

Økonomisk kriminalitet i utvikling

Av Jan Georg Christophersen

Title in English: Economic Crime in Development

Abstract

Economic crime is a broad concept encompassing illicit activities that undermine financial systems, economic stability, and development. Its evolution, growth, and impact are influenced by technological and regulatory frameworks. Economic crime has existed throughout history, evolving alongside economies. Early forms included counterfeiting, tax evasion, and fraud. As economies become more complex, so do economic crime, including corporate fraud, money laundering and cybercrime. In the pre-industrial era simple fraud, bribery, and smuggling were common. The rise of corporations led to financial fraud, insider trading, and tax evasion. In the 20th century white-collar crime became more prevalent, with banking fraud and organized crime growing. 21st century digitalization led to cyber fraud, cryptocurrency scams, and sophisticated money laundering techniques. Several factors contribute to the increase in economic crime. Globalization as cross-border transactions make it easier to hide illicit fraud. Digital platforms facilitate cyber fraud and financial crimes. Regulatory loopholes and weak laws allow financial criminals to exploit legal gaps. Governmental and corporate corruption foster financial misconduct. Impact on development as loss of capital due to fraud and corruption, reduces investment. Economic crime often benefits the wealthy, while harming the poor. This undermines institution and weakens trust in financial and legal systems. Economic crime continues to evolve with technological and economic changes. Stronger regulatory measures, international cooperation, and advanced forensic techniques are necessary to combat its growth and mitigate its impact on economic development.

Innholdsfortegnelse

Abstract	2
1. Innledning	3
2. Teoretiske spørsmål	3
2.1 Hvordan forstå og forklare økonomisk kriminalitet	3
2.2 Er økonomisk kriminalitet unntaket eller normen	4
2.3 Hvordan påvirker digitalisering økonomisk kriminalitet	5
2.4 Hvordan balanseres reguleringer og innovasjon	5
3. Empiriske spørsmål	6
3.1 Hvordan kan økonomisk kriminalitet utvikles i lys av økonomiske kriser og globale spenninger	6
3.2 Hvilken effekt har storfinans og manipulasjon på selskapers økonomiske kriminalitet	8
3.4 Hvilke nye kriminalitetsformer oppstår i digitale økonomier	10
4. Slutninger og blikk på framtiden	12
Referanser	12

1. Innledning

Økonomisk kriminalitet, som blant annet inkluderer hvitvasking, skatteunndragelse, korrupsjon og markedsmanipulasjon har blitt en stadig større utfordring i en globalisert og digitalisert økonomi. Fra Panama Papers til kryptovaluta-svindel ser vi hvordan myndigheter strever med å regulere og avdekke denne type lovbrudd.

Særlig i kjølvannet av økonomiske kriser og teknologiske nyvinninger har økonomisk kriminalitet fått nye former. Digitale valutaer og anonyme transaksjoner utfordrer tradisjonelle reguleringsmekanismer, samtidig som myndigheter forsøker å styrke kontrollen. Dette reiser viktige spørsmål om effektivitet og lovgivning med etiske implikasjoner.

Denne artikkel vil undersøke hvordan økonomisk kriminalitet har utviklet seg i lys av digitalisering og globalisering. Spesielt vil det bli diskutert hvilke mekanismer som muliggjør økonomisk kriminalitet, og i hvilken grad eksisterende tiltak er effektive.

Artikkelen er strukturert som følger: Først presenteres sentrale teoretiske perspektiver på økonomisk kriminalitet. Deretter analyseres nyere eksempler på økonomisk kriminalitet, med fokus på digitale og internasjonale dimensjoner. Til slutt diskuteres utfordringer og muligheter for framtidens kriminalitetsbekjempelse.

2. Teoretiske spørsmål

2.1 Hvordan forstå og forklare økonomisk kriminalitet

Økonomisk kriminalitet er studert av for eksempel bedrageri, korrupsjon, hvitvasking, skatteunndragelse og markedsmanipulasjon. De viktigste spørsmålene innenfor feltet i dag kan deles inn i teoretiske og empiriske dimensjoner.

Tradisjonelle teorier som rasjonell valgteori (folk begår økonomisk kriminalitet fordi gevinsten overstiger risikoen) utfordres av nyere perspektiver som institusjonell teori (hvordan regler, normer og kultur muliggjør økonomisk kriminalitet). Her kan det være av avgjørende betydning å vise til politikere og privatpersoner som involverer seg i økonomiske transaksjoner, spekulasjon for egen regning eller som rådgir andre om kjøp eller salg av for eksempel aksjer. Grunnen er åpenbar, politikere sitter med innsideinformasjon, likeså, kan næringslivsfolk også ha opplysninger om strukturelle endringer i bedrifter. Regler og forskrifter er politikkens område, som derfor har kunnskap om endringer i statlig eierskap, og ny lovgivning som angår det private næringsliv. Her kan det foreligge markedsmanipulasjon som er forbudt i henhold til norsk straffelovgivning og reguleres primært gjennom verdipapirhandelloven (vphl), ikke straffeloven direkte.

Økonomisk kriminalitet skjer ikke i et vakuum – den blir muliggjort av regler, normer og kultur i samfunnet og i spesifikke bransjer. Hvis det forekommer hull i lovgivningen, det vil si hvis lover og reguleringer er uklar eller har smutthull, kan enkeltpersoner og bedrifter utnytte dette til ulovlig økonomisk gevinst (f.eks. skjermte verdier i skatteparadiser, eller benytte kreative regnskapstriks).

Når myndigheter eller tilsynsorganer mangler ressurser eller kompetanse, blir det lettere å slippe unna med økonomisk kriminalitet. Hvis konsekvensene av økonomisk kriminalitet er små sammenlignet med den potensielle gevinsten, kan dette virke som en oppmuntring til lovbrudd.

Når det gjelder sosiale normer kan man snakke om aspekter av «gråsoner». I noen miljøer er det en utbredt holdning om at skatteunndragelse, korrupsjon eller hvitvasking er «vanlig praksis» snarere enn alvorlige lovbrudd. I visse forbindelser eller nettverk kan lojalitet til kolleger, familie eller organisasjoner gå foran lovlydighet, noe som kan føre til taushet eller medvirkning til ulovlige handlinger. Konkurranserepress er det når det er forventet at man skal maksimere fortjenesten, derved kan det skape et miljø der uetiske og ulovlige handlinger blir normalisert.

Kultur og verdier kan være individualisme og profittjag. I samfunn hvor suksess måles utelukkende i penger og makt, kan noen være villige til å bryte loven for å oppnå økonomiske fordeler. I selskaper med sterke hierarkier kan ledere misbruke sin posisjon til økonomisk kriminalitet, mens ansatte føler seg presset til å følge ordre. Vi kan se dette som tillitskultur. I noen land eller bransjer er det høy tillit til at folk opptrer ærlig, noe som kan utnyttes av de som ønsker å begå svindel uten å bli oppdaget.

Økonomisk kriminalitet blir altså ikke bare et resultat av enkeltpersoners grådighet, men også av strukturer og normer som gir rom for eller til og med oppmuntrer til slike holdninger.

2.2 Er økonomisk kriminalitet unntaket eller normen

Noen forsker hevder at økonomisk kriminalitet er et systematisk problem snarere enn en avvikende handling – særlig i bransjer med høy økonomisk gevinst og lav sannsynlighet for straffeforfølgelse.

Økonomisk kriminalitet er ikke normen i Norge, men heller ikke uvanlig ifølge en nasjonal omfangsundersøkelse fra 2023 (Regjeringen.no; «Nasjonal omfangsundersøkelse av økonomisk kriminalitet rettet mot virksomheter og kommuner», VISTA analyse; Kriminalitet – SSB – Statistisk sentralbyrå 17. juni 2020; Anmeldte lovbrudd og ofre – SSB – Statistisk sentralbyrå, 31.mai 2024; Flere har økonomiske vansker – SSB – Statistisk sentralbyrå, 11. april 2024; Meld. St. 34 (2020-2021) – regjeringen.no).

Det framgår av rapportene at omtrent 10 prosent av virksomhetene har vært utsatt for økonomisk kriminalitet i 2021. For virksomheter med fem eller flere ansatte var andelen 17 prosent. Dette nivået har vært stabilt sammenlignet med en tilsvarende undersøkelse fra 2008. Blant kommunene oppga cirka 14 prosent å ha vært utsatt for økonomisk kriminalitet, hovedsakelig i form av bedrageri. Disse tallene tyder på at selv om økonomisk kriminalitet ikke er normen er det en betydelig utfordring som krever kontinuerlig oppmerksomhet og forebyggende tiltak.

2.3 Hvordan påvirker digitalisering økonomisk kriminalitet

Kryptovaluta, kunstig intelligens og desentraliserte finanssystemer skaper nye muligheter for økonomisk kriminalitet, samtidig som de utfordrer tradisjonelle kontrollmekanismer.

Digitalisering har både redusert og økt risikoen for økonomisk kriminalitet. På den ene siden har den forbedret sporbarheten, automatisert kontrollrutiner og styrket overvåkingen av finansielle transaksjoner. På den andre siden har den skapt nye muligheter for svindel, hacking og hvitvasking.

Når det gjelder de positive effektene kommer bedre sporbarhet og transparens inn. Digitale transaksjoner etterlater elektroniske spor som gjør det vanskeligere å skjule ulovlige aktiviteter. Automatisert overvåking ved hjelp av kunstig intelligens (KI) og maskinlæring oppdages mistenkelige transaksjoner og flagger dem i sanntid. Sterkere regulering gjennom digitale løsninger gjør det lettere for myndigheter å overvåke selskaper og enkeltpersoner, for eksempel gjennom rapporteringskrav som også kalles Foreign Account Tax Compliance (FATCA)-kontrollopplysninger og anti-hvitvaskingsregler Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)-pakken som utgjør ny EU-lovgivning fra 2024. Hertil kommer raskere ettersøkning gjennom Big Data og analyseverktøy hjelper politimyndigheter og banker med å avsløre økonomisk kriminalitet mer effektivt.

Men utav dette kommer også negative effekter. Økt risiko for cyberkriminalitet som phishing, hacking og ransomware gjør det enklere å stjele penger eller manipulere finansielle systemer. Nye former for svindel kan være digitale, som investeringsbedrageri, kryptovaluta-svindel og deepfake-teknologi gjør det vanskelig å avdekke svindel. Hertil kommer anonymitet i transaksjoner hvor kryptovaluta og anonyme betalingsløsninger kan skjule ulovlige penger og hindre myndighetenes innsyn. I denne sammenheng bør man ta i betraktning bruk av automatiserte angrep – KI-drevne svindelmetoder kan manipulere systemer i stor skala, for eksempel ved automatisert innsidehandel eller falske fakturaer.

Skulle man trekke noen konklusjon av dette er det at digitalisering har gjort økonomisk kriminalitet mer sofistikert, men også lettere å oppdage. Effektiv regulering, bedre cybersikkerhet og avanserte overvåkningssystemer er avgjørende for å redusere risikoen.

2.4 Hvordan balanseres reguleringer og innovasjon

Strengere reguleringer kan hindre kriminalitet, men også bremse økonomisk vekst og innovasjon. Så hvor mye kontroll er for mye?

Balansereregulering og innovasjon i kampen mot økonomisk kriminalitet er en kompleks oppgave som krever nøye vurdering. Effektive tiltak bør hindre kriminell aktivitet uten å hemme teknologisk og økonomisk utvikling. Reguleringen bør tilpasses risikoen ved ulike teknologier og tjenester. Dette innebærer å fokusere på områder med høy risiko for økonomisk kriminalitet, samtidig som man gir rom for innovasjon i lavrisikoområder.

Tett samarbeid mellom myndigheter og næringsliv er følsomt. For eksempel har regjeringen tatt initiativet til en gjennomgang av lovverket for å fjerne hindringer i bekjempelsen av svindel og annen økonomisk kriminalitet, dette blir støttet av Finans Norge (24. 09.2024).

Iverksetting av ny teknologi kan skje ved å ta i bruk avanserte teknologier som kunstig intelligens og maskinlæring som igjen kan forbedre evnen til å oppdage og forhindre økonomisk kriminalitet. Disse teknologien kan analysere store datamengder for å identifisere mistenkelige mønster og transaksjoner.

Regelverket bør også være dynamisk og kunne tilpasses raskt til teknologiske endringer. Dette krever kontinuerlig overvåking av nye trusler og muligheter innen økonomisk kriminalitet. Oppmerksomhet på forebygging og bevisstgjøring er å investere i opplæring blant ansatte og kunder, som dermed kan bidra til å redusere risikoen for økonomisk kriminalitet. For eksempel har DNB rapportert (3. februar 2025) om økt bedrageri rettet mot både enkeltpersoner og bedrifter, dette understreker behovet for økt årvåkenhet.

Internasjonalt samarbeid er en forutsetning fordi økonomisk kriminalitet ofte er grenseoverskridende. Derfor er internasjonalt samarbeid avgjørende for å harmonisere reguleringer og dele informasjon effektivt.

En vellykket balanse mellom regulering og innovasjon krever en helhetlig tilnærming som kombinerer risikobasert regulering, samarbeid på tvers av sektorer, teknologisk innovasjon og kontinuerlig tilpassing av regelverket. Dette vil bidra til å bekjempe økonomisk kriminalitet uten å hemme økonomisk og teknologisk framgang.

3. Empiriske spørsmål

3.1 Hvordan kan økonomisk kriminalitet utvikles i lys av økonomiske kriser og globale spenninger

For eksempel har finanskrisen i 2008, Covid-19-pandemien og krigen i Ukraina ført til økt svindel knyttet til økonomiske transaksjoner, støtteordninger og sanksjonsomgåelse. Finansmarkedene kollapset etter at investeringsbanken Lehman Brothers gikk konkurs i september 2008. Gjennområnne amerikanske boliglån, pakket inn i kompliserte produkter, utløste den største globale økonomiske nedturen siden 1930-tallet.

Finanskrisen i 2008 var et resultat av en rekke faktorer, inkludert risikable utlånspraksiser, utilstrekkelig regulering og kompleksiteten i finansielle produkter. Selv om disse handlingene bidro til krisen, var det få tilfeller der enkeltpersoner eller institusjoner ble straffeforfulgt for direkte lovbrudd. Mange av aktivitetene som førte til krisen, som utstedelse av «subprime-lån» og videresalg av disse som verdipapirer, var lovlige innenfor datidens regulatoriske rammer.

Etter krisen ble det imidlertid avdekket at flere finansinstitusjoner hadde deltatt i uetiske eller villedende praksiser, som feilinformasjon og risiko knyttet til finansielle produkter. Dette førte til økt oppmerksomhet på behovet for strengere reguleringer og tilsyn med finanssektoren for å

forhindre lignende kriser i framtiden (Store Norske Leksikon, tilgang 19. mars 2025; Norges Bank, Endring av bankreguleringen etter finanskrisen i 2008 – Norge Bank, tilgang 19.03.2025).

Lehman Brothers sin konkurs i 2008 var en av de mest betydningsfulle hendelsene under finanskrisen. En viktig faktor i kollapsen var bruken av en regnskapspraksis kjent som «Repo 105». Dette er en regnskapsteknikk som Lehman Brothers Holdings Inc, brukte for midlertidig å fjerne opptil 50 milliarder dollar av eiendeler fra balanse i månedene fram til konkursen i 2008.

Teknikken innebærer å selge verdipapirer til en investeringsbank og deretter umiddelbart godta å kjøpe dem tilbake til en høyere pris, med differansen registrert som en «gjenkjøpsavtale» eller «repo» på Lehmans balanse. Fordi verdipapirene faktisk ikke ble solgt, forble de i Lehmans bøker, men ble klassifisert som «solgt» for regnskapsformål. Ifølge rapporten fra Anton R. Valukas, utnevnt som gransker av konkursretten, ble denne praksisen brukt til å manipulere finansielle rapporter og skjule selskapenes reelle risikoeksponering. (Wikipedia, tilgang 03.03.2025).

Til tross for disse avsløringene ble ingen ledere i Lehman Brothers straffeforfulgt for kriminelle handlinger, knytte til konkursen. Teknikken var lovlig, men den ble kritisert av noen for å gi et falskt inntrykk av Lehman Brothers økonomiske helse.

Dette har vært gjenstand for omfattende debatt og kritikk i etterkant av finanskrisen (Wikipedia, Rapport of Anton R. Valukas, tilgang 03.03.2025.; Finanskrisen i 2008 – Norges Bank, tilgang 03.03.2008.; Investopedia.com (2024) The Collapse of Lehman Brothers: A Case Study – Investopedia 9. desember 2024.; Papers.ssrn.com (2016). The Analysis of the Collapse of Lehman Brothers.; The Lehman Brothers Bankruptcy A: Overview – SSRN, tilgang 7. april 2015).

Covid-19 pandemien har hatt en betydelig innvirkning på økonomisk kriminalitet, både i Norge og internasjonalt. Kriminelle aktører har utnyttet kritesituasjonen til å begå ulike former for økonomiske lovbrudd,

En metode var misbruk av støtteordninger og permitteringsordninger. I Norge har det vært tilfeller der bedrifter har utnyttet permitteringsordninger ved å permittere ansatte som fortsatt arbeidet, noe som utgjør trygdebedrageri. Økokrim har også påpekt risikoen for misbruk av statlige støtteordninger etablert under pandemien, hvor både kriminelle opportuniste og ellers lovlydige personer i desperasjon har søkt å sikre økonomisk vinning.

Økt digitalisering og nye sårbarheter er andre metoder. Pandemien har akselerert overgangen til digitale plattformer, noe som har skapt nye muligheter for kriminelle. Økt bruk av digitale verktøy har ført til flere sikkerhetshendelser og sosiale manipuleringsangrep. Omtrent 7 prosent av virksomhetene har rapportert økonomisk tap eller svekket markedsposisjon som følge av slike hendelser (Meld St. 29 (2019-2020)).

Videre viser en nasjonal omfangsundersøkelse av økonomisk kriminalitet fra 2023 at omtrent 10 prosent av offentlige og private virksomhet ble utsatt for minst én form for økonomisk kriminalitet (Vista Analyse, 2023/01, ISBN 978-82-8126-613-1).

Utnyttelse av sårbare arbeidstakere er heller ikke ukjent. Den økonomiske nedgangen i mange land har gjort Norge attraktivt for arbeidstakere fra lavinntektsland. Disse sårbare arbeidstakerne risikerer å bli utnyttet av kriminelle aktører. Dette øker trusselen om arbeidslivskriminalitet.

Når det gjelder internasjonale treder har det vært en økning i svindel rettet mot både enkeltpersoner og virksomheter. Kriminelle har utnyttet pandemien til å kapitalisere på usikkerhet og økt etterspørsel etter visse produkter, noe som har ført til en oppblomstring av svindel og økonomisk og finansiell kriminalitet.

Disse trendene understreker behovet for økt årvåkenhet og styrket innsats mot økonomisk kriminalitet i kjølvannet av pandemien (Meld. St. 29 (2019-2020) Regjeringen.no; STRASAK-rapporten T1 2020 – Politiet.no; concilium.europa.eu EU's bekjempelse av organisert kriminalitet – Consilium).

Krigen i Ukraina har ført til en økning i økonomisk kriminalitet på flere måter, både i og utenfor konfliktområdet. Noen av de viktigste faktorene inkluderer: økt korrupsjon og underslag av bistandsmidler. Krigen har ført til en massiv tilstrømming av bistand og donasjoner til Ukraina. Dette har skapt muligheter for korrupsjon, hvor midlene enten forsvinner eller blir misbrukt. Det har vært rapporter om at enkelte aktører har tilegnet seg bistandsmidler urettmessig (Busol og Romanyk, 2023; Malkovska og Serdiuk, 2019). Sikkerheten og tilliten i samfunnet er sterkt svekket (Serdiuk mfl., 2023).

Med de omfattende økonomiske sanksjonene mot Russland har russiske oligarker og kriminelle nettverk forsøkt å skjule eller flytte verdier gjennom komplekse finansielle transaksjoner. Dette har økt behovet for hvitvasking av penger i ulike land, inkludert skatteparadiser.

Våpensmugling og svartebørs har ført til at den store mengden våpen som er sendt til Ukraina har skapt en risiko for at noen havner på det illegale markedet. Det har vært bekymringer for at våpen kan ende opp hos kriminelle organisasjoner i Europa.

Svindel og falske innsamlingsaksjoner er andre former hvor krigen har gitt opphav til en rekke svindelforsøk. Kriminelle utgir seg for å samle inn penger til Ukraina, men egentlig beholder de midlene selv. Dette skjer både gjennom falske veldedighetsorganisasjoner og digitale svindelmetoder (Trivedi-Bateman, Markovska and Serdiuk, 2024).

Økt menneskehandel og utnyttelse av flyktninger er nok en metode. Millioner av ukrainske flyktninger har vært sårbare for menneskehandel og utnyttelse. Kriminelle nettverk har benyttet krisen til å forlede flyktninger inn i tvangsarbeid, prostitusjon og andre former for utnyttelse.

Cyberkriminalitet og hacking hvor både statlige og ikke-statlige aktører har økt sine cyberoperasjoner. Russiske hackergrupper har vært aktive i å angripe vestlige finansinstitusjoner, mens andre har utnyttet krigen til å spre phishing-angrep og økonomisk svindel på nettet.

Krigen har dermed skapt en rekke muligheter for økonomisk kriminalitet, både i Ukraina og indirekte i resten av verden (Melnychuk, 2023).

3.2 Hvilken effekt har storfinans og manipulasjon på selskapers økonomiske kriminalitet

Økonomisk kriminalitet omfatter ulovlige handlinger som bedrageri, korrupsjon, hvitvasking og markedsmanipulasjon, og involverer både enkeltpersoner og selskaper. Store finansinstitusjoner, ofte referert til som «storfinans», kan spille ulike roller i denne sammenhengen (Finans Norge: Hvitvasking og terrorfinansiering, 23.01.2025).

Finansinstitusjoner er ofte mål for økonomisk kriminalitet, som bedrageri og hvitvasking. I 2024 rapporterte Den norske Bank (DNB) en økning i bedrageriforsøk på 39 %, hvor forsøkene involverte rundt 2,5 milliarder kroner. Finansinstitusjoner spiller en viktig rolle i å forebygge og avdekke økonomisk kriminalitet. De er pålagt å ha systemer for å identifisere mistenkelige transaksjoner og rapportere disse til myndighetene.

Manipulasjon i økonomisk kriminalitet kan innebære bruk av falsk informasjon eller villedende praksis for å oppnå økonomisk vinning. Dette kan inkludere innsidehandel eller markedsmanipulasjon, som er ulovlige handlinger knyttet til handel med finansielle instrumenter (Verdipapirhandelloven paragraf 3-1. (Markedsmisbruksforordningen) https://lovdata.no/dokument/NL/lov/2007-06-29-75/*#sareModal.

For å bekjempe økonomisk kriminalitet er samarbeid mellom finansinstitusjoner, myndigheter og andre aktører avgjørende. Dette inkluderer deling av informasjon, implementering av effektive kontrollsystemer og kontinuerlig overvåking av transaksjoner for å avdekke og forhindre ulovlige aktiviteter.

Skandaler som lekkasjene Panama Papers, publisert 3. april 2016 og Pandora Papers, 3. oktober 2021 viser hvordan verdier skjules og muliggjør hvitvasking av penger og andre verdier hvor både stater, selskaper og enkeltpersoner kan gjennomføre ulovlige transaksjoner. I dette arbeidet benyttes eksemplet med Danske Bank som illustrasjon på den praktiske gjennomføringen av hvitvasking.

Danske Bank har vært involvert i en omfattende hvitvaskingsskandale knyttet til bakens tidligere filial i Estland. Mellom 2007 og 2015 ble det avdekket at omtrent 200 milliarder euro i mistenkelige transaksjoner ble behandlet gjennom denne filialen.

I desember 2022 erkjente Danske Bank straffskyld for svindel mot andre banker og godtok å betale en bot på 2.06 milliarder dollar (tilsvarende over 20 milliarder norske kroner) til amerikanske og danske myndigheter.

Skandalen førte til endringer i bankens ledelse. Den daværende konsernsjefen, trakk seg fra stillingen i 2018 som følge av avsløringene.

I januar 2025 annonserte USAs justisdepartement at myndighetene ville overføre 50 millioner dollar av inndratte midler til Estland, som en anerkjennelse for landets assistanse i etterforskningen og rettsforfølgelsen av Danske Bank. (Reuters, 08.01.2025).

Denne saken har hatt vidtrekkende konsekvenser for banksektoren i Europa og har ført til strengere reguleringer og økt fokus på bekjempelse av hvitvasking i finansinstitusjoner.

3.3 Hvordan fungerer tiltak mot økonomisk kriminalitet i praksis

Det er usikkerhet rundt hvordan effektive tiltak som strengere reguleringer, økt tilsyn og automatisert og overvåkning faktisk virker.

I Norge omfatter dette en kombinasjon av forebyggende strategier, lovgivning, aktører, samt opplæring og bevisstgjøring. Disse tiltakene fungerer i praksis på følgende måte: Regjeringen har utviklet handlingsplaner for å bekjempe økonomisk kriminalitet, som inkluderer initiativer for å

styrke lovgivningen, forbedre informasjonsmeldingene mellom etater og øke bevisstheten om økonomisk kriminalitet.

For å effektivt bekjempe økonomisk kriminalitet samarbeider ulike offentlige etater tett. For eksempel har Arbeidstilsynet, NAV, Skatteetaten og politiet etablert samlokaliserte enheter mot arbeidsmarkeds kriminalitet i flere byer som Oslo, Bergen og Stavanger. Disse enhetene deler informasjon og koordinerer tiltak for å avdekke og forhindre ulovlige aktivitet.

Finansnæringen og offentlige aktører samarbeider gjennom initiativer som Offentlig-Privat Samarbeid mot økonomisk kriminalitet (OPS ØK). Dette samarbeidet fokuserer på å forhindre økonomisk kriminalitet ved å dele informasjon og utvikle felles strategier.

Bedrifter og organisasjoner gjennomfører opplæringsprogrammer for ansatt for å øke bevisstheten om økonomisk kriminalitet og misligheter. En helhetlig tilnærming til opplæring er avgjørende for effektiv forebygging, avdekking og håndtering av slike saker.

Økokrim fungerer som den sentrale enheten for etterforskning og påtale av økonomisk kriminalitet og miljøkriminalitet i Norge (Økokrim, 2024). De samarbeider med andre politienheter og offentlige etater for å avdekke og straffeforfølge økonomiske lovbrudd. Disse tiltakene viser hvordan Norge arbeider systematisk og koordinert for å bekjempe økonomisk kriminalitet gjennom lovgiving, samarbeid og opplæring (Handlingsplan, 2011).

3.4 Hvilke nye kriminalitetsformer oppstår i digitale økonomier

I digitale økonomier har framveksten av teknologi gitt opphav til nye former for kriminalitet. For eksempel phishing og sosial manipulering hvor kriminelle bruker e-poster, meldinger eller falske nettsteder for å forlede individer til å avsløre sensitive opplysninger som passord eller kreditkontoinformasjon. I 2022 ble det registrert over 4,7 millioner målrettede phishing-kampanjer globalt (Nysnø, 2023).

Løsepengevirus (ransomware betraktes som ondsinnet programvare som krypterer offerets data, og angriperne krever løsepenger for å gjenopprette tilgangen. Dette har blitt en betydelig trussel mot både private og offentlige institusjoner.

Identitetstyveri og bedrageri er når uautoriserte aktører stjeler personopplysninger for å begå svindel, som å åpne kontoer eller ta opp lån i andres navn.

Økonomisk svindel og fakturabedrageri er når virksomheter blir forledet til å betale falske fakturaer eller overføre penger til svindlere som utgir seg for å være legitime partnere. Dette er en økende utfordring i næringslivet.

Hacking og datainnbrudd skjer når uautoriserte aktører bryter seg inn i datasystemer for å stjele, endre eller ødelegge informasjon. Dette kan føre til økonomiske tap og skade på omdømme. Digital spionasje hvor aktører infiltrerer systemer for å samle sensitiv informasjon, ofte med mål om å påvirke økonomiske eller politiske forhold.

Sabotasje av kritisk infrastruktur er digitale angrep rettet mot essensielle tjenester som strømforsyning, vannforsyning eller helsevesen, med potensielt alvorlige konsekvenser for samfunnet.

Misbruk av kunstig intelligens er når produktiv (generativ) kunstig intelligens brukes for å skape overbevisende falsk informasjon eller «deepfakes», noe som kan forsterke omfanget og alvorlighetsgraden av cyberkriminalitet.

Pop-up-kriminalitet er raskt oppstått og kortvarig kriminelle aktiviteter som utnytter digitale plattformer. Disse er ofte vanskelig å spore og bekjempe.

Økning i digitale bedragerier, spesielt blant unge, hvor kriminelle utnytter digitale kanaler for å svindle ofre, skaper bekymring.

Hvitvasking av kryptovaluta handler om å skjule opprinnelsen til penger som stammer fra kriminell aktivitet, ved å bruke kryptovaluta og digitale verktøy som gjør pengestrømmen vanskelig å spore. Dette ligner på tradisjonell hvitvasking, men foregår i det digitale rom.

Kriminelle bruker kryptobørser, minibanker, eller Peer-to-Peer (P2P)-nettverk for å kjøpe kryptovaluta med «skitne» penger. Pengen sendes gjennom en rekke transaksjoner – gjerne via miksetjenester (mixes/tumblers) som blander midlene med andres for å skjule spor. Dette skjer gjennom desentraliserte børser (DEXs) som er en plattform som muliggjør kryptovalutahandel gjennom blokkjedebaserte smarte kontrakter i stedet for en sentralisert ordrebok som ikke krever KYC (kundekontroll). Hvitvaskingslovens krav om å kjenne kunden (KYC-prisippet). Privatlivs-coins som Monero (XMR) eller Zcash (ZEC) som er designet for anonymitet. Midlene føres tilbake til det «lovlige» systemet, f.eks. ved å kjøpe varer/tjenester, eller konverteres tilbake til fiat-penger på en annen børs.

Bekjempelsen av disse former for kriminalitet skjer i første rekke gjennom at regulære børser KYC/AML-lover (anti-hvitvasking) følges. Med andre ord «Know Your Customer» og benytt «Anti Money Laundering». Blockchain-analysefirmaer som Chainalysis og Ellipic sporer mistenkelige transaksjoner. Internasjonalt samarbeid (for eksempel Interpol, Europol) er avgjørende. Nye lover i EU og USA styrker reguleringen av kryptosektoren.

I Norge er hvitvaskingsloven av 2018 det sentrale regelverket og Finanstilsynet spiller en viktig rolle i etterlevelsen, og Økokrim i etterforskningen. Det private næringslivet har gjennom bankene innført strengere krav for å håndtere risikoen for hvitvasking, særlig tiltak som dokumentasjonskrav. Banker er generelt tilbakeholdende med samarbeid med kryptorelatert virksomheter på grunn av usikkerhet rundt reguleringene.

Kryptovaluta representerer en høy iboende risiko for hvitvasking og terrorfinansiering i Norge. Dette skyldes blant annet muligheten for anonyme transaksjoner og manglende reguleringer.

Et annet eksempel er Non-fungible tokens (NFT-er), digitale eiendeler lagret på blockchain. Det betyr at de ikke er utskiftbare, men er unike og kan ikke kopieres eller endres. De er altså kryptografiske, men i motsetning til andre kryptoer finnes det bare én av sitt slag. Digitale eiendeler er et marked som har økt svært mye de senere år. Digitale eiendeler brukes til å representere elementer i digitale filer, og anvendes i hovedsak som bevis på eierskap. Disse forhold er avgjørende for å forstå og bekjempe økonomisk kriminalitet i dages globale økonomi. Kriminalitetsformene understreker behovet for kontinuerlig overvåking, oppdatering av sikkerhetssystemer og økt bevissthet blant både individer og organisasjoner for å beskytte seg i den digitale økonomien (Kruize, 2013).

4. Slutninger og blikk på framtiden

Den raske digitaliseringen av økonomien har ført til en økning i økonomisk kriminalitet, der kriminelle utnytter teknologiske fremskritt for å begå mer sofistikerte lovbrudd. Dette inkluderer bruken av anonymiserende betalingsmetoder og salg av spesialiserte kriminelle tjenester på det mørke markedet. For å møte disse utfordringen er det avgjørende med et tett samarbeid mellom offentlige myndigheter og private aktører. Deling av data og informasjon kan bidra til å avdekke og forhindre digitale trusler. Videre er investering i cybersikkerhet og kontinuerlig oppdatering av sikkerhetssystemer essensielt for å beskytte mot nye angrepsmetoder. I framtiden vil kampen mot økonomisk kriminalitet i digitale økonomier kreve en kombinasjon av teknologisk innovasjon, styrket lovgivning og økt bevissthet blant både bedrifter og enkeltpersoner. Bare gjennom en helhetlig tilnærming kan vi effektivt bekjempe denne stadig utviklede trusselen (skatteetaten.no (2024); Økokrim, (2024); Finanstilsynet.no 2022).

Referanser

- Anmeldte lovbrudd og ofre- SSB – Statistisk sentralbyrå, 31. mai 2024.
- Busol, O. and Ramanyk, B. (2023). Corruption prevention in Ukraine through the prism of elite mentality. *Baltic Journal of Economic Studies*, 2023, - baltijapublishing.lv
- DNB, (2025). Økonomisk kriminalitet er et samfunnsproblem. *Finansiell Trygghet: Hvem kan du stole på?*
- Finanstilsynet (2022). Digital finans og IT-riisiko. Oslo. *Finanstilsynet* (tilgang 1. juni 2022).
- Finans Norge, (2024). Lovverk for bekjempelse av kriminalite: Bank, Digitalisering, Trygge forbrukere, økonomisk kriminalitet. (Tilgang 24.september 2024).
- Flere har økonomiske vansker – SSB – Statistisk sentralbyrå 11. april 2024.
- Handlingsplan, (2011) Regjeringens handlingsplan mot økonomisk kriminalitet. Oslo: Justis- og politidepartementet/Finansdepartementet.
- Investopedia. com (2024). The Collapse of Lehman Brothers: A Case Study. *Investopedia* 9. Desember 20024.
- Kriminalitet – SSB – Statistisk sentralbyrå, 17.juni 2020.
- Kruize, P. (2013). Kriminalitet i en digitalisert verden. Identitetstyveri og bedrageri på internettet. Det Juridiske Fakultet, Københavns Universitet.
- Norges Bank (2025). (Finanskrisen i 2008.(tilgang 03.03.2025).
- Meld. St. 29. (2019-2020).
- Meld. St. 34 (2020-2021).
- Melnychuk, T, (2023). Organized Crime in Ukraine and Its Models in Transition. *Springer Briefs in Law (BRIEFLAW)*, pp. 41 – 91.
- Markovska, A. and Serdyuk, O.O. (2019). The perception of corruption in the daily life of Ukraine. In Van Duyn, Serdyuk, A. et all (eds). *Construction and organizing crime in Europe* (pp. 313-337).: Eleven Publishing.

- Nysnø, J. (2023). Dette er de største digitale truslene. Rapport Telenor: 14. september 2023.
- Papers.ssrn.com (2015). The Lehman Brothers Bankruptcy A: Overview – SSRN, tilgang 7. April 2015.
- Serdiuk, O. O., Bygaychuk, K., Matiuskova, T., Kuzia, L., Danylenko, I., Shcherbakova, I., Markovaska, A., & Sokurenko, V. (Eds.) (2023). *Security and trust 2022: according to the results of research 2013-2022 conducted in Kharkiv region*. <http://doi.org/10.32631/sf2022>
- Report of Anton R. Valukas, tilgang 03.03.2025.
- Skatteetaten.no (2024). Det er et samfunnsproblem at økonomisk kriminalitet får lav prioritet. Publisert 06.02.2024.
- Store Norske Leksikon (2025). Tilgang 19. mars 2025.
- Trividi-Batman, N., Markovska, A., and Serdiuk, O. O. (2024). The role of morality in coeducation, theft, and violence in a Ukrainian context. *European Journal on Criminal Policy and Research*, 2024 – Springer.
- VISTA Analyse (2023/01). Nasjonal omfangsundersøkelse av økonomisk kriminalitet rettet mot virksomheter og kommuner. *Regjeringen.no* (ISBN – 978-82-8126-613-1).
- Økokrim, (2024). Økokrims trusselvurdering: Omfattende trusler mot samfunn og næringsliv. Oslo. *Økokrim*.
- Økokrim, (2024). Miljøkrim. Oslo: *Økokrim*. Årgang 27/Nummer 2. 2024.