsjettet for 2022.

Da politikerene på stortinget ikke kunne stille til intervju, ble andre metoder brukt for å avdekke politikken på temaet.

Partiprogrammer og stortingsgrupper Samtlige partier på stortinget ble kontaktet og spurt om deres syn på problemstillingen. Alle partiprogram ble også gjennomgått for å undersøke om noen av partiene har identifisert noe syn rundt grensene av anti-hvitvaskingsovervåkning.

Resultatet var nedslående. Ingen partier som svarte, og ingen av partiprogrammene, hadde noen offisielle meninger eller politikk på temaet. Noen er derimot skeptisk til mer overvåkning på et mer generelt nivå. Ett eksempel er svaret fra Miljøpartiet de Grønne (MDG), som ikke vil ha mer overvåkning enn i dag.

> *«[...] Vi er allerede sterke tilhengere av personvern og folks rettsikkerhet, og vil i alle fall ikke gå noe lenger enn dagens praksiser. [...] Det er også viktig å gi Økokrim tilstrekkelig med kapasitet og økonomiske midler slik at deres arbeidsoppgaver i minst mulig grad blir flyttet over på bl.a banker, slik at man ikke utvider mandatet og potensialet for overvåkning fra ikke-statlige aktører.»*
>
> (Axel Klanderud (MPG), via epost, 8 november 2021)

Her uttrykker MDG både en skepsis til overvåkningen, men også måten den er overvåket på. De er også skeptiske til privatiseringen av politiarbeidet.

Tidligere finansminister Siv Jensen Den eneste offentlige uttalelsen som ble funnet og som kom inn på problematikken, var en tale av daværende Finansmister Siv Jensen (Fremskrittspartiet) under Hvitvaskingskonferansen[43] i 2019 med et åpningsinnlegg om hvitvasking og viktigheten av AML/CFT arbeidet (Jensen, 2019). Talen er i og for seg i stor grad en ganske vanlig åpningstale men lite konkret, men hun sier mye om hva som forventes, men lite om hvor grensene bør gå.

Gjenomgående gjennom hele talen er det fokus på at det er er viktig at bankene avdekker og rapporterer mistanke til politiet. Senere i talen legger Jensen også fokus på at det ikke må overrapporteres *«[...] fordi man ønsker å vise at man tar arbeidet på alvor»*, og snakker om at det må være en balanse.

På starten av talen sier Jensen (2019) derimot noe som er interessant. Hun peker ikke bare på hvitvasking og terrorfinansiering, men også tilknyttet kriminalitet.

> *«Og det er nettopp Norges rolle i å bekjempe hvitvasking, terrorfinansiering og* ***tilknyttet kriminalitet*** *jeg vil snakke om.»* (Jensen, 2019)

[43] Hvitvaskingskonferansen er norges største og eneste årlige konferanse for AML/CFT og arrangeres gjennom et samarbeid mellom Økokrim, Finanstilsynet, og Finans Norge, og har over 400 deltagere hvert år.

Hva denne andre *«tilknyttede kriminaliteten»* er, nevnes ikke videre i talen, men det kan bli tolket i retningen av en bredere tilnærming til AML arbeidet.

6 Diskusjon

Analysen viser at det ikke er noen klar øvre grense for hvor mye overvåkning som skal foretas i forbindelse med anti-hvitvasking og anti-terrorfinansieringsarbeidet. Så hvordan gå fram for å finne hvor denne grensen skal gå?

6.1 Hvor skal grensen gå?

Å finne en god definisjon på ovennevnte grense, kan utføres fra flere vinkler, slik som det er gjort i denne oppgaven. Resultatene fra analysen peker i retning av at problematikken ikke har et enkelt svar. Samtidig er dette et område få bryr seg om, til tross for at det medfører overvåkning av store deler av samfunnet (Amicelle, 2011).

For å tilnærme seg et svar på hvor denne grensen skal gå, kreves at en ser på forholdsmessigheten, konsekvensene, kostnaden av tiltakene, samt rollefordelingen mellom aktørene, internasjonale relasjoner og forpliktelser, samt hvilken teknologi som kan tas i bruk.

Isolert sett er det klart at den teknologien, som i stadig større grad blir tatt i bruk, vil medføre en utvidelse av overvåkningen, selv om kravene eller antall ansatte ikke nødvendigvis øker. Her er det altså en teknologisk drevet net-widening effekt. Et moderne overvåkningssystem er grunnleggende forskjellig fra de som gjerne diskuteres i litteraturen. Det er også her tegn på at forskningslitteraturen undervurderer hvor mye denne økningen i analytisk kapasitet påvirker overvåkningstrykket. Teknologien må altså tas med i vurderingen av hvor en øvre grense skal gå.

Norge er, som beskrevet i Delkapittel 5.1, forpliktet av en del internasjonale avtaler og samarbeid innen AML/CFT arbeidet. Norge har ikke anledning, uten konsekvenser, å selv avgjøre hvor en øvre grense skal gå, hvis denne øvre grensen strider mot disse internasjonale forpliktelsene. Det er derfor klart at internasjonale relasjoner og avtaler må vurderes når en øvre grensene skal settes.

Rollefordelingen mellom staten og private aktører blir problematisert av flere, blant annet Favarel-Garrigues et al. (2011), noe som også kommer klart fram under intervjuene med bankene, og svar fra noen politiske partier. Rollefordelingen mellom bankene og politiet var ett av hovedtemaene som ble identifisert. Dette reflekteres også noe i media hvor Amundsen (2021) skriver om hvordan politiet overlater arbeidet til bankene.

Som Amicelle & Favarel-Garrigues (2012) postulerer, så kan en av årsakene til at så få bryr

Tabell 1: Antall rapporteringer per meldertype motatt av Økokrim. Tallene er per 17 November 2021. Tallene er motatt på bakgrunn av innsynskrav til Økokrim.

Meldertype	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**Sum**	**Snitt**
Advokater m.fl.	12	10	13	24	33	14	**106**	**18**
Andre jf. Hv-loven §4	97	191	119	191	346	420	**1 364**	**227**
Banker	6 266	5 599	6 888	7 604	8 539	9 469	**44 365**	**7 394**
e-pengeforetak	0	1	7	25	23	11	**67**	**13**
Forhandlere av gjenstander	56	34	0	0	0	0	**90**	**45**
Forsikringsselskap	68	77	108	259	306	265	**1 083**	**181**
Meglere	134	424	574	979	1 154	1 546	**4 811**	**802**
Pensjonskasser	0	0	0	0	0	0	**0**	**0**
Postoperatører	0	0	0	0	0	0	**0**	**0**
Regnskapsførere	69	66	61	57	92	81	**426**	**71**
Revisorer	50	51	42	46	57	30	**276**	**46**
Verdipapirforetak mv.	9	5	4	9	11	12	**50**	**8**
Virksomhet for betalingsformidling	2 013	2 442	2 932	2 338	2 131	2 195	**14 051**	**2 342**
Sum	**8 774**	**8 900**	**10 748**	**11 532**	**12 692**	**14 043**	**66 689**	**11 115**

seg om AML/CFT-overvåkningen være at det ikke er staten som gjennomfører denne, og at befolkningen er mindre skeptisk til ikke-statlig overvåkning. Det kan derfor konkluderes med at hvem som gjennomfører overvåkningen også er viktig for vurderingen av hvor en øvre grense skal gå.

Som nevnt innledningsvis, er kostnaden av AML/CFT arbeidet enorm. Det er vesentlig flere som jobber med AML/CFT i bankene, enn det er ansatte i Økokrim (173 årsverk). Det er ingen overdrivelse å sammenlikne antall AML/CFT årsverk med det totale antall politifaglige ansatte i politiet[44]. Dette fordrer spørsmål om samfunnets investeringer er verdt effekten. Knutsen & Støle-Hansen (2020) skriver i sin masteroppgave om myndighetenes tiltak fungerer, og kommer fram til at det er liten bevist effekt av arbeidet.

Arbeidet med AML/CFT hos de rapporteringspliktige institusjonene som er omfattet av Hvitvaskingsloven, fører til i snitt over 11.000 meldinger om mistenkelige transaksjoner per år, som sendes til Økokrim, og antallet er stigende (se Tabell 1). Økokrim har 17 ansatte tilknyttet

[44] DNB anslår over tusen årsverk, Danske Bank noe liknende (tre tusen fordelt på hele konsernet), og en av informantene estimerte ca. fem tusen årsverk i Norge totalt. Politiet hadde, per 31 august 2021, 11.423 årsverk innen politifaglige roller (Politiet, 2021).

dette arbeidet[45] (Langved et al., 2020), og tidligere leder for anti-hvitvasking i DNB, Roar Østby, uttalte i 2020 at *«Det er ingen vits i å ringe Økokrim»*, siden de ikke har kapasitet til å etterforske (Langved et al., 2020). Dette er ikke å overdrive, for ved 17 ansatte medfører det at hver av disse må etterforske nesten tre mistenkelige meldinger hver dag[46]. Her må det også huskes at hver melding som større banker sender, allerede er utredet av etterforskere i bankene.

Noe AML/CFT overvåkning må alltid være på plass i bankene og finansinstitusjonene, men ved et visst nivå er det ikke lenger kostnadseffektivt for samfunnet. AML/CFT arbeidet blir i praksis en ekstra skatt på samfunnet, for kostnadene bankene har til dette blir i stor grad sendt videre til forbrukerne. Teoretisk sett kunne disse midlene heller bli brukt til andre tiltak, som blant annet mer politi. Det er derfor naturlig at også kostnaden ved overvåkningen er en del av vurderingen av hvor grensen for AML/CFT overvåkning skal gå.

Flere, som Amicelle & Iafolla (2017), Amoore & de Goede (2005), og de Goede (2011) trekker fram negative konsekvenser av AML/CFT overvåkningen som en utfordring. Konsekvensene som trekkes frem, er blant annet marginalisering, ekskludering, og utfordringer rundt uskyldspresumsjonen[47] At de negative konsekvensene av overvåkningen bør vurderes i avgjørelsen av hvor den øvre grensen for AML/CFT overvåkingen skal gå, er udiskutabelt.

For samfunnet er det viktigere å avdekke noen kriminelle handlinger enn andre, og hvor hensiktsmessig ett tiltak er for å avdekke lovbruddet må stå i forhold til dette. Som diskutert i Delkapittel 5.1 sier Hvitvaskingsloven at arbeidet skal være risikostyrt, og kan grupperes i tre forskjellige kategorier; direkte- og indirekte dekket av loven, og ikke dekket av loven.

Hvordan loven er strukturert kan få resultater, som kan gå imot den vanlige rettsoppfattelsen. Dette kan illustreres med to eksempler, hvor det ene, som kan anses som heller lite viktig, er indirekte dekket av loven, mens det andre som kan vurderes til å være svært viktig, men dekkes ikke [48].

Eksempel 6.1. Bruk av sparekonto som depositumkonto ved utleie
Å benytte en vanlig sparekonto som depositumkonto ved utleie er brudd på Husleieloven § 3-5. Å ikke tilbakebetale depositumet med renter er teknisk sett bedrageri (Straffeloven §§ 371 og 373), selv om det er snakk om svært små beløp.

[45] Det er sendt forespørsel til Økokrim for å etterprøve dette antallet, men de *«ønsker ikke dele informasjon om antall ansatte i ulike stillingskategorier eller hvor mange ansatte den enkelte avdeling»*. De opplyser om at det er 173 som jobber fast i Økokrim totalt. De opplyser også at *«alle MT-rapportene blir behandlet umiddelbart og det foreligger ingen backlogg»*.

[46] 11.115 meldinger / (17 stillinger × 230 arbeidsdager) = 2.8 meldinger per stilling per arbeidsdag

[47] At noen antas uskyldig inntil de er dømt (Frøberg, 2016, s. 63). Argumentasjonen til de Goede (2011) er at en som svartelistes blir *«straffes»* før de blir dømt.

[48] Begge eksemplene er basert på ekte hendelser og vurdert og bekreftet av en jurist som jobber med Hvitvaskingsloven til daglig. En argumentasjon kan gjøres for at det er profittmotivert kriminalitet i forbindelse med eventuelle salg av nakenbilder (barnepornografi) i Eksempel 6.2, noe som ses bortifra for eksempelets skyld.

Eksempel 6.1 beskrives et lovbrudd som er svært vanlig, men kan anses som trivielt, men som dekkes av Hvitvaskingsloven. Dalsbø (2019) skriver at det hvert år kan avdekkes mer enn ti tusen tilfeller av dette bare gjennom DNB alene. Er denne typen kriminell handling så viktig at samfunnet skal overvåkes for å finne det? Mange vil si *«nei»*.

Eksempel 6.2. Mindreårig jente med *«Sugardaddy»*[49]
Når en voksen mann rutinemessig overfører beløp opptill flere tusen kroner til en jente på 14-15 år, uten å ha noen annen relasjon, og hvor noen av meldingene er seksuelt ladet, er det naturlig å mistenke brudd på Straffelovens paragrafer om pedofili, grooming, og barnepornografi (Straffeloven §§ 229-311).

I Eksempel 6.2 beskrives det en case som er motsatt av Eksempel 6.1, en sak som samfunnet anser som svært viktig, men som ikke dekkes at Hvitvaskingsloven, og hvor bankene derfor ikke har hjemmel til å utforske. Hvilket av eksemplene som er viktigst for samfunnet å avdekke fremstår som klart. Bankene etterspør derfor større klarhet rundt blant annet slike situasjoner.

Eksempel 6.1 og 6.2 illustrerer hvordan dagens lovverk ikke nødvendigvis følger en vanlig rettsoppfattelse, og hvor det kan være behov for justeringer i lovverket eller forskrifter. Eksempler som disse viser også hvorfor hvilke lovbrudd som ligger til grunn for hvitvaskingen, også er viktig i vurderingen av hvor grensen for overvåkning skal gå. Overvåkningen må være forholdsmessig til lovbruddene som avdekkes.

7 Konklusjon

Det er klart at overvåkningstrykket fra AML/CFT arbeidet stadig øker, samtidig som stadig mer data samles inn og flere avanserte metoder blir tatt i bruk. Denne oppgaven har utforsket utfordringene med å sette en øvre grense for denne overvåkningen, og sett på hvordan en kan gå fram for å finne den.

Arbeidet med å sette en øvre grense bør ha politisk forankring, og ikke overlates til risikovurderinger hos bankene slik det gjøres i dag. Det bør også klargjøres hvilke lovbrudd som skal avdekkes og som fordrer overvåkning, altså hvilke kriminelle handlinger som er *«viktige nok»*. Det er klart at det i praksis ikke bare er hvitvasking og terrorfinansiering disse systemene kan og blir brukt mot.

Denne oppgaven er ikke uten sine svakheter, og flere faktorer og vurderinger kunne vært inkluderert i analysen. Ett tema som ikke er inkludert, som kunne ha en naturlig plass i diskusjonen, er personvernlovgivningen. Andre relevante emner er hvordan de overvåkedes

[49] Vollan & Ersfjord (2019) beskriver en *«Sugardaddy»* er en eldre mann som ønsker et forhold med en person (som oftest yngre kvinne), og som er villig til å gi penger og/eller gaver for å få tilbringe tid med personen. Dette er i forbindelse med *«Sugardating»*, og jenten som mottar gavene eller pengene kalles en *«Sugarbabe»*.

adferd påvirkes, samt andre overvåkningsaktiviteter bankene gjennomfører, eksempelvis anti-svindel-overvåkning. Det er også antatt at det må være en viss AML/CFT overvåkning, noe som kunne blitt problematisert ytterligere.

Det er også behov for mer forskning på AML/CFT overvåkningen. Rollefordelingen mellom stat og finansinstitusjoner er i liten grad dekket av forskningen i relasjon til AML/CFT overvåkningen. Etterretningen hos bankene, grunnlaget for risikoanalysene, og etterretningssamarbeidet mellom banker og myndigheter har så langt heller ikke blitt dekket.

Referanser

AAG (1995). Australia's Attorney-General (AAG)- Criminal Code Act 1995. www.legislation.gov.au/Details/C2021C00360.

Amicelle, A. (2011). Towards a 'new' political anatomy of financial surveillance. *Security dialogue*, 42(2), 161–178.

Amicelle, A. & Favarel-Garrigues, G. (2012). Financial surveillance: Who cares? *Journal of cultural economy*, 5(1), 105–124.

Amicelle, A. & Iafolla, V. (2017). Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing. *The British Journal of Criminology*, 58(4), 845–863.

Amoore, L. & de Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Crime, law, and social change*, 43(2), 149–173.

Amundsen, B. (2021). Politiet overlater etterforskningen av økonomisk kriminalitet til de mistenkte, i ***Forskning.no***. https://forskning.no/finans-kriminalitet-politikk/politiet-overlater-etterforskningen-av-okonomisk-kriminalitet-til-de-mistenkte/1841798. Besøkt: 2021-11-16.

Ball, K., Haggerty, K., & Lyon, D. (2012). *Routledge handbook of surveillance studies*. Abingdon: Routledge.

Bjørgan, L. & Kolseth, H. I. M. (2021). Mann pågrepet og siktet for medvirkning til voldtekt i Filippinene. www.nrk.no/trondelag/tronder-i-40-arene-pagrepet-og-siktet-for-medvirkning-til-voldtekt-i-filippinene-1.15671203. Besøkt: 2021-11-03.

Boekhout van Solinge, T. (2008). Crime, conflicts and ecology in africa. In T. Sollund (Ed.), *Global Harms: Ecological Crime and Speciesism*. Nova Science.

Buzan, B., Wæver, O., Wæver, O., De Wilde, J., et al. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Chriss, J. J. (2019). *Social Control*. Polity Press.

Dalsbø, V. K. (2019). Pass opp for sleipe bolighaier, i ***DNB Nyheter***. https://www.dnb.no/dnbnyheter/no/bolig/pass-opp-for-sleipe-bolighaier. Besøkt: 2021-11-22.

de Goede, M. (2011). Blacklisting and the ban: Contesting targeted sanctions in europe. *Security Dialogue*, 42(6), 499–515.

de Goede, M. (2012). The swift affair and the global politics of european security. *Journal of common market studies*, 50(2), 214–230.

DNB (2021a). Combating money laundering and terrorist financing. https://www.dnb.no/en/about-us/csr/Financial-crime/aml.html. Besøkt: 2021-10-26.

DNB (2021b). DNB-konsernet. www.dnb.no/om-oss/om-dnb.html. Besøkt: 2021-11-09.

Dreżewski, R., Sepielak, J., & Filipkowski, W. (2015). The application of social network analysis algorithms in a system supporting money laundering detection. *Information Sciences*, 295, 18–32.

Dvergsdal, H. & Elster, A. C. (2019). stordata, i ***Store Norske Leksikon***. https://snl.no/stordata. Besøkt: 2021-11-22.

EDPS (2021). The European Data Protection Supervisor (EDPS) - Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals. https://edps.europa.eu/data-protection/our-work/publications/opinions/anti-money-laundering-and-countering-financing_en.

European Commission (2021). Money laundering. https://ec.europa.eu/home-affairs/policies/internal-security/organised-crime-and-human-trafficking/money-laundering_en. Besøkt: 2021-10-24.

Europol (2021). EUROPOL – Senior Specialist – European Cyber Crime Centre (EC3) – Operations (AD7). https://www.europol.europa.eu/careers-procurement/vacancies/vacancy/497. Stillingsutlysning. Besøkt: 2021-11-09.

FATF (2012). *The FATF Recommendations - International Standards on Conbating Money Laundering and the Financing of Terorism & Proliferation*. Recomendations, Financial Action Task Force. Sist opptadert: Oktober 2021.

FATF (2015). *The Financial Action Task Force (FATF)* - Money Laundering. www.fatf-gafi.org/faq/moneylaundering/. Besøkt: 2021-10-22.

FATF (2018a). *Financial Flows from Human Trafficking*. Report, Financial Action Task Force.

FATF (2018b). *Professional Money Laundering*. Report, Financial Action Task Force.

Favarel-Garrigues, G., Godefroy, T., & Lascoumes, P. (2011). Reluctant partners?: Banks in the fight against money laundering and terrorism financing in france. *Security Dialogue*, 42(2), 179–196.

Finansdepartementet (2003a). Forskrift om bruk av informasjons- og kommunikasjonsteknologi (ikt).
https://lovdata.no/dokument/SF/forskrift/2003-05-21-630.

Finansdepartementet (2003b). *Ot.prp. nr. 72 (2002–2003) - Lov om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. (hvitvaskingsloven)*. Departementenes sikkerhets- og serviceorganisasjon.

Finansdepartementet (2018). Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven).
https://lovdata.no/dokument/NL/lov/2018-06-01-23/.

Finanstilsynet (2019). Veileder til hvitvaskingsloven. Rundskriv 8/2019. www.finanstilsynet.no / nyhetsarkiv / rundskriv / 2019 / veileder - til - hvitvaskingsloven/.

Finanstilsynet (2021). Vedtak om overtredelsesgebyr. Brev - 19/12479. www.finanstilsynet.no / nyhetsarkiv / brev / 2021 / vedtak - om - overtredelsesgebyr5/.

FinCEN (2021). Financial Crimes Enforcement Network. History of Anti-Money Laundering Laws. www.fincen.gov/history-anti-money-laundering-laws. Besøkt: 2021-11-09.

Freeman, M. (2011). The sources of terrorist financing: Theory and typology. *Studies in Conflict & Terrorism*, 34(6), 461–475.

Frøberg, T. (2016). *Alminnelig strafferett i et nøtteskall.* Gyldendal.

Godefroy, T., Lascoumes, P., & Favarel-Garrigues, G. (2012). *Tools and securitization: the instrumentation of AML/CTF policies in French banks.* Post-Print hal-02404571, HAL.

Hegge, P. E. (2015). Sikkerhetisering, i ***Aftenposten***. www.aftenposten.no/kultur/i/4Wo6/sikkerhetisering. Besøkt: 2021-05-24.

Jensen, S. (2019). Åpningsinnlegg på Hvitvaskingskonferansen 2019. www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/fin/taler-og-innlegg/ministerens-taler-og-artikler/taler-og-artikler-

av-finansminister-si-2/2019/apningsinnlegg-pa-hvitvaskingskonferansen-2019/id2678215/. Tale. Besøkt: 2021-11-03.

Jost, P. M. & Sandhu, H. S. (2000). The hawala alternative remittance system and its role in money laundering. Interpol.

Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control*.

Justis- og beredskapsdepartementet (2005). Lov om straff (straffeloven). https://lovdata.no/dokument/NL/lov/2005-05-20-28/.

Kaufmann, M. (2018). Kriminalitetskontroll eller sikkerhetspolitikk? *Nytt Norsk Tidsskrift*, 35(01), 21–31.

Knutsen, A. H. & Støle-Hansen, I. (2020). Anti-hvitvasking i norge: Fungerer myndighetenes tiltak? Master's thesis, University of Agder.

Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering-a critical review. *IEEE access*, 9, 82300–82317.

Langved, , Klevstrand, A., & Trumpy, J. (2020). Tidligere antihvitvaskingssjef i DNB: – Det er ikke noen vits i å ringe Økokrim, i ***Dagens Næringsliv***. https://www.dn.no/kriminalitet/hvitvasking/okokrim/dnb/tidligere-antihvitvaskingssjef-i-dnb-det-er-ikke-noen-vits-i-a-ringe-okokrim/2-1-737499. Besøkt: 2021-11-16.

Levi, M. (2002). Money laundering and its regulation. *The Annals of the American Academy of Political and Social Science*, 582(1), 181–194.

Levi, M. (2010). Combating the Financing of Terrorism. *British journal of criminology*, 50(4), 650–669.

Li, X., Liu, S., Li, Z., Han, X., Shi, C., Hooi, B., Huang, H., & Cheng, X. (2020). Flowscope: Spotting money laundering based on graphs. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34 (pp. 4731–4738).

LNRS (2021). *The True Cost of Financial Crime Compliance Report* . Global report, LexisNexis Risk Solutions.

Lomell, H. M. (2012). Punishing the uncommitted crime: prevention, pre-emption, precaution and the transformation of criminal law. In *Justice and Security in the 21st Century* (pp. 99–116). Routledge.

Løkke, E. (2018). Hva er overvåkning? https://www.civita.no/politisk-ordbok/hva-er-overvakning. Besøkt: 2021-11-19.

Marx, G. T. (2015). Surveillance studies. *International encyclopedia of the social & behavioral sciences*, 23(2), 733–741.

Meijer, A. & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration*, 42(12), 1031–1039.

Nogala, D. (1995). The future role of technology in policing.

Norges Bank (2020). Sedler og Mynter: Årsrapport (Internett versjon) 2020. https://www.norges-bank.no/tema/Statistikk/Seddel-og-mynterstatistikk/.

Norris, C. & Armstrong, G. (2020). *The maximum surveillance society: The rise of CCTV*. Routledge.

Pasley, F. D. (2020). *AL CAPONE-The Biography of a Self-Made Man*. Edizioni Savine.

Pettersen, S. & Wainio, C. M. (2021). Anti-hvitvaskingsarbeidet i norge. Master's thesis, NTNU.

Pleune, T. (2018). Validating AML Models Under the NYDFS Part 504 AML Requirement, i ***Corporate Compliance Insights***. https://www.corporatecomplianceinsights.com/validating-aml-models-nydfs-part-504-aml-requirement/. Besøkt: 2021-11-12.

Politiet (2021). Bemanning og dekningsgrad. https://www.politiet.no/aktuelt-tall-og-fakta/tall-og-fakta/bemanning/. Besøkt: 2021-11-21.

Ratcliffe, J. H. (2016). *Intelligence-led policing*. Routledge.

Rui, J. P. (2012). *Hvitvasking: Fenomenet, regelverket, nye strategier*. Universitetsforlaget.

Rui, J. P., Ringen, G. H., & Frivold, K. R. (2021). *Hvitvaskingsloven : lov 1. juni 2018 nr.23 om tiltak mot hvitvasking og terrorfinansiering : lovkommentar*. Oslo: Universitetsforlaget.

Singh, K. & Best, P. (2019). Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, 34, 100418.

Skilbrei, M.-L. (2019). *Kvalitative metoder : planlegging, gjennomføring og etisk refleksjon*. Bergen: Fagbokforlaget, 1. utgave. edition.

Suszek, D. (2015). *The Art of Money Laundering*. Uavhengig publisering.

Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: the state of research in key areas. *Pacific Accounting Review*.

Ugelvik, T. (2019). *Sosial kontroll*. Universitetsforlaget.

Unger, B. & Van der Linde, D. (2013). *Research handbook on money laundering*. Edward Elgar Publishing.

UNODC (2021). United Nations Office on Drugs and Crime (UNODC) - combating terrorist financing. www.unodc.org/unodc/en/terrorism/expertise/combating-terrorist-financing.html. Besøkt: 2021-10-25.

Verhage, A. (2011). *The anti money laundering complex and the compliance industry*. Routledge.

Vollan, M. & Ersfjord, E. (2019). «Pernille» (23) har valgt sugardating som livsstil: – Du mister sjela di litt, i ***Nrk.no***. https://www.nrk.no/trondelag/ifolge-datingekspert-har-det-blitt-en-trend-for-studenter-a-velger-sugardating-som-livsstil-1.14346846. Besøkt: 2021-11-22.

Wagner, L., Siller, D., & Landa, R. (2020). People and forests at risk: Organized crime, trafficking in persons and deforestation in chihuahua, mexico.

Wegner, R. B. (2015). *Strafferett : spesiell del*. Drammen: Vett Viten. 2. utg.

A Intervjuguide

Intervjuguiden i denne analysen er brukt under alle intervjuer som er utført. Intervjuene ble satt opp for å vare mellom 15 og 30 minutter, og gjennomført over Microsoft Teams (Videokonferanseverktøy). Strukturen valgt var et semi-strukturert intervju, hvor spørsmålene mest ble brukt for å komme innom temaene heller enn stilt i direkte ordlyd.

Spørsmålene:

1. Hvor går, og hvor bør, den øvre grensen for hvor mye overvåkning norske banker skal gjennomføre i jakten etter Hvitvasking og Terrorfinansiering?
2. Mener du AML/CFT bør være et område bankene konkurrerer på?
3. Hva tenker du å sentralisere Transaksjons Monitorering og Sanksjons Screening?
4. Hvordan tenker du AML/CFT området vil utvikle seg videre?

Antall ord: 12.000
+ fotnoter: 1.186
+ forord og tillegg: 370
Totalt: 13.556