Riksrevisjonen

Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT

Dokument 3:5 (2020–2021)

Forside:
Bilde av politiperson foran dataskjerm. Foto: Gorm Kallestad/NTB
ISBN-978-82-8229-499-7

Til Stortinget

Riksrevisjonen legger med dette fram Dokument 3:5 (2020–2021) *Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT*.

Dokumentet har følgende inndeling:

- Riksrevisjonens konklusjoner, merknader, anbefalinger, departementets oppfølging og Riksrevisjonens sluttmerknad
- vedlegg 1: Riksrevisjonens brev til statsråden
- vedlegg 2: statsrådens svar
- vedlegg 3: forvaltningsrevisjonsrapport med vurderinger

Riksrevisjonen benytter følgende begreper for kritikk, med denne rangeringen etter høyest alvorlighetsgrad:

- **Svært alvorlig** brukes ved forhold der konsekvensene for samfunnet eller berørte borgere er svært alvorlige, for eksempel risiko for liv eller helse.
- **Alvorlig** benyttes ved forhold som kan ha betydelige konsekvenser for samfunnet eller berørte borgere, eller der summen av feil og mangler er så stor at dette må anses som alvorlig i seg selv.
- **Sterkt kritikkverdig** angir forhold som har mindre alvorlige konsekvenser, men gjelder saker med prinsipiell eller stor betydning.
- **Kritikkverdig** brukes for å karakterisere mangelfull forvaltning der konsekvensene ikke nødvendigvis er alvorlige. Dette kan gjelde feil og mangler som har økonomiske konsekvenser, overtredelse av regelverk eller saker som er tatt opp tidligere og som fortsatt ikke er rettet opp.

Riksrevisjonen, 2. februar 2021

For riksrevisorkollegiet

Per-Kristian Foss
riksrevisor

Innhold

Justis- og beredskapsdepartementet

Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT

Politiets ansvar og hovedoppgaver er i henhold til politiloven å ivareta borgernes rettssikkerhet, trygghet og alminnelige velferd. Politiet skal forebygge og forhindre straffbare handlinger og avdekke, stanse og forfølge lovbrudd og straffbare forhold.

Målet med undersøkelsen har vært å vurdere om politi- og påtalemyndigheten har oversikt over, etterforsker og oppklarer IKT-kriminalitet i samsvar med føringer gitt av Stortinget, herunder om politiet ivaretar sin primæroppgave på dette området i samsvar med politiloven. For å belyse politiets innsats mot IKT-kriminalitet er tre utvalgte kriminalitetsområder undersøkt: internettrelaterte seksuelle overgrep, økonomisk IKT-kriminalitet (bedragerier og identitetskrenkelser) og «ren» IKT-kriminalitet (datainnbrudd og uberettiget befatning med tilgangsdata).

Med økende digitalisering av samfunnet øker også kriminaliteten som skjer på digitale flater. Mye av kriminaliteten, som bedragerier og seksuelle overgrep, utføres nå som IKT-kriminalitet. Politiets straffesaksstatistikk viser at den tradisjonelle kriminaliteten som skjer i det fysiske rom har vært i nedgang over flere år. Samtidig peker flere kilder i retning av at det har skjedd en samtidig vekst i IKT-kriminalitet som ikke fanges opp av straffesaksstatistikken. IKT-kriminalitet er i denne undersøkelsen definert som kriminalitet som er rettet mot datasystemer og/eller datanettverk, eller kriminalitet der sentrale elementer av handlingsforløpet utføres ved hjelp av datasystemer og/eller datanettverk.[1]

IKT-kriminalitet forekommer både som alvorlig og mindre alvorlig kriminalitet. Alvorlig IKT-kriminalitet treffer barn og unge i form av seksuelle overgrep via internett, rammer private virksomheter og medfører store verdimessige tap. Alvorlig IKT-kriminalitet rammer offentlige og private institusjoner som har kritiske samfunnsoppdrag. IKT-kriminalitet rammer også norske borgere og private virksomheter i form av for eksempel ID-tyverier, nettbankbedragerier og andre svindelformer på internett.

IKT-kriminalitet håndteres av politidistriktene og av særorgan som Kripos og ØKOKRIM. Politidistriktene har opprettet enheter for digitalt politiarbeid som bistår i etterforskningen av IKT-kriminalitet, og i sikring og analyse av elektroniske spor. Disse enhetene har i dag en avgjørende rolle, ikke bare i etterforskningen av IKT-kriminalitet, men også i etterforskningen av drap, vold og andre saker som ikke er IKT-kriminalitet fordi digitale spor forekommer i de fleste straffesaker.

Undersøkelsen har blant annet tatt utgangspunkt i disse vedtakene og forutsetningene fra Stortinget:

- *Lov 4. august 1995 nr. 53 om politiet (politiloven)*.
- *Lov 20. mai 2005 nr. 28 om straff (straffeloven)*.
- *Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven)*.
- Innst. 306 S (2014–2015), jf. Prop. 61 LS (2014–2015) *Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen)*
- Innst. 187 S (2017–2018), jf. Meld. St. 38 (2016–2017) *IKT-sikkerhet - Et felles ansvar*
- Innst. 6 S (2018–2019), jf. Prop. 1 S (2018–2019) *Justis- og beredskapsdepartementet*

Rapporten ble lagt fram for Justis- og beredskapsdepartementet ved brev 19. oktober 2020. Departementet har i brev 11. november 2020 gitt kommentarer til rapporten. Kommentarene er i hovedsak innarbeidet i rapporten og i dette dokumentet.

Rapporten, oversendingsbrevet fra riksrevisorkollegiet til departementet 9. desember 2020 og svaret fra statsråden 8. januar 2021 følger som vedlegg.

[1] Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom*

1 Konklusjoner

- Politiets evne til å avdekke og oppklare IKT-kriminalitet har klare svakheter som samlet sett er alvorlige.
  - Politiet mangler kompetanse innenfor etterforskning av IKT-kriminalitet.
  - Tiltakene for å styrke politiets kapasitet til etterforskning av IKT-kriminalitet holder ikke tritt med utfordringene.
  - Svakheter ved støttesystemer fører til ineffektiv ressursbruk og manglende oppklaring av IKT-kriminalitet.
  - Manglende samordning mellom distrikter gir utfordringer for oppklaring av IKT-kriminalitet.
  - Utfordringer ved internasjonalt samarbeid bidrar til lav oppklaring av IKT-kriminalitet.
- Politiet mangler oversikt over IKT-kriminalitet.
- Politiet prioriterer i liten grad etterforskning og oppklaring av ren IKT-kriminalitet.
- Tips og etterretning om internettrelaterte seksuelle overgrep øker og utfordrer politiets kapasitet.
- Politiet mangler kapasitet til å møte utviklingen innenfor økonomisk IKT-kriminalitet.
- IKT-kriminalitet har i liten grad vært prioritert av Politidirektoratet og Justis- og beredskapsdepartementet.

2 Riksrevisjonens merknader

2.1 Politiets evne til å avdekke og oppklare IKT-kriminalitet har klare svakheter som samlet sett er alvorlige

Politiets ansvar, mål og oppgaver framgår av politiloven. Å avdekke, stanse og straffeforfølge kriminell virksomhet og straffbare forhold er blant politiets sentrale primæroppgaver. Denne undersøkelsen viser at Politidirektoratet og Justis- og beredskapsdepartementet over mange år har vært klar over at politiets kompetanse, kapasitet, støttesystemer, samordning og internasjonale samarbeid ikke henger tritt med kriminalitetsutviklingen med et større innslag av IKT-kriminalitet. Den anmeldte kriminaliteten har gått ned over flere år, samtidig er det mye som tyder på at IKT-kriminaliteten øker slik regjeringen selv slår fast i Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden*. I perioden etter 22. juli 2011 og i forbindelse med politireformen er politiet tilført betydelige ressurser, og bemanningen har økt med over 20 prosent. Budsjettøkningen er i liten grad utnyttet til å styrke politiets evne til å håndtere IKT-kriminalitet, men har i stedet gått til andre prioriterte oppgaver, ifølge Justis- og beredskapsdepartementet.

Konsekvensene for barn, unge, privatpersoner og virksomheter som utsettes for IKT-kriminalitet kan være dramatiske. Samlet sett mener Riksrevisjonen at svakhetene i politiets evne til å avdekke og oppklare IKT-kriminalitet er alvorlige.

2.1.1 Politiet mangler kompetanse til å bekjempe IKT-kriminalitet

I Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar* understrekes det at digital kompetanse må bygges i alle politidistrikt slik at politiet har tilstrekkelige forutsetninger for å bekjempe IKT-kriminalitet. At politiet mangler kompetanse for å bekjempe IKT-kriminalitet er slått fast i en rekke rapporter, utredninger og strategier helt tilbake til 2012. Senest i årsrapporten for 2019 skriver Politidirektoratet at politiet mangler kompetanse til å møte utfordringene på dette området. Regjeringen peker også i Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden* på at IKT-kriminalitet og digitalisering av kriminaliteten utfordrer politiets kompetanse. Utfordringene gjelder kompetanse på alle nivåer i politiet: basiskompetanse, spesialistkompetanse og påtalekompetanse.

Det har vært kjent over mange år at basiskompetansen i politidistriktene har vært svak innenfor området IKT-kriminalitet. Manglende kompetanse i politiets førstelinje som består av ordenstjeneste/patruljer, kriminalvakt og saksmottak fører til at IKT-kriminalitet håndteres feil i den viktige initiale fasen. Spor sikres ikke riktig, feil etterforskningsskritt tas, saker registreres feil, og saker som enkelt kan oppklares, henlegges. Flere politidistrikt, for eksempel Oslo og Trøndelag, har tatt konsekvensen av dette og styrket kompetansen i

førstelinjen med blant annet fagkontakter innenfor digitalt politiarbeid. Selv om grunnutdanningen på Politihøgskolen er styrket innenfor digitalt politiarbeid, og digitalt politiarbeid er tatt inn i den årlige obligatoriske utdanningen for etterforskere og påtalejurister, ser dette foreløpig ut til i liten grad å ha styrket basiskompetansen.

Spesialistkompetansen som finnes hos enheter for digitalt politiarbeid (DPA) og hos særorganene Kripos og ØKOKRIM er noe styrket. DPA-kompetansen brukes i hovedsak til sikring av elektroniske spor i alvorlige saker som seksuallovbrudd, grov vold, drap og narkotika. Kapasiteten hos særorganene til etterforskning av alvorlig og teknologisk krevende IKT-kriminalitet er begrenset. Mulighetene til å rekruttere sivil spesialistkompetanse som dataingeniører og informatikere begrenses av målet om to politiårsverk per tusen innbyggere. Dette er kompetanse som vil være avgjørende for å kunne bekjempe utviklingen i kriminaliteten på dette området. Politiets spesialistkompetanse er i tillegg ettertraktet i næringslivet og i andre deler av offentlig sektor som håndterer dataangrep. Konsekvensen av dette er at alvorlig, teknologikrevende IKT-kriminalitet nedprioriteres, og det har ført til at virksomheter i næringslivet søker bistand andre steder enn hos politiet når de utsettes for alvorlig IKT-kriminalitet. Etter Riksrevisjonens vurdering har dette ført til manglende tillit til politiets innsats på området.

Påtalemyndighetens kompetanse innenfor digitalt politiarbeid og IKT-kriminalitet har over flere år vært påpekt som mangelfull i både politidistriktene og den høyere påtalemyndighet. Påtalejuristene i politidistriktene baserer seg i hovedsak på erfaringsbasert læring og tar i liten grad etter- og videreutdanning. Etterutdanningstilbudet ved Politihøgskolen for påtalejuristene er også svært begrenset og omfatter ikke opplæring innenfor digitalt politiarbeid. Et av punktene i Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet fra 2015 var å utarbeide en plan for å styrke påtalemyndighetens digitale kompetanse, men dette har foreløpig ikke ført til konkrete tiltak. Påtalejuristene tar påtaleavgjørelser om henleggelse og tiltalebeslutning, og lav kompetanse innenfor IKT-kriminalitet kan både føre til svak bekjempelse av IKT-kriminalitet generelt og svekke rettssikkerheten for fornærmede og tiltalte i IKT-kriminalitetssaker. Dette forsterkes ytterligere ved det økte omfanget av både IKT-kriminalitet og digitale bevis i straffesaksbehandlingen.

Riksrevisjonen mener det er alvorlig at det ikke er tatt tilstrekkelige grep for å styrke politi- og påtalemyndighetens kompetanse på IKT-kriminalitet. Manglende kompetanse kan utgjøre et rettssikkerhetsproblem ved at saker henlegges uten etterforskning, eller ved at de blir feilbehandlet. Uten nødvendig kompetanse til å bekjempe IKT-kriminalitet mister politiet også tillit i befolkningen og hos private og offentlige virksomheter som utsettes for denne kriminaliteten, noe som er alvorlig.

2.1.2 Tiltakene for å styrke politiets kapasitet til etterforskning av IKT-kriminalitet holder ikke tritt med utfordringene

I Meld. St. 29 (2011–2012) *Samfunnssikkerhet* ble det slått fast at IKT-kriminaliteten var i kraftig vekst og at politiet stod overfor store utfordringer på dette området. Selv om antallet årsverk i politiet (unntatt PST) har økt med 24 prosent (3392 årsverk) i perioden 2012 til august 2020, har få av disse tilfalt etterforskningsfeltet. I henhold til Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden* er etterforskningsarbeidet styrket etter politireformen ved at sakene håndteres mer enhetlig i felles straffesaksinntak (FSI) i distriktene, og ved at kvaliteten på straffesaksarbeidet er bedret etter etterforskningsløftet. Undersøkelsen viser imidlertid at etterforskningskapasiteten fortsatt er en utfordring innenfor området IKT-kriminalitet.

En utfordring på området IKT-kriminalitet er at dataetterforskere skal sikre elektroniske spor i et vidt spekter av saker, samtidig som de skal bistå i etterforskning av IKT-kriminalitet. Kapasiteten innenfor digitalt politiarbeid og etterforskning av IKT-kriminalitet brukes i all hovedsak til å sikre elektroniske spor i de alvorligste straffesakene, som drap, grov vold, grove narkotikasaker og alvorlige sedelighetssaker. Begrenset kapasitet fører til krevende etterforskningsfaglige prioriteringer mellom de sakstypene Riksadvokaten framhever som prioriterte i sitt årlige mål- og prioriteringsskriv. Sikring av elektroniske spor i de prioriterte, alvorlige straffesakene fører til at IKT-kriminalitet på andre områder nedprioriteres, for eksempel økonomisk IKT-kriminalitet. Også ren IKT-kriminalitet som Riksadvokaten lenge har vært opptatt av at skal prioriteres, blir nedprioritert. Undersøkelser viser at næringslivet og befolkningen har lavere tillit til politiet når det gjelder IKT-kriminalitet enn annen kriminalitet, og at saker i mange tilfeller derfor ikke anmeldes. En konsekvens av dette er at virksomheter og privatpersoner henvender seg til private aktører i stedet for til politiet for bistand når de utsettes for IKT-kriminalitet.

Det er iverksatt flere tiltak for å styrke politiets kapasitet til å etterforske IKT-kriminalitet og sikre elektroniske spor. Opprettelsen av enheter for digitalt politiarbeid (DPA) i alle politidistrikt i forbindelse med politireformen og Nasjonalt cyberkrimsenter (NC3) ved Kripos fra januar 2019 er to av de viktigste tiltakene. Ambisjonene for NC3, som er frontet som en stor satsing innenfor bekjempelsen av IKT-kriminalitet, er nedjustert fra 200 ansatte innen utgangen av 2021 til 150 ansatte innen utgangen av 2022. Om lag 80 av de ansatte i NC3 var allerede ansatt i Kripos ved opprettelsen av senteret. NC3 skal bistå distriktene og etterforske noen særlig alvorlige saker selv. Per i dag har senteret kapasitet til å etterforske en–to større saker i året, og de mener også selv at dette er mest hensiktsmessig. Det vil si at etterforskningen av IKT-kriminalitetssakene i all hovedsak må skje i distriktene. Konsekvensene av lav kapasitet i DPA og NC3 er at teknologikrevende IKT-kriminalitet henlegges. Sakene blir for store, komplekse og ressurskrevende å etterforske for politidistriktene.

Mange politidistrikter har utfordringer med å sikre kontinuiteten i kapasiteten til etterforskning av de alvorligste sakene, for eksempel internettrelaterte seksuelle overgrep. Mange saker skal etterforskes, og det er høyt gjennomtrekk av etterforskere, noe som blant annet skyldes at mange av lønnsmessige årsaker ønsker seg til ordenstjeneste framfor etterforskning.[2] For politiutdannede er det få incentiver til å velge en karriere innenfor etterforskning av denne typen saker.

Riksrevisjonen mener det er sterkt kritikkverdig at det ikke er gjort mer for å omstille politiet og sikre tilstrekkelig kapasitet til å takle et kriminalitetsbilde med stadig større innslag av IKT-kriminalitet og behov for etterforskning av elektroniske spor.

2.1.3 Svakheter ved støttesystemer fører til ineffektiv ressursbruk og manglende oppklaring av IKT-kriminalitet

I prosessen med å innhente, sikre og analysere digitale bevis bruker enhetene for digitalt politiarbeid (DPA) blant annet spesialiserte programmer, teknisk utstyr, lagringsmedier og digital infrastruktur (støttesystemer). Svakheter ved politiets støttesystemer har hatt konsekvenser for politiets arbeid med å etterforske og oppklare IKT-kriminalitet over flere år.

I Innst. 306 S (2014–2015) viser justiskomiteen til at riktig bruk av digitale verktøy er avgjørende for politiets evne og mulighet til å løse sitt samfunnsoppdrag. Arbeidsmetoder og arbeidsprosesser må sikre effektiv disponering av politiressursene og legge til rette for raskere etterforskning med høyere kvalitet. I Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar* vises det til at verktøyene for å håndtere digitale spor må være oppdaterte i tråd med den teknologiske utviklingen, og at politiets etterforskningsmetoder må holde tritt med de kriminelles bruk av moderne teknologi.

Utfordringene forbundet med støttesystemer har vært kjent over lengre tid og er omtalt i en rekke rapporter, første gang i 2012.[3] Riksrevisjonen mener Politidirektoratet burde ha sørget for en nasjonal samordning av innkjøp, drift og administrasjon av utstyr og programvare som brukes av DPA-enhetene. Bedre støttesystemer kunne gjort samordningen mellom politidistriktene enklere og effektivisert politiets arbeid. Dette kunne bidratt til at politiet kunne etterforsket og oppklart flere saker. Riksrevisjonen mener det er sterkt kritikkverdig at disse utfordringene ikke er tatt tak i.

Manglende nasjonal samordning av innkjøp, drift og administrasjon av utstyr og programvare

Politiet viser i en rapport fra 2019 til utfordringer og konsekvenser når det gjelder innkjøp, drift og administrasjon av utstyr og programvare, blant annet disse:[4]

- Det er ikke klart definert hvem som har ansvar for drift og vedlikehold av utstyr og programvare.
- Det er ingen nasjonal innkjøpsavtale som benyttes ved innkjøp og fornyelse av lisenser. Lokalt fremforhandlede priser på lisenser gir sannsynligvis høyere totalkostnader for politiet.
- Det er ingen føringer på hva slags utstyr det minimum skal være ved ulike enheter i politiet, og det er stor variasjon i utstyrsparken mellom politidistriktene.
- Det er mye gammelt utstyr som er modent for utskifting uten at det er planer for å skifte dette ut.

[2] Justis- og beredskapsdepartementet, (2019) *Rapport fra arbeidsgruppe som har sett på saksflyt i saker som gjelder overgrep mot barn*, oppnevnt av Justis- og beredskapsdepartementet 26. juli 2018, rapport publisert 13. mars 2019.
[3] Politidirektoratet, (2012) *Politiet i det digitale samfunnet: En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett.*
[4] Politiet, (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning, faggrupperapport utarbeidet av en arbeidsgruppe på oppdrag fra Politidirektoratet, datert 9. september 2019.*

- Ansatte i DPA-enhetene bruker mye tid og ressurser til oppfølging av programvarelisenser, og mange distrikter har ikke nødvendige programmer for å utføre arbeidet. Noen har begrensninger med hensyn til kapasitet i form av få lisenser på viktige verktøy på grunn av høye lisenskostnader.

Flere av politidistriktene som er intervjuet, samt Politidirektoratet, mener det i større grad enn i dag burde vært tatt et nasjonalt ansvar for innkjøp, administrasjon og sikring av støttesystemer og verktøy til digitalt politiarbeid. Undersøkelsen viser at når innkjøp og drift av programvare og utstyr er overlatt til det enkelte politidistrikt, bruker dataetterforskere betydelig med tid og ressurser på dette, noe som bidrar til en ineffektiv ressursbruk i en etat som fra før opplever et hardt press på ressursene.

Manglende retningslinjer, rutiner og standarder for sikring av digitale bevis

Undersøkelsen viser at flere politidistrikter mener det er behov for retningslinjer og rutiner for det digitale politiarbeidet. Utarbeidelse av rutiner og veiledere blir i for stor grad opp til det enkelte distrikt og det etterlyses tydeligere nasjonale føringer for hvordan digitale bevis skal innhentes, analyseres og etterforskes. Mange enheter for digitalt politiarbeid savner støttesystemer for å utføre oppgavene funksjonen har ansvar for. Dette er et teknisk og ofte komplisert område av etterforskningen hvor det mangler sentrale føringer på hvilke verktøy, metoder og retningslinjer som skal gjelde. Mangelen på føringer har bidratt til ineffektivitet og utvikling av lokal praksis som ikke nødvendigvis er i tråd med ønsket praksis. Manglende føringer kan også være en rettssikkerhetsutfordring når innhenting og tolkning av elektroniske bevis skjer på ulike måter i ulike politidistrikt. Fagmiljøet har anbefalt at det iverksettes tiltak, og Politidirektoratet ga derfor i 2020 et oppdrag til faggruppen for datatekniske undersøkelser og internettrelatert etterforskning om å utarbeide retningslinjer for politiets håndtering og gjennomgang av digitale beslag for ulike brukergrupper, med vekt på initialfasen. De primære brukergruppene er her politipatruljer og felles straffesaksinntak (FSI). Retningslinjene vil bli utarbeidet i samarbeid med Riksadvokaten.

Mangler ved datainfrastruktur og beslagsnett

Undersøkelsen viser at politiet mangler en tilfredsstillende infrastruktur for håndtering av digitale beslag. Politiets IKT-tjenester utviklet i perioden 2016–2019 et digitalt lagringsnett (*Digitale spor og beslag* – DSB-nett) for digitale beslag, som er tatt i bruk av alle politidistrikt med unntak av Oslo politidistrikt. Det nye beslagsnettet tilfredsstiller i liten grad anbefalinger fra Kripos når det gjelder håndtering av beslag fra etterforskning av internettrelaterte seksuelle overgrep. Nettet møter heller ikke behovene distriktene har, og det har vært preget av manglende brukerinvolvering. Undersøkelsen viser at det er for lite lagringsplass tilgjengelig, og at nettet ikke er tilkoblet alle lokasjoner/steder som har behov for det. Mange politidistrikt mener det nye beslagsnettet ikke dekker, eller bare i noen grad dekker, det faktiske behovet DPA-enhetene har for transport, oppbevaring og arkivering av elektronisk bevismateriale.

En stor utfordring for politiet i etterforskning av internettrelaterte seksuelle overgrep mot barn og unge, og annen IKT-kriminalitet, er omfanget av digitale beslag. DPA-enhetene bruker en stor andel tiden til å gjennomgå av denne typen beslag. Kripos foreslo en nasjonal løsning for håndtering av overgrepsmateriale i 2016/2017 som fortsatt ikke er iverksatt. Norsk politi har derfor ikke en enhetlig måte å behandle internettrelaterte seksuelle overgrep som omhandler bildedeling, -distribusjon og -produksjon. Digitale beslag gjennomgås i hvert enkelt distrikt uten særlig samordning. Politiet mangler en nasjonal løsning som kan bidra til å samordne etterforskningen på tvers av politidistrikter og gjøre informasjon mer tilgjengelig for analyse og etterforskning. Uten en nasjonal løsning blir politiets arbeid mindre effektivt.

Fagmiljøet har foreslått å videreutvikle lagringsnettet slik at det i større grad kan imøtekomme de behovene politidistriktene har, men det er ikke prioritert av Politidirektoratet. Direktoratet er kjent med at lagringsnettet foreløpig har begrensninger, og at distriktene fortsatt bruker betydelige ressurser fordi det sentrale nettet mangler analysemuligheter. Politidirektoratet ser at det er potensial for å samordne beslagshåndtering og -gjennomgang i politidistriktene for å utnytte etterforskningskapasiteten på en bedre måte. En videreutvikling av blant annet DSB-nettet vil kunne bidra til å løse utfordringer på dette området. Manglende prioritering og leveranser fra Politidirektoratet og Politiets IKT-tjenester fører til at utfordringene vedvarer. Politidirektoratet påpeker i intervju at det har tatt for lang tid å få på plass sentrale løsninger, som DSB-nett.

2.1.4 Manglende samordning gir utfordringer for oppklaring av IKT-kriminalitet

Det framgår av Innst. 306 S (2014–2015) en forventning om at større organisatoriske enheter og en mer helhetlig organisering av politidistriktene vil styrke forutsetningene for systematisk kunnskapsutvikling og kunnskapsdeling i politiet. Nasjonal styring og samordning mellom distriktene, samarbeid mellom

politidistriktene og evne til å se sammenheng i innkommende saker hos felles straffesaksinntak vil være avgjørende for å avdekke og effektivt etterforske IKT-kriminalitet.

IKT-kriminalitet kjennetegnes ved at den ikke tar hensyn til grenser, den rammer gjerne på tvers av politidistrikter og landegrenser. Gjerningspersoner som står bak internettrelaterte seksuelle overgrep og nettbedragerier, og som opererer på tvers av distriktsgrenser, kan gå under radaren. Saker kan virke små og ubetydelige i et enkelt område, men kan ha et stort omfang nasjonalt eller internasjonalt. Kripos har påpekt manglende nasjonal samordning og koordinering av politiets innsats mot internettrelaterte seksuelle overgrep, og næringslivet har påpekt tilsvarende mangler innenfor økonomisk IKT-kriminalitet. Slik det framstår i dag, evner politiet i liten grad å se kriminalitetsbildet på tvers av distriktsgrenser og sette inn effektive tiltak for å forhindre eller effektivt bekjempe IKT-kriminaliteten. Nasjonal styring og samordning av innsatsen mot alvorlig kriminalitet på dette området er svak.

Den viktigste ressursen i arbeidet med å oppklare IKT-kriminalitetssaker, DPA-enhetene, bærer preg av å være ulikt organisert på ulike nivåer i politiorganisasjonen. Dette preger flere av politidistriktene negativt og skaper mål- og interessekonflikter.[5] Ulik organisering av DPA-enhetene gir utfordringer med hensyn til kunnskapsdeling og kompetanseutvikling. Det mangler nasjonale rammeverk, fagstyring og føringer for organisering av funksjonen. Digitalt politiarbeid blir for lite synlig nasjonalt, og det gir ikke nødvendig framdrift i arbeidet med å omstille politiet til endringene i kriminalitetsbildet med mer IKT-kriminalitet. Fagkontakter for digitalt politiarbeid kan også være en viktig ressurs for å oppklare IKT-kriminalitetssaker, men brukes i varierende grad i politidistriktene. Tanken bak fagkontaktene er at de skal avlaste DPA-enhetene ved å være rådgiver for egen enhet når det gjelder elektroniske spor. DPA-enheten i flere distrikter etterlyser nasjonale retningslinjer for hvilken rolle og kompetanse fagkontaktene skal ha.

Gjennom etableringen av felles straffesaksinntak (FSI) er det lagt opp til en mer enhetlig og standardisert håndtering av innkommende saker. I intervju sier flere politidistrikter at FSI er et steg i riktig retning, men det finnes flere forbedringspunkter. For FSI er det generelt en utfordring med tilgang på riktig utstyr, programvare og kompetanse som kan sikre riktig prioritering og håndtering av saker i innledende fase. FSIs evne til å se sammenheng mellom innkommende saker vil derfor være avgjørende for å kunne avdekke store sakskomplekser. FSI mangler imidlertid rutiner og evne til å oppdage disse sammenhengene og trendene i kriminalitetsbildet. Organiserte kriminelle som utøver IKT-kriminalitet mot mange ofre samtidig blir derfor i liten grad avslørt. Dette bekreftes av større næringslivsaktører som er intervjuet i forbindelse med undersøkelsen.

Riksrevisjonen anser det som alvorlig at politiet ikke har bedre nasjonal samordning og koordinering av politidistriktene. Konsekvensene av dette kan være at politiet ikke ser saker i sammenheng, og dermed ikke ser alvorlighetsgraden ved store sakskomplekser. Saker kan dermed henlegges på feilaktig grunnlag.

2.1.5 Utfordringer ved internasjonalt samarbeid bidrar til lav oppklaring av IKT-kriminalitet

I Prop. 1 S (2018–2019) for Justis- og beredskapsdepartementet presiseres det at lovbrudd ofte har internasjonale koblinger og gjennomføres av kriminelle nettverk som ikke følger landegrensene. Dette vil i mange saker bety at et godt internasjonalt samarbeid er en forutsetning for å bekjempe grenseoverskridende kriminalitet. Fra 2016 har Riksadvokaten sagt at internasjonalt samarbeid må vektlegges i oppfølgingen av IKT-kriminalitet.

Undersøkelsen viser at internasjonalt samarbeid i mange sammenhenger er avgjørende for oppklaring, men politiet utfordres av ulikheter i landenes lovgivning som gjør det krevende å opprettholde en effektiv kriminalitetsbekjempelse og straffeforfølging.[6]

Politidistriktene som er intervjuet sier at IKT-kriminalitetssakene med spor eller gjerningsperson utenlands ofte henlegges av hensyn til tids- og ressursbruken som ofte går med i slike saker. En sak må være høyt prioritert for at samarbeid med andre land igangsettes. Dette gjelder både ved behov for gjennomføring av avhør utenlands og ved innhenting av bevis fra tjenesteleverandører i utlandet. Sakene er ikke nødvendigvis vanskeligere å etterforske, men selve prosessen for bistands- og rettsanmodninger oppleves som kompleks

[5] Politidirektoratet, (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning*, faggrupperapport utarbeidet av en arbeidsgruppe på oppdrag fra Politidirektoratet, datert 9. september 2019.
[6] NOU 2017:11, *Bedre Bistand. Bedre beredskap. Fremtidig organisering av politiets særorganer*.

og det kan ta mange måneder eller år før svar eller bistand kommer. Anmodninger til andre lands myndigheter og samarbeid med internasjonale tjenesteleverandører er utfordrende og tidkrevende.[7]

Politiet har i utgangspunktet ikke tilgang til brukerdata som er eldre enn 21 dager. Dette betyr at innhenting av IP-adresser som er brukt til pålogging hos utenlandske tjenesteleverandører, som Facebook og Google, må skje innen 21 dager.[8] Informasjon fra digitale tjenesteleverandører og sosiale medier som Microsoft, Google, Facebook og Snapchat kan være avgjørende som bevis i straffesaker. 21-dagersgrensen innebærer i praksis at saker hvor IP-adresser ikke sjekkes innen fristen på 21 dager, ofte henlegges. Dette er påpekt som et problem av politiet gjentatte ganger over de siste ti årene. Det etterlyses også et felles nasjonalt kontaktpunkt i politiet når det gjelder dialogen med internasjonale tjenesteleverandører. Ifølge Justis- og beredskapsdepartementet arbeides det nå med å endre lovgivningen på dette området, og et høringsnotat om lovendring er under utarbeidelse i samarbeid med Kommunal- og moderniseringsdepartementet.

Det er også andre forhold som bidrar til at etterforskning av saker med internasjonale forgreninger er vanskelig. Politidistriktene peker på mangel på etablerte rutiner for internasjonalt samarbeid, som fører til at sporsikring ikke skjer raskt nok. Det er begrenset med nasjonale støttedokumenter når det gjelder internasjonalt politisamarbeid eller rettslig samarbeid. Politidistrikter og Kripos er også enig i at KO:DE, politiets fagportal, bør forbedres og gjøres mer brukervennlig. Videre er det ulik kompetanse på dette feltet i politidistriktene. Dette bidrar til forskjeller mellom distriktene når det gjelder forfølging av spor og etterforskningskritt utenlands.

Utfordringene i det internasjonale politisamarbeidet bidrar til at kriminelle unnslipper rettsforfølging når de opererer på tvers av landegrenser. Disse svakhetene utnyttes av kriminelle nettverk. Slik det internasjonale samarbeidet er i dag, er forutsetningene for effektiv bekjempelse av kriminalitet med internasjonale forgreninger ikke til stede. Utfordringene på området har vært der over lang tid og har ikke vært tilstrekkelig vektlagt av politiet. Riksrevisjonen anser det som kritikkverdig at Justis- og beredskapsdepartementet og Politidirektoratet ikke har tatt tak i utfordringene på dette området på et tidligere tidspunkt.

2.2 Politiet prioriterer i liten grad etterforskning og oppklaring av datainnbrudd

Straffesaksbehandlingen skal bidra til redusert kriminalitet ved at straffbare forhold avdekkes og oppklares slik at skyldige effektivt kan straffeforfølges og ilegges adekvat reaksjon.[9] Riksadvokaten har siden 2005 sagt at alvorlig IKT-kriminalitet som datainnbrudd skal prioriteres, i tillegg til flere andre alvorlige kriminalitetstyper, blant annet seksualforbrytelser. For å se på hvordan politiet har fulgt opp disse kravene har Riksrevisjonen gjort beregninger av tidsbruk på saker[10] per straffebud og sett på oppklaringsandelen. Oppklaringsandel og beregningene av tidsbruk viser variasjon mellom de ulike kriminalitetsområdene.

Ren IKT-kriminalitet i form av alvorlige datainnbrudd inntreffer hyppigere og kan innebære blant annet store økonomiske tap. Gjennomsnittlig tidsbruk på etterforskning av ren IKT-kriminalitet, som omfatter straffebestemmelser Riksadvokaten har sagt skal prioriteres, er lav. Ren IKT-kriminalitet har i tillegg den laveste oppklaringsandelen av de sakstypene som er undersøkt. Enhetene for digitalt politiarbeid (DPA) bruker lite tid på etterforskning av teknologikrevende kriminalitet, deriblant ren IKT-kriminalitet.

Riksrevisjonen mener det er alvorlig at politiet i liten grad etterforsker og oppklarer ren IKT-kriminalitet som for eksempel datainnbrudd. Dette fører til at privatpersoner og virksomheter heller henvender seg til andre aktører enn politiet for bistand når de utsettes for slik kriminalitet.[11]

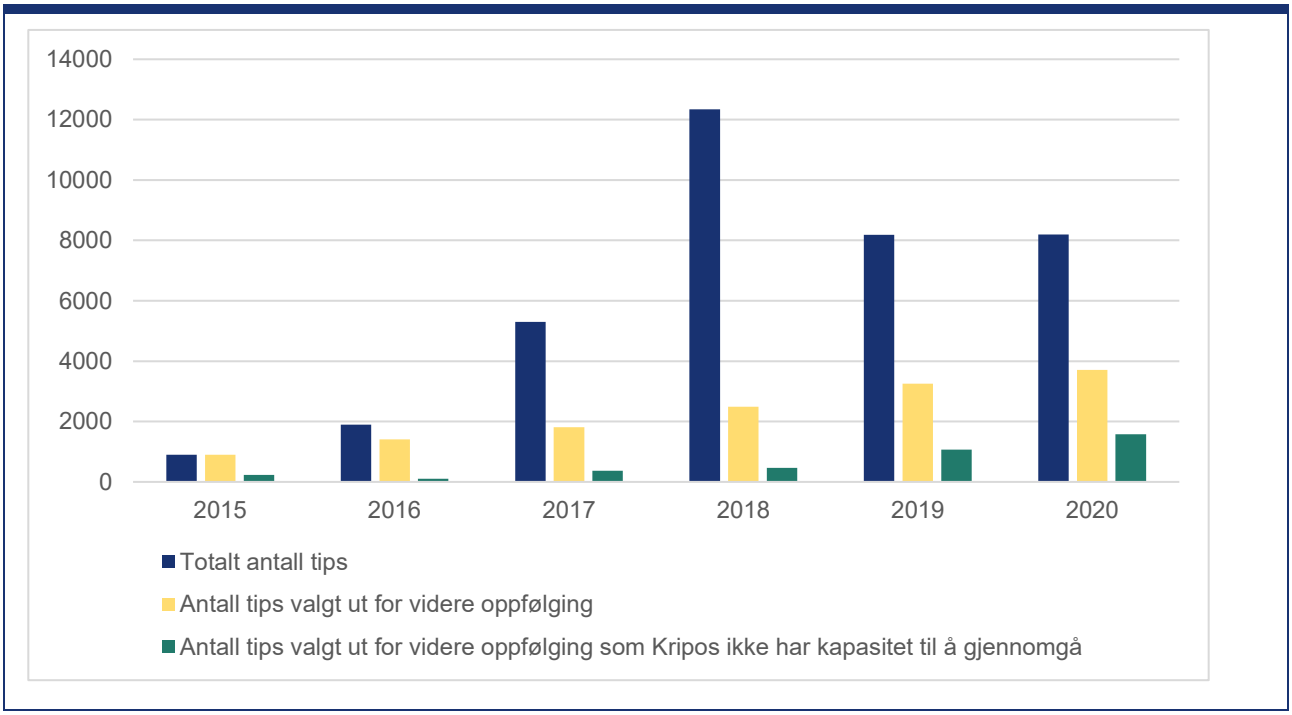
[7] NOU 2017:11, *Bedre Bistand. Bedre beredskap. Fremtidig organisering av politiets særorganer*.
[8] Politidirektoratet, (2017) *Trusler og utfordringer innen IKT-kriminalitet (2017)*.
[9] Riksadvokaten, (2019) *Mål- og prioriteringer for straffesaksbehandlingen i 2019 - politiet og statsadvokatene,* rundskriv 1/2019.
[10] Tidsbrukstallene er basert på estimater fra politiets kapasitetsundersøkelse.
[11] Politiets egen innbyggerundersøkelse viser at publikum har lav tillit til politiet på det dette saksområdet.

2.3 Tips og etterretning om internettrelaterte seksuelle overgrep øker og utfordrer politiets kapasitet

Riksadvokaten har over flere år pekt på at internettrelaterte seksuelle overgrep mot barn og unge er et økende samfunnsproblem. Etterforskning av alvorlig misbruk og overgrep mot barn på internett er derfor et høyt prioritert område.

Omfanget av tips og etterretning om internettrelaterte seksuelle overgrep har økt betydelig i perioden 2015–2020. Kripos mottar daglig tips og annen informasjon fra aktører i andre land om norske brukere som har lastet ned eller delt overgrepsmateriale. Bare i 2018 mottok Kripos mer enn 12 000 tips.[12] Figur 1 viser tips Kripos mottok om internettrelaterte seksuelle overgrep i perioden 2015–2020.

Figur 1 Tips til Kripos om internettrelaterte seksuelle overgrep i perioden 2015–2020



Kilde: Kripos

Av den totale mengden tips Kripos mottar velges det ut et antall tips for videre oppfølging (gule søyler). Dette er tips det det foreligger mistanke om straffbare forhold.[13] Figur 1 viser at Kripos opparbeider seg stadig økende restanser (grønne søyler) blant sakene som velges ut for videre oppfølging. Mer enn 40 prosent av sakene valgt ut for videre oppfølging ble ikke gjennomgått av kapasitetsmessige grunner i 2020. Politiet utsettes med andre ord for en økende mengde informasjon som det kan se ut til å ikke være kapasitet til å gjennomgå. Tilsvarende situasjon finnes i mange av politidistriktene som må prioritere etterforskningskapasiteten til de mest alvorlige sakene hvor det er mistanke om pågående overgrep.

Tidsbruken for etterforskning av internettrelaterte seksuelle overgrep er generelt høy og oppklaringsandelen er også høy. Politiet oppklarte 64 prosent av alle seksuallovbrudd i 2018 og 63 prosent i 2019. Samtidig er det kjent at mange av sakene anmeldes av politiet selv. Det er grunn til å anta at dette i hovedsak er alvorlige saker med høy sannsynlighet for oppklaring. Alvorlige seksuallovbrudd mot barn kan ikke

[12] Den store hovedvekten av tips Kripos mottar på dette området er internettrelaterte seksuelle overgrep. Mer enn 80 prosent kommer fra NCMEC. Det kan forekomme tips som dreier seg om andre straffbare forhold, som fysiske seksuelle overgrep og andre krenkelser (ulovlig bildedeling av voksne, seksuell utpressing av voksne m.m.). Dette gjelder spesielt i tipskanalen på tips.politiet.no og på e-post, der Kripos mottar tips direkte fra publikum. I tillegg kan det komme tips, spesielt fra NCMEC, som ikke er straffbare etter norsk lovgiving (etter vurdering av det vedlagte materialet) eller der det tipses om barn som har delt bilder/filmer av seg selv der de for eksempel tuller og viser seg nakne. Det kan også komme tips som dreier seg om upassende kommentarer på YouTube eller lignende, som heller ikke nødvendigvis er straffbart.

[13] I de aller fleste tipsene som blir prioritert for videre arbeid, er det mistanke om straffbare forhold, men Kripos kan også velge å gå videre med tips der barn har delt materiale av seg selv naken eller lignende. Da er det ikke nødvendigvis mistanke om et straffbart forhold, men Kripos ønsker likevel å følge opp tipset for å sikre at materialet legges i Interpols database for overgrepsmateriale (ICSE), og at barnet kan følges opp med en forebyggende samtale eller andre relevante tiltak avhengig av type materiale som er delt (for eksempel om det framstår utelukkende som spøk/morsomheter, eller om det er bekymringsverdige utsagn eller antydninger).

henlegges uten at det er gjennomført etterforskningskritt ifølge politidistriktene som er intervjuet. Omfanget av overgrep via internett øker, politiet avdekker flere ofre og saker, og ofre for seksuallovbrudd anmelder i økende grad forholdet til politiet.[14] Gitt den begrensede etterforskningskapasiteten må politiet prioritere de alvorligste sakene hvor sannsynligheten for positiv påtaleavgjørelse er størst. Tips og etterretning om lovbrudd fører derfor ikke alltid til opprettelse av sak på grunn av etterforskningsplikten og manglende etterforskningskapasitet. Oversikten over anmeldte forhold vil derfor heller ikke nødvendigvis gi et dekkende bilde av det faktiske antallet saker på dette området. Konsekvensen av dette er at mange saker ikke etterforskes og oppklares.

Politiet har prioritert etterforskning og oppklaring av internettrelaterte seksuelle overgrep over flere år. Likevel øker omfanget av saker. Politiets etterforskningskapasitet utfordres av store, omfattende nettovergrepssaker med mange fornærmede. Det er foreslått tiltak for å kunne tilskjære[15] saker med mange fornærmede, noe som vil kunne bidra til å avlaste politiet. Dette vil imidlertid ikke nødvendigvis løse utfordringene forbundet med manglende kontinuitet i etterforskningskapasiteten. Politiet har utfordringer med å rekruttere og beholde etterforskningskompetanse- og kapasitet fordi incentivene for politiutdannede til å velge seg en karrierevei innenfor dette området mangler. Dette bidrar til å forsterke utfordringene.

Riksrevisjonen mener det er alvorlig at politiet har utfordringer med å beholde etterforskningskompetanse og -kapasitet innenfor etterforskning av internettrelaterte seksuelle overgrep. Dette kan ha store konsekvenser når saksmengden øker og ofrene i sakene ofte er barn og unge.

2.4 Politiet mangler kapasitet til å møte utviklingen innenfor økonomisk IKT-kriminalitet

I det årlige mål- og prioriteringsskrivet framhever Riksadvokaten at alvorlig økonomisk kriminalitet skal prioriteres.

Økonomisk IKT-kriminalitet kan være kjærlighetssvindel via internett, investeringsbedragerier, svindel med bankkort, direktørsvindel, fakturabedragerier, osv. Fornærmede i hele landet utsettes daglig for denne typen svindel. Bedrageriene er ofte systematiske og avanserte med organiserte kriminelle som gjerningspersoner. Slik kriminalitet utgjør en stor andel av den samlede IKT-kriminaliteten. Digitaliseringen har gjort det enklere for kriminelle å svindle virksomheter og privatpersoner fra lokasjoner i andre land med liten oppdagelsesrisiko. Større næringslivsaktører rapporterer om en stor økning i økonomisk IKT-kriminalitet mot norske borgere og virksomheter.

Oppklaringsprosenten er lav både for IKT-kriminalitet og annen kriminalitet innenfor økonomiområdet. En sannsynlig årsak til dette er at flertallet av saker anses som mindre alvorlige (særlig bedragerier og ID-krenkelser) og henlegges. Selv om økonomisk kriminalitet ikke nødvendigvis er et prioritert område i de årlige prioriteringsskrivene, har riksadvokaten i intervju uttrykt bekymring over den høye henleggelsesprosenten innenfor denne formen for kriminalitet. Riksadvokaten har også trukket fram at politiet har både kapasitets- og kompetanseutfordringer innenfor IKT-kriminalitet og økonomisk kriminalitet.

Det mangler en nasjonal koordinering av innsatsen mot økonomisk IKT-kriminalitet. Manglende etterforskningskapasitet og manglende evne til å se sammenheng i anmeldte saker fører til henleggelser, også der hvor det er grunn til å tro at organisert kriminalitet står bak. Det er eksempler på at større sakskomplekser med organiserte kriminelle er etterforsket og oppklart av politidistriktene, for eksempel direktørsvindel og såkalt Olga-svindel.[16] Der politiet setter inn ressurser er det flere eksempler på at større, internasjonale kriminelle nettverk er avslørt og straffeforfulgt. Sakene som etterforskes er ofte ressurskrevende og politidistriktene må av hensyn til tid og ressurser nøye seg med å forsøke å stanse pengeoverføringer og uten å etterforske sakene til oppklaring og straffeforfølging. IKT-kriminalitet og økonomisk kriminalitet utfordres også av at sakene nedprioriteres til fordel for mer alvorlig kriminalitet, i form av seksuallovbrudd, drap og alvorlig narkotikakriminalitet.

Riksrevisjonen slutter seg til Riksadvokatens bekymring for den høye henleggelsesprosenten og politiets kapasitets- og kompetanseutfordringer innenfor IKT-kriminalitet og økonomisk kriminalitet.

---

[14] Politidirektoratet (2019) *STRASAK-rapporten - Anmeldt kriminalitet og politiets straffesaksbehandling*, rapport utgitt 28. februar 2020.
[15] Å tilskjære en sak handler om å avgrense bevisførsel og omfang til vesentlige forhold for å effektivisere straffesaksbehandlingen.
[16] Olga-svindel: Kriminelle tar kontakt med offer via telefon og utgir seg for å representere offerets bank. Bedrageriene foregår via internett og hadde i løpet av 2020 en aktiv periode.

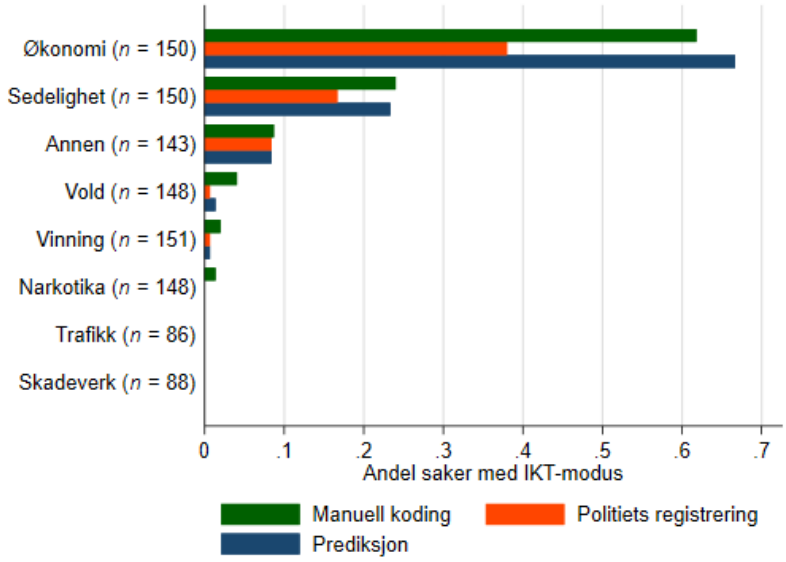
2.5 Politiet mangler oversikt over IKT-kriminalitet

Effektive forebyggende og kriminalitetsbekjempende tiltak forutsetter et kunnskapsbasert politiarbeid som vektlegger analyse og etterretning. Dette er vektlagt i politiets etterretningsdoktrine, i nærpolitireformen og i den siste politimeldingen. I Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet fra 2015 er det etterlyst kunnskaps- og analysegrunnlag, men det er fortsatt ikke på plass. Området IKT-kriminalitet lider av en uklar definisjon av hva IKT-kriminalitet er, begrenset oversikt over anmeldt IKT-kriminalitet, store mørketall og mangel på etterretning og systematisk kunnskapsbygging.

Uklarhet rundt begrepet IKT-kriminalitet har skapt utfordringer. Fenomenet omtales med ulike begreper som datakriminalitet, cyberkriminalitet, digital kriminalitet og IKT-relatert kriminalitet. Definisjonen av IKT-kriminalitet, slik den er brukt i flere sentrale rapporter og strategier er ikke operasjonalisert, og det åpner for skjønnsbasert fastsettelse av hva som skal regnes som IKT-kriminalitet. Dette fører til at begrepet tolkes forskjellig av distrikter, særorgan og nasjonale myndigheter. Uklarheten rundt definisjonen gjør det vanskelig å skaffe oversikt og IKT-kriminalitet sammenblandes med kriminalitet med elektroniske spor og digitalisering. Uklarheten kan ha medvirket til mangel på effektive strategier og tiltak på området.

For å utvikle et kunnskapsgrunnlag for trusselvurderinger på området, innførte Politidirektoratet moduskoder for IKT-relatert kriminalitet fra 2018. Disse har bidratt til å gi politiet en viss oversikt over forekomsten av IKT-kriminalitet, men de underestimerer omfanget. Riksrevisjonen har ved manuell gjennomgang og maskinlæring[17] identifisert anmeldt IKT-kriminalitet i 2018. Figur 2 viser andel IKT-kriminalitet innenfor ulike sakskategorier, basert på ulike metoder for registrering.

Figur 2 Andel IKT-kriminalitet per kriminalitetstype i et utvalg av 1072 saker – basert på manuell koding, politiets modusregistrering og maskinlæringsmodellen[18] (N = 1072)



Kilde: Riksrevisjonens stratifiserte utvalg av 1072 saker av anmeldte saker i 2018.

Figuren viser at omfanget av IKT-kriminalitet er betydelig høyere enn det man skulle anta kun ved å forholde seg til politiets IKT-moduskoding. Anslaget som er basert på den manuelle kodingen er i tillegg konservativt,

[17] Maskinlæring er en spesialisering innen kunstig intelligens hvor man bruker statistiske metoder for å la datamaskiner finne mønstre i store datamengder. Basert på vår manuelle klassifisering av IKT-kriminalitet for 1072 saker utviklet Riksrevisjonen en maskinlæringsmodell for å klassifisere alle anmeldte saker i 2018 som IKT-kriminalitet eller ikke. Maskinlæringsmodellen klassifiserte 21 500 saker av totalt 334 544 anmeldte saker i 2018 som IKT-kriminalitet. Resultatet fra maskinlæringsmodellen har deretter blitt brukt videre for å fastslå om IKT-kriminalitet etterforskes og oppklares.

[18] Kriminalitetstypen «Annen» omfatter lovbrudd som hensynsløs atferd, unnlatt å etterkomme pålegg (politiloven § 5), ordensforstyrrelser, brudd på kontaktforbud og ulovlig bevæpning på offentlig sted. Miljø og arbeidsmiljø er utelatt fordi det finnes svært få saker innenfor disse kategorien i utvalget.

hvilket kan bety at omfanget er høyere enn det som framgår av figuren. Av de manuelt gjennomgåtte sakene er den høyeste andelen IKT-kriminalitet innenfor økonomi (62 prosent), sedelighet (24 prosent) og kategorien annen (9 prosent).[19] Riksrevisjonens maskinlæringsmodell indikerer også at omfanget er større enn det politiet har grunnlag for å anslå basert på IKT-moduskoding.

En viktig forutsetning for å kunne etablere et kunnskapsgrunnlag for bekjempelse av IKT-kriminalitet er å ha oversikt over den IKT-kriminaliteten som anmeldes og ha innsikt i mørketallene. Mørketall på området er store som følge av at næringsliv, offentlige virksomheter og befolkningen i liten grad anmelder IKT-kriminalitet. Omfanget av mørketall varierer med kriminalitetstype. Innenfor internettrelaterte seksuelle overgrep har man kommet lenger i å kartlegge mørketallene, men også her er det store mørketall. På andre områder har politiet mindre oversikt over mørketall. Større næringslivsaktører har tilbudt seg å dele etterretningsinformasjon med politiet, men politiet mangler kapasitet og systemer for å motta denne typen kunnskap og har derfor avvist slike initiativ. Samlet bidrar manglende oversikt over både mørketall og den anmeldte IKT-kriminaliteten til å gjøre området uoversiktlig.

Etterretning og systematisk kunnskapsbygging som grunnlag for strategier og metodeutvikling har vært nedprioritert. Politiet utnytter i liten grad tilgjengelig kunnskap i egne saksbehandlingssystemer og fra andre kilder for å innrette etterforskningskapasiteten effektivt. Kripos har hatt ansvar for IKT-kriminalitet over lang tid, men NC3 oppgir at det ikke har vært kapasitet til å samle etterretning for ren IKT-kriminalitet og økonomisk IKT-kriminalitet. Innenfor internettrelaterte seksuelle overgrep finnes det etterretningskunnskap, men tilgjengelig kunnskap fra pågående saker og tipstjenester blir i for liten grad sammenstilt og analysert for å effektivisere innsatsen i politidistrikter og særorgan. Politidistriktene har heller ikke samlet etterretningsinformasjon eller systematisert tilgjengelig kunnskap på disse områdene. Mangel på etterretning har bidratt til at politiet mangler det informasjonsgrunnlaget som er nødvendig for å iverksette effektive, kriminalitetsbekjempende tiltak på området.

Riksrevisjonen mener det er kritikkverdig at politiet mangler oversikt over IKT-kriminaliteten. En uklar definisjon, manglende oversikt over anmeldt IKT-kriminalitet, mørketall og mangel på etterretning har ført til den manglende oversikten. Dette har bidratt til at politiet mangler det informasjonsgrunnlaget som er nødvendig for å iverksette effektive, kriminalitetsbekjempende tiltak på området. Over tid kan dette ha ført til at en nødvendig omstilling av organisasjonen tilpasset et endret kriminalitetsbilde ikke har skjedd i tilstrekkelig grad.

2.6 IKT-kriminalitet har i liten grad vært prioritert av Politidirektoratet og Justis- og beredskapsdepartementet

I henhold til *reglement for økonomistyring i staten* § 7 skal ansvarlige departementer fastsette mål, styringsparametere og krav til rapportering for underliggende virksomheter. Styring, oppfølging, kontroll og forvaltning må tilpasses virksomhetens egenart, risiko og vesentlighet, jf. § 4.

Riksrevisjonens undersøkelse viser at de øverste ansvarlige for politiets virksomhet, Justis- og beredskapsdepartementet og Politidirektoratet, har styringsinformasjon og beslutningsgrunnlag som tilsier at politiet trenger omstilling til endringer i kriminalitetsbildet. Likevel er det ikke tatt tilstrekkelig grep i styringen for å omstille politiet. Justis- og beredskapsdepartementet mener andre prioriteringer har vært viktigere de senere årene, men peker samtidig på at Politidirektoratet og politidirektøren har handlingsrom til å ta grep når de mener det er behov for det. Politidirektoratet mener de har synliggjort utfordringene for departementet, men at det ikke har vært rom for å prioritere dette området fordi andre hensyn har veid tyngre. Når departementet har vært kjent med utfordringene, og Politidirektoratet ikke har prioritert området, er det vår vurdering at Justis- og beredskapsdepartementet burde hatt en tettere og tydeligere styring, jf. kravet om at styringen skal tilpasses risiko og vesentlighet.

Riksadvokaten har årlig siden 2005 sagt at alvorlig IKT-kriminalitet skal prioriteres i mål- og prioriteringsskriv. Riksadvokaten mener IKT-kriminalitet ikke har fått den oppmerksomheten kriminalitetsutviklingen tilsier, fra departement og direktorat, politidistrikter og den høyere påtalemyndighet. Dette gjelder både de alvorlige lovbruddene på området, og de mindre alvorlige sakene. Få saker anmeldes, få anmeldte saker etterforskes, og det er et lavt antall positive påtaleavgjørelser.

[19] Med 95 prosent sikkerhet kan vi si at andelen IKT-kriminalitet i populasjonen av saker ligger mellom 53−70 prosent innen økonomisk kriminalitet, 17−32 prosent innen sedelighet og 4−14 prosent innen annen

Politiets primæroppgave i henhold til politilovens § 2 er å beskytte, forebygge, avdekke og stanse kriminell virksomhet. Digitaliseringen av samfunnet medfører at en større andel av kriminaliteten er IKT-kriminalitet. Når kriminell virksomhet i form av IKT-kriminalitet utgjør en økende trussel for norske borgere og virksomheter, er det rimelig å kunne forvente at nasjonale politimyndigheter sørger for at politiet møter utfordringene offensivt. Det er lite i denne undersøkelsen som tyder på at dette området er prioritert utover at politidistriktene og Kripos har brukt betydelig med etterforskningsressurser på internettrelaterte seksuelle overgrep. Men også her foreligger det anbefalinger om tiltak fra flere år tilbake som fortsatt ikke er iverksatt. Dette er tiltak som kunne effektivisert etterforskningen og kanskje bidratt til å avdekke flere lovbrudd.

Riksrevisjonen mener det er sterkt kritikkverdig at det ikke er tatt høyde for denne utviklingen i gjennomføringen av politireformen, og at noe av den oppbemanningen som har funnet sted for å nå målet om to politiårsverk per tusen innbyggere, ikke er avsatt til å møte de utfordringene IKT-kriminaliteten medfører. Riksrevisjonen er klar over at politiet står overfor betydelige prioriteringsutfordringer med mange og krevende oppgaver som skal følges opp samtidig. Konsekvensen av en manglende prioritering av dette området er imidlertid at alvorlig kriminalitet ikke etterforskes og oppklares, og at norske borgere og virksomheter mister tillit til politiet og lar være å anmelde lovbrudd.

3 Riksrevisjonens anbefalinger

Riksrevisjonen anbefaler Justis- og beredskapsdepartementet:

- å tydeliggjøre rutiner og ansvar for etterforskning av IKT-kriminalitet
- bedre kapasiteten innenfor etterforskning av IKT-kriminalitet og sikring av elektroniske spor
- å styrke den nasjonale samordningen av etterforskningen av IKT-kriminalitet mellom involverte politidistrikt og særorgan
- å styrke kunnskapsgrunnlaget om IKT-kriminalitet og framtidige utfordringer
- å styrke og etterforskningskompetansen innenfor IKT-kriminalitet for i større grad å kunne forebygge, avdekke og etterforske alvorlig kriminalitet på dette området
- å samordne innkjøp og administrasjon av programvare og utstyr som brukes av enheter for digitalt politiarbeid og særorgan
- å utvikle sentralt lagringsnett slik at det i større grad kan brukes for å analysere innsamlet bevismateriale og støtte etterforskningen

4 Departementets oppfølging

Statsråden viser til at Riksrevisjonens rapport er grundig, og at den dokumenterer at flere sider ved politiets arbeid med IKT-kriminalitet kan forbedres, noe regjeringen også gir uttrykk for i Meld. St. 29 (2019-2020) *Politimeldingen – et politi for fremtiden*. Statsråden viser videre til at Riksrevisjonens undersøkelse vil være et godt grunnlag for læring og videreutvikling på dette viktige området.

Statsråden understreker at det er sentralt at politi- og påtalemyndigheten styrker sin evne til å håndtere IKT-kriminalitet, ettersom kriminaliteten i økende grad foregår i det digitale rom. Dette er avgjørende for å forebygge, forhindre og stanse kriminalitet og for å kunne føre saker for retten. Politi- og påtalemyndighetens evne til å håndtere IKT-kriminalitet er ikke minst viktig for å bygge tillit i befolkningen. Statsråden viser for øvrig til at all kriminalitet foregår enten i det digitale rom eller med digitale virkemidler, og at IKT-kriminalitet ikke er én sakstype. Kriminelle innenfor alle kriminalitetstyper – fra overgrep til vinning – utnytter det digitale rom. For å håndtere denne utviklingen har politi- og påtalemyndighetens arbeid blitt betydelig utviklet, ifølge statsråden. Statsråden trekker fram politiets forebyggende rolle og dialog med barn og unge gjennom nettpatruljer og tilstedeværelse på sosiale medier. Dette er viktige tiltak i regjeringens satsing på å forebygge vold og overgrep mot barn og unge.

Justis- og beredskapsdepartementet vil i oppfølging av Riksrevisjonens anbefalinger særlig legge vekt på å styrke kunnskapsgrunnlaget og å utvikle regelverket, kompetanse og internasjonalt samarbeid. Departementet vil også prioritere å følge opp området i etatsstyringen av politiet.

Statsråden er enig i at det er behov for å styrke kunnskapsgrunnlaget om IKT-kriminalitet og peker på at statistikkutvikling, analyser og informasjonsdeling nasjonalt og internasjonalt vil bidra til dette. Det vil også bli utviklet en ny nasjonal trygghetsundersøkelse som vil gi et grunnlag for å utvikle en situasjonsbeskrivelse av kriminalitetsutviklingen som det kan oppnås enighet om. Selvrapportert opplevd kriminalitet vil ses i sammenheng med straffesaksstatistikken for å få et mer realistisk bilde av omfanget av kriminaliteten, også på det digitale området. Situasjonsbeskrivelsen vil gi viktig informasjon til befolkningen og for politikkutviklingen på området. Departementet vil også vurdere det forebyggende arbeidet, der andre offentlige og private virksomheter inngår i et viktig samspill med politiet.

Statsråden vil legge fram en strategi mot internettrelaterte overgrep mot barn i 2021. Strategien vil legge til rette for en tverrsektoriell innsats og samordning av relevante aktører. Et viktig mål vil være å styrke befolkningens evne til å håndtere nettrelatert risiko og forebygge overgrep.

Statsråden viser til flere pågående regelverksprosesser som vil understøtte politiets og påtalemyndighetens arbeid med IKT-kriminalitet. Blant forslagene som er sendt på høring, er et forslag om å innføre plikt for tilbydere av ekomtjenester til å lagre IP-adresser over tid, et forslag om å endre reglene om adgangen til å avgrense etterforsking og påtale i omfattende straffesaker, og et forslag om å ta inn en bestemmelse i straffeloven som rammer serieovergrep.

Når det gjelder internasjonalt samarbeid er statsråden bekymret for hindre i etterforskningen på tvers av landegrenser, men understreker at problemene ikke kan løses av Norge alene. Statsråden peker på utstrakt internasjonalt samarbeid gjennom ulike kanaler, deriblant arbeidet med en tilleggsprotokoll til Budapest-konvensjonen om IKT-kriminalitet.

Statsråden vil i tråd med prinsipper for god etatsstyring være varsom med å gi detaljerte instrukser i etatsstyringen av politiet på området.. Etaten vil i stedet få tydelige krav om hvilke resultater den skal levere. Politiet står daglig i en krevende situasjon hvor flere prioriterte saksområder skal løses med begrensede ressurser. Det innebærer at enkelte typer IKT-kriminalitet ikke gis tilstrekkelig prioritet. Politiet må også avveie hva som er hensiktsmessige systemer for håndtere bevis, og om dette skal løses gjennom sentralt utviklede løsninger eller om ressursene skal utnyttes til andre formål.

Statsråden viser til at Politidirektoratet allerede har igangsatt flere tiltak som vil bidra til å følge opp Riksrevisjonens anbefalinger. Direktoratet vil:

- tydeliggjøre grensesnitt mellom Kripos/Politiets nasjonale cyberkrimsenter (NC3) og politidistriktene (fristen for dette er 1. tertial 2021)
- styrke politiets kapasitet innenfor etterforskning av IKT-kriminalitet og sikring av elektroniske spor
- utarbeide en rutine for å styrke politiets håndtering og gjennomgang av digitale beslag for ulike brukergrupper, med særlig vekt på initialfasen
- styrke samordningen av innkjøp og administrasjon når det gjelder programvare og utstyr, i samarbeid med Nasjonalt cyberkrimsenter (NC3) og Politiets IKT-tjenester (PIT)
- Gjennomføre en pilotundersøkelse om sentral lagring av bevismateriale som skal danne grunnlag for nasjonal utrulling av et sentralt lagringsnett (Politiets IKT-tjenester, Oslo Politidistrikt og Vest Politidistrikt deltar)

Statsråden vil følge opp arbeidet i den løpende styringsdialogen, og vil gå i dialog med Riksadvokaten om behov for tiltak hos Den høyere påtalemyndighet. Statsråden minner samtidig om at politiet har gjennomført en omfattende reform i den perioden Riksrevisjonen har undersøkt (2016–2019). Arbeidet med reformen har vært svært ressurskrevende, men har ifølge statsråden hevet kvaliteten på politiets arbeid. Blant annet blir seksuallovbrudd tatt tak i på en bedre måte i dag. Statsråden vil i det forebyggende arbeidet framover legge stor vekt på dialog med andre aktører i samfunnet. Hele bredden av kriminelle handlinger i det digitale rom må håndteres, og de ulike aktørene må trekke i samme retning.

5 Riksrevisjonens sluttmerknad

Riksrevisjonen har ingen ytterligere merknader.

Saken sendes Stortinget.

Vedtatt i Riksrevisjonens møte 21. januar 2021

Per-Kristian Foss **Per Rune Henriksen**

Anne Tingelstad Wøien **Gunn Karin Gjul** **Arve Lønnum**

_____
Jens Gunvaldsen

Vedlegg

Vedlegg 1:

Riksrevisjonens brev til statsråden i Justis- og beredskapsdepartementet

Riksrevisjonen

Vår saksbehandler
Tom Næss 22241228
Vår dato
09.12.2020
Deres dato

Vår referanse
2019/00917-55
Deres referanse

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Att: Statsråd Monica Mæland

Oversendelse av Dokument 3:x om politiets innsats mot IKT-kriminalitet til Justis- og beredskapsdepartementet

Vedlagt oversendes utkast til Dokument 3:4 (2020–2021) *Riksrevisjonens undersøkelse om politiets innsats mot IKT-kriminalitet.*

Dokumentet er basert på rapport oversendt Justis- og beredskapsdepartementet ved vårt brev 19. oktober 2020, og på departementets svar 11. november 2020.

Statsråden bes redegjøre for hvordan departementet vil følge opp Riksrevisjonens konklusjoner og anbefalinger, og eventuelt om departementet er uenig med Riksrevisjonen.

Departementets oppfølging vil bli sammenfattet i det endelige dokumentet til Stortinget. Statsrådens svar vil i sin helhet bli vedlagt dokumentet. Det bes om at svaret oversendes som pdf lagret fra Word, ikke skannet som bilde, slik at innholdet kan gjøres tilgjengelig for alle i samsvar med krav til universell utforming.

Svarfrist: 8. januar 2021.

For riksrevisorkollegiet

Per-Kristian Foss
riksrevisor

Vedlegg:

Utkast til Dokument 3:4 (2020–2021) Riksrevisjonens undersøkelse av politiets innsats mot IKT-kriminalitet

Brevet er godkjent og ekspedert digitalt.

Vedlegg 2:

Statsrådens svar

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Justis- og beredskapsministeren

Riksrevisjonen
Postboks 6835 St Olavs plass

0130 OSLO

Deres ref.	Vår ref.	Dato
	19/167 - KMØ	08.01.2021

Statsrådens kommentarer til Dok. 3 - IKT-kriminalitet

1. BAKGRUNN

Jeg viser til Riksrevisjonens brev 9. desember 2020 hvor jeg blir bedt om å redegjøre for hvordan departementet vil følge opp Riksrevisjonens konklusjoner og anbefalinger i Dokument 3:4 (2020–2021) *Riksrevisjonens undersøkelse om politiets innsats mot IKT-kriminalitet.*

2. DEPARTEMENTETS KOMMENTARER

2.1 Innledning

Riksrevisjonens rapport er grundig og dokumenterer at det er flere sider ved politiets arbeid med IKT-kriminalitet som kan forbedres. Dette er i tråd med mine egne vurderinger, noe regjeringen bl.a. gir uttrykk for i Meld. St. 29 (2019-2020) *Politimeldingen – et politi for fremtiden*. Utviklingen på dette området går raskt, men jeg er glad Riksrevisjonen har notert seg at temaet er blitt løftet av Justis- og beredskapsdepartementet, både i politimeldingen og andre dokumenter.

Riksrevisjonens undersøkelse vil være et godt grunnlag for læring og videreutvikling på dette viktige området. Riksrevisjonen har gått metodisk inn i statistikkgrunnlaget innenfor anmeldt kriminalitet for å skape et bedre kunnskapsgrunnlag om kriminalitet som treffer det digitale området. Dette vil være et nyttig bidrag til vårt videre arbeid.

Jeg vil innledningsvis understreke at når kriminaliteten i økende grad foregår i det digitale rom, er det sentralt at også politiet og påtalemyndigheten styrker sin evne til å

håndtere kriminalitet som er rettet mot ikt-systemer, eller som foregår ved hjelp av ikt. En slik evne er sentral for å forebygge, forhindre, stanse og iretteføre kriminalitet, og for å bygge tillit i befolkningen. Det er også viktig å vise til at kriminalitet i det digitale rom, og med digitale virkemidler, er en integrert del av *alle* kriminalitetsområder. IKT-kriminalitet er ikke én sakstype, ettersom det digitale rom utnyttes og utfordres av kriminelle aktører innenfor alle kriminalitetstyper, fra overgrep til vinning. En slik tilnærming vil etter mitt syn bidra til en bedre forståelse for hvilke utfordringer vi står overfor.

Jeg vil samtidig vise til at det har skjedd en betydelig utvikling av politiets og påtalemyndighetens arbeid mot kriminalitet i det digitale rom og med digitale virkemidler. Jeg vil fremheve politiets forebyggende rolle og at politiet har etablert dialog med særlig barn og ungdom gjennom nettpatruljer og tilstedeværelse i sosiale medier. Dette er viktige tiltak i regjeringens satsing på å forebygge og avdekke vold og overgrep mot barn og unge, selv om det ligger utenfor hva denne rapporten har sett på.

I *Meld. St. 29 (2019-2020) Politimeldingen – et politi for fremtiden* har jeg orientert Stortinget om arbeidet med å bekjempe digital kriminalitet gjennom blant annet kunnskapsutvikling, etterretning, forebygging, metode- og regelverksutvikling, etterforskning, internasjonalt samarbeid og rekruttering.

2.2 Departementets oppfølging

I departementets oppfølging av Riksrevisjonens anbefalinger vil jeg særlig vektlegge å videreutvikle kunnskapsgrunnlaget, bidra med regelverksutvikling, rette oppmerksomhet mot kompetanse og internasjonalt samarbeid, samt følge opp dette området i departementets styring av politiet.

Når det gjelder *kunnskapsgrunnlaget* er jeg enig i at det er behov for mer kunnskap om kriminalitet i det digitale rom og kriminalitet som utføres med digitale virkemidler. En rekke tiltak vil bidra til dette, herunder statistikkutvikling, analyser og økt informasjonsdeling med ulike samarbeidspartnere nasjonalt og internasjonalt. Flere FoU-prosjekter er i gang og under planlegging.

Kunnskapsgrunnlaget vil også styrkes gjennom blant annet en ny nasjonal trygghetsundersøkelse som departementet nå vil gjennomføre. Undersøkelsen vil gi kunnskap som gjør at vi kan utvikle en mer omforent situasjonsbeskrivelse av kriminalitetsutviklingen i Norge, blant annet ved å bedre forstå hvor utsatt befolkningen er for ulike hovedgrupper av lovbrudd. Ved å se statistikk om straffesakskjeden i sammenheng med selvrapportert opplevd kriminalitet i befolkningen, vil vi få et mer realistisk bilde av omfang av kriminalitet, også på det digitale området. Dette vil være viktig informasjon for befolkningen generelt, men den vil være særlig viktig som et grunnlag for politikkutviklingen på feltet.

Departementet vil i tillegg vurdere politiets forebyggende rolle i det digitale rom, der andre offentlige og private virksomheter inngår i et viktig samspill med politiet. Justissektoren skal også videreutvikle og delta i internasjonalt kunnskapssamarbeid.

Jeg vil i 2021 legge fram en strategi mot internettrelaterte overgrep mot barn. Strategien skal legge grunnlag for en tverrsektoriell innsats, slik at politi, hjelpeapparat og øvrige aktører samordner sitt arbeid. Et viktig mål er at befolkningen gjennom råd og hjelp rustes til å håndtere nettrelatert risiko, og på den måten forebygger overgrep.

På *regelverksområdet* pågår det flere relevante prosesser som vil bidra til å understøtte politiets og påtalemyndighetens arbeid med IKT-kriminalitet. Sammen med distrikts- og digitaliseringsministeren har jeg sendt et forslag på høring om å innføre plikt for tilbydere av ekomtjenester til å lagre IP-adresser over tid. Videre har jeg sendt et forslag på høring om å endre reglene om adgangen til å avgrense etterforsking og påtale i omfattende straffesaker, og å innta en bestemmelse i straffeloven som rammer serieovergrep. Begge disse forslagene vil, dersom de blir vedtatt, gi politiet mer effektive virkemidler til å organisere sitt arbeid med IKT-kriminalitet på en hensiktsmessig måte.

Analysen av *internasjonalt samarbeid* gjelder i stor grad bekymringer knyttet til etterforskningshindre på tvers av grenser. Dette er en bekymring jeg deler, men som det ikke er mulig å løse for ett land alene. Nettopp derfor har politiet et utstrakt internasjonalt samarbeid, både globalt gjennom INTERPOL og FN, regionalt gjennom EU/Schengen, og med nære samarbeidsland som eksempelvis de nordiske landene. Europarådet med Budapestkonvensjonen (om IKT-kriminalitet) og arbeidet med en ny tilleggsprotokoll om etterforskingssamarbeid er særlig relevant her. Dette er arbeid vi vil følge opp og videreutvikle.

2.3 Oppfølging i politiet

God etatsstyring innebærer å trekke opp mål og rammer, og overlate de løpende administrative og faglige vurderingene til virksomhetsleder. Dersom det stilles detaljerte krav på ett område, vil dette kunne svekke virksomhetsleders mulighet til å ta ansvar for helheten. Departementet bør derfor være varsom med å gripe inn med detaljerte instrukser på enkeltområder, men i stedet stille tydelige krav om hvilke resultater virksomheten skal levere.

Politiet må håndtere en krevende balanse mellom de saker som skal prioriteres og mengden av ressurser som står til rådighet. Dette innebærer, som det også fremgår av rapporten, at enkelte typer IKT-kriminalitet ikke gis tilstrekkelig prioritet.

Politiet skal sørge for hensiktsmessige systemer for bevishåndtering. Hvorvidt dette betyr at det skal utvikles et sentralt lagringsnett for å analysere innsamlet bevismateriale, må baseres på politifaglige vurderinger og veies opp mot annen bruk av de samme ressursene.

Politidirektoratet (POD) har allerede igangsatt flere tiltak i politiet som vil bidra til å følge opp Riksrevisjonens anbefalinger i denne rapporten.

- Det pågår et arbeid med Kripos for å tydeliggjøre grensesnittet mellom Kripos/Politiets nasjonale cyberkrimsenter (NC3) og politidistriktene, med frist

1. tertial 2021, jf. anbefalingen om å tydeliggjøre rutiner og ansvar for etterforskning av IKT-kriminalitet.

- I tillegg har POD varslet at politiets kapasitet innen etterforskning av IKT-kriminalitet og sikring av elektroniske spor skal styrkes ytterligere. Det har i seg selv vært en svært viktig prioritering å etablere Enhet for digitalt politiarbeid (DPA) i samtlige politidistrikter.
- POD opplyser at det skal utarbeides en rutine for å styrke politiets håndtering og gjennomgang av digitale beslag for ulike brukergrupper, med fokus på initialfasen.
- POD er i gang med å styrke samordningen av innkjøp og administrasjon av programvare og utstyr i samarbeid med NC3 og Politiets IKT-tjenester (PIT).
- Når det gjelder anbefalingen om å utvikle sentralt lagringsnett slik at det i større grad kan brukes for å analysere innsamlet bevismateriale og støtte etterforskningen, opplyser POD at det pågår en pilotundersøkelse om sentral lagring som inkluderer PIT, Oslo Politidistrikt og Vest Politidistrikt. Funn fra denne undersøkelsen skal danne grunnlag for nasjonal utrulling.

POD vil arbeide videre med utgangspunkt i Riksrevisjonens anbefalinger. Jeg vil følge opp dette arbeidet i den løpende styringsdialogen, og jeg vil gå i dialog med Riksadvokaten om behov for tiltak hos Den høyere påtalemyndighet.

2.4 Avsluttende kommentar

Samtidig vil jeg minne om at vi i den perioden Riksrevisjonen har undersøkt (2016-2019), gjennomførte den mest omfattende reformen politi- og lensmannsetaten har vært igjennom. Arbeidet med å gjennomføre politireformen har vært svært ressurskrevende for store deler av organisasjonen, men har også bidratt til høyere kvalitet på politiets arbeid og at politiet har tatt tak i kriminalitet som tidligere ble for lavt prioritert – ikke minst seksuallovbrudd.

Jeg vil fremover også legge stor vekt på hvordan andre aktører i samfunnet kan bidra til den forebyggende innsatsen også på dette området. Hele bredden av kriminelle handlinger i det digitale rom må håndteres, ikke bare enkelte kriminalitetstyper, og de ulike aktørene på et sammensatt og krevende område må trekke i samme retning.

Med hilsen

Monica Mæland

Vedlegg 3:

Rapport: Politiets innsats mot kriminalitet ved bruk av IKT

Revisjonen er gjennomført som en forvaltningsrevisjon etter Lov om Riksrevisjonen § 9, tredje ledd og Instruks om Riksrevisjonens virksomhet § 9. Revisjonen er gjennomført i samsvar med Faglige retningslinjer for forvaltningsrevisjon i Riksrevisjonen og INTOSAIs standard for forvaltningsrevisjon (ISSAI 3000).

Innhold

Tabelloversikt

Figuroversikt

Faktaboksoversikt

Ordliste og forkortelser

BL	Forkortelse for BasisLøsning, politiets elektroniske straffesakssystem
Dataetterforsker	Brukes både om sivilt ansatte ingeniører og politiutdannede som har spesialisert seg på datatekniske undersøkelser.
Datatekniske undersøkelser	Tekniske operasjoner som er nødvendige for å innhente, sikre, gjenfinne og tilrettelegge for gjennomgang og analyse av elektroniske spor. Politiet kan imidlertid også innhente og benytte elektroniske spor uten særskilte datatekniske undersøkelser. Innhenting av informasjon fra åpne nettsider er et eksempel på dette.
Digitalt politiarbeid	Det arbeidet politiet gjør for å innhente, sikre og analysere digitale beslag, bevis og spor som er avgjørende for straffeforfølgningen av et lovbrudd.
Direktørsvindel	Direktørsvindel, også kalt CEO-svindel eller BEC-svindel (Business Email Compromise), innebærer at en ansatt med myndighet til å foreta betalinger lures til å betale en falsk faktura eller foreta en uautorisert overføring fra bedriftens konto. Svindelen utføres med hjelp av e-post og SMS fra personer som utgir seg for å representere ledelsen i bedriften.
Elektroniske bevis	Elektroniske spor som har relevans i iretteføringen av et kriminelt forhold.
Elektroniske spor	Elektronisk informasjon som er relevant for politiet. Dette kan være data som knytter seg til en hendelse, for eksempel tidspunktet for sending av en e-post, avsenderens og mottakerens IP-adresse med videre, eller innholdsdata, for eksempel teksten i en e-post.
IKT-moduskoder	Politiet innførte fra 2018 egne moduskoder i saksbehandlingssystemet BL for å kunne identifisere IKT-kriminalitetssaker. Eksempler er «Ved bruk av datasystem» og «Ved utnyttelse av feil/svakhet i digital autentiseringsløsning».
Indicia	Politiets etterretnings- og søkesystem
KO:DE	Politiets fagportal, administreres og vedlikeholdes av Kripos
Kripos	Kriminalpolitisentralen – nasjonal enhet for bekjempelse av organisert og annen alvorlig kriminalitet.
Modus operandi	Fra latin, betyr framgangsmåte/handlingsmønster for gjennomføring av en kriminell handling. I dagligtale brukes ofte bare modus.
NC3	Nasjonalt cyberkrimsenter – nasjonalt senter for forebygging, avdekking og bekjempelse av trusler og kriminalitet i det digitale rom. Utvikler metoder og gir bistand til politidistriktene samt etterforsker egne saker innen cyberkriminalitet. Del av Kripos.

PAL for STRASAK	Politiets analyse- og ledelsessystem
Phishing	Phishing, på norsk også kalt nettfiske, er en betegnelse på digital snoking eller «fisking» etter sensitiv informasjon, som passord eller kredittkortnummer. Uttrykket kommer fra engelsk fishing, der f-en er erstattet med «ph», som er vanlig hackersjargong.
PO	Politioperativt system – politiets elektroniske vaktjournal
PSV	Politimesterens styringsverktøy
Ransomware	Samme som løsepengevirus.
Sakstrekk	Rutiner eller regler for hvilken enhet som har ansvar for etterforskning av hvilke saker innen et politidistrikt. Fellesenhet for påtale har ansvaret for sakstrekksreglene.
SO	Seksuelle overgrep
Sikring av data	Omfatter gjennomføringen av beslag, teknisk framgangsmåte for ivaretakelse av data samt dokumentasjon av at sikringen er foretatt på korrekt måte. Én metode for slik sikring er speilkopiering.
Speilkopiering/speiling	Kopiering av et lagringsmedium (harddisk, mobiltelefon, minneplugg, osv.) elektronisk ved bruk av spesialtilpasset utstyr og programvare, slik at kopien skal være identisk med innholdet på lagringsmediet som ble kopiert.
Straffebud	Sammensatt av ordene straff og bud (forbud). Henviser til at straffebestemmelser inneholder et forbud og samtidig angivelse av straff.
STRASAK	Politiets elektroniske straffesaksjournal. Integrert mot BL og PAL for STRASAK
Vishing	Form for kriminell telefonsvindel eller stemmefisking der man bruker sosiale teknikker over telefon for å få tilgang til privat personlig og økonomisk informasjon.

1 Innledning

1.1 Bakgrunn

Norge er et rikt land og et av verdens mest digitaliserte land. Den teknologiske utviklingen åpner opp for nye kriminalitetsområder og effektiviserer utførelsen av tradisjonell kriminalitet. Private og offentlige oppgaver, funksjoner og verdier flyttes over på nett, og bidrar til at kriminalitet utført mot, eller ved hjelp av datasystemer, bli en stadig større del av det totale kriminalitetsbildet.[1]

I Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom* er IKT-kriminalitet omtalt som kriminalitet enten rettet mot datasystemer og/eller datanettverk, eller der sentrale elementer av handlingsforløpet utføres ved hjelp av datasystemer og/eller datanettverk. IKT-kriminalitet kan forekomme innen de fleste kriminalitetstyper, men forekommer hyppigere der IKT-verktøy og internett gjør det enklere å begå kriminell aktivitet. Dette gjelder for eksempel på sedelighetsområdet, hvor internettrelaterte seksuelle overgrep mot barn og unge opptar en stor del av politiets etterforskningskapasitet. Også innen økonomisk kriminalitet forekommer IKT-kriminalitet hyppig i form av for eksempel nettbedragerier og ID-tyverier. Medienes dekning viser også at alvorlig IKT-kriminalitet forekommer og får stor oppmerksomhet. Nettovergrepssaker med mange hundre fornærmede barn og unge, og datainnbrudd hos store næringslivsaktører som Hydro, er eksempler på saker som har skapt stor oppmerksomhet de siste årene.

IKT-kriminalitet er ingen ny utfordring for norsk politi. De siste 10–15 årene har IKT-kriminalitet vært gjenstand for flere utredninger, rapporter og strategier. I Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden* viser regjeringen til at mye arbeid er gjort, og at politiets arbeid med IKT-kriminalitet videreutvikles. Kriminalitetsbildet i det digitale rom endrer seg, og politiets arbeid med IKT-kriminalitet vil ifølge regjeringen kreve videre utvikling og oppfølging framover. Dette gjelder både kriminalitet som utøves i det digitale rom eller ved hjelp av IKT, og kriminalitet som utøves mot IKT-utstyr eller IKT-systemer.

Det har vært en nedgang på om lag 25 prosent i totalt antall anmeldelser de siste femten årene. Trenden er den samme i mange andre vestlige land. I henhold til Meld. St. 29 (2019–2020) skyldes nedgangen kraftig nedgang i eiendomstyverier og vinningslovbrudd. Oslo politidistrikt viser i en trendrapport til at digitaliseringen av sosial samhandling kan ha ført til at ofrene i mindre grad velger å politianmelde dem. I tillegg anses ofte digitale lovbrudd som resultat av manglende IKT-sikkerhet, og løses med styrking av sikkerheten snarere enn med rettsliggjøring. Omfanget av kriminalitet som ikke anmeldes, er imidlertid vanskelig å anslå.[2] Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) fra 2019 som gjennomføres av Næringslivets sikkerhetsråd, viser at aktører i næringslivet som rammes av IKT-kriminalitet, i liten grad anmelder sakene til politiet.[3]

I 2017 uttalte Sjef Kripos til media at norsk politi mangler kompetanse og kapasitet til å bekjempe IKT-kriminalitet.[4] I en rekke rapporter, utredninger og strategier de siste ti årene er det pekt på at politiet mangler oversikt, kompetanse, kapasitet og teknologi til å håndtere endringene i kriminalitetsbildet. Politidirektøren sa senest i årsrapporten for Politidirektoratet for 2019 at politiet har et stort behov for å utvikle bedre evne til å møte data- og IKT-relatert kriminalitet. Politidirektøren viser videre til at investeringsbehovet er betydelig, og at politiet i mindre grad vil kunne møte utfordringene uten særlig styrking.

1.2 Sentrale begrep i undersøkelsen

IKT-kriminalitet omtales med ulike begreper som cyberkriminalitet, datakriminalitet og IKT-relatert kriminalitet. I denne undersøkelsen brukes gjennomgående IKT-kriminalitet som begrep. IKT-kriminalitet kan forekomme innen de fleste kriminalitetstyper og kan ramme privatpersoner, private bedrifter og offentlige virksomheter.[5] IKT-kriminalitet er IKT-relaterte handlinger og hendelser som er kriminalisert etter norsk lov, og dekker i utgangspunktet to innganger til kriminalitet:[6]

---

[1] Politidirektoratet (2017) *Trusler og utfordringer innen IKT-kriminalitet*.
[2] Oslo politidistrikt (2018) *Trender i kriminalitet 2018–2021. Digitale og Globale utfordringer*.
[3] Næringslivets sikkerhetsråd (2019) *Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) 2019*.
[4] Politiforum (2017) *Norsk politi sakker akterut på nett*, artikkel i Politiforum 26. juni 2017.
[5] Politidirektoratet (2017) *Trusler og utfordringer innen IKT-kriminalitet (2017)*.
[6] Justis- og beredskapsdepartementet (2015) *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, utgitt av Justis- og beredskapsdepartementet 26. juni 2015.

- kriminalitet som retter seg mot datasystemer og teknologi. Eksempler kan være hackerangrep, datainnbrudd, dataangrep, sabotasje, industrispionasje, og blokkering av internett-tjenester. Det er dette som ofte omtales som «ren» datakriminalitet.
- kriminalitet der vesentlige/sentrale deler av den kriminelle handlingen og hendelsesforløpet skjer ved hjelp av datasystemer, utstyr eller nettverk. Straffbare forhold som tidligere ble begått i det fysiske rom skjer nå via internett. Eksempler kan være kjøp og salg av narkotika, deling av overgrepsmateriale, ID-tyverier, bedragerier og krenkelser av privatlivets fred.

Internettrelaterte seksuelle overgrep omtales med ulike begreper. Nettovergrep, nettrelaterte sedelighetslovbrudd og grooming er noen eksempler. Begrepene kan variere med hva slags seksuallovbrudd som gjennomføres. Kripos bruker begrepet internettrelaterte seksuelle overgrep for å tydeliggjøre at det er seksuelle overgrep det handler om. Internettrelaterte seksuelle overgrep brukes derfor om seksuallovbrudd som er IKT-kriminalitet.

Økonomisk IKT-kriminalitet er et begrep som betegner IKT-kriminalitet som gjennomføres med hensikt om å oppnå økonomisk gevinst. Eksempler kan være bedrageri, ID-tyveri osv.

«Ren» IKT-kriminalitet er et begrep som brukes om former for kriminalitet som er gjort mulig gjennom digitaliseringen av samfunnet med internett og digitale verktøy. Dette er kriminalitet rettet mot datasystemer og/eller datanettverk. Eksempler er datainnbrudd/hackerangrep, blokkering av internettjenester og dataskadeverk/virus.

1.3 Mål og problemstillinger

Målet med undersøkelsen er å vurdere om politi- og påtalemyndigheten har oversikt, etterforsker og oppklarer IKT-kriminalitet i samsvar med føringer gitt av Stortinget.

Problemstillinger:

1. Hvilken oversikt har politiet over IKT-kriminaliteten?
2. Etterforsker og oppklarer politi- og påtalemyndigheten IKT-kriminalitet?
   2.1. Blir IKT-kriminalitet etterforsket?
   2.2. Blir anmeldt IKT-kriminalitet oppklart?
3. Hvilke faktorer hindrer oppklaring av IKT-kriminalitet?
   3.1. Har politi- og påtalemyndigheten tilstrekkelig kapasitet og kompetanse til å avdekke og oppklare IKT-kriminalitet?
   3.2. Hvordan bidrar støttesystemer til å avdekke og oppklare IKT-kriminalitet?
   3.3. Sørger organiseringen og ansvarsdelingen i distriktene og nasjonalt for effektiv avdekking og oppklaring av IKT-kriminalitet?
   3.4. Bruker politiet internasjonalt samarbeid til å avdekke og oppklare IKT-kriminalitet?
4. Hvordan ivaretas styring og oppfølging av politiets innsats mot IKT-kriminalitet?
   4.1. Ivaretar Justis- og beredskapsdepartementet sitt overordnede ansvar for styring og oppfølging av arbeidet med IKT-kriminalitet?
   4.2. Ivaretar Politidirektoratet sitt ansvar for styring og oppfølging av IKT-kriminalitet?

For å illustrere hvordan politiet arbeider med IKT-kriminalitet, er innsatsen mot tre utvalgte kriminalitetstyper undersøkt:

- internettrelaterte seksuelle overgrep
- økonomisk IKT-kriminalitet i form av bedragerier og identitetskrenkelser
- «ren» IKT-kriminalitet i form av datainnbrudd og uberettiget befatning med tilgangsdata

Undersøkelsen omfatter i hovedsak politidistriktenes etterforskning av IKT-kriminalitet og behandler ikke det forebyggende arbeidet på området.

2 Metodisk tilnærming og gjennomføring

For å belyse problemstillingene er det gjennomført analyse av straffesaksstatistikk, en kartlegging av enhet for digitalt politiarbeid i politidistriktene, dokumentanalyse og intervjuer. Datainnsamlingen ble gjennomført i perioden fra mai 2019 til august 2020.

Undersøkelsesperioden er fra 2016 til og med 2019. Analysen av forekomst og oppklaring av IKT-kriminalitet blant anmeldte saker er gjennomført kun for 2018. For å vise utvikling i anmeldte, etterforskede og påtaleavgjorte saker er det gjort ulike statistiske sammenstillinger som hovedsakelig dekker perioden fra 2016 til 2019.

2.1 Analyse av straffesaksstatistikken

For å kunne analysere forekomst, etterforskning og oppklaring av IKT-kriminalitet var det nødvendig å identifisere IKT-kriminalitet i straffesaksstatistikken. Identifiseringen av IKT-kriminalitet tar utgangspunkt i året 2018 fordi det var dette året politiet innførte IKT-moduskoder. Fordi metodene for å identifisere IKT-kriminalitet var svært ressurskrevende, har det ikke vært mulig å gjennomføre tilsvarende analyser for 2019 og 2020.

Identifisering av IKT-kriminalitet ble gjort ved en manuell gjennomgang av et tilfeldig utvalg saker, og ved å utvikle en maskinlæringsmodell for å predikere IKT-kriminalitetsstatus for alle anmeldte saker fra 2018. Maskinlæringsmodellen bygger på den manuelle gjennomgangen. Resultatet fra maskinlæringsmodellen har deretter blitt brukt videre for å fastslå om IKT-kriminalitet etterforskes og oppklares.

2.1.1 Manuell gjennomgang av 1072 saker

For å få oversikt over andel av avgitte anmeldelser som kan kategoriseres som IKT-kriminalitet, ble anmeldelsesdokumenter for registrerte anmeldelser i 2018 innhentet maskinelt fra Politiets IKT-tjenester.

Nærmere om framgangsmåten:

1. Maskinell uthenting av anmeldelsesdokumenter fra alle registrerte saker i politiets saksbehandlingssystem BL i 2018. Totalt 296 345 saker og til sammen 396 917 anmeldelsesdokumenter.
2. Uttrekk av anmeldelsesdokumenter fra 1072 tilfeldig valgte saker, for manuell gjennomgang og klassifisering.
3. Manuell klassifisering av 1072 saker som IKT-kriminalitet og annen kriminalitet basert på anmeldelsesdokumentet i hver enkelt sak.

Utvalget av saker for manuell gjennomgang ble gjort med to mål for øye:

1. Å estimere andelen IKT-kriminalitet innenfor ulike sakskategorier[7]
2. Å muliggjøre utvikling og testing av en maskinlæringsmodell for å klassifisere alle saker i 2018 som enten IKT-kriminalitet eller *ikke* IKT-kriminalitet.

For å nå det første målet måtte hver sakskategori være tilstrekkelig representert i utvalget. Det ble løst ved å stratifisere utvalget etter sakskategorier. For å nå det andre målet var det nødvendig å ha et tilstrekkelig antall IKT-kriminalitetssaker i utvalget. Enkelte sakskategorier inneholder svært lite IKT-kriminalitet. Vi valgte derfor å trekke et *disproporsjonalt stratifisert utvalg* av 1072 saker. Utvalget inneholder færre saker fra sakskategoriene trafikk og skadeverk fordi det var grunnlag for å anta at forekomst av IKT-kriminalitet var lavere her[8] enn fra de øvrige seks sakskategoriene.[9] Tabell 1 viser hvordan sakene fordeler seg på sakskategorier i det endelige utvalget og i populasjonen av anmeldte saker.

[7] Anmeldte lovbrudd klassifiseres i sakskategorier eller kriminalitetstyper, for eksempel sedelighet, økonomi, trafikk, vold, osv.
[8] Intervjuer i forundersøkelsen og utforsking av statistikken tilsa at forekomsten var lav.
[9] Vi delte inn sakene i åtte sakskategorier (tabell 1). Kategoriseringen er lik politiets, med to justeringer: kategoriene «miljø» og «arbeidsmiljø» ble plassert under kategorien «annen» siden det er få saker i de kategoriene.

Tabell 1 Populasjon og utvalg av anmeldte saker i 2018 etter sakskategori

Sakskategori	Anmeldte saker 2018		Utvalg av saker	
	Antall	*Prosent*	*Antall*	*Prosent*
ANNEN	42626	13,4	150	14,0
NARKOTIKA	35309	11,1	148	13,8
SEDELIGHET	8406	2,6	150	14,0
SKADEVERK	16912	5,3	88	8,2
TRAFIKK	54107	17,0	86	8,0
VINNING	99447	31,2	150	14,0
VOLD	32716	10,3	150	14,0
ØKONOMI	29425	9,2	150	14,0
Totalt	**318948**	**100,0**	1072	100,0

Kilde: Politidirektoratet, Strasak. Delsaker er ekskludert, som i Politidirektoratets oversikt over anmeldte saker i den årlige Strasak-rapporten.

For hver av de 1072 sakene kodet vi manuelt hvorvidt saken hadde IKT-modus[10] i tråd med definisjonen av IKT-kriminalitet. Modus er en kode i BL som brukes for å beskrive metoden gjerningspersonen bruker for å begå lovbruddet. Et eksempel på dette er IKT-moduskodene «Ved bruk av datasystem» og «Ved utnyttelse av feil/svakhet i digital autentiseringsløsning». Vi tok utgangspunkt i anmeldelsesteksten, og kodet saken som *IKT-kriminalitet* ved klare indikasjoner på IKT-modus eller om IKT-modus var eneste tenkelig modus; *ikke IKT-kriminalitet* ved klare indikasjoner på annen modus enn IKT eller IKT-modus er utenkelig; og *vet ikke* hvis IKT-modus var tenkelig, men informasjonen ikke tillot en sikker slutning. Det var i tillegg avgjørende at lovbruddet og saksbeskrivelsen hadde sammenheng med omtale av modus i anmeldelsesdokumentet for å kodes som IKT-kriminalitet. Lovbrudd som skyldtes for eksempel fysisk vold, ville derfor ikke kunne klassifiseres som IKT-kriminalitet selv ved registrert IKT-modus.

For å sikre at regler for koding var likt forstått, gjennomførte vi en pilotering hvor fire personer kodet 30 tilfeldig utvalgte saker. Dette ble brukt som utgangspunkt for å få en omforent forståelse av kriteriene.

Deretter ble 100 saker fra utvalget gjennomgått av de samme fire personene, for å vurdere samsvar mellom koderne. For beregning av samsvarsrate mellom kodere, se vedlegg 1.

De resterende sakene ble delt i to, hvor to grupper på to personer kodet de samme sakene. Avvikende koding ble gjennomgått av de fire koderne i fellesskap for endelig koding av saken.

For seks sakstyper[11], hvorav tre forekom relativt hyppig, var det fortsatt vanskelig å endelig avgjøre kodingen. For å fastslå endelig status på disse sakene ble det innhentet synspunkter fra en referansegruppe bestående av fem dataetterforskere og fem politiadvokater fra politidistrikt og særorgan, se nærmere omtale i punkt 2.6. Det ble valgt å legge seg på en konservativ tolkning av tilbakemeldingene for ikke å overestimere andelen IKT-kriminalitet. For nærmere beskrivelse se vedlegg 1.

2.1.2 Prediksjon ved maskinlæring

For å klassifisere enkeltsaker ble det benyttet en maskinlæringsmodell. Målet med modellen var å klassifisere saker enten som IKT-kriminalitet, eller som ikke IKT-kriminalitet. Utgangspunktet for klassifiseringen var anmeldelsesteksten, samt korte tekstlige beskrivelser av saken (modussammendrag og saksbeskrivelse). I arbeidet med modellen, ble det først gjort en jobb for å identifisere og hente ut relevant tekst fra anmeldelsesdokumentet (text mining). Deretter ble teksten brutt opp i enkeltord og konvertert til

[10] Modus, forkortelse for *modus operandi* fra latin, er et annet ord for metoden gjerningsperson bruker for å begå lovbruddet.
[11] Sakstyper som forekom relativt hyppig, var ID-krenkelser/bedragerier hvor svindel med kort var involvert, svindel med elektronisk meldekort til NAV og narkotikaovertredelser (forsøk på import av narkotika via post).

numeriske variabler. Disse ble brukt som grunnlag for å trene en modell basert på kjent klasse (IKT-kriminalitet eller ikke IKT-kriminalitet). Det metodiske opplegget er detaljert beskrevet i vedlegg 2.

Det har ikke vært mulig å trekke ut anmeldelsesteksten for alle sakene i populasjonen. Dette skyldes blant annet at noen av tekstene ikke har vært mulig å lese maskinelt og konvertere til tekst.[12] For at det skal være et tekstlig grunnlag til så mange saker som mulig, er anmeldelsesteksten slått sammen med saksbeskrivelsen som er registrert i STRASAK, og modussammendraget.

Valg av variabler, kalt features, til modellen har stort betydning for hvor god den endelige modellen blir. Det er derfor gjort en større jobb med å velge ut relevante features. For å velge ut ord til modellen, er det benyttet en algoritme som heter TD-IDF. Denne algoritmen vekter ord etter hvor frekvente de er i det aktuelle dokumentet som analyseres, opp mot den inverse frekvensen av ordet i hele korpuset.[13] Denne tilnærmingen gjør at ord som er mer spesifikke for et dokument (for eksempel en anmeldelse av IKT-kriminalitet), og som samtidig er uvanlig i andre dokumenter, vektes høyere.

For å velge features, er det først trukket ut 150 ord med høyest TD-IDF-vekt fra IKT-krimsaker og 150 ord med høyest TD-IDF-vekt fra ikke-IKT-krimsaker. Ord som finnes i begge listene er så fjernet, og 70 ord med størst forskjell er så valgt fra de to listene. Det er gjort en ytterligere jobb med å opprette nye synonymer, slik at det totalt er 71 features som inngår i modellen. Alle features er vektet før bruk i modellen. Vektingen er gjennomført ved å ta den naturlige logaritmen til frekvensen av et ord i et dokument, relativt til det totale antallet ord i dokumentet.

Det er testet flere ulike algoritmer for å gjennomføre klassifiseringen av saker. I valg av endelig modell er både modellens effektivitet med tanke på å gi gode prediksjoner, og modellens forklarbarhet vurdert. Maskinlæringsmodeller kan deles inn i «hvit boks» og «sort boks»-modeller. Førstnevnte er mer transparent når det gjelder å forklare hvordan modellen har kommet fram til et gitt resultat, men samtidig er de gjerne mindre effektive enn «sort boks»-modeller. Hvis det er mulig å benytte en «hvit boks»-modell med omtrent lik effektivitet som det beste «sort boks»-alternativet, så vil denne være å foretrekke.

Effektiviteten til modellene ble vurdert med Matthews korrelasjonskoeffisient. Dette er et mål som tar høyde for at klassene som skal predikeres, ikke er jevnstore. I datamaterialet som ble benyttet som input til maskinlæringsmodellene, var omtrent 14 prosent av sakene klassifisert som IKT-krim. Denne skjevfordelingen medfører at vanlige mål for en modells effektivitet, kan gi misvisende svar.

Følgende modeller ble testet[14]:

- Naïve Bayes («hvit boks»-modell)
- Random Forest («sort boks»-modell)
- XGBoost («sort boks»-modell)
- Support Vector Machines (SVM) («sort boks»-modell)

For å teste modellenes effektivitet, ble modellene testet på «ukjente» data. Av totalt 1081[15] saker som var manuelt kodet og tilgjengelig for modellen, ble 944 saker brukt for å trening og test av modellen og 137 saker for å validere modellen. Da resultatene var sensitive for hvordan splitten i trenings- og testdata ble gjort, ble det benyttet 5-foldet kryssvalidering[16] hvor et gjennomsnitt av modellens MCC ble benyttet for å vurdere modellen.

Kjøringer av modellene viste at alle «sort boks»-modellene hadde bedre effektivitet, målt ved MCC, enn «hvit boks»-modellen som ble testet (Naïve Bayes). Denne modellen ble derfor utelukket. Av de gjenstående modellene, viste gjentatte kjøringer at SVM var den modellen som ga minst overtrening. Det vil si at det var minst forskjell i MCC mellom treningsdata og test- og valideringsdata. SVM ga en MCC på 0,82 (0,79), med

[12] Eksempler på dette er håndskrevne dokumenter. I noen tilfeller har det heller ikke vært mulig å identifisere hvilket dokument, eller del av dokumentet som inneholder anmeldelsesteksten.
[13] Et korpus er en samling av elektroniske tekster som gjengir forekomster av språklige ytringer. Korpuset representer språkbruk som har funnet sted i en naturlig sammenheng i skriftlig eller muntlig form. Et slikt materiale kan brukes som datagrunnlag for forskning innen empiriske grener av språkvitenskapelige fag, slik som korpuslingvistikk, og til utvikling av dataapplikasjoner innen språkteknologi. Kilde: Store norske leksikon.
[14] Det ble også testet en tilnærming ved bruk av nevrale nettverk og dyp læring. Denne tilnærmingen ble lagt bort da det ikke var mulig å få tilstrekkelig god kvalitet på det tekstlige grunnlaget for modellen til å få tilfredsstillende effektivitet.
[15] Tallet inkluderer de 1072 sakene som ble trukket tilfeldig og 30 saker som ble brukt i pilotering. Ikke alle sakene hadde tilgjengelig tekst, og totalen ble derfor 1081 saker.
[16] Datasettet blir delt inn i fem deler. For hver kjøring blir fire deler brukt til å trene modellen, mens en del blir holdt utenfor for å teste modellen. For hver kjøring blir modellens effektivitet på testdatasettet målt. Ved vurdering av modellen tas det et gjennomsnitt av effektiviteten på testdata fra alle kjøringene.

en presisjon[17] på 0,85 (0,84 på valideringsdata). Modellen er bedre til å klassifisere saker som ikke er IKT-kriminalitet korrekt, enn saker som er IKT-kriminalitet.[18]

Den ferdig trenede modellen ble kjørt på det fulle datasettet på 334 544 saker. Av disse har 286 726 saker anmeldelsestekst, 47 814 saker har kun saksbeskrivelse og modussammendrag, og for 4 saker er kun modussammendrag tilgjengelig.

2.1.3 Kvantitative analyser av etterforskning og oppklaring av IKT-kriminalitet

Det er gjennomført ulike kvantitative analyser av anmeldte saker, fordeling på kriminalitetstyper og statistikkgrupper osv. basert på uttrekk av anmeldte saker per år fra BL/STRASAK. Det er innhentet ulike uttrekk av data som benyttes i undersøkelsen. Fordi ny straffelov trådte i kraft 1. oktober 2015 og politireformen trådte i kraft 1. januar 2016, er det i all hovedsak tatt utgangspunkt i registrerte saker for perioden 2016–2019, men det er også benyttet data fra perioden 2014–2015 i enkelte figurer og tabeller.

For å belyse etterforskning av IKT-kriminalitet estimerer vi gjennomsnittlig tidsbruk på IKT-kriminalitetssaker og sammenligner tidsbruken i IKT-kriminalitetssaker med tidsbruk i andre saker innenfor samme statistikkgruppe. Data på tidsbruk i straffesaksbehandlingen kommer fra Politidirektoratets kapasitetsundersøkelse.[19,20] Kapasitetsundersøkelsen estimerte tidsbruk ved først å hente inn alle registrerte rutiner på straffesaker i BL for 2017 og 2018. For alle rutiner er gjennomsnittlig tidsbruk beregnet, samt for ikke-registrerte aktiviteter, gjennom workshoper med politimedarbeidere i åtte politidistrikter.[21] Til slutt koblet de tidsbruksestimatene på rutinedataene for hver straffesak.

Kapasitetsundersøkelsens data inneholder ikke tidsbruksestimater for hver enkelt sak; dataene finnes i 21 tabeller med rutiner (en per sakskategori), og 84 tabeller med tidsbruksestimater (en per politirolle innenfor hver sakskategori).

For dataene vi bruker i våre analyser, mangler det tidsbruksestimater for 6,5 prosent av sakene. Omtrent 90 prosent av sakene med manglende data er vedleggsaker. Hovedgrunnen til at disse sakene mangler data, er at politiet registrerer alle rutiner for mange vedleggsaker under den tilhørende hovedsaken.[22] For å unngå overestimering av gjennomsnittlig tidsbruk per sak gir vi derfor vedleggsakene med manglende data verdien 0. Dette påvirker fordelingen av *tidsbruk per sak*, men vil gi et mer rimelig estimat av *gjennomsnittlig tidsbruk innenfor kategorier*, siden gjennomsnittet ikke påvirkes av fordelingen av tidsbruk innenfor kategorier.

For å analysere oppklaring av IKT-kriminalitet er det innhentet uttrekk av data fra Politiets IKT-tjenester, som drifter og utvikler BL/STRASAK. Oppklaring av alle registrerte saker i 2018 er analysert ved å se på avgjørelser for disse sakene tatt fram til 26. august 2020. Vi bruker politiets egen operasjonalisering av oppklaring (se underkapittel 7.1).

Data om mistenkte gjerningspersoner og fornærmede er innhentet for 2018 og 2019. Data er brukt for å kontrollere for saker med mange fornærmede i analysen av oppklaring. Enkelte nettovergrepssaker kan generere flere hundre saker fordi det opprettes sak på hver enkelt fornærmet. Dette er i tråd med Riksadvokatens instrukser selv om det gir betydelige utslag på oppklarte saker når et større sakskompleks går til tiltalebeslutning.

2.2 Kartleggingsundersøkelse til enhet for digitalt politiarbeid

Det er gjennomført en kartleggingsundersøkelse til enhet for digitalt politiarbeid (DPA) i alle 12 politidistrikter. Undersøkelsen ble sendt til leder for DPA i hvert distrikt. Alle DPA-enhetene besvarte undersøkelsen.

Formålet med kartleggingen var å undersøke hvilke arbeidsoppgaver som gjennomføres, hvor mange ansatte og stillingshjemler som finnes, hvilken kompetanse og kapasitet DPA har, bruk av fagkontakter[23],

[17] Sanne positive delt på summen av sanne positive og falske positive.
[18] Modellen har en spesifisitet på 0,97 (0,99) og en sensitivitet på 0,85 (0,79).
[19] Kapasitet er her forstått som tilgjengelige ressurser, i form av årsverk, og tidsbruk på ulike oppgaver på straffesaksfeltet.
[20] Politidirektoratet, 2019 *Kapasitetsvurdering av etterforskningsområdet*.
[21] Etterforskningsledelse er et eksempel på en aktivitet som ikke registreres.
[22] Korrespondanse med forfatter av Kapasitetsundersøkelsen.
[23] Fagkontakter er politiansatte som har fått enkel opplæring i sikring og håndtering av elektroniske spor. Fagkontaktene gir råd om håndtering av elektroniske spor innen den enheten de arbeider, og er faglig kontaktledd mellom egen enhet og enhet for digitalt politiarbeid.

erfaring med støttesystemer og spørsmål som gjaldt rapportering, økonomi/budsjett og styring. Skjema ble testet ut på en av DPA-lederne før det ble sendt ut.

Kompetansekartleggingsdelen ble utviklet med bakgrunn i et skjema for kompetansekartlegging utviklet av DPA i Vest politidistrikt. Skjemaet er basert på *Rammer og retningslinjer for etablering av nye politidistrikter* og *Nasjonale rolledefinisjoner med kompetansekrav – etterforskningsløftet*, som begge er utgitt av Politidirektoratet.[24] DPA-lederne ble bedt om å vurdere sine ansattes kompetanse innen områder som forventes ivaretatt av enheten. Dette ble gjort for å unngå at hver enkelt vurderer egen kompetanse.

2.3 Intervjuer

Det er gjennomført intervjuer med Justis- og beredskapsdepartementet, Riksadvokaten, Politidirektoratet, Kripos og ØKOKRIM. Videre er følgende fem politidistrikter intervjuet i denne rekkefølgen: Møre og Romsdal, Oslo, Vest, Trøndelag og Nordland. Politidistriktene ble valgt med bakgrunn i størrelse (antall saker / antall ansatte) og geografisk beliggenhet. Hensikten med intervjuene var å få utdypet hvilke erfaringer politidistriktene har med etterforskning av IKT-kriminalitet. I alle politidistrikter ble det gjennomført intervjuer med fellesenheter med ansvar for etterforskning av seksuallovbrudd og økonomisk kriminalitet, og enhet for digitalt politiarbeid. Påtalemyndigheten var representert i ett eller flere intervjuer i hvert distrikt. I Oslo og Nordland er det også gjennomført intervjuer med enkelte geografiske driftsenheter. I Oslo politidistrikt ble det gjennomført egne møter med næringslivskontakt og stabsfunksjonen virksomhetsstyring.

Det ble utviklet en temaguide for gjennomføring av intervjuene som dekket følgende:

- oversikt over IKT-kriminalitet
- etterforskning av IKT-kriminalitet
- oppklaring av IKT-kriminalitet
- erfaring med hvordan følgende faktorer påvirker oppklaring av IKT-kriminalitetssaker:
  - kapasitet
  - kompetanse
  - støttesystemer
  - organisering
  - internasjonalt arbeid
- styring og oppfølging av digitalt politiarbeid og arbeid med IKT-kriminalitet
- etterforskning innen dybdeområdene ren IKT-kriminalitet, økonomisk IKT-kriminalitet og internettrelaterte seksuelle overgrep

I intervjuer med ansvarlige for økonomisk kriminalitet ble det tatt opp erfaringer med oversikt, etterforskning og oppklaring av IKT-kriminalitet. Tilsvarende ble gjort i møter med enheter med ansvar for seksuallovbrudd.

I tillegg til møtene med politiet er det gjennomført en rekke møter i revisjonen og forundersøkelsen med aktører som opplever IKT-kriminalitet eller har særskilt kunnskap om dette, blant andre Politihøgskolen, representanter fra flere større norske selskaper, NTNU Gjøvik, NorSIS og Næringslivets sikkerhetsråd. Representanter fra prosjektgruppen deltok også på en nasjonal fagkonferanse for digitalt politiarbeid hvor deltakere fra alle landets politidistrikter og særorgan deltok.

Det er også gjennomført flere intervjuer med Kripos, Politiets IKT-tjenester og Politidirektoratet underveis i undersøkelsen for å ta opp spørsmål som gjaldt straffesaksstatistikken, uttrekk av anmeldelsesdokumenter og andre forhold.

Møtene ble i all hovedsak avholdt fysisk. På grunn av covid-19-epidemien ble de siste intervjuene med Riksadvokaten, Justis- og beredskapsdepartementet, Politidirektoratet, Kripos og ØKOKRIM avholdt som digitale møter. Det ble skrevet referater fra intervjuene med de statlige aktørene, som ble verifisert av intervjuobjektene i etterkant. Det ble ikke produsert verifiserte referater fra møter med de andre aktørene.

[24] Politidirektoratet (2017) *Rammer og retningslinjer for etablering av nye politidistrikter*, Versjon 1.2, 16. juni 2017; Politidirektoratet (2018) Nasjonale rollebeskrivelser med kompetansekrav – etterforskningsfeltet. Versjon 0,7, utgitt i 2018.

2.4 Dokumentanalyse

Det er innhentet dokumentasjon fra Politidirektoratet, Kripos og politidistriktene som belyser arbeidet med IKT-kriminalitet i politiet. Fra Politidirektoratet er det innhentet rapporter, utredninger, styringsdokumentasjon, og annen relevant dokumentasjon. I forbindelse med intervjuer med politidistriktene ble det framlagt dokumenter som belyser de fem valgte distriktenes arbeid med IKT-kriminalitet, som for eksempel organisasjonskart, rutiner for saksfordeling, rapporter, statistikk på utvalgte områder osv.

En rekke sentrale rapporter og dokumenter er gjennomgått som beskriver status og utfordringer i arbeidet med IKT-kriminalitet i perioden 2012–2020. IKT-kriminalitet har vært gjenstand for flere utredninger og strategier.[25]

Sentrale styringsdokumenter er innhentet for perioden 2017–2020. Fra Justis- og beredskapsdepartementet er det innhentet tildelingsbrev. Fra Politidirektoratet er det innhentet ulike styringsdokumenter som disponeringsskriv, resultatavtaler, årsrapporter, strategier, virksomhetsplaner, handlingsplaner og andre relevante styringsdokumenter. Dokumentene er analysert for å forstå hvordan innsatsen mot IKT-kriminalitet styres av nasjonale myndigheter og i politidistriktene. I tillegg er rapporteringen fra politidistrikter, særorgan og Politidirektoratet gjennomgått for å analysere hvilke aktiviteter, resultater, utfordringer og annet som er rapportert oppover i styringskjeden.

Inspeksjonsrapporter fra regionale statsadvokatembeters inspeksjoner av etterforskningsinnsatsen i politidistrikter og særorgan fra undersøkelsesperioden er innhentet og gjennomgått.

2.5 Dybdestudier av tre kriminalitetstyper

På grunnlag av råd fra referansegruppen ble det gjort et utvalg på tre områder som er nærmere gjennomgått i revisjonen. IKT-kriminalitet forekommer hyppigere innen enkelte områder enn andre, og politiets innsats vil også variere fra ett saksområde til et annet. Å se på IKT-kriminalitet generelt ville derfor være vanskelig, uten å se nærmere på innsatsen innen utvalgte områder. I tillegg til den generelle gjennomgangen av oppfølgingen av IKT-kriminalitet ble det derfor valgt ut tre områder for dybdegjennomgang. Disse områdene er valgt med utgangspunkt i resultater fra politiets innføring av IKT-moduskoding og etter konferanse med medlemmer av referansegruppen.

- Internettrelaterte seksuelle overgrep: I Politidirektoratets årlige gjennomgang av straffesaksstatistikken for 2018 ble det pekt på en betydelig økning i internettrelaterte saker hvor fornærmede er under 16 år. Flere politidistrikter har hatt eller har for tiden store og omfattende saker på dette området. Det brukes betydelige etterforskningsressurser og teknisk kompetanse på disse sakene.
- Økonomisk IKT-kriminalitet (bedragerier og ID-tyverier): Innføringen av tvungen IKT-moduskoding ved registrering av anmeldelser viser at det er særlig mange lovbrudd av typen bedrageri og identitetskrenkelse med IKT-modus. Det var også kjent fra politiets innbyggerundersøkelse at nettsvindel og bedragerier er noe befolkningen er bekymret for å bli utsatt for.
- Ren IKT-kriminalitet: De nye kriminalitetsformene som er oppstått som følge av digitaliseringen av samfunnet var naturlig å ha med i undersøkelsen. Eksempler på kriminalitet på dette området kan være datainnbrudd/hacking og dataskadeverk. Sakene kjennetegnes ofte av at metodene er teknologisk avanserte og sakene kan være både kompetanse- og ressurskrevende å etterforske.

2.6 Referansegruppe

En referansegruppe er brukt underveis i undersøkelsen for å kvalitetssikre metoder, resultater av analyser og tolkning av fakta om politiets arbeid med IKT-kriminalitet. Referansegruppen besto av fem ledere/ansatte ved DPA i tre politidistrikter og Nasjonalt cyberkrimsenter (NC3) ved Kripos. I tillegg har fem representanter for påtalemyndigheten deltatt fra politidistrikter, Det nasjonale statsadvokatembetet for bekjempelse av organisert og annen alvorlig kriminalitet (NAST), Kripos og ØKOKRIM. I tillegg til de ti har leder for internrevisjonen og leder for analyseseksjonen i Politidirektoratet deltatt. Referansegruppen har gitt sine

[25] Politidirektoratet (2012) *Politiet i det digitale samfunnet: En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett*; Politidirektoratet, 2015 *Overordnet nasjonal strategi for bekjempelse av datakriminalitet - Datakrimstrategien;* Justis- og beredskapsdepartementet (2015) *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, utgitt av Justis- og beredskapsdepartementet 26. juni 2015; Politidirektoratet (2017) *Trusler og utfordringer innen IKT-kriminalitet*.

innspill gjennom tre møter og skriftlig per e-post med hensyn til kriterier for klassifisering av saker som IKT-kriminalitet. Bruken av en referansegruppe og tilgangen til fagpersonene som har deltatt, ble klarert med Justis- og beredskapsdepartementet, Politidirektoratet og respektive politimestre.

I det første møtet, før igangsetting av undersøkelsen, ga gruppen tilbakemelding på det analytiske opplegget for undersøkelsen, inkludert problemstillinger, metode, dybdeundersøkelser og opplegget for klassifisering av IKT-kriminalitet.

Det andre møtet ble gjennomført i begynnelsen av mars 2020. I møtet ble status for arbeid med undersøkelsen gjennomgått, og det ble gitt innspill til klassifiseringen av IKT-kriminalitet og til en spørreundersøkelse til ansatte i Enhet for digitalt politiarbeid. I etterkant ble denne spørreundersøkelsen gjort om til et kartleggingsskjema som ble sendt til ledere for DPA i mai 2020. Svarene fra DPA-lederne ble avgitt i andre halvdel av mai 2020.

Det tredje møtet ble gjennomført i august 2020. I dette møtet ble undersøkelsens resultater gjennomgått og diskutert. Dette ble gjort for å sikre en balansert gjengivelse av fakta i rapporten og tolkning av resultater av kvantitative og kvalitative analyser.

3 Revisjonskriterier

Revisjonskriteriene er utledet fra Stortingets behandling av relevante stortingsproposisjoner og -meldinger. Lover, bevilgningsreglementet og reglement for økonomistyring i staten er også kilder til revisjonskriterier. Det samme gjelder mål og prioriteringer og andre føringer som Riksadvokaten har foretatt med hjemmel i lov.

3.1 Overordnede føringer for oppfølgingen av IKT-kriminalitet

Regjeringens mål for straffesakskjeden er å redusere alvorlig kriminalitet, styrke forebyggingen av kriminalitet og en mer effektiv straffesakskjede.[26] Kampen mot alvorlig kriminalitet er i henhold til Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn* ett av åtte områder som er spesielt viktig for samfunnssikkerheten. I Innst. 326 S (2016–2017), jf. Meld. St. 10 (2016–2017) uttrykker justiskomiteen bekymring for at utviklingen og økningen av alvorlig kriminalitet i samfunnet kan bidra til at borgerne opplever større utrygghet.

I Innst. 306 S (2014–2015), jf. Prop. 61 LS (2014–2015) *Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen)* viser justiskomiteen til at politiet i dag møter et annet kriminalitetsbilde enn for kun noen få år siden, samtidig som det er høye krav i befolkningen til politiets arbeid. Komiteen mener dette øker behovet for at politiet er i stand til å være en organisasjon i stadig endring, med både personellmessige og teknologiske tilpasninger som gjør oppgaveløsningen gradvis bedre.

I henhold til Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom* er IKT-kriminalitet kriminalitet som enten er rettet mot datasystemer og/eller datanettverk, eller der sentrale elementer av handlingsforløpet utføres ved hjelp av datasystemer og/eller datanettverk. Regjeringen viser i Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar* til at IKT-kriminalitet øker i omfang. Ved behandlingen av Meld. St. 38 (2016–2017) viste justiskomiteen til at et sentralt område i arbeidet med å forebygge, avdekke og etterforske kriminalitet nå handler om IKT-kriminalitet.[27] Justiskomiteen registrerer at IKT-kriminalitet øker i omfang både når det gjelder kriminalitet rettet mot selve IKT-systemet og kriminelle handlinger begått ved hjelp av IKT. Justiskomiteen registrerer at Meld. St. 38 (2016–2017) dokumenterer et behov for å styrke politiets kompetanse og kapasitet på området. Justiskomiteen framhever i Innst. 306 S (2014–2015) at cyberkriminalitet kan omfatte blant annet terrorhandlinger, grooming, spredning av overgrepsbilder av barn og voksne, samt økonomisk kriminalitet i stort eller lite omfang. Komiteen mener det er avgjørende at politiet har tilstrekkelig kompetanse både lokalt og nasjonalt til å møte utfordringene fra IKT-kriminalitet.[28]

3.2 Riksadvokatens krav om prioritering av alvorlig IKT-kriminalitet

Riksadvokaten står for den faglige ledelsen av straffesaksbehandlingen og påtalemyndigheten, jf. straffeprosessloven § 56 andre ledd og påtaleinstruksens § 7-5 tredje ledd. Dette ansvaret operasjonaliseres årlig av Riksadvokaten gjennom et mål- og prioriteringsskriv til alle landets politidistrikt. Regjeringens mål for straffesakskjeden legges til grunn. Generelt er Riksadvokatens mål for straffesaksbehandlingen høy kvalitet, høy oppklaringsprosent, kort saksbehandlingstid og adekvat reaksjon. I rundskrivet bestemmer Riksadvokaten videre hvilke forbrytelsestyper som skal gis høyest prioritet. Det angis også hvilke saker som skal prioriteres ved iverksettelse og gjennomføring av etterforskning.

Riksadvokaten har i perioden 2012–2019 sagt at alvorlig IKT-kriminalitet skal prioriteres i tillegg til flere andre alvorlige kriminalitetstyper, blant annet alvorlige seksuallovbrudd.[29] For perioden 2016–2019 har Riksadvokaten understreket at misbruk og overgrep mot barn via internett skal prioriteres.[30] Og i perioden 2015–2019 har Riksadvokaten uttalt at politiets innsats mot alvorlige dataangrep, datainnbrudd og annen IKT-kriminalitet skal intensiveres. I samme periode anfører Riksadvokaten at IKT-kriminalitet er sterkt økende i omfang og kompleksitet, samtidig som relativt få lovbrudd straffeforfølges. Disse sakene krever høy

[26] Prop 1 S (2018-2019) for Justis- og beredskapsdepartementet.
[27] Innst. 187 S (2017–2018).
[28] Jf. Prop. 61 LS (2014-2015) *Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen)*.
[29] Riksadvokatens Mål- og prioriteringsskriv fra perioden 2012-2019.
[30] Riksadvokatens Mål- og prioriteringsskriv fra perioden 2015-2019.

teknologisk kompetanse. For å kunne avdekke flere alvorlige straffbare forhold er det nødvendig å legge til rette for et tillitsfullt samarbeid mellom politidistriktene, Kripos og næringslivet, ifølge Riksadvokaten. Fra 2016 har også Riksadvokaten sagt at internasjonalt samarbeid må vektlegges i oppfølgingen av IKT-kriminalitet. Innenfor rammen av de sentrale prioriteringene er det fortsatt rom for regionale og lokale prioriteringer i tråd med den faktiske kriminalitetssituasjonen i distriktet og forventet utvikling.[31]

Flertallet i justiskomiteen understreker i Innst. 306 S (2014–2015) betydningen av at Riksadvokatens prioriteringer på etterforskningsområdet etterleves, og at tilsynsrapporter fra statsadvokater blir fulgt opp. Flertallet i komiteen anser unnlatelser på disse feltene som svært alvorlige. Videre forventer flertallet at departementet etablerer rutiner for oppfølging av politidistrikt som har avvik, for eksempel ved at politimesteren og riksadvokatens representant sammen konkluderer med hva de konkrete oppfølgingspunktene skal være for å fjerne avviket.[32]

3.3 Krav til politi- og påtalemyndigheten

Politiets ansvar, mål og oppgaver er forankret i lov om politiet (politiloven). Politiet skal i henhold til politiloven § 1. *Ansvar og mål* være et ledd i samfunnets samlede innsats for å fremme og befeste borgeres rettssikkerhet, trygghet og alminnelige velferd gjennom forebyggende, håndhevende og hjelpende virksomhet.

3.3.1 Krav til etterforskning og oppklaring av straffesaker

Straffesaksbehandlingen skal bidra til redusert kriminalitet ved at straffbare forhold avdekkes og oppklares, slik at skyldige effektivt kan straffeforfølges og få en adekvat reaksjon. Straffesaksbehandlingen skal innrettes slik at den vekker tillit i samfunnet. Politimesteren og sjefen for enkelte av særorganene har ansvaret for straffesaksbehandlingen i sitt distrikt og ved sin enhet. I dette ligger et ansvar for at fastsatte mål fra Riksadvokaten nås.[33]

Et sentralt mål for politiets etterforskning er at den skal føre til oppklaring av sakene. De prioriterte sakene skal søkes oppklart så langt råd er, og ved knapphet på ressurser gis forrang. Særlig høye krav til oppklaring gjelder kriminalitet som vold og seksuallovbrudd.[34] Riksadvokaten viser til at kriminelle handlinger som inkluderer bruk av IKT-verktøy eller tjenester, eller som er direkte rettet mot teknologi, infrastruktur eller datasystemer, representerer utfordringer som setter på prøve tilliten og troverdigheten til politiets evne til effektiv kriminalitetsbekjempelse. Riksadvokaten pekte i 2019 på at oppklaring på dette området derfor er særlig viktig.[35]

I Innst. 306 S (2014–2015) understreker flertallet i justiskomiteen sterkt betydningen av god fagledelse innenfor etterforskningsfeltet. Dette skal ivareta både effektiv kriminalitetsbekjempelse og god rettssikkerhet. Flertallet vil spesielt peke på at det etableres arbeidsformer og rutiner som ivaretar klare ansvarsforhold og gode kontrollprosedyrer. Videre understreker flertallet at det er et lederansvar å legge til rette for systematisk læring og erfaringsutveksling innen etterforskningsfeltet.[36]

I henhold til Prop. 1 S (2018–2019) har en voksende andel av kriminaliteten et digitalt element. Regjeringen viser derfor til at politiet og påtalemyndigheten må ha nødvendig utstyr, kompetanse og kapasitet for å møte denne utviklingen. I Innst. 306 S (2014–2015) viser justiskomiteen til at riktig bruk av digitale verktøy er avgjørende for politiets evne og mulighet til å løse sitt samfunnsoppdrag. Arbeidsmetoder og arbeidsprosesser må sikre effektiv disponering av politiressursene og legge til rette for raskere etterforskning med høyere kvalitet. Tilstanden til politiets IKT-systemer er en avgjørende forutsetning for at dette skal kunne gjennomføres.

[31] Riksadvokaten, Rundskriv 1/2019 *Mål- og prioriteringer for straffesaksbehandlingen i 2019 – politiet og statsadvokatene.*
[32] Jf. Prop. 61 LS (2014–2015) *Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen).*
[33] Riksadvokaten, 2018 *Kvalitetskrav til straffesaksbehandlingen i politiet og ved statsadvokatembetene mv. (kvalitetsrundskrivet)*, Rundskriv 3/2018.
[34] Riksadvokaten, 2018 *Kvalitetskrav til straffesaksbehandlingen i politiet og ved statsadvokatembetene mv. (kvalitetsrundskrivet)*, Rundskriv 3/2018.
[35] Riksadvokaten, Rundskriv 1/2019 *Mål- og prioriteringer for straffesaksbehandlingen i 2019 – politiet og statsadvokatene.*
[36] Innst. 306 S (2014–2015), s. 20.

3.3.2 Krav til kompetanse

I henhold til Prop. 1 S (2018–2019) for Justis- og beredskapsdepartementet går den samlede kriminaliteten ned. Samtidig øker meldinger om vold og seksuallovbrudd, det blir flere krevende saker innen økonomisk kriminalitet og arbeidslivskriminalitet, og det er flere saker som retter seg mot IKT-system eller der IKT blir benyttet for å utføre kriminaliteten. Dette fører til større kompleksitet i sakene, gjør etterforskingen mer tid- og ressurskrevende og krever ny kompetanse i politiet. Dette tilsier ifølge regjeringen at politi og påtalemyndigheten må ha nødvendig utstyr, kompetanse og kapasitet til å møte denne utviklingen. I tillegg til den tradisjonelle politi- og påtalefaglige kompetansen er det behov for flere med særskilt kompetanse innenfor IKT.[37]

Justiskomiteen viser i Innst. 6 S (2018–2019), jf. Prop 1 S (2018–2019) til at kriminaliteten oftere rammer IKT-systemer, at den blir utført ved hjelp av digitale kanaler, og at straffesaker har digitale bevis. Komiteen er derfor opptatt av at politiet og påtalemyndigheten har kompetanse og kapasitet til å møte denne utviklingen. Komiteen viser til at politiets oppgave er å avdekke, etterforske og forebygge kriminalitet. Det er viktig at politiet utrustes med de nødvendige midler for at samfunnsoppdraget kan utføres på en forsvarlig måte.[38]

I Innst. 306 S (2014–2015) viser et flertall i justiskomiteen til at større og færre politidistrikt vil gi mer kompetanse til å etterforske og forebygge kriminalitet i hvert enkelt politidistrikt. Flertallet forventer at det med større politidistrikter blir etablert mer robuste fagmiljøer i hvert enkelt politidistrikt. Flertallet forventer at det etableres sikre effektive systemer for erfaringslæring i politiet gjennom IKT-verktøy og andre relevante mekanismer, slik at kunnskap deles mellom alle i organisasjonen som har nytte av den.[39] Det går videre fram av Innst. 306 S (2014–2015) at flertallet i justiskomiteen ber regjeringen følge opp flere konkrete punkter for å bedre kultur, ledelse og holdninger i politiet. Ett av disse er at det skal legges til rette for at også personer med annen utdannelse enn politihøgskolen skal kunne få videre- og etterutdanningstilbud ved Politihøgskolen.

Justiskomiteen viser i Innst. 6 S (2017–2018), jf. Prop. 1 S (2017–2018) for Justis- og beredskapsdepartementet til den viktige tilsynsoppgaven statsadvokatembetene har overfor politidistriktene, som innebærer å kontrollere om kvaliteten, oppnådde mål og prioriteringer er i tråd med føringene fra Stortinget og Riksadvokaten. Komiteen understreker at denne typen aktivitet ikke må bli nedprioritert. Komiteen peker videre på at det er en forutsetning for en effektiv straffesakskjede at den høyere påtalemakten har tilstrekkelige ressurser til rådighet. Sakene som de håndterer, øker i kompleksitet og omfang og krever store ressurser. Rask og korrekt saksbehandling er en viktig garanti for rettssikkerheten.

I henhold til Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar* er regjeringen opptatt av at digital kompetanse må bygges i alle politidistrikt slik at politiet har tilstrekkelige forutsetninger for å bekjempe IKT-kriminalitet. For at politiet skal ha nødvendig kompetanse, må politiutdanningen styrkes. Det gjelder både grunnutdanningen og etter- og videreutdanningen. Ansatte uten politiutdanning, inkludert spesialister med høy teknologisk spisskompetanse, bør få politifaglig tilleggsutdanning. Det vises videre til et dokumentert behov for å styrke politiets kompetanse og kapasitet på området. Det vises også til at politiets egen omverdensanalyse fra 2015 peker på at tempoet i teknologiutviklingen er så høyt at politiet hele tiden utfordres. Utviklingen stiller nye krav til politiets oppgaveløsning, i form av både mer spisset kompetanse og ny teknologi. Justiskomiteen mener etableringen av et senter er viktig i denne sammenhengen, jf. Innst.187 S (2017–2018). Komiteen stiller seg positiv til å opprette et nasjonalt senter for å forebygge og bekjempe IKT-kriminalitet (Cyber Crime Center).

3.3.3 Krav til organisering og ansvarsdeling

Justis- og beredskapsdepartementet har det overordnede ansvaret for styringen av politi- og lensmannsetaten, inkludert myndighet til å gi bestemmelser om organisatoriske spørsmål, blant annet samarbeidsordninger mellom distrikter, jf. politiloven § 16. Politidirektoratet har ansvaret for faglig ledelse, styring, oppfølging og utvikling av politidistriktene og særorganene i henhold til tildelingsbrev, med de

[37] Prop. 1 S (2018–2019) fra Justis- og beredskapsdepartementet.
[38] Innst. 6 S (2018–2019), s. 32.
[39] Innst. 306 S (2014–2015), s. 31.

begrensninger som følger av at den overordnede faglige ledelsen av straffesaksbehandlingen hører under den høyere påtalemyndighet.[40]

Ifølge Prop. 61 LS (2014–2015) skal påtalejurister og etterforskere samhandle for å få en mest mulig effektiv straffesaksbehandling. Videre skal politiet i større grad innhente spisskompetanse utenfor etaten, for eksempel innen økonomi og teknologi, til bruk i etterforskning.[41] Det framgår av Innst. 306 S (2014–2015) en forventning om at større organisatoriske enheter og en mer helhetlig organisering av politidistriktene vil styrke forutsetningene for systematisk kunnskapsutvikling og kunnskapsdeling. Justiskomiteen viser videre til at politiets oppgaver i stor grad må løses i samarbeid med andre aktører.[42]

3.3.4 Krav til internasjonalt samarbeid innen området IKT-kriminalitet

Lovbrudd har ofte internasjonale koblinger, gjennomføres av kriminelle nettverk som ikke følger landegrensene, hvilket i mange saker vil bety at et godt internasjonalt arbeid er en forutsetning for bekjempelse av grenseoverskridende kriminalitet.[43]

Europarådets konvensjon nr. 185 om datakriminalitet (Budapestkonvensjonen) ble ratifisert av Norge i 2006. Så langt har 39 europarådsmedlemsstater og seks ikke-medlemsstater, deriblant USA og Japan, sluttet seg til konvensjonen. Partene til Budapestkonvensjonen har forpliktet seg til gjensidig strafferettslig samarbeid i saker vedrørende datakriminalitet, herunder til å bistå hverandre med innhenting av elektroniske bevis for datakriminalitet.[44]

Utenriks- og forsvarskomiteen uttaler at komiteen ser med stor bekymring på den kapasitet offentlige og private aktører har til å foreta digitale angrep. Komiteen viser til at digitale trusler innebærer internett som kommunikasjonskanal koblet opp mot aktivisme, organisert kriminalitet og terrorvirksomhet og at det må rettes tiltak mot alle disse områdene. Komiteen viser videre til viktigheten av kontinuerlig involvering av næringslivet slik at man får innhentet innsikt, vurderinger og bekymringer fra næringslivet.[45]

3.4 Krav til styring og oppfølging

Stortinget stiller krav til forvaltningen om mål- og resultatstyring gjennom *bevilgningsreglementet*.[46] Kravene er videreført og konkretisert i *reglement for økonomistyring i staten* og *bestemmelser om økonomistyring i staten*.

I henhold til *reglement for økonomistyring i staten* § 4 skal virksomhetene fastsette mål og resultatkrav innenfor rammen av disponible ressurser og forutsetninger gitt av overordnet myndighet, og sikre at fastsatte mål og resultatkrav oppnås, at ressursbruken er effektiv, og at virksomheten drives i samsvar med gjeldende lover og regler. Virksomheten er ansvarlig for å sikre tilstrekkelig styringsinformasjon og forsvarlig beslutningsgrunnlag.

I henhold til *reglement for økonomistyring i staten* § 7 skal ansvarlige departementer fastsette mål, styringsparametere og krav til rapportering for underliggende virksomheter. Styring, oppfølging, kontroll og forvaltning må tilpasses virksomhetens egenart, risiko og vesentlighet, jf. § 4. Departementet har videre et overordnet ansvar for at styringsdialogen mellom departementet og virksomheten fungerer på en hensiktsmessig måte, og at virksomheten rapporterer relevant og pålitelig resultatinformasjon.[47] Alle virksomheter skal innenfor sitt ansvarsområde sikre at fastsatte mål og resultatkrav oppnås på en effektiv måte, og rapportere om måloppnåelse og resultater internt og til overordnet myndighet, jf. § 9.

[40] Innst. 306 S (2014–2015), s. 35.
[41] Prop. 61 LS (2014–2015), s. 27.
[42] Innst. 306 S (2014–2015), s. 31.
[43] Prop. 1 S (2018–2019) for Justis- og beredskapsdepartementet.
[44] Innst. O.nr. 53 (2004–2005), jf. Ot.prp.nr. 40 (2004–2005).
[45] Innst. 199 S (2015–2016), jf. Meld. St. 37 (2014–2015).
[46] Bevilgningsreglementet, vedtatt av Stortinget 26. mai 2005, jf. Innst.S.nr.187 (2004–2005).
[47] *Reglement for økonomistyring i staten* og *bestemmelser om økonomistyring i staten,* fastsatt 12. desember 2003 med endringer, senest 5. november 2015.

4 Politiets organisering og ansvarsdeling

Dette kapittelet gir en kortfattet oversikt over organisering og ansvarsdeling i justissektoren. Kun de mest sentrale funksjonene som er relevante for IKT-kriminalitet, er omtalt.

Politiets primæroppgave er å forebygge og håndheve brudd på lover som inneholder en straffetrussel, jf. lov om politiet av 1. oktober 1995 nr. 53 (politiloven). IKT-kriminalitet som omfattes av straffelovens bestemmelser skal på lik linje med annen kriminalitet forebygges, avdekkes og straffeforfølges. Politiets oppgaver og organisering følger for øvrig av politilovens bestemmelser.

4.1 Nasjonale myndigheter

Justis- og beredskapsdepartementet har det øverste ansvaret for politiets virksomhet i Norge og legger rammene med sine planer, mål og bevilgninger. Departementets ansvar består blant annet av å forvalte og følge opp regelverk, skaffe til veie og fordele ressurser og fastsette, kommunisere og kontrollere sentrale mål og resultatkrav.[48]

Politidirektoratet har ansvaret for styring, utvikling, oppfølging og faglig ledelse av politidistriktene og politiets særorganer. Direktoratet har ansvaret for å gjennomføre regjeringens politikk i henhold til tildelingsbrev, oppdragsbrev og andre oppdrag gitt i styringsdialogen.[49]

Påtalemyndigheten har et overordnet og faglig ansvar for straffesaksbehandlingen i politiet og påtalemyndigheten leder etterforskningen av straffesaker og tar påtalebeslutning for eksempel om henleggelse, tiltalebeslutning eller påtaleunnlatelse. Påtalemyndigheten er organisert på to nivåer:

- Den høyere påtalemyndighet omfatter alle statsadvokatregionene, Det nasjonale statsadvokatembetet, ØKOKRIM og Riksadvokatembetet. **Riksadvokaten** har det overordnede faglige ansvaret for straffesaksbehandlingen, er øverste leder for påtalemyndigheten, og fastsetter generelle retningslinjer for prioritering av etterforskning og gjennomføringen av straffesaker, blant annet ved årlige mål- og prioriteringsrundskriv.
- Den lokale påtalemyndigheten er politiadvokatene i politidistriktene. Politiadvokatene er ansvarlig for og leder etterforskingen av straffesaker, og avgjør hvilke bevis som skal innhentes. Politiadvokatene er direkte underlagt statsadvokatene i enkeltsaker.[50]

4.2 Politidistriktene

Politidistriktene har ansvaret for polititjenester, forvaltningsoppgaver og sivile rettspleieoppgaver innenfor et geografisk område. Politidistriktene er administrativt og faglig underlagt Politidirektoratet. I straffesaksbehandlingen er politidistriktene underlagt Riksadvokatens faglige ledelse.

Internt i politidistriktene vil det være fellesenheter eller geografiske driftsenheter som ivaretar etterforskningen. Anmeldt IKT-kriminalitet forekommer innen flere sakskategorier, men forekommer hyppigere innen seksuallovbrudd og økonomisk kriminalitet. I bekjempelsen av IKT-kriminalitet er det derfor etterforskningsressursene på disse områdene med bistand fra enhet for digitalt politiarbeid som ivaretar etterforskningen.

4.2.1 Enhet for digitalt politiarbeid (DPA)

I forbindelse med opprettelsen av nye politidistrikter introduserer Politidirektoratet i 2017 funksjonen digitalt politiarbeid (DPA) som nå er etablert i alle politidistrikter. Funksjonens formål er å ivareta en «bred, effektiv og hensiktsmessig bruk av digital informasjon og elektroniske spor i politiarbeidet».[51] Med politiarbeid menes både etterretning, operativt politiarbeid, forebygging, etterforskning og iretteføring (føre sak for retten). Gjennom utnyttelse av teknologi og elektroniske spor skal funksjonen sikre at flere straffesaker kan etterforskes raskt, og med god kvalitet i bevissikring, analyse og metodebruk.

---

[48] Justis- og beredskapsdepartementet (2018) *Hovedinstruks til politidirektøren*, fastsatt av Justis- og beredskapsdepartementet, 16. januar 2018.
[49] Justis- og beredskapsdepartementet (2018) *Hovedinstruks til politidirektøren*, fastsatt av Justis- og beredskapsdepartementet, 16. januar 2018.
[50] NOU 2017: 5 *En påtalemyndighet for fremtiden – påtaleanalysen.*
[51] Politidirektoratet (2017) *Rammer og retningslinjer for etablering av nye politidistrikter*, versjon 1.2, 16. juni 2017.

Funksjonens hovedoppgaver er å

- sørge for at riktig og relevant digital informasjon sikres, analyseres og benyttes i politiarbeidet til rett tid ved å gjøre mer arbeid med sikring og foreløpig gjennomgang av digital informasjon *på åstedet*
- tilrettelegge for at hele politiet kan være til stede på internett og utføre politiarbeid der, blant annet ved kriminalitetsforebyggende *nettpatruljer*
- sørge for at de ulike fagmiljøene, som etterforskning og kriminalitetsforebygging, har kompetanse til å forstå og utføre enklere sikring og gjennomgang av digital informasjon
- bistå med sikring og tilrettelegging av digital informasjon, utføre de mest anvendte datatekniske undersøkelser av nettverksdata og digitale enheter som ikke krever spesielle, kostbare laboratoriefunksjoner
- bistå med å forebygge og etterforske datakriminalitet der etterforskningen er svært teknologikrevende, og sørge for at disse håndteres med tilstrekkelig datateknisk kompetanse

Mandatet er bredt og omfatter i praksis omtrent all kriminalitet ettersom elektroniske spor nå forekommer innen nesten alle kriminalitetsområder. I tillegg skal det være en funksjon med spesialkompetanse innen teknologikrevende datakriminalitet som også skal drive forebyggende arbeid.

4.3 Særorgan

4.3.1 Kripos

Kripos er faglig og administrativt underlagt Politidirektoratet og påtalemessig underlagt Det nasjonale statsadvokatembete for bekjempelse av organisert og annen alvorlig kriminalitet (NAST). Bistand til politidistriktene innen taktisk og teknisk etterforskning og etterforskning av komplekse saker innenfor organisert og annen alvorlig kriminalitet er organets hovedoppgaver. Kripos er nasjonalt kompetansesenter innen sporsikring og bekjempelse av IKT-kriminalitet.[52] Kripos kan også etter anmodning fra politimester overta etterforskningsansvar, jf. påtaleinstruksens § 37-4, jf. § 37-3.[53] I henhold til påtaleinstruksens § 37-3 fjerde ledd kan Kripos etterforske alvorlig IKT-kriminalitet. Kripos utfører datakrimetterforskning, metodeutvikling innen datatekniske undersøkelser og bidrar internasjonalt med utvikling av arbeidsmetodikk samt maskinvare og programvare til bruk i kriminalitetsbekjempelse.[54]

4.3.2 Nasjonalt cyberkrimsenter (NC3)

NC3 er organisert som en avdeling i Kripos. NC3 ble offisielt åpnet 25. januar 2019 for å bekjempe IKT-kriminalitet gjennom etterretning, metodeutvikling, forebygging, etterforskning, sikring av digitale spor samt patruljering på nett. Senteret skal sikre en nasjonal, robust kapasitet på bekjempelse av IKT-kriminalitet og internettrelaterte seksuelle overgrep mot barn.[55]

4.3.3 ØKOKRIM

ØKOKRIM er faglig og administrativt underlagt Politidirektoratet, men er som eget statsadvokatembete påtalemessig underlagt Riksadvokaten. ØKOKRIM har ansvar for å etterforske og iretteføre særlig alvorlige eller prinsipielle lovovertredelser innen økonomisk kriminalitet og miljøkriminalitet. ØKOKRIM yter bistand til politidistriktene og bidrar til kompetansebygging og -deling. ØKOKRIM kan etterforske saker på eget initiativ eller overta saker fra lokal påtalemyndighet.[56] ØKOKRIM har med sitt ansvar en rekke saker der digitale verktøy og spor er en integrert og viktig del.[57] ØKOKRIM har ikke nedfelt i sitt mandat at de skal etterforske IKT-kriminalitet.

---

[52] NOU 2017:11 *Bedre bistand. Bedre beredskap.*
[53] Justis- og beredskapsdepartementet (2019) *Rapport fra arbeidsgruppe som har sett på saksflyt i saker som gjelder overgrep mot barn, oppnevnt av Justis- og beredskapsdepartementet 26. juli 2018*, rapport publisert 13. mars 2019.
[54] NOU 2017: 11 Bedre bistand. Bedre beredskap.
[55] Politiet (2019) *Nasjonalt cyberkrimsenter (NC3)*, aksessert 29. juni 2020.
[56] Straffeloven § 321 til § 326, § 332 til § 346 og kapittel 30 og 31, skatte- og avgiftslovgivningen, valutalovgivningen, prisloven, verdipapirhandelloven, forurensingsloven, arbeidsmiljøloven og andre lovovertredelser som naturlig faller inn under økonomisk kriminalitet og miljøkriminalitet, jf. påtaleinstruksen § 35-4.
[57] NOU 2017:11 *Bedre bistand. Bedre beredskap.*

4.3.4 Politihøgskolen

Politihøgskolen (PHS) er et særorgan underlagt Politidirektoratet og politiets utdanningsinstitusjon med hovedoppgaver knyttet til grunn- og masterutdanning, etter- og videreutdanning, samt forskning og formidling. PHS tilbyr utdanning innen digitalt politiarbeid og sikring av elektroniske spor, og utfører forskning på politiets håndtering av IKT-kriminalitet.

5 Politiets oversikt over IKT-kriminaliteten

Dette kapitlet omhandler politiets oversikt over IKT-kriminalitet. Dette belyses ved gjennomgang av hva slags statistikk politiet har på området, og problemer knyttet til denne statistikken. Denne oversikten blir deretter sammenstilt med Riksrevisjonens egne undersøkelser av forekomst av IKT-kriminalitet blant registrert kriminalitet. Uklarheter knyttet til begrepet og lovreguleringer blir også gjennomgått. Politiet mangler oversikt over den anmeldte IKT-kriminaliteten. Det er også store mørketall fordi IKT-kriminalitet anmeldes i mindre grad enn annen kriminalitet. I tillegg forstås begrepet IKT-kriminalitet forskjellig av ulike aktører.

5.1 Uklarhet rundt IKT-kriminalitetsbegrepet

Begrepet IKT-kriminalitet brukes i sentrale strategier og rapporter [58], men forstås ulikt. For eksempel settes det i noen sammenhenger likhetstegn mellom politiets kompetanse og kapasitet til sikring av elektroniske spor og politiets evne til bekjempelse av IKT-kriminalitet. Elektroniske spor, spor etterlatt på media som pc, mobil, internett, lagringsmedier osv. foreligger i mange saker uten at det betyr at det er begått IKT-kriminalitet. Definisjonen av IKT-kriminalitet (se kapittel 1.2) inneholder en presisering av at IKT-elementet må være «vesentlig/sentralt». En mobiltelefon kan for eksempel utgjøre et sporsted som er sentralt for å knytte en mistenkt til et straffbart forhold, men om selve den straffbare handlingen er utført i det fysiske rom, er ikke lovbruddet IKT-kriminalitet slik vi forstår definisjonen som ligger til grunn for denne undersøkelsen. Hva som gjør IKT-elementet vesentlig/sentralt, må operasjonaliseres og vil være åpent for grader av skjønn. Dette fører til at IKT-kriminalitetsbegrepet ikke forstås likt av alle aktører.

Det forekommer også at digitalisering av politiet og politiets tjenester trekkes inn i diskusjonen om IKT-kriminalitet. Et eksempel er politiets tilstedeværelse på internett, som framstilles som et sentralt tiltak for bekjempelse av IKT-kriminalitet, men som i like stor grad handler om digitalisering av politiets tjenester og å være til stede for publikum der de er.[59]

Uklarheten rundt bruken av begrepet kommenteres av Politidirektoratet i et innspill til revidering av Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet i 2018[60]:

> *«Strategien tar utgangspunkt i en definisjon av IKT-kriminalitet […] benyttet i en rekke dokumenter og sammenhenger. […] I tillegg omhandler strategien «elektroniske spor» og «politiarbeid på internett» […]. Med dette utgangspunkt favner strategien svært vidt. […], noe som gjør at strategien i praksis mangler avgrensning. […] På denne måten har man i realiteten åpnet for at alt som har med «data» og «digitalisering» å gjøre kan være eller er omfattet av strategien.»*[61]

Den samme uklarheten er også omtalt i en prosjektrapport fra et pilotprosjekt bestilt av Justis- og beredskapsdepartementet i Oslo politidistrikt om digitalt politiarbeid:

> *«I løpet av prosjektperioden har det blitt gjennomført samtaler med en rekke tjenestepersoner både i Politiet, Kripos, Politidirektoratet og Justisdepartementet. Ofte når datakriminalitet og eventuelle tiltak skal diskuteres så stopper diskusjonen allerede i startgropen, da man ikke finner en god definisjon som er praktisk mulig for politiet å benytte. […] Prosjektgruppens inntrykk er at mangelen på gode definisjoner vanskeliggjør arbeidet med relevante tiltak. Avhengig av hvem du diskuterer med kan mye og lite defineres som datakriminalitet.»*[62]

I Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden,* kapittel 7 *Digital kriminalitet får nye utslag og må møtes på nye måter* brukes fem forskjellige begrep. I hovedsak brukes digital kriminalitet og IKT-kriminalitet, men «kriminalitet som begås i eller gjennom internett», «internettrelatert kriminalitet» og

---

[58] Politidirektoratet (2012) *Politiet i det digitale samfunnet – en arbeidsgrupperapport om: elektroniske spor; IKT-kriminalitet. og politiarbeid på Internett;* Politidirektoratet, 2015 *Datakrimstrategien*; Justis- og beredskapsdepartementet, 2015 *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, lansert 26. juni 2015.

[59] Politidirektoratet (2018), *Innspill til revisjon - strategi for bekjempelse av IKT-kriminalitet.* 15. januar 2018. Unntatt offentligheten. Innspillet om revidering av strategien er sendt som representantens innspill som del av deltakelsen i referansegruppen, og representerer nødvendigvis ikke Politidirektoratets endelige eller helhetlige syn på saken.

[60] Justis- og beredskapsdepartementet (2015) *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, utgitt av Justis- og beredskapsdepartementet 26. juni 2015.

[61] Politidirektoratet (2018) *Innspill til revisjon - strategi for bekjempelse av IKT-kriminalitet.* 15. januar 2018. Unntatt offentligheten. Innspillet om revidering av strategien er sendtsendt som representantens innspill som del av deltakelsen i referansegruppen, og representerer nødvendigvis ikke Politidirektoratets endelige eller helhetlige syn på saken.

[62] Oslo politidistrikt (2018) *Digitalt politiarbeid – Anbefaling.* Rapport til Politidirektoratet datert 23. januar 2018.

«cyberkriminalitet» er også uttrykk som brukes. I meldingen omtales IKT-kriminalitet som «kriminalitet som utøves i det digitale rom eller ved hjelp av IKT, og kriminalitet som utøves mot IKT-utstyr eller IKT-systemer».[63] Denne definisjonen ligger nær definisjonen som er brukt i andre sentrale rapporter og strategier på området, men er videre ved at presisering av at IKT-elementet må være sentralt/vesentlig er tatt bort.

Nasjonale aktørers synspunkter på begrepsbruk

Nasjonalt cyberkrimsenter (NC3) ved Kripos uttaler i intervju at begrepet IKT-kriminalitet har skapt utfordringer ettersom ulike aktører legger ulik forståelse i hva begrepet omfatter. Dette kan ha medført at politiet har vært sene med å omstille seg til endringer i kriminalitetsutviklingen. Den manglende klarheten rundt hva definisjonen omfatter, gjør begrepet krevende å forholde seg til, gir rom for individuell fortolkning og kan skape forventninger, ifølge NC3. Det kan være at IKT-kriminalitet betraktes som noe «andre» skal ta seg av, for eksempel NC3, mens det faktisk griper inn i store deler av politiets arbeid. Denne uklarheten rundt begrepet og subjektive oppfatninger av hva det innebærer, gjør det også vanskelig for NC3 å avklare hvilke resultater som faktisk forventes av enheten. Forventingene oppleves som bredere enn det NC3 faktisk vil kunne klare å levere. Ifølge NC3 selv har de kapasitet til å ta 1–2 saker i året, i tillegg til å bistå distriktene. De har ikke kapasitet til å ta alle alvorlige IKT-krimsaker. NC3 har derfor vurdert nye begrep for å beskrive teknologisk avansert IKT-kriminalitet. Blant annet et begrep som handler om hvor teknologiintensiv en kriminell handling er.

En betydelig andel av IKT-kriminaliteten er bedragerier, ID-tyverier og annen økonomisk kriminalitet. I særorganutredningen[64] vises det til at **ØKOKRIM** ved saksinntak legger vekt på teknologiaspektet, men ser ikke økonomisk IKT-kriminalitet som et eget uavhengig kriminalitetsområde. ØKOKRIM sier i intervju at de vurderer det slik at de aller fleste forbrytelser i dag i større eller mindre grad blir foretatt ved hjelp av IKT-verktøy, og mener IKT-komponenten ikke er det mest vesentlige. Det er andre dimensjoner ved kriminaliteten som er viktigere. Et overgrep er et overgrep om det begås på nett eller fysisk, og det samme gjelder for bedragerier, ifølge ØKOKRIM.

Riksadvokaten viser i intervju til at utgangspunktet for begrepsdefinisjonen, som også er tatt inn i Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet, kommer fra Konvensjonen om datakriminalitet[65], som trådte i kraft i Norge i 2006. Definisjonen er ikke endret siden 2001, og Riksadvokaten påpeker at dette er uheldig da det har vært en stor teknologisk utvikling siden 2001. Utfordringen med definisjonen er at den også inkluderer lovbrudd som bruker IKT-verktøy til å gjennomføre den straffbare handlingen. Det medfører at definisjonen omfatter en stadig større andel av den begåtte kriminaliteten ettersom den teknologiske utviklingen fortsetter. Riksadvokaten påpeker at det skaper utfordringer for både å kunne måle og styre innsatsen på området. Prioritering av saker og fordeling av ressurser blir vanskelig når begrepet ikke er tilstrekkelig avgrenset. Det er forskjell mellom IKT-kriminalitet som retter seg mot IKT-systemer og datasystemer, og kriminalitet som bruker IKT-verktøy i gjennomføringen. Det stilles også andre kompetansekrav til å etterforske den «rene» IKT-kriminaliteten, som angrep på datasystemer, sammenlignet med kriminalitet hvor IKT kun er brukt i gjennomføringen av andre straffbare handlinger. Riksadvokaten trekker fram at det kan stilles spørsmål om hvor godt egnet begrepsdefinisjonen er for å gjøre gode og riktige analyser av kriminalitetsbekjempelsen på området gitt at den omfatter alle lovbrudd hvor det er benyttet IKT-verktøy.

Politidirektoratet viser i intervju til at de allerede tidlig i grunnlagsdokumenter og i strategien har vært tydelig på tredelingen av IKT-kriminalitetsbegrepet («ren» IKT-krim, kriminalitet hvor IKT er modus, og elektroniske spor). POD mener at uklarhet i begrepet ikke har vært en utfordring når det gjelder å vite hvor man skal identifisere utfordringer, eller vite hvor man trenger mer ressurser og kompetanse. De sier det likevel kan ha vært en utfordring når det gjelder kommunikasjon, både internt og eksternt.

Justis- og beredskapsdepartementet bekrefter at begrepet IKT-kriminalitet ikke oppfattes som et enkelt og operativt begrep. IKT-kriminalitet er ifølge departementet et vanskelig begrep å bruke fordi alle oppfatter forskjellige ting med det og fordi IKT-kriminaliteten har utviklet seg.

[63] Meld. St. 29 (2019–2020)2021) *Politimeldingen – et politi for fremtiden.*?
[64] NOU 2017: 11 *Bedre bistand. Bedre beredskap.*
[65] *Konvensjonen om datakriminalitet – ETS nr. 185* underskrevet i Budapest november 2001.

5.2 Lovregulering av IKT-kriminalitet

Straffelovgivningen angir hva som er ulovlig, hvilke straffer som skal brukes, og hvor strenge de skal være. Selv om det er kun et fåtall lovbestemmelser i straffeloven som eksplisitt nevner data eller datasystem, vil flere lovbestemmelser kunne komme til anvendelse i saker hvor det er snakk om IKT-kriminalitet.

Digitaliseringen av samfunnet, hvor stadig flere offentlige og private oppgaver og funksjoner flyttes på nett, har også ført til at lovbestemmelser som før gjaldt tjenester og funksjoner som ikke hadde noe med datasystemer å gjøre, også kan få anvendelse på hendelser i det digitale rom. **Internettrelaterte seksuelle overgrep** vil som regel handle om brudd med en eller flere straffebestemmelser i *Kapittel 26. Seksuallovbrudd* i straffeloven. Flere av straffebestemmelsene kan brukes både om IKT-kriminalitet og kriminalitet begått i det fysiske rom, for eksempel *§ 299. Voldtekt av barn under 14 år.* Tilsvarende gjelder **økonomisk IKT-kriminalitet**, for eksempel et bedrageri begått via internett – ofte omtalt som nettbedrageri. Her anvendes bedrageribestemmelsene i *Kapittel 30. Bedrageri, skattesvik og lignende økonomisk kriminalitet.* I dag begås mange bedragerier via internett, men det er ikke uvanlig med fysiske bedragerier i forbindelse med for eksempel omsetning av varer og tjenester.

Innen **ren IKT-kriminalitet** er et eksempel *§ 192 Anslag mot infrastruktur* med en strafferamme på inntil 10 år. Denne bestemmelsen kan anvendes ved både fysiske og digitale angrep. NSM rapporterer at det jevnlig skjer målrettede anslag mot kritisk infrastruktur i form av IKT-kriminalitet.[66] Selv om det like gjerne kan være kriminelle som stater som begår handlingen vil det ikke synes i straffesaksstatistikken fordi kun en meget liten andel av anslagene blir anmeldt. Tilsvarende gjelder skadeverksbestemmelsene, for eksempel *§ 352 Grovt skadeverk,* med en strafferamme på inntil 15 år. Et eksempel på grovt skadeverk er tjenestenektangrep.[67] Flertallet av saker innen straffebestemmelsen grovt skadeverk er likevel fysiske skadeverk på bygninger, kjøretøy eller andre fysiske objekter.

Særskilte straffebestemmelser for IKT-kriminalitet ble utredet i midten av 2000-årene. Arbeidet resulterte i et *kapittel 21. Vern av informasjon og informasjonsutveksling*.[68] Kapitlet består av straffebestemmelser som kan anvendes på IKT-kriminalitet:

- § 201 Uberettiget befatning med tilgangsdata, dataprogram mv.: bot eller fengsel inntil 1 år
- § 202 Identitetskrenkelse: bot eller fengsel inntil 2 år
- § 203 Uberettiget tilgang til fjernsynssignaler mv.: bot eller fengsel inntil 1 år, og inntil 3 år ved grov overtredelse
- § 204 Innbrudd i datasystem: bot eller fengsel inntil 2 år
- § 205 Krenkelse av retten til privat kommunikasjon: bot eller fengsel inntil 2 år
- § 206 Fare for driftshindring: bot eller fengsel inntil 2 år
- § 207 Krenkelse av forretningshemmelighet: bot eller fengsel inntil 2 år
- § 208 Rettsstridig tilegnelse av forretningshemmelighet: bot eller fengsel inntil 1 år

I tillegg til ovennevnte ble det tatt inn enkeltbestemmelser som omhandler IKT-kriminalitet. Blant annet:

- §§ 351–353 Skadeverk: fra bot til fengsel inntil 15 år, avhengig av forholdets grovhet
- §§ 371–374 Bedrageri: fra bot til fengsel inntil 6 år, avhengig av forholdets grovhet[69]

Få av lovbestemmelsene som er gjengitt ovenfor, omhandler kun IKT-kriminalitet, med unntak av straffebudene som nevner dette eksplisitt: *§ 201 Uberettiget befatning med tilgangsdata, dataprogram mv., § 204 Innbrudd i datasystem (datainnbrudd), § 351 Skadeverk, annet ledd (dataskadeverk) § 371 bokstav b (databedrageri).* For statistikkformål vil det likevel kun være *§ 201 Uberettiget befatning med tilgangsdata mv.* og *§ 204 Innbrudd i datasystem* som vil kunne brukes for å få oversikt over IKT-kriminalitet fordi det ikke skilles ikke mellom fysiske og digitale bedragerier (§ 371) og skadeverk (§ 351) i kriminalitetsstatistikken.

---

[66] Se for eksempel NSM (2019) *Helhetlig digitalt risikobilde 2019*.
[67] Aftenposten (2012) *Dømt for nettangrep mot DNB, bloggtjenester og PST*, artikkel publisert 14.12.2013 [24.3.2020].
[68] Politidirektoratet (2015) *Overordnet nasjonal strategi for bekjempelse av datakriminalitet (Datakrimstrategien)*, Utredning fra gruppe oppnevnt av Politidirektoratet etter oppdrag fra Justis- og beredskapsdepartementet i brev av 1. november 2013. Avgitt Justis- og beredskapsdepartementet 12. mai 2015.
[69] Her skilles det på bedrageri § 371 (a) og § 371 (b) databedrageri. Databedrageri er definert slik: «bruker uriktig eller ufullstendig opplysning, endrer data eller datasystem, disponerer over et kredittkort eller debetkort som tilhører en annen, eller på annen måte uberettiget påvirker resultatet av en automatisert databehandling, og derved volder tap eller fare for tap for noen.» Straffes med inntil 2 år. Grovt bedrageri straffes med fengsel inntil 6 år. Mindre bedrageri straffes med bot. Dette straffebudet omfatter følgelig også §§ 372 Grovt bedrageri og 373 Mindre bedrageri.

Bestemmelsene i kapittel 21 i den nye straffeloven[70] har lave strafferammer på mellom 1 og 3 år. Strafferammen bestemmes ut fra lovbruddets alvor eller straffeverdighet. Det vil si hvor straffeverdig eller alvorlig det er å angripe den beskyttelsesverdige interessen, og i hvor stor grad lovovertrederen er å bebreide.[71] Justis- og beredskapsdepartementet sier i intervju at å heve strafferammen utelukkende for å sikre at slike saker gis høyere prioritet, uten at en heving av strafferammen kan begrunnes i de nevnte hensyn, vil bryte med retningslinjene som straffeloven bygger på. Departementet presiserer imidlertid at det ikke avviser at en eventuell gjennomgang kan vise at en økning i strafferammen kan begrunnes i slike hensyn.

Riksadvokaten og enkelte av politidistriktene viser i intervju til at lave strafferammer kan være en utfordring for prioritering av saker i saksmottak. Sakene kan bli lavere prioritert og henlagt før etterforskingsskritt tas. I intervju oppgir Riksadvokaten at strafferammene på området i større grad kan være tilpasset «hackere på gutterommet» enn IKT-kriminalitet utført av organiserte kriminelle. Det er imidlertid mulig å kombinere straffebud. På den måten kan strafferammene bli høye nok til at saken ansees som alvorlig. Kompetanse i saksmottaket, for eksempel hos Felles straffesaksinntak (FSI), til å vurdere alvoret i en datainnbruddssak uavhengig av strafferammen, kan derfor være avgjørende.

Riksadvokaten uttaler i intervju at de anser at det er en fare for at alvorlighetsdimensjonen ved saker er blitt for statisk, og at det vurderes om det bør være to tilnærminger til alvorlighetsbegrepet: strafferammen i den enkelte sak og omfanget av fenomenet under ett. Dersom IKT-kriminaliteten eller annen kriminalitet blir en massekriminalitet med sterke uheldige innvirkninger på samfunnet, kan det anses som alvorlig kriminalitet. Utfordringen med å ha et slikt makroperspektiv innenfor IKT-kriminaliteten er mangelen på informasjon om omfanget (statistikk og etterretning). Riksadvokaten er beredt til å gi styringssignaler om dette, men det forutsetter tilstrekkelig etterretning og informasjon om omfanget.

Faktaboks 1 Forklaring av begreper i straffebestemmelser som omhandler IKT-kriminalitet i kapittel 21 i straffeloven

Uberettiget befatning med tilgangsdata, dataprogram, mv.: Handler i hovedsak om misbruk av passord, adgangskoder eller krypteringsnøkler for å skaffe seg tilgang til et datasystem. Typisk vil dette handle om kriminalitet som har som formål å finne informasjon, for eksempel forretningshemmeligheter, misbruke informasjon som del av for eksempel direktørsvindel eller fakturabedragerier. Hackere vil ofte ha dette som første mål for å skaffe seg videre tilgang til virksomheten eller privatpersoners beskyttede informasjon.

Identitetskrenkelse: Bruk av en annens identitet på internett kan ha flere formål, som eksempelvis å oppnå en økonomisk vinning for seg selv eller andre, påføre tap eller ulempe for andre og å komme i kontakt med barn med tanke på senere å utnytte dem seksuelt. Ofte omtalt som ID-tyveri eller identitetstyveri i dagligtale. Kriminelle bruker ID-tyverier for å kjøpe varer, åpne bankkonto, registrere telefonabonnement, søke om kredittkort/lån ved bruk av annens identitet, osv.

Datainnbrudd: Uberettiget inntrengning i et datasystem for å skaffe seg tilgang til beskyttet informasjon. Ofte også omtalt som dataangrep som utføres av statlige og kriminelle aktører. Flere større saker er kjent fra Norge, blant annet saker som har angått Hydro, Visma og Helse Sør-Øst.

Dataskadeverk: Typiske dataskadeverk vil være spredning av virus, ransomware eller malware som skader virksomheters datasystemer. Eller tjenestenektangrep, også kjent som et DDoS-angrep (Distributed Denial of Service), hvor angriperen forsøker å hindre at legitime brukere får tilgang til en tjeneste eller informasjon.

Databedrageri: Bedragerier har det til felles at hensikten må være å skaffe seg selv eller andre uberettiget vinning. Databedragerier skiller seg fra andre bedragerier ved at lovbruddet skjer via data, programvare eller lignende. For eksempel ved uberettiget bruk av andres kredittkort eller debetkort i situasjoner hvor slike kort ikke kontrolleres av mennesker.

[70] Trådte i kraft 1. oktober 2015.
[71] Fra intervju med Justis- og beredskapsdepartementet.

5.3 Innføring av IKT-modus i 2018

Anmeldelser registreres i politiets saksbehandlingssystem, Basisløsninger (BL), som brukes daglig av etterforskere og påtalemyndigheten for etterforskning og påtaleavgjørelse. Sakene som registreres i BL, speiles til Straffesaksregisteret (STRASAK). STRASAK er et register over alle registrerte straffbare handlinger/anmeldelser med ulike opplysninger om den som anmelder, lovbruddet, metode som er brukt (modus[72]), navn på fornærmede, mistenkte, osv. STRASAK er grunnlag for interne rapporter og statistikker i politiet, som for eksempel den årlige STRASAK-rapporten fra Politidirektoratet, og uoffisiell statistikk for saksbehandlingstid og oppklaringsprosent for straffesaker.[73]

IKT-kriminalitet er ikke mulig å skille ut som egen kriminalitetskategori, på linje med sedelighet og økonomisk kriminalitet i BL/STRASAK. Utgangspunktet for disse kategoriene er straffebestemmelse, og som tidligere nevnt er det kun noen få straffebestemmelser som kan brukes for å skille ut IKT-kriminalitet.

Som del av Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet fikk Politidirektoratet i oppdrag i 2015 å etablere en sentralisert statistikkrapportering med hensiktsmessige statistikk-koder for IKT-kriminalitet. I stedet for å utarbeide egne statistikk-koder for IKT-kriminalitet valgte Politidirektoratet å innføre tvungen bruk av IKT-modus for en rekke statistikkgrupper fra 1. januar 2018.[74] Innføringen av IKT-moduskoder skulle fange opp den anmeldte IKT-kriminaliteten. Innføringen av IKT-modus la grunnlaget for et eget kapittel om IKT-kriminalitet i den årlige straffesaksstatistikken for 2018.[75]

Totalt 16 255 saker er registrert med IKT-moduskoder i 2018. Det tilsvarer 5,1 prosent av alle anmeldte saker dette året. IKT-modus opptrer hyppigst innen kriminalitetstypene økonomi, annen[76] og seksuallovbrudd. Politidirektoratet tok imidlertid forbehold om gyldigheten (validiteten) i modusregistreringen. IKT-modusregistreringen hadde flere svakheter[77]:

- Det var forskjell på praksis for, og omfang av, modusregistering mellom politidistrikter.
- Det var uklart hva som var gjort for å sikre systematisk og hensiktsmessig registrering.
- Det var uklart om det var gjort noe lokalt for å undersøke validiteten til dataene i etterkant og ta tak i eventuelle problemer.

Politidirektoratet var derfor usikker på om tallene ga et riktig bilde av mengden IKT-relaterte saker og politiets håndtering av dem. Rapportering av antall saker med IKT-moduskoder inngikk ikke i Politidirektoratets statistikkrapportering for året 2019.

5.4 Registrering av IKT-kriminalitet i BL

Den manuelle gjennomgangen av saker viser at registreringspraksis i BL varierer. Anmeldelser og lovbrudd skal registreres på riktig straffebestemmelser og kodes med riktig straffebud og modus, jf. påtaleinstruksen § 7-1 jf. § 2-1. For den som skal registrere en sak er det 782 straffebud (straffebestemmelser), 45 hovedmodusoperandi og 584 unike *modus operandi* å registrere en sak på. Etter at saken er registrert, skal alle saker ettergås av påtalejurist. Dette for å sikre at rett straffebud er anvendt. Det er ingen rutiner for ettergåelse av moduskoder.

Moduskodene er ikke gjensidig utelukkende, og bortsett fra ved noen lovbrudd er det opp til den enkelte som registrerer saken hvilke moduser som blir registrert. Basert på utforsking av saker i BL/STRASAK ser det ut til være forskjellig praksis for koding av modus. Forskjellige dimensjoner ved kriminaliteten blandes sammen – for eksempel er det vanlig å angi kjønn og alder på offer som modus i sedelighetssaker som gjelder mindreårige. Ved narkotikaforseelser er det vanlig å registrere type narkotika som modus. For en rekke straffebud er det obligatorisk å registrere IKT-modus, men for øvrige straffebud er det opp til den som registrerer saken om modus blir registrert.

---

[72] Modus, forkortelse for *modus operandi* fra latin, er de metoder som ble benyttet av gjerningspersonen. Gjerningspersonens *modus operandi* kan hjelpe politiet i deres identifikasjon og til å se sammenheng mellom forbrytelser.
[73] BL (Basisløsninger) ble tatt i bruk i 1996 og brukes i dag i alle distrikt og særorgan som saksbehandlingssystem for politi og påtalemyndigheten i straffesaksbehandlingen, jf. NOU 2003: 21 *Kriminalitetsbekjempelse og personvern*. BL skal kvalitetssikre straffesaksarbeidet, og gi effektiv ressurs- og straffesaksbehandling. BL skal også bidra til at informasjon fra den enkelte straffesak kan gjenbrukes ved alle typer politiarbeid for statistikkformål, etterretning/spaning og etterforskning av andre saker enn den opprinnelige. Alle opplysninger i en sak behandles i BL fra anmeldelse til avslutning.
[74] Politidirektoratet (2018) Brev til politidistrikt og særorgan om etablering av statistikk og innføring av tvungen modus for IKT-kriminalitet 8. januar
[75] Politiet (2019) *STRASAK-rapporten 2018: Anmeldt kriminalitet og politiets straffesaksbehandling*.
[76] Kriminalitetstypen Annen består blant annet av hensynsløs atferd, unnlatt å etterkomme pålegg (politiloven § 5), ordensforstyrrelser, brudd på kontaktforbud og ulovlig bevæpning på offentlig sted.
[77] Politiet (2019) *STRASAK-rapporten 2018: Anmeldt kriminalitet og politiets straffesaksbehandling*. 15. februar, side 88.

I intervju viser flere av politidistriktene til at BL/STRASAK i liten grad brukes for å få oversikt over kriminalitetsbildet. Det kan være at registrerte data anses for å ha lav kvalitet, eller at registreringspraksis og bruk av kodeverk er feil eller har svakheter. Den manuelle saksgjennomgangen viser for eksempel at 35 av 150 saker klassifisert som IKT-kriminalitet har ukjente transaksjoner fra konto som modus. De fleste slike saker dreier seg om en form for kortsvindel, hvor metoden for å få fatt i kortopplysninger kan variere fra tyveri til datainnbrudd. Sakene er registrert på flere ulike straffebestemmelser: bedrageri/mindre bedrageri (29), identitetskrenkelse (3), datainnbrudd (2) og heleri (1). Dette viser at ett og samme lovbrudd kan ende opp på ulike straffebud avhengig av modus som brukt. Sannsynligheten for feilregistrering er også høy fordi saksområdet og metoder som brukes er komplekse.[78]

Politidistrikt som er intervjuet, viser til at variasjon i registreringspraksis og mangler ved registrering og koding av saker i BL/STRASAK gir utfordringer. En sak kan kodes av en i førstelinje som mangler kompetanse til å registrere sakene med riktig straffebud og modus. For den som registrerer saken i krimvakt, FSI og av andre i førstelinje kan det være for mange valg og koder tilgjengelig i BL. Det kan være vanskelig å finne riktig straffebud og modus. De fleste er mest opptatt av å finne riktig straffebud, modusregistreringen oppleves som mindre viktig og kan ofte bli feil. Heller ikke påtalejuristene, som kvalitetssikrer registrert straffebud, er opptatt av å få moduskodingen riktig, ifølge politidistriktene.

5.5 Omfanget av IKT-kriminalitet

Justis- og beredskapsdepartementet skriver i sin IKT-kriminalitetsstrategi fra 2015 at det mangler oversikt over kriminalitetsutvikling og nasjonale hendelser på IKT-feltet som faller innenfor politiets ansvarsområde. En sentral del av departementets strategi for å bekjempe IKT-kriminalitet ble derfor å etablere kunnskap om og oversikt over IKT-kriminalitet ved å etablere statistikk. Ifølge Justis- og beredskapsdepartementet er et godt kunnskapsgrunnlag viktig for å målrette innsatsen og utarbeide trusselvurderinger som kan danne grunnlag for iverksetting av tiltak.

5.5.1 Identifisering av IKT-kriminalitetssaker for 2018

Riksrevisjonen har gjennomført en manuell gjennomgang og utviklet en maskinlæringsmodell for å identifisere IKT-kriminalitet i saker registrert i 2018. Den manuelle gjennomgangen kom fram til at 148 av 1072 utvalgte saker er IKT-kriminalitet. Maskinlæringsmodellen klassifiserte 21 500 saker av totalt 334 544 registrerte saker i 2018.[79]

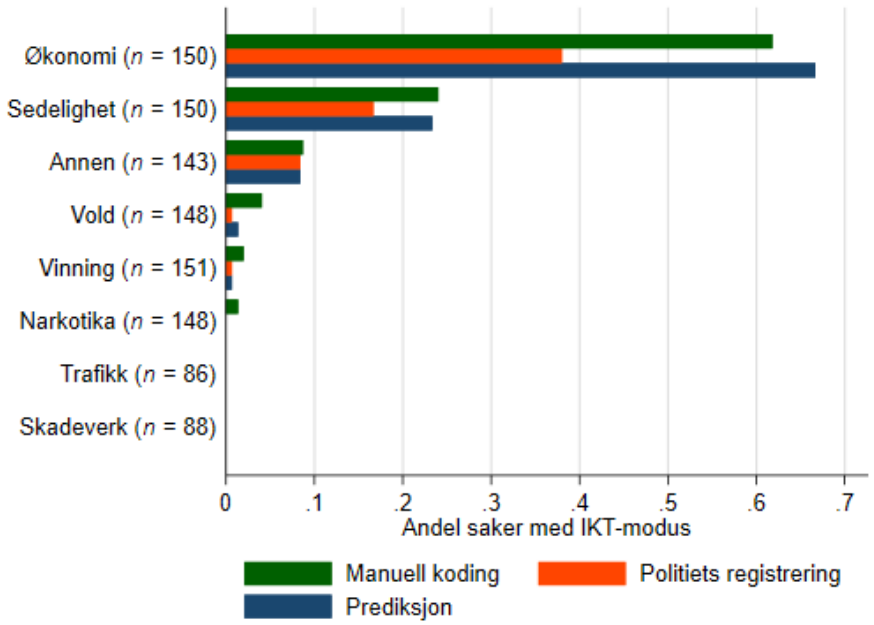
Den manuelle gjennomgangen gjør det mulig å evaluere hvor presis politiets modusregistrering er. Gjennomgangen viser at politiets registrering fanger opp kun 57 prosent av sakene som manuelt er kodet som IKT-kriminalitet.[80] Politiets registrering av IKT-modus fanger derimot opp de fleste saker som ikke er IKT-kriminalitet, ifølge den manuelle kodingen (98,9 prosent samsvar). Samlet sett samsvarer politiets registrering med den manuelle kodingen i 92,9 prosent av de utvalgte sakene.

Maskinlæringsmodellens klassifisering er mer presis enn politiets registrering. Samsvaret med den manuelle kodingen er samlet sett 3 prosentpoeng høyere for maskinlæringsmodellen enn for politiets registrering.[81] Når det gjelder klassifisering av saker som ikke er IKT-kriminalitet, er modellens samsvar marginalt (1 prosentpoeng) dårligere enn politiets registrering. Men modellen er betydelig bedre enn politiets registrering til å fange opp IKT-kriminalitet: 84,5 prosent av sakene som manuelt ble kodet som IKT-kriminalitet, klassifiserer også modellen som IKT-kriminalitet. Siden vi i de neste kapitlene vil legge vekt på politiets håndtering av IKT-kriminaliteten, er maskinlæringsmodellens klassifisering å foretrekke foran politiets registrering.

Figur 1 viser andelen saker i utvalget på 1072 saker klassifisert som IKT-kriminalitet per kriminalitetstype fra den manuelle kodingen (grønn), politiets IKT-modusregistrering (rød) og maskinlæringsmodellens prediksjon (blå).

[78] Nasjonalt tverretatlig analyse- og etterretningssenter (2019) *Bedrageri mot næringslivet*.
[79] Undersøkelsessaker og delsaker inngår.
[80] Forvirringsmatrise (confusion matrix) finnes i Vedlegg 1. Ti saker kodet som «vet ikke» er ikke med i beregningene.
[81] Samsvar mellom den manuelle klassifiseringen, politiets IKT-modusregistrering og maskinlæringsmodellen er vist i vedlegg 2 og 3.

Figur 1 Andel IKT-kriminalitet for utvalg av saker ifølge manuell koding, politiets modusregistrering og maskinlæringsmodellens prediksjon etter kriminalitetstype* (N=1072)



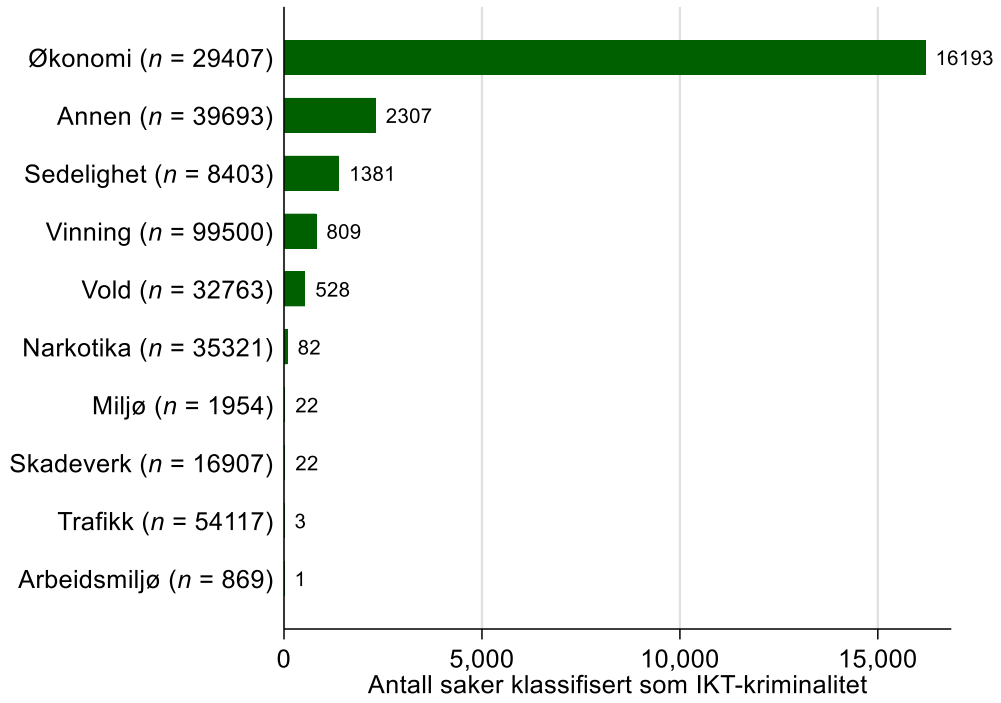
Kilde: Riksrevisjonens stratifiserte utvalg av 1072 saker fra STRASAK-tabellen for saker anmeldt i 2018. Kriminalitetstypen «Annen» omfatter lovbrudd som hensynsløs atferd, unnlatt å etterkomme pålegg (politiloven § 5), ordensforstyrrelser, brudd på kontaktforbud og ulovlig bevæpning på offentlig sted.
* Miljø og arbeidsmiljø er utelatt fordi det finnes svært få saker innenfor disse kategorien i utvalget. n viser antall saker i utvalget.

Den manuelle klassifiseringen viser at andelen IKT-kriminalitet er størst innen kriminalitetstypene økonomi (62 prosent), sedelighet (24 prosent) og annen (9 prosent). Med 95 prosent sikkerhet kan vi si at andelen IKT-kriminalitet i populasjonen av saker ligger mellom 53−70 prosent innen økonomisk kriminalitet, 17−32 prosent innen sedelighet og 4−14 prosent innen annen kriminalitet.[82] Figuren viser videre at resultatet fra den manuelle klassifiseringen samsvarer mer med maskinlæringsmodellen enn med politiets modusregistrering. Generelt tilsier den manuelle kodingen at det finnes betydelig mer IKT-kriminalitet enn det som framgår av politiets registrering, særlig innenfor økonomiområdet.

Det totale antallet IKT-kriminalitetssaker som ble identifisert av maskinlæringsmodellen blant anmeldte saker i 2018 innen hver enkelt kriminalitetstype, er gjengitt i figur 2 nedenfor.

[82] Figur med punktestimater og konfidensintervaller for alle kriminalitetstyper finnes i vedlegg 1.

Figur 2 Antall saker registrert i 2018 klassifisert som IKT-kriminalitet av maskinlæringsmodellen etter kriminalitetstype (N=318934)



Kilde: STRASAK og Riksrevisjonen
N viser det totale antall saker innenfor hver enkelt kriminalitetstype. Datagrunnlaget inkluderer ikke undersøkelsessaker og delsaker.

Figuren viser at maskinlæringsmodellen identifiserer et stort antall IKT-kriminalitetssaker innen kategoriene økonomi, annen og sedelighet. Antallet IKT-kriminalitetssaker innen kriminalitetstypene økonomi og sedelighet omtales i kapittel 5.5.2 og 5.5.3. Kategorien «Annen» utgjorde 12 prosent av alle anmeldelser politiet mottok i 2018 og 2019.

Det har ikke vært mulig å undersøke utviklingen i IKT-kriminalitet over tid i denne undersøkelsen. Selv om den totale mengden kriminalitet har gått ned de siste årene, antas det at IKT-kriminaliteten stiger.[83]

5.5.2 Omfang av internettrelaterte seksuelle overgrep

I 2018 var det 1381 internettrelaterte seksuelle overgrepssaker, av totalt 8403 saker i sedelighetskategorien. I 2018 og 2019 utgjorde seksuallovbruddene (sedelighet) 2–3 prosent av alle registrerte anmeldelser. IKT-kriminalitet på dette området er i all hovedsak internettrelaterte seksuelle overgrep mot barn og unge under 16 år. Straffebestemmelser som forekommer hyppig innen IKT-kriminalitet er §§ 310 og 311 som omhandler framstilling/framvisning av seksuelle overgrep mot barn, § 305 seksuelt krenkende atferd overfor barn og § 298 seksuelt krenkende atferd. Av alle identifiserte IKT-kriminalitetssaker utgjør sedelighetssakene totalt 17–18 prosent.

Antallet anmeldelser av alle typer seksuallovbrudd økte med 18,3 prosent (en økning på 1044 saker) fra 2015 til 2019. Anmeldelser innen enkelte lovbruddstyper har hatt en enda større økning. Økningen skyldes, ifølge Politidirektoratet, en reell økning i overgrep på internett, at politiet avdekker flere ofre og saker, og at ofre for seksuallovbrudd i større grad enn tidligere anmelder forholdet til politiet.[84] Sakene er ofte omfattende å etterforske fordi en gjerningsperson kan begå overgrep mot mange fornærmede samtidig.[85] I rapporter fra

[83] Politidirektoratet (2017) *Trusler og utfordringer innen IKT-kriminalitet*; Oslo politidistrikt (2018) *Trender i kriminalitet 2018–2021. Digitale og globale utfordringer.*
[84] Politidirektoratet (2019) STRASAK-rapporten - Anmeldt kriminalitet og politiets straffesaksbehandling, rapport utgitt 28. februar 2020.
[85] Politidirektoratet (2019) STRASAK-rapporten - Anmeldt kriminalitet og politiets straffesaksbehandling, rapport utgitt 28. februar 2020.

Kripos, Statsadvokaten i Hordaland, Sogn og Fjordane og NOVA pekes det på at internett står stadig mer sentralt i mange seksualsaker, men at det foreløpig ikke har vært mulig å skille ut nettrelaterte sedelighetsovergrep fra andre seksuallovbrudd i politiets straffesakssystem. Det har derfor manglet sikker statistikk for sakstypen.[86, 87, 88]

5.5.3 Omfang av økonomisk IKT-kriminalitet

Økonomisakene utgjorde 9 prosent av alle anmeldte saker i 2018 og 2019. Av disse 28 946 sakene er 15 755 klassifisert som økonomisk IKT-kriminalitet. Hyppigst forekommende lovbrudd innen IKT-kriminalitet (og generelt) er bedragerier og identitetskrenkelser. Økonomisakene utgjør om lag 75 prosent av alle identifiserte IKT-kriminalitetssaker. Innenfor straffebudene bedrageri og identitetskrenkelser er det registrert en økning i anmeldelser. Ifølge Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) økte antallet anmeldte bedragerier i perioden fra 2009 til 2018 med 36 prosent.[89,90] I samme periode ble det samlede antallet lovbrudd redusert med 20 prosent. Antallet ID-tyverier økte med 39 prosent i perioden fra 2016 til 2018, men har gått noe ned i 2019.[91]

5.5.4 Omfang av ren IKT-kriminalitet

Omfanget av ren IKT-kriminalitet er vanskelig å anslå ettersom det kun er to straffebestemmelser som egner seg for uttrekk av statistikk for denne kriminalitetstypen (§ 201 Uberettiget befatning med tilgangsdata mv. og § 204 Innbrudd i datasystem). Øvrige, relevante straffebestemmelser består av både IKT-kriminalitet og annen kriminalitet. Hvis vi tar utgangspunkt i disse to straffebestemmelsene, ble 461 rene IKT-kriminalitetssaker anmeldt i 2018. Ifølge Politidirektoratet øker ren IKT-kriminalitet i alvorlighet, utbredelse og kompleksitet som følge av teknologiutviklingen og vår avhengighet til teknologi og internett.[92] Antallet registrerte datainnbrudd har økt betydelig i perioden 2016–2019. Selv om det totale antallet registrerte saker er lavt, kan alvorlighetsgraden i denne typen saker være høy. Større datainnbruddssaker omtales jevnlig av media og demonstrerer hvor alvorlig denne typen kriminalitet kan være. Bare i løpet av 2020 har det vært flere alvorlige datainnbrudd hos Norfund, rederiet Vard og Stortinget.

5.6 Mørketall innen IKT-kriminalitet

Justis- og beredskapsdepartementet vedkjenner omfanget av mørketall[93] på området i sin strategi for bekjempelse av IKT-kriminalitet fra 2015. Omfanget av IKT-kriminalitet er sannsynligvis langt mer utbredt enn det som går fram av politiets statistikk. Departementet pekte i strategien på at det er viktig med bedre oversikt for å kunne målrette politiets innsats for bedre å forebygge, avverge, avdekke, etterforske og straffeforfølge slike lovbrudd. Tiltakene som nevnes for å utbedre problemer, er nye statistikkkoder, gode veiledninger og rutiner for registrering av anmeldelser, sikring av Mørketallsundersøkelsen til Næringslivets Sikkerhetsråd (NSR), og årlige trusselvurderinger for å bedre kunnskaps- og analysegrunnlaget. I tillegg blir det foreslått å se på andre rapporteringsmåter, for å få bukt med mørketallene.[94] Det er også slått fast i tidligere rapporter at det er avgjørende med etterretning for å få oversikt over mørketallene og avdekke IKT-kriminalitet.[95]

Det er flere grunner til å anta at mørketallene er særlig store innen kriminalitetstypen IKT-kriminalitet.[96] Den politianmeldte kriminaliteten i Norge har gått ned over flere år. Ifølge en rapport fra Oslo politidistrikt er reduksjonen i perioden 2013–2018 på 30 prosent innen politidistriktet. Oslo politidistrikt viser til at en lignende trend finnes i mange andre land. Dette skyldes at kriminaliteten digitaliseres i takt med at økonomiske verdier flytter seg til det digitale domenet, og nedgangen merkes særlig innen vinningslovbrudd

---

[86] Kripos (2019) *Seksuell utnyttelse av barn og unge over internett*, rapport fra Kripos, mars 2019.
[87] Hordaland, Sogn og Fjordane Statsadvokatembeter, 2019 *Rapport etter tilsyn med Vest politidistrikt sin innsats mot vold og sedelighet/voldtekt*, rapport datert 30. oktober 2019.
[88] NOVA (2018) *Nettovergrep mot barn i Norge 2015-2017*, NOVA rapport 10/18.
[89] Det er noe usikkerhet rundt tallene da ny straffelov trådde i kraft 1. oktober 2015 og medføre endringer i registreringskoder, blant annet ble nye koder for mindre bedrageri, forsøk på bedrageri og forsøk på grovt bedrageri ble lagt til som mye lovbestemmelser, mens andre bestemmelser ble opphevet.
[90] Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) (2019) Bedrageri mot næringslivet.
[91] Norsk senter for informasjonssikring (2020) *Fersk undersøkelse – 100 000 har vært utsatt for ID-tyveri*, 9. mars.2020.
[92] Politidirektoratet (2019) *STRASAK-rapporten – anmeldt kriminalitet og politiets straffesaksbehandling*.
[93] Mørketall er det tallmessige uttrykket for forholdet mellom uoppdaget og oppdaget forekomst av et uønsket fenomen.
[94] Justis- og beredskapsdepartementet (2015) Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet.
[95] Politidirektoratet (2012) *Politiet i det digitale samfunnet - En arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på Internett.*
[96] NOU 2017: 11 *Bedre bistand. Bedre beredskap*. s. 37-38.

og tradisjonelle, «analoge» deler av kriminaliteten. Nedgangen i anmeldt kriminalitet er derfor ikke nødvendigvis en positiv utvikling ettersom den faktiske kriminalitetsutviklingen ikke er kjent. Ifølge Oslo politidistrikt er dette i seg selv en alvorlig utfordring for styring av politiet framover. «Digital» kriminalitet anmeldes i mindre grad og synes ikke i statistikken, ifølge Oslo politidistrikt. Privatpersoner og virksomheter kunne i mye større grad enn i dag ha anmeldt saker, men gjør det ikke fordi kriminaliteten ikke oppdages av fornærmede, tilliten til politiet er lav på dette området, man er redd for eget og virksomhetens omdømme osv.[97]

5.6.1 Mørketall for seksuallovbrudd og internettrelaterte seksuelle overgrep

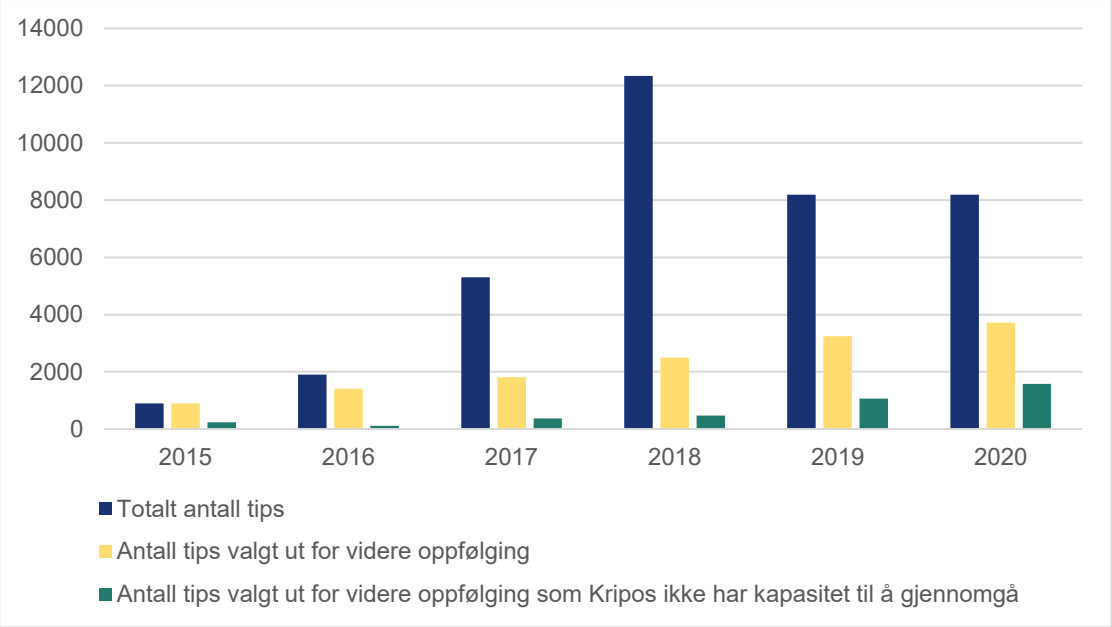
I den årlige gjennomgangen av straffesaksstatistikken for 2019 skriver Politidirektoratet at det har vært store mørketall innen kriminalitetstypen seksuallovbrudd. Det har vært en betydelig økning i anmeldelser når det kommer til internettrelaterte saker hvor fornærmede er under 16 år de siste årene. Det har vært en ambisjon å avdekke og straffeforfølge flere saker. Selv om nettovergrepssaker har fått stor oppmerksomhet i media, antar Politidirektoratet at mørketallene fremdeles er høye. Årsaken til dette er at ofrene kan føle skam, skyld eller fordi de er forledet til å tro at de kommuniserer med en annen enn den de trodde på nett.[98]

En kilde til kunnskap om omfanget av internettrelaterte seksuelle overgrep er tips. Kripos tar imot tips og informasjon om nedlasting av overgrepsmateriale fra ulike kilder, både nasjonalt og gjennom internasjonale organisasjoner og politisamarbeid. Antallet tips har økt betydelig i perioden 2015–2019. I tillegg til tipsene Kripos mottar, gjennomfører flere politidistrikter egen overvåking gjennom verktøy som ICACCOPS og GRIDCOPS.[99] Dette er programmer for overvåking av ulovlig nedlasting av merket overgrepsmateriale fra ulike fildelingsplattformer.[100]

Kripos håndterer tips i sedelighetssaker i noe som kalles Saksbehandlingsprosjektet. Alle tips som kommer fra tjenestetilbydere, National Center for Missing and Exploited Children (NCMEC) og National Child Exploitation Coordination Center (NCECC) i USA, Europol, Interpol, tipstelefon, utspringssaker (fra andre saker) og lignende, inngår i saksbehandlingsprosjektet. Kun straffbare forhold tas inn i saksbehandlingsprosjektet. I intervju sier Kripos at de ikke har kapasitet til å gå gjennom alle tipsene som kommer inn hvert år. De anslår at det kommer inn om lag 10 000 tips årlig bare fra NCMEC. Kripos estimerer at de gikk gjennom omkring 45 prosent av alle tips som kom inn 2019. Kripos har en prioriteringsordning, der hver sak får en verdi. Kripos venter imidlertid på en ny løsning som er utviklet av Europol, og håper denne kan hjelpe med det som i dag er manuelt arbeid. Figur 3 viser antall tips Kripos har mottatt, hvor mange tips som velges ut for videre behandling, og hvor mange tips Kripos ikke har kapasitet til å gjennomgå i perioden 2015–2020. Antallet tips valgt ut for videre behandling er beregnet med utgangspunkt i saker som de har valgt å gå videre med.

[97] Oslo politidistrikt (2018) *Trender i kriminalitet 2018-2021 - Digitale og lokale utfordringer*.
[98] Politiet (2020) *STRASAK-rapporten 2019: Anmeldt kriminalitet og politiets straffesaksbehandling*.
[99] Intervju med Trøndelag politidistrikt.
[100] Forskjellen på disse er primært at programmene monitorer ulike fildelingsnettverk. Programmene identifiserer IP-adressene som deler bildene. Politiet kan også se hvor mange filer en IP-adresse har hatt befatning med, og hva slags type bilder. Selv om programmene monitorerer bare en liten del av internett får de mange treff. Imidlertid er det reelle tallet mye høyere. Dette er både fordi programmene kun kan monitorere filer som allerede er kjente for politiet, og fordi mange bruker andre fildelingsnettverk, VPN-løsninger eller mørkenettet (Dark Web).

Figur 3 Tips mottatt hos Kripos som gjelder internettrelaterte seksuelle overgrep i perioden 2015–2020



Kilde: Kripos

Figur 3 viser at tipsmengden har økt betraktelig i perioden 2015–2018 og ligger stabilt på et høyt nivå i 2019 og 2020. Antallet tips Kripos velger ut for videre behandling øker og det samme gjør antall tips Kripos ikke har kapasitet til å gjennomgå. Dette er en indikasjon på at antallet alvorlige saker hvor det mistenkes straffbare forhold øker, og at Kripos' kapasitet til gjennomgang av disse sakene utfordres. Mer enn 40 prosent av tipsene som ble valgt ut for videre oppfølging ble ikke gjennomgått av kapasitetsmessige grunner i 2020.

Politiet har, i motsetning til hva som er tilfelle på andre kriminalitetsområder, tilgang til informasjon om lovbrudd og mulige gjerningspersoner via etterretningssamarbeid med andre lands politimyndigheter, samt tips. Informasjonen er ofte tilgjengelig som IP-adresser som brukes for nedlasting og deling av overgrepsmateriale. En utfordring for politiet i håndteringen av tips og etterretningsinformasjon er etterforsknings- og påtaleplikten. Alvorlige seksuallovbrudd mot barn kan ikke henlegges uten at det er gjennomført etterforskningskritt, ifølge politidistriktene som er intervjuet. Dette fører til at politiet velger å anmelde de sakene de har kapasitet til å gjennomføre og hvor sannsynlighet for positiv påtaleavgjørelse er størst. Flere politidistrikter oppgir at de må prioritere blant alvorlige saker innen dette området. Tips og etterretning om lovbrudd fører ikke alltid til opprettelse av sak på grunn av etterforskningsplikten og manglende etterforskningskapasitet. Oversikten over anmeldte forhold vil derfor ikke gi et dekkende bilde av det faktiske antallet saker på dette området.

Kripos anser ikke etterforskningsplikten, slik den er definert av Riksadvokaten, som reell i betydningen av plikt til å etterforske alle tips om seksuallovbrudd. Kripos kjenner ikke til praksisen politidistriktene viser til når det gjelder å kun anmelde de alvorligste sakene av hensyn til etterforskningsplikten. Politiet har en handlingsplikt for å avverge og stanse kriminalitet. Det finnes mye informasjon som ikke ender med anmeldelse i politiets systemer, dette gjelder alle typer kriminalitet og anses ikke som bevisst unnlatelse for å skjære klar av etterforskningsplikten.

Riksadvokaten viser til at etterforskingsplikten er regulert i straffeprosessloven § 224, hvor det heter at etterforsking foretas når det som følge av anmeldelse mv. er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige. Det skal dermed foretas en konkret og skjønnsmessig vurdering i det enkelte tilfelle om det er «rimelig grunn» til å iverksette etterforsking. I sedelighetssaker som omfatter barn, vil utfallet av denne vurderingen likevel oftest gi seg selv. I praksis kan det derfor langt på vei sies å være en etterforskingsplikt for denne sakstypen. Når det gjelder håndtering av tips og etterretning om lovbrudd på dette området har Riksadvokaten begrenset innsikt i dette, og det er derfor vanskelig å mene noe om utbredelsen av en slik praksis. For blant annet nettovergrepssaker opplever Riksadvokaten at det er en lojal etterfølgelse av prioriteringsdirektivene. En konsekvent praksis med hensyn til å ikke etterforske

saker man har tips og etterretning om, er ikke akseptabel, gitt at det dreier seg om tips og etterretningsinformasjon som tilsier at det foreligger etterforskingsplikt, dvs. at de aktuelle opplysningene gir rimelig grunn til å undersøke om det foreligger straffbart forhold. Når en slik praksis ifølge enkelte politidistrikt skyldes ressurs- og kapasitetsutfordringer, kan en del av løsningen – for omfattende overgrepssaker – være lovforslaget Riksadvokaten har oversendt Justis- og beredskapsdepartementet. Lovforslaget gjelder «serieovergripere», og går ut på å etterforske og iretteføre de mest omfattende sakene på en mer effektiv måte.[101]

5.6.2 Mørketall for økonomisk kriminalitet og ren IKT-kriminalitet

Mørketallene for økonomisk kriminalitet og ren IKT-kriminalitet er sannsynligvis store. Undersøkelser gjennomført av Næringslivets sikkerhetsråd (NSR)[102], Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES)[103] og Norsk senter for informasjonssikring (NorSIS)[104] viser at både privatpersoner, offentlige etater og private virksomheter utsettes for økonomisk og ren IKT-kriminalitet.

Omfanget av datainnbrudd og lignende kriminelle handlinger mot norske virksomheter, som registreres av Nasjonal sikkerhetsmyndighet (NSM) gjennom deres kanaler, viser at en svært liten andel av disse sakene blir anmeldt. NSM registrerer at norske virksomheter daglig utsettes for digitale hendelser gjennom varslingssystemet for digital infrastruktur (VDI) og FCKS-samarbeidet.[105] NSM registrerte totalt 19 712 uønskede hendelser mot informasjonssystem i Norge i 2018. 4689 av disse ble prioritert for oppfølging av NSM. Det var et titalls alvorlige hendelser i 2018. De mest alvorlige sakene var mer komplekse, sofistikerte og krevende enn tidligere.[106] I sine rapporter skriver NSM at det både er stater og kriminelle som står bak slike datainnbrudd.

Mange av sakene næringslivet melder fra om, dreier seg om bedragerier i forskjellige former. Flere større bedrifter har kontaktet politiet angående saker de har fanget opp i sine systemer. En større næringslivsaktør henvendte seg til Oslo politidistrikt i 2018 med et forslag om å begynne å anmelde et fåtall saker og etter hvert øke antall anmeldelser når politiet fikk større kapasitet. Selskapet har oppgitt til politiet at de kunne ha anmeldt langt flere saker. Oslo politidistrikt konkluderte med at det ikke er hensiktsmessig at slike saker anmeldes. Det ble vist til at næringslivsaktører satt på store mengder potensielle anmeldelser, og at dersom disse ble anmeldt, ville det legge beslag på en uforholdsmessig stor andel av politidistriktets ressurser til registrering av saker. Det ville kunne føre til restanser på registrering og utfordringer med hensyn til innhenting av IP-adresser innenfor fristen på 21 dager. Det ble også antatt at mesteparten av sakene var vinningssaker, og at de ville bli henlagt fordi vinningssaker ikke er prioritert.[107]

DNB rapporterer årlig om datainnbrudd og annen kriminalitet mot virksomheten. I 2019 rapporterte DNB at antallet dataangrep mot virksomheten økte fra 310 i 2013 til 6523 i 2018; en 20-dobling på seks år. DNB avdekket sju angrep med alvorlig skadepotensial i 2018. Alle angrep ble avverget, og ingen saker førte til skade eller datalekkasje.[108]

Ifølge en undersøkelse gjennomført av NSR rapporterer kun 11 prosent av undersøkte virksomheter sikkerhetshendelser til politiet. 1 av 7 virksomheter opplevde forsøk på datainnbrudd eller hacking, og rundt 1 av 9 virksomheter opplevde virus og/eller malwareinfeksjon.[109] Et gjennomgående funn i NSRs undersøkelser er den lave andelen avdekket kriminalitet som faktisk anmeldes til politiet. Tendensen har vært stigende over flere år. Ifølge NSR er årsakene til manglende anmeldelser at politiet som regel henlegger saken, anmeldelser er for ressurs- og tidkrevende, virksomheten behandler slike saker internt,

---

[101] Riksadvokaten (2019) Etterforsknings- og påtalepliktens grenser i omfattende nettovergrepssaker - Et nytt straffebud om serieovergrep - mulige lovendringer, brev til Lovavdelingen, Justis- og beredskapsdepartementet, 10. september 2019.
[102] Næringslivets sikkerhetsråd, 2019 *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2019*. Gjennomført av Opinion AS for Næringslivets Sikkerhetsråd
[103] Nasjonalt tverretatlig analyse- og etterretningssenter (2019) *Bedrageri mot næringslivet.* Nasjonalt tverretatlig analyse- og etterretningssenter startet opp 2. mai 2016 og består av representanter fra Riksadvokaten, Politidirektoratet, ØKOKRIM, Skatteetaten, Tollvesenet, Arbeidstilsynet, NAV og andre kontrolletater. Senterets formål er å legge til rette for at politiet og kontrolletatene bedre kan utnytte
den samlede analyse- og etterretningsinformasjon etatene besitter. Senteret skal utarbeide kunnskapsbasert grunnlag for politiets og kontrolletatenes egne og felles tverretatlige prioriteringer. Dette skal bidra til å utvikle og gjennomføre en mer målrettet, effektiv, slagkraftig og treffsikker bekjempelse av økonomisk kriminalitet, herunder arbeidslivskriminalitet.
[104] KANTAR TNS (2020) *Politiets innbyggerundersøkelse 2019*.
[105] Felles cyberkoordineringssenter består av representanter fra NSM, Etterretningstjenesten, PST og Kripos. Koordinerer partenes håndtering av IKT-sikkerhetshendelser.
[106] NSM (2019) *Årsrapport 2018*.
[107] Oslo politidistrikt (2018) *Datakriminalitet rettet mot næringslivet*, internt notat datert 9. april 2018.
[108] DNB (2020) *Trusselvurdering 2020*, offentliggjort 13. mai 2020.
[109] Næringslivets sikkerhetsråd, 2020 *Mørketallsundersøkelsen 2020*. Gjennomført av Opinion AS for Næringslivets Sikkerhetsråd.

manglende tillit til politiets kompetanse, frykt for å svekke virksomhetens omdømme, og mangelfulle forsikringer.[110]

NTAES har gjennomført en undersøkelse der det pekes det på flere forhold som kan forklare mørketallene for kriminaliteten som rammer næringslivet. NTAES peker på at dette kan forklares ved at politiet har en lav oppklaringsprosent ved bedragerier, opplevelsen av at det er ressurskrevende å anmelde, samt manglende mulighet til å få tilbake det økonomiske tapet. Små og mellomstore foretak er særlig utsatt, dette antas å ha sammenheng med at disse ofte mangler kunnskap og kapasitet til å sikre seg mot denne type kriminalitet. Konsekvensen av de store mørketallene er at politiet er lite kjent med modus og trender i kriminalitetsbildet på dette området, og det mangler oversikt over hvem som utsettes for bedragerier.[111]

NorSIS' årlige undersøkelse av omfanget av identitetstyveri og sikring av identitet gir anslag for den økonomiske IKT-kriminaliteten som rammer privatpersoner. NorSIS gjennomfører undersøkelsen i samarbeid med skatteetaten. I 2017 var det 3,3 prosent, i 2018 3,9 prosent, og i 2019 2,5 prosent av befolkningen over 18 år som sa at de hadde vært utsatt for identitetstyveri i løpet av de siste to årene. Overført betyr disse tallene at om lag 150 000 personer i 2018, og om lag 100 000 personer i 2019 ble utsatt for denne typen kriminalitet.[112] I 2018 mottok politiet 3618 anmeldelser av identitetskrenkelser. Dette tyder på at en veldig liten andel av de som utsettes for denne typen svindel, anmelder saken. Dette støttes av tall fra politiets innbyggerundersøkelse. Kun 23 prosent av de som oppgir at de blir utsatt for svindel eller bedrageri på internett, anmelder forholdet til politiet.[113]

Finanstilsynet utgir en årlig risiko- og sårbarhetsanalyse som oppsummerer IKT-sikkerhetsarbeidet i finanssektoren og hvordan bransjen etterlever relevant regelverk. I rapporten for 2019 vises det til at finansforetakene opplever økning i forsøk på digital kriminalitet mot deres systemer, men at angrepene stanses før de får konsekvenser. Kontinuerlig overvåkning av transaksjoner og styrkingen av innsatsen hos bankene bidrar sannsynligvis også til å holde tapene nede. Finansforetakenes kunder blir imidlertid i økende grad utsatt for svindel.[114]

- Bank-ID og påloggingsinformasjon på avveie: tap på 42 millioner kroner i andre halvår 2019.
- Sosial manipulering: I 2019 ble de totale tapene anslått til 500 millioner kroner som følge av direktørsvindel, fakturabedrageri, kjærlighetssvindel osv. Tapene økte med 67 prosent fra 2018 til 2019.
- Misbruk av betalingskort: 190 millioner kroner i 2019. Tapstallene økte med 28 prosent fra 2018 hvor særlig misbruk av kortinformasjon ved internetthandel øker.

DNB rapporterer at det forekommer en stor mengde kortsvindel, kortbedrageri eller ID-tyverier mot privatpersoner. IKT-kriminalitet her er primært internettbedrageri hvor kortet ikke er stjålet eller til stede ved transaksjonen, kalt Card Not Present (CNP-bedrageri). Tall fra BITS AS, som overvåker korthandel i Norge, viser at det samlede misbruket av kort ved internetthandel/CNP-bedrageri i Norge vokser. Dette er svindel hvor opplysninger om offerets bankkort utnyttes ved bestilling av varer og tjenester.[115] DNB estimerte at det ble gjort over 4000 forsøk på bedragerier mot banken og bankens kunder i en samlet størrelsesorden på 1,2 milliarder kroner i 2020. Banken registrerer at kundene utsettes for ulike former for bedragerier, jf. faktaboks 2.

Faktaboks 2 Hyppig forekommende former for bedrageri

Ifølge rapporten fra DNB er noen av de vanligste bedrageriene:

- Vishing (voice phishing) – mest kjent som «Olga-svindel». Kriminelle tar kontakt med offer og utgir seg for å representere offerets bank. Bedrageriene kommer i perioder, og hadde i løpet av 2020 en aktiv periode.
- Investeringsbedrageri – fornærmede lures til å investere i fiktive verdipapirer, bitcoin eller andre kryptovalutaer. Denne formen for bedrageri har ifølge DNB vokst med 125 prosent fra 2019 til 2020.

[110] Næringslivets sikkerhetsråd, 2019 *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2019*. Gjennomført av Opinion AS for Næringslivets Sikkerhetsråd.
[111] Nasjonalt tverretatlig analyse - og etterretningssenter (2019) *Bedrageri mot næringslivet*.
[112] NorSIS (2019) *Nordmenn og digital sikkerhetskultur*, årlig rapport som utgis av NorSIS med støttte fra Justis- og beredskapsdepartementet..
[113] KANTAR TNS (2020) *Politiets innbyggerundersøkelse 2019*.
[114] Finanstilsynet (2020) Risiko- og sårbarhetsanalyse 2020.
[115] DNB (2020) *Trusselvurdering 2020*, offentliggjort 13. mai 2020.

- Kjærlighetsbedrageri – ofte også omtalt som Nigeria-svindel. Bedragerier hvor fornærmede forelsker seg og lures til å overføre penger til utenlandske konti. Brukes også etter hvert for hvitvaskingsformål. Har en stabil utvikling.
- Business email compromise (BEC) eller phishing – ofte brukt mot bedriftskunder og omfatter direktørsvindel, falske fakturaer, spoofing (oppringing fra falske numre) og kompromitterte e-postkontoer. Her forekommer de største og groveste bedrageriene, men beløpene kan variere fra noen tusen til 150 millioner kroner, som var det største beløpet i 2019.

Kilde: DNB (2020) *Trusselvurdering 2020*, offentliggjort 13. mai 2020.

Selv om kriminaliteten ikke synes i kriminalitetsstatistikken, har politiet mulighet til å drive etterretning for å få kunnskap om kriminalitetsbildet. Næringslivet har etterlyst et tettere samarbeid for å utveksle informasjon som kan være av relevans for politiet i etterretningsøyemed. Ifølge Kripos har imidlertid politiet ikke kapasitet eller systemer til å ta imot digital etterretningsinformasjon av den typen som større næringslivsaktører har sagt at de kan dele med politiet.

6 Etterforskning av IKT-kriminalitet

En av politiets viktigste oppgaver er å etterforske og straffeforfølge lovbrudd. I dette kapitlet undersøker vi hvor mye tid politiet brukte på etterforskning av IKT-kriminalitet generelt og innen de tre områdene ren IKT-kriminalitet og IKT-kriminalitet innen sedelighet og økonomi i 2018. Tallene blir sammenlignet med tidsbruken på saker som ikke er IKT-kriminalitet. Den gjennomsnittlige tidsbruken på IKT-kriminalitet er betydelig høyere innenfor sedelighetsområdet enn IKT-kriminalitet innenfor andre kriminalitetsområder. Tidsbruken er lav innen etterforskning av økonomiske IKT-kriminalitet og ren IKT-kriminalitet. Tidsbruken for IKT-kriminalitet er høyere innenfor sedelighetsfeltet og marginalt lavere innenfor økonomifeltet sammenlignet med andre saker innenfor samme straffebestemmelse som ikke er IKT-kriminalitet.

6.1 Etterforskning generelt og innen IKT-kriminalitet spesielt

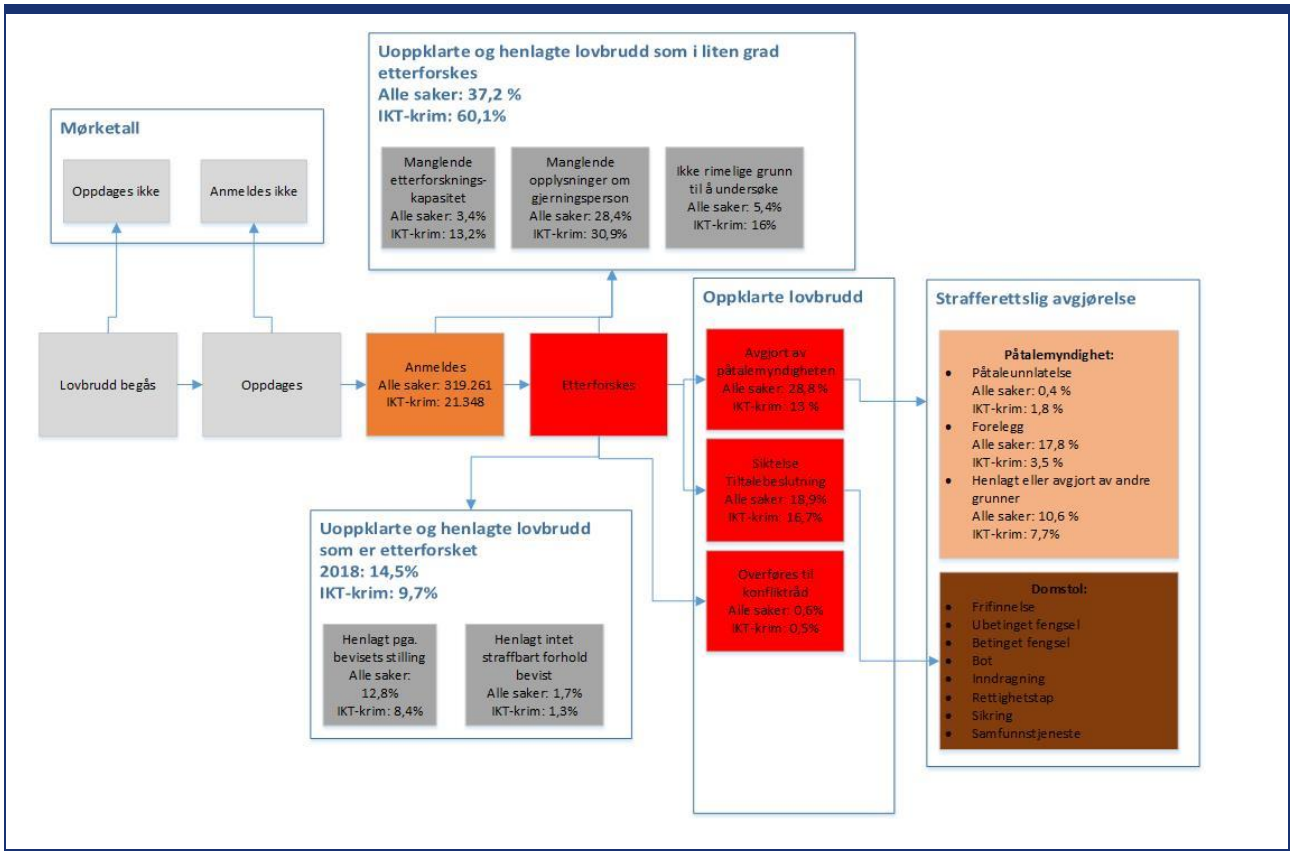
For politi- og påtalemyndigheten er etterforskning en kjerneoppgave. 40 prosent av personellressursene i politiet har etterforskning som hovedoppgave. I tillegg bidrar alle politiutdannede og store deler av den øvrige organisasjonen til etterforskningen. Etterforskningens mål er å skaffe til veie nødvendige opplysninger for kunne avgjøre spørsmål om tiltale og forberede sakens rettsbehandling.[116]

Figur 4 nedenfor illustrerer hvordan et lovbrudd håndteres etter anmeldelse. Anmeldelser blir enten umiddelbart henlagt og ender opp som et uoppklart lovbrudd, eller de etterforskes. Etter etterforskning kan saken få flere utfall, hvor de mest vanlige avgjørelsene i 2018 var henleggelse, forelegg, siktelse (med begjæring om tilståelsesdom), tiltalebeslutning eller overføring til konfliktråd. Henleggelser, forelegg og overføring til konfliktråd avgjøres av påtalemyndigheten. Siktelser med begjæring om tilståelsesdom og tiltalebeslutning besluttes av påtalemyndigheten, men oversendes til domstolene for en endelig strafferettslig avgjørelse.

Foto: Stein Bjørge / Aftenposten / NTB

[116] Politidirektoratet og Riksadvokaten, 2016 *Handlingsplan for løft av etterforskningsfeltet.*

Figur 4 Håndtering av anmeldte lovbrudd, inkludert IKT-kriminalitet, i 2018



Kilde: Riksrevisjonen, SSB. Utviklet basert på figur gjengitt i SSB-rapport 2000/13 *Statistikk over anmeldte lovbrudd og registrerte ofre*.

Ifølge noen av politidistriktene som er intervjuet, er det et generelt mål at lavt prioriterte saker skal henlegges raskt ved felles straffesaksinntak. Ser vi generelt på påtaleavgjørelser som ofte vil forekomme i saker som henlegges tidlig (manglende etterforskningskapasitet, manglende opplysninger om gjerningsperson og ikke rimelig grunn til å undersøke) utgjorde disse 37,2 prosent av alle saker som ble registrert i 2018. Flertallet av disse sakene ble henlagt uten etterforskning.[117] Det forekommer at disse påtaleavgjørelsene brukes i saker som har vært under etterforskning, men dette er kun unntaksvis. En rekke lovbrudd oppdages av politiet og straffes ved forelegg. Typiske lovbrudd kan være trafikklovbrudd og ordensforstyrrelser. Lovbruddet oppdages i det handlingen begås, og det kan vanskelig argumenteres for at politiet bruker betydelig etterforskningskapasitet på å oppklare lovbruddet.[118] Forelegg utgjorde 17,8 prosent av alle saker i 2018. Legger vi sammen de tidlig henlagte og uoppklarte sakene uten etterforskning og forelegg utgjør de 55 prosent av alle saker som ble registrert i 2018. Det kan argumenteres for at dette er saker hvor det i liten grad foregår etterforskning.

De resterende 45 prosentene av sakene behandles ved felles straffesaksinntak, eller fordeles til andre enheter (geografiske enheter eller fellesenheter) for videre etterforskning. Sakene avgjøres deretter av påtalemyndigheten med hensyn til om saken skal bringes inn for domstolene, eller avgjøres av påtalemyndigheten.

I Politidirektoratets årlige statistikk finnes det ikke oversikt over hvor mange saker som etterforskes. I stedet brukes påtaleavgjorte saker som et mål. Bak påtalekodene ligger det svært mange ulike saksforløp. Dette gir derfor ikke et godt bilde av politiets innsats på området. SSB regner alle saker som er rettskraftig avgjort, som etterforsket.[119] Dette målet sier også svært lite om hva slags arbeid som ligger bak hver enkelt sak. Dette er politiet selv klar over, og som en del av etterforskningsløftet ble Kapasitetsvurderingen av

[117] Lokale sakstrekksnstrukser for politidistriktene og intervjuer med politidistriktene.
[118] Enkelte typer foreleggsaker kan være ressurskrevende å etterforske, for eksempel enkelte typer miljøkriminalitet og saker som gjelder foretak. Dette er imidlertid en meget liten andel av foreleggene.
[119] SSB (2019) *Etterforskede lovbrudd*, publisert statistikk fra SSB på byråets nettsider, aksessert 8.10.2020.

etterforskningsområdet utarbeidet i 2019. I rapportens forord skriver Politidirektoratet at de for første gang kan gi et faktabasert svar på tilgjengelig kapasitet på etterforskningsfeltet og hvordan den benyttes. Videre skriver de at undersøkelsen gir svar på hvilke konsekvenser endringer i kriminaliteten, og krav til kvalitet og saksbehandlingstid, har for kapasitetsbehovet framover. [120]

Kapasitetsundersøkelsen estimerte tidsbruk til etterforskning ved først å hente inn alle registrerte rutiner på straffesaker i BL for 2017 og 2018. For alle rutiner er gjennomsnittlig tidsbruk beregnet. For aktiviteter som ikke registreres i BL, er det innhentet tidsbruksdata basert på workshoper med politimedarbeidere i åtte politidistrikter. Til slutt koblet de tidsbruksestimatene på rutinedataene for hver straffesak. Politidirektoratets Kapasitetsundersøkelse gir imidlertid ikke et klart svar på om en sak er etterforsket ettersom det ikke finnes formelle krav til hva som må til av etterforskningsskritt for å regne en sak som etterforsket. Men undersøkelsen er en god kilde til data på aktiviteter og tidsbruk i straffesaksbehandlingen.[121] I stedet for å undersøke etterforskning som en dikotom variabel ser vi derfor heller på hvor mye tid politiet i gjennomsnitt bruker på behandling av ulike typer straffesaker.

6.2 Tidsbruk i etterforskning av IKT-kriminalitet

For å undersøke i hvor stor grad politiet etterforsker IKT-kriminalitetssakene, bruker vi tidsbruksdata fra Kapasitetsundersøkelsen. Ved å koble identifiserte IKT-kriminalitetssaker fra maskinlæring med tidsbruksdataene fra Kapasitetsundersøkelsen kan vi undersøke hvordan tidsbruken fordeler seg mellom IKT-kriminalitet og annen kriminalitet.

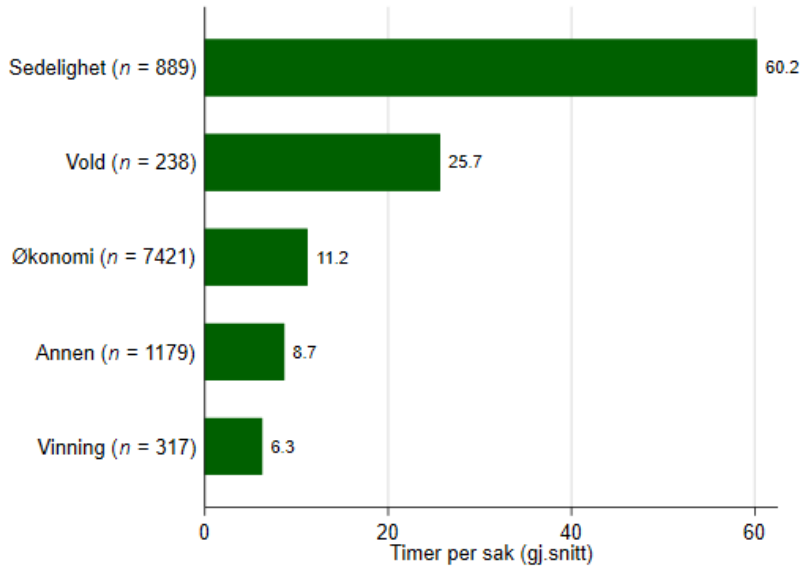
Tidsbruksdataene inkluderer alle hovedprosessene i straffesaksbehandlingen, fra iverksetting av sak, via etterforskning, påtaleavgjørelse og domstolsbehandling, til avslutning av sak. Vi inkluderer tid brukt på alle prosessene utenom domstolsbehandling, fordi domstolsbehandling skjer i etterkant av etterforskningen og er en prosess etterforskere bruker lite tid på.

En utfordring er at dataene for IKT-kriminalitet inkluderer alle saker registrert i 2018, men det mangler tidsbruksdata for 2019 og 2020.[122] Vi har derfor ikke opplysninger om tidsbruk for saker der etterforskningen starter i 2018 og fortsetter i 2019 og 2020. For å minimere dette problemet er det sett på tidsbruk bare for saker registrert i første halvdel av 2018. Like fullt vil sannsynligvis tidsbruksestimatene generelt ligge noe under den faktiske totale tidsbruken.[123]

Figur 5 viser hvor mye tid som er brukt til etterforskning av IKT-kriminalitetssakene innenfor de fem mest relevante kriminalitetstypene.

[120] Politidirektoratet (2019) *Kapasitetsvurdering av etterforskningsområdet*.
[121] Politidirektoratet (2019) *Kapasitetsvurdering av etterforskningsområdet*. En grunn er at ikke alle aktiviteter er enkle å klassifisere som etterforskning eller en annen prosess i straffesaksbehandlingen. En annen grunn er at aktiviteter for et uvisst antall vedleggssaker er registrert under hovedsaken i politiets saksbehandlingssystem. En del saker som faktisk er etterforsket vil derfor fremstå som ikke etterforsket basert på aktivitetsdataene. En annen relevant kilde er den registrerte avgjørelsen av saken, som blant annet viser om saken ble henlagt. Men selv om færre av de henlagte sakene enn de oppklarte sakene er etterforsket, kan man ikke forutsette at ingen henlagte saker er etterforsket.
[122] Politidirektoratet planlegger å gjennomføre kapasitetsundersøkelse av tidsbruk på etterforskning høsten 2020, men foreløpig har ikke tallene vært tilgjengeligetilgjengelig for bruk i denne undersøkelsen (28.9.2020).
[123] Seksjon 2.1.3 beskriver data og metode i mer detalj.

Figur 5 Gjennomsnittlig tidsbruk i 2018 per IKT-kriminalitetssak etter kriminalitetstype*



Kilde: Politidirektoratets kapasitetsundersøkelse og identifiserte IKT-kriminalitetssaker fra maskinlæring.
* Kriminalitetstyper med færre enn 100 IKT-kriminalitetssaker registrert i 2018 er ikke vist i figuren. Bare IKT-kriminalitetssaker registrert i første halvdel av 2018 er inkludert.

Tidsbruken varierer mye mellom kriminalitetstypene, fra 60,2 timer i gjennomsnitt for IKT-kriminalitet innen sedelighet til 6,3 timer i gjennomsnitt for IKT-kriminalitet i vinningssaker. Denne variasjonen synes generelt å gjenspeile Riksadvokatens føringer om å prioritere alvorlig sedelighetskriminalitet og voldskriminalitet.[124]

6.3 Etterforskning av internettrelaterte seksuelle overgrep

Norge er forpliktet gjennom internasjonale avtaler til å kriminalisere og straffeforfølge seksuell utnytting av barn, inkludert nettrelaterte seksuallovbrudd. Beskyttelse av barn mot seksuell utnytting og seksuelt misbruk er nedfelt i en egen konvensjon vedtatt av Europarådets ministerkomite i juli 2007. Konvensjonen bygger på FNs barnekonvensjon og stiller krav til nasjonal lovgivning og straffesaksbehandling. Den inneholder også bestemmelser om forebyggende tiltak og prinsipper for behandlingstilbud og andre tiltak overfor gjerningspersoner.[125]

Etterforskning av seksuallovbrudd, med voksne og unge som fornærmede, er høyt prioritert av Riksadvokaten. Riksadvokaten viser til at seksuallovbrudd er integritetskrenkende kriminalitet og et alvorlig samfunns- og folkehelseproblem, og stiller derfor krav til en særlig høy oppklaring i denne sakskategorien.[126] Antallet seksuallovbruddssaker økte med 18 prosent fra 2015 til 2019, og økningen har vært betydelig høyere for enkelte straffebestemmelser. Dette gjelder særlig voldtekt, seksuallovbrudd mot barn under 16 år og andre seksuallovbrudd. Økningen i seksuallovbrudd mot barn og unge under 16 år medfører en betydelig økt ressursbruk til etterforskning og straffesaksbehandling fordi antallet fornærmede i en enkelt sak kan være høyt, og fordi for eksempel gjennomføring av tilrettelagte avhør er tid- og ressurskrevende.

Etterforskningen av alvorlige internettrelaterte seksuelle overgrep har siden 2013 vært gjennomført i de fleste politidistrikt som større operasjoner fordi etterforskningene ofte blir omfattende. Det første større etterforskningsprosjektet var Operasjon Share, som Kripos gjennomførte fra 2013. Skjult spaning på

[124] Riksadvokaten (2019) *Mål- og prioriteringsskriv for 2019.*
[125] *Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk*. Vedtatt av ministerkomiteen 12. juli 2007 på det 1002. møte for ministrenes stedfortredere.
[126] Riksadvokaten (2019) *Mål- og prioriteringsskriv for 2019.*

fildelingsnettverket edonkey2000 ble starten på en stor etterforskningsinnsats som resulterte i 68 saker og 73 siktede. Samtlige politidistrikter ble involvert i etterforskningen av de mistenkte.[127]

Fra april 2015, og i perioden etter, har alle politidistrikt igangsatt større etterforskningsprosjekter av internettrelaterte seksuelle overgrep. Det første prosjektet var Operasjon Duck i Trøndelag politidistrikt, som pågikk i perioden 2015–2017.[128] Erfaringene fra Operasjon Duck ledet til opprettelse av lignende etterforskningsoperasjoner i flere andre politidistrikter. Det foreløpig sist kjente er operasjon Cirius i Nordland politidistrikt, som startet opp i desember 2019.

Faktaboks 3 Operasjon Duck

Operasjon Duck ble igangsatt av Trøndelag politidistrikt fra april 2015. Om lag 20 etterforskere deltok i operasjonen, som varte i 14 måneder. Prosjektet ble sammensatt av analytikere (analyse av sammenhengen mellom saker), datakrimteknikere (identifisering og sikring av spor og bevis), taktiske etterforskere (avhør og generell etterforskning), spesialister på avhør av barn (tilrettelagte avhør) og dedikert påtaleledelse og etterforskningsledelse. Mer enn 50 straffesaker ble registrert, og minst 13 personer ble dømt, og i tillegg bidro etterforskningen til opprettelse av saker i flere andre politidistrikt. Ifølge Trøndelag politidistrikt førte operasjonen til oppbygging av verdifull kompetanse innen etterforskning av seksuelle overgrep mot barn på internett og opprettelse av større etterforskningsoperasjoner i andre distrikt.

Kilde: Intervju med Trøndelag politidistrikt; NOVA (2019) Nettovergrep mot barn i Norge 2015–2017, NOVA-rapport 10/18.

Etterforskningsoperasjonene viser hvor høyt prioritert disse sakene har vært hos Kripos og i politidistriktene. Operasjonene har bidratt til en betydelig kompetansebygging. Mange ansatte har deltatt i etterforskningen fra ulike enheter internt, og opprulling av store saker med forgreninger til mange politidistrikter og utenlands har fått betydelig oppmerksomhet. En rekke gjerningspersoner er straffeforfulgt og dømt som direkte resultat av disse operasjonene.[129]

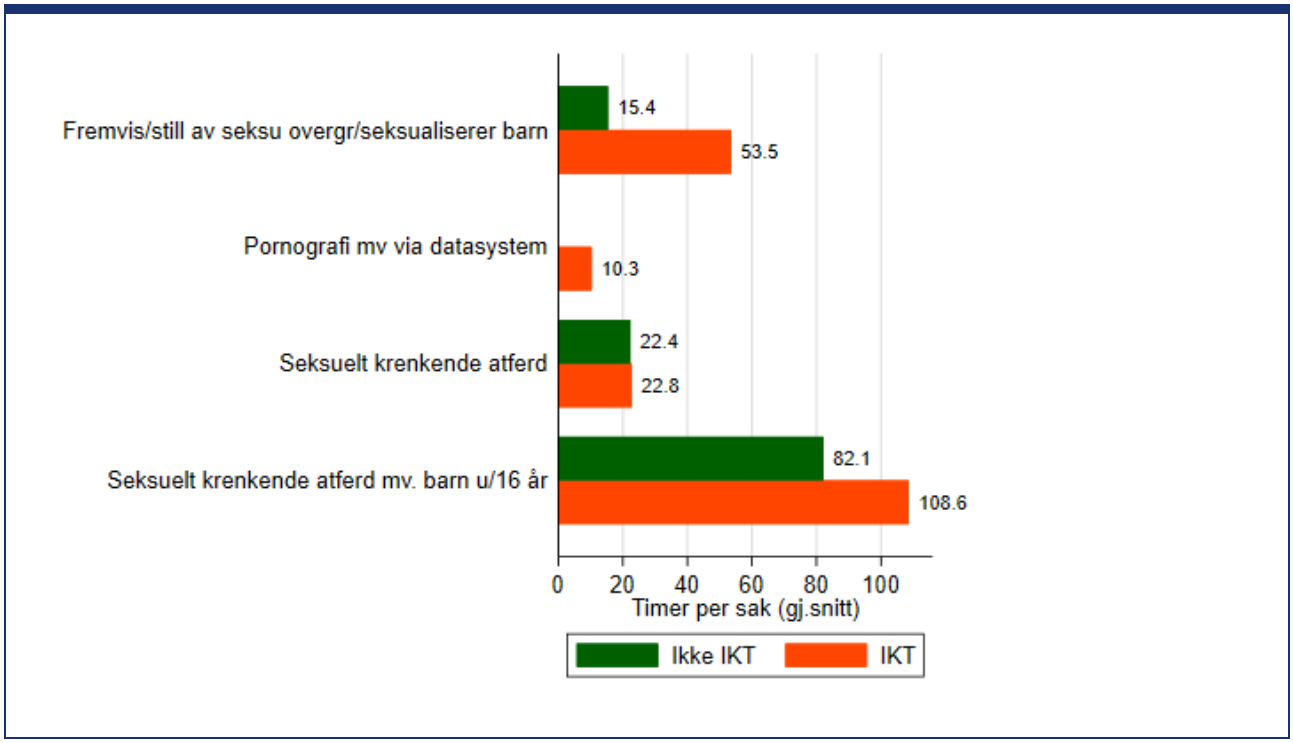
En arbeidsgruppe nedsatt av Justis- og beredskapsdepartementet gikk gjennom saksflyt i saker om vold og seksuelle overgrep mot barn i 2018–2019. Arbeidsgruppen viser til at det kan synes som om saker begått over internett prioriteres ned, fordi sakene er tidkrevende og krever omfattende gjennomgang av beslagsmateriale. Selv om distriktene er tilført kompetanse og utstyr som tidligere var forbeholdt Kripos, er det store variasjoner ifølge arbeidsgruppen. Det vises også til at evalueringer av saker viser at det i politidistriktene er manglende kapasitet, tilgjengelige ressurser samt verktøy som gjør at sikring og gjennomgang av beslagene tar lang tid. I tillegg er det varierende kompetanse, og det brukes ulik metodikk. Det har vært opp til hvert enkelt politidistrikt med forskjellige lokale løsninger, også internt i politidistriktene, om hvordan dette håndteres slik at disse sakene har fått ulik behandling og prioritet.[130] Riksadvokaten viser i intervju til at det i praksis foreligger en etterforskningsplikt i disse sakene. Manglende saksbehandlingskapasitet anses ikke som akseptabel grunn for å ikke foreta seg noe fra politi- og påtalemyndigheten.[131]

6.3.1 Tidsbruk på internettrelaterte seksuelle overgrep

Figur 6 viser gjennomsnittlig tidsbruk for IKT-kriminalitet og andre saker innen statistikkgrupper på seksuallovbruddsområdet med minst 100 IKT-kriminalitetssaker.[132]

[127] NRK (2013) *Flere pågrepet for overgrepsbilder*, artikkel publisert 5.12.2013.
[128] Bergens Tidende (tidende, 2016) *Nå må de skille fantasier fra ekte overgrep*, artikkel publisert 25.11.2016.
[129] Hordaland, Sogn og Fjordane statsadvokatembeter (2019) *Rapport etter tilsyn med Vest politidistrikt sin innsats mot vold og sedelighet/voldtekt*, rapport datert 30. oktober 2019.
[130] Justis- og beredskapsdepartementet (2019) *Rapport fra arbeidsgruppe som har sett på saksflyt i saker som gjelder overgrep mot barn, oppnevnt av Justis- og beredskapsdepartementet 26. juli 2018*, rapport publisert 13. mars 2019.
[131] Riksadvokaten (2019) *Etterforsknings- og påtalepliktens grenser i omfattende nettovergrepssaker - Et nytt straffebud om serieovergrep - mulige lovendringer*, brev til Lovavdelingen, Justis- og beredskapsdepartementet, 10. september 2019.
[132] Ved å sammenligne tidsbruken innenfor samme statistikkgruppe sikrer vi at sakene som sammenlignes har mest mulig lik alvorlighetsgrad.

Figur 6 Gjennomsnittlig tidsbruk i 2018 per sak innen seksuallovbrudd, etter straffebestemmelser/statistikkgruppe



Kilde: Politidirektoratets kapasitetsundersøkelse og identifiserte IKT-kriminalitetssaker fra maskinlæring.
Forklaring: Straffebestemmelser/statistikkgrupper med færre enn 100 IKT-kriminalitetssaker er ikke vist i figuren. «IKT» er IKT-kriminalitet og «Ikke IKT» er annen kriminalitet. I grunnlagstallene er delsaker er tatt ut og figuren inkluderer kun tidsbruk i løpet av kalenderåret 2018. Bare saker registrert i første halvdel av 2018 er inkludert.

Generelt brukes det mest etterforskningsressurser per sak innenfor straffebestemmelsene seksuelt krenkende atferd overfor barn og fremvisning/fremstilling av seksuelle overgrep mot barn eller av materiale som seksualiserer barn. Tidsbruken er spesielt høy for seksuelt krenkende atferd overfor barn. Politiet bruker i gjennomsnitt over 100 timer på å etterforske slike IKT-kriminalitetssaker, mens de i gjennomsnitt bruker 10 timer på pornografi via datasystem.

Innenfor de to statistikkgruppene som omhandler barn, og særlig for fremvisning/fremstilling av seksuelle overgrep, brukes det mer tid på IKT-kriminalitetssaker enn på andre saker.[133] Innenfor seksuelt krenkende atferd er det ingen statistisk signifikant forskjell på tidsbruk mellom IKT-kriminalitet og andre saker.[134]

Tidsbruksdataene viser at politiet bruker mer tid på IKT-kriminalitet enn på andre saker innen seksuallovbruddsområdet. Ifølge saksflytrapporten fra 2019 er internettrelaterte seksuelle overgrep mer tids- og ressurskrevende å etterforske.[135] Størrelsen på bevismaterialet som må gjennomgås, er oftere større enn hva tilfellet er i andre sedelighetssaker som skjer i det fysiske rom.[136] Gjennomgang av bevismateriale og identifisering av gjerningspersoner er også en utfordring.[137] At dette i tillegg er en høyt prioritert sakstype, kan være årsak til den høye tidsbruken.

[133] Forskjellen på gjennomsnittlig tidsbruk innenfor de to statistikkgruppene er statistisk signifikant på 5 %-nivå (i tohalet t-test for uavhengige grupper med ulik varians). Se vedlegg 4.
[134] Vi sammenligner ikke IKT-kriminalitet med andre saker innenfor pornografi via datasystem, siden bare fire saker i den statistikkgruppen er klassifisert som ikke IKT. Det er også sannsynlig at noen saker er feilklassifisert som ikke IKT-kriminalitet innenfor pornografi via datasystem og fremvisning/fremstilling av seksuelle overgrep mot barn. I den manuelle kodingen ble alle 15 sakene i disse statistikkgruppene klassifisert som IKT-kriminalitet, mens maskinlæringsmodellen klassifiserte 13 av de 15 sakene som IKT-kriminalitet.
[135] Justis- og beredskapsdepartementet (2019) *Rapport fra arbeidsgruppe som har sett på saksflyt i saker som gjelder overgrep mot barn, oppnevnt av Justis- og beredskapsdepartementet 26. juli 2018*, rapport publisert 13. mars 2019.
[136] Politidirektoratet (2017) *STRASAK-rapporten - Anmeldt kriminalitet og politiets straffesaksbehandling*, rapport utgitt 23. januar 2018.
[137] Justis- og beredskapsdepartementet, 2019 *Rapport fra arbeidsgruppe som har sett på saksflyt i saker som gjelder overgrep mot barn, oppnevnt av Justis- og beredskapsdepartementet 26. juli 2018*, rapport publisert 13. mars 2019.

6.4 Etterforskning av økonomisk IKT-kriminalitet

I det årlige mål- og prioriteringsskrivet framhever Riksadvokaten at alvorlig økonomisk kriminalitet skal prioriteres. Riksadvokaten anfører at dette normalt vil «lede til at det legges stor vekt på å bekjempe den profesjonelle kriminalitet/kriminelle nettverk og straffbare handlinger som rammer særlig utsatte grupper. Ved blant annet vinningskriminalitet bør i tillegg graden av integritetskrenkelse, størrelsen på det tap handlingen påfører fornærmede, om handlingen rammer fornærmede særlig hardt og omfanget av gjerningspersonens utbytte, stå sentralt.»[138]

Lokale straffesaksinstrukser for det enkelte politidistrikt, også kalt trekkinstruksen, bygger på nasjonal straffesaksinstruks[139], og beskriver hvordan innkomne saker skal håndteres og fordeles med hensyn til etterforskning i hvert enkelt politidistrikt. Gjennomgang av lokale straffesaksinstrukser fra fem politidistrikter viser at det i hovedsak er slik at økonomisk kriminalitet i form av bedragerier og ID-tyverier (hvor hyppigheten av IKT-kriminalitet er størst) etterforskes både av geografiske driftsenheter og fellesenheter. Alvorlige saker, gjerne over visse beløpsgrenser, etterforskes av fellesenheter. Dette er i tråd med de generelle anbefalingene som ligger i nasjonal straffesaksinstruks, som sier at de mest alvorlige sakene normalt bør behandles ved Felles enhet for etterforskning.[140]

Flere av politidistriktene peker i intervju på utfordringer med hensyn til prioritering av etterforskning av økonomisk kriminalitet. Vest politidistrikt viser til at økonomisk kriminalitet befinner seg lavt på stigen av prioriterte saker ettersom strafferammene er lavere. Strafferammer er viktig for prioritering av saker, men også for tilgang til verktøykassen av tilgjengelige etterforskningsmetoder. Der spor fører utenlands og bistand fra utenlandsk politi er nødvendig, vil heller ikke utenlandsk politi gi prioritet til saker med lave strafferammer, ifølge Vest politidistrikt. Flere politidistrikter poengterer i intervju at det er enklere å etterforske og oppklare saker der sporene ikke fører ut av landet, og at disse sakene derfor ofte prioriteres framfor saker der spor fører ut av landet. Flere understreker også at samarbeid med banker om å stoppe pengeoverføringer vektlegges, og at politiet lykkes med å stoppe pengetransaksjoner i flere saker, men oppklaring blir ikke prioritert fordi det blir for ressurskrevende å forfølge spor og gjerningspersoner utenlands.

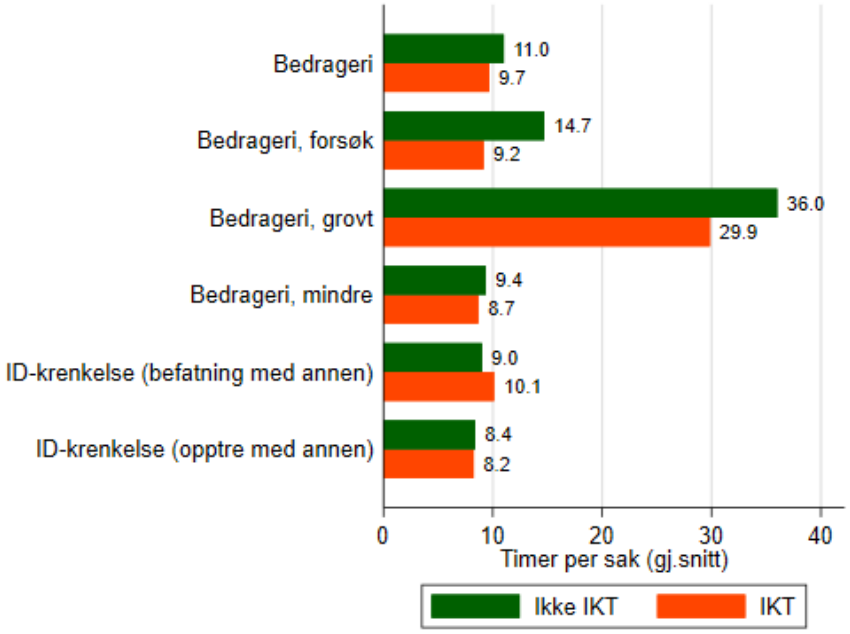
Oslo politidistrikt har mange private virksomheter i sitt ansvarsområde, og derfor også erfaring med mange typer økonomisk IKT-kriminalitet. Ifølge Geografisk driftsenhet Sentrum i Oslo politidistrikt blir bedragerisaker under en viss beløpsgrense i liten grad prioritert. Konsekvensen er at oppdagelsesrisiko blir lav for de kriminelle som utfører IKT-kriminalitet og bedragerier på internett. Etterforskning av slike saker utvikler seg ofte raskt med hensyn til kompleksitet og alvorlighet, og genererer ofte store datamengder. Fellesenhet for spesialsaker og økonomi i Oslo politidistrikt med ansvar for alvorlige, prioriterte saker viser til at et høyt antall saker blir henlagt på grunn av manglende kapasitet. Digitale verktøy brukes i flertallet av saker de har ansvar for. Seksjonen bruker etterretning og en ny saksvektingsmodell som grunnlag for prioritering av saker. Det prioriteres å gå etter hovedgjerningspersoner i alvorlige saker, saker som berører eldre mennesker og utviklingshemmede, og der hvor aktørene er profesjonelle. Mange av sakene hvor gjerningspersoner befinner seg i utlandet henlegges fordi det tar lang tid å få svar, eller fordi det ikke kommer svar, på rettsanmodninger.

6.4.1 Tidsbruk på etterforskning av økonomisk IKT-kriminalitet

Figur 7 viser gjennomsnittlig tidsbruk etter modus og statistikkgruppe innen økonomisk kriminalitet.

[138] Riksadvokaten (2020) *Mål og prioriteringer for straffesaksbehandlingen i 2020*, rundskriv 1/2020, 15. februar 2020.
[139] Den nasjonale straffesaksinstruksen skal sikre en mest mulig lik oppgaveutførelse av straffesaksarbeidet i politidistriktene. Den tar for seg roller og overordnede føringer, blant annet fordeling av saker mellom geografisk enheter og fellesenhetene. De såkalte «trekkinstruksene» er beskrevet på et overordnet nivå. Innenfor disse rammene, skal hvert politidistrikt utarbeide en lokal straffesaksinstruks..
[140] Riksadvokaten og Politidirektoratet (2017) *Nasjonal straffesaksinstruks*.

Figur 7 Gjennomsnittlig tidsbruk i 2018 per sak innen økonomisk kriminalitet, etter straffebestemmelse/statistikkgruppe*



Kilde: Politidirektoratets kapasitetsundersøkelse og identifiserte IKT-kriminalitetssaker fra maskinlæring.
Forklaring: Statistikkgrupper med færre enn 100 IKT-kriminalitetssaker er ikke vist i figuren. «IKT» er IKT-kriminalitet og «Ikke IKT» er annen kriminalitet. I grunnlagstallene er delsaker er tatt ut og figuren inkluderer kun tidsbruk i løpet av kalenderåret 2018. Bare saker registrert i første halvdel av 2018 er inkludert. 95 %-konfidensintervaller vises med sorte utstikkere.

Det brukes klart mest tid på grove bedragerier, som regnes som alvorlig kriminalitet. De øvrige sakstypene med betydelig innslag av IKT-kriminalitet har gjennomgående lav gjennomsnittlig tidsbruk i 2018. En viktig grunn er at mange saker henlegges uten etterforskning fordi kapasiteten er begrenset, og mindre alvorlige bedragerier og ID-krenkelser har lav prioritet. Innenfor disse sakstypene ble over to tredeler av sakene registrert i 2018 henlagt på grunn av manglende opplysninger om gjerningsperson (38 prosent), ikke rimelig grunn til å undersøke (18 prosent) eller manglende saksbehandlingskapasitet (16 prosent).

Politiet brukte noe færre timer i snitt på etterforskning av IKT-kriminalitet enn andre saker innenfor to av statistikkgruppene: bedrageriforsøk (5,5 timer mindre) og grovt bedrageri (6,3 timer mindre). Forskjellen er statistisk signifikant på 95 %-nivå for bedrageriforsøk, men ikke for grovt bedrageri.[141] For de fire andre statistikkgruppene i figuren er forskjellene i tidsbruk mellom IKT-kriminalitet og ikke IKT-kriminalitet liten (under 1,5 time). Likevel er forskjellen innen ordinære bedragerier – hvor det ble brukt 1,3 færre timer på IKT-kriminalitet enn på andre saker – statistisk signifikant. Generelt viser altså dataene en svak tendens til at politiet bruker mindre tid på IKT-kriminalitet enn på andre saker innenfor økonomiområdet.

6.5 Etterforskning av ren IKT-kriminalitet

Riksadvokaten har over mange år sagt at alvorlig IKT-kriminalitet i form av datainnbrudd skal prioriteres.[142]

Politidistriktene har ansvar for etterforskning av ren IKT-kriminalitet på linje med annen kriminalitet. Saksansvaret kan både ligge hos Felles enhet for etterforskning og geografisk driftsenhet, om geografisk driftsenhet har tilstrekkelig kompetanse til å etterforske en slik sak. Det er opp til Felles enhet for påtale å avgjøre hvor saksansvaret skal ligge. Ved vurderingen skal det ses hen til om saken omfattes av riksadvokatens sentrale og landsdekkende prioriteringer. I praksis innebærer dette at det i stor grad er opp til

[141] Tohalet t-test for uavhengige grupper med ulik varians. Se vedlegg 4.
[142] Riksadvokaten (2020) *Mål og prioriteringer for straffesaksbehandlingen i 2020*. Rundskriv 1/2020.

den lokale politimester og leder for Felles enhet for påtale å bestemme hvor etterforskningsansvaret for IKT-kriminalitet skal ligge, herunder alvorlig IKT-kriminalitet.[143]

Ifølge *Rammer og retningslinjer for etablering av nye politidistrikter* skal enhet for digitalt politiarbeid (DPA) «bistå med å forebygge og etterforske datakriminalitet der etterforskningen er svært teknologikrevende, og sørge for at disse håndteres med tilstrekkelig datateknisk kompetanse». I praksis utfører DPA i liten grad denne type oppgaver med unntak av saker som gjelder internettrelaterte overgrep mot barn. I gjennomsnitt brukte DPA-enhetene bare fem prosent av tiden på etterforskning av teknologikrevende datakriminalitet/IKT-kriminalitet, ifølge vår kartleggingsundersøkelse.[144] DPA-enheten som brukte mest tid på dette var Møre og Romsdal (15 prosent). Enhetene i Finnmark, Sør-Vest og Troms brukte ikke tid på dette. Fire av tolv DPA-ledere mener det er meget viktig å forebygge, etterforske og utføre analyse i datakriminalitetssaker (datainnbrudd, dataskadeverk osv.) der etterforskningen er svært teknologikrevende, eller der bruk av teknologi er en avgjørende forutsetning for å begå kriminaliteten. Tre DPA-ledere mener dette er mindre viktige oppgaver.

Større næringslivsaktører som er kontaktet i forbindelse med undersøkelsen, mener politiet i for liten grad etterforsker ren IKT-kriminalitet og økonomisk IKT-kriminalitet. Næringslivsaktørene sier tidshensyn ofte er kritisk i sakene, og at politiet ikke har kompetanse eller evne til å reagere raskt nok til å være til hjelp i kritiske situasjoner hvor for eksempel løsepengevirus setter et selskap ut av spill. Næringslivsaktørene henvender seg i stedet til private selskaper for bistand.

I intervju sier Enhet sentrum (ENS) i Oslo politidistrikt følgende om etterforskning av denne sakstypen:

> *«Datainnbrudd er krevende å etterforske for et distrikt eller for geografiske driftsenheter. Dette gjelder for alle politidistrikter. ENS mener derfor at etterforskning av slike saker bør sentraliseres til NC3 hos Kripos. Andre land har gode erfaringer med en slik organisering av etterforskningsinnsatsen på dette området. Da får man også bedre kontakt og samarbeid med sikkerhetsbransjen.»*

NC3 viser i intervju til at det ikke er tallfestede krav til antall saker som skal etterforskes og iretteføres på dette feltet, og politiet har i praksis aldri reelt prioritert dette i sin styring. En av årsakene til dette kan ifølge Kripos være at det er vanskelig å relatere seg til kriminalitet som ikke begås i det fysiske rom. Dette er saker som ses på som IKT-sikkerhetsutfordringer eller et «IKT-problem».

6.5.1 Tidsbruk på etterforskning av ren IKT-kriminalitet

Gjennomsnittlig tidsbruk på etterforskning av rene IKT-kriminalitetssaker er omtrent på nivå med gjennomsnittlig tidsbruk for annen økonomisk IKT-kriminalitet. For datainnbruddssaker var den 15,7 timer og for uberettiget befatning med tilgangsdata 11,4 timer per sak i 2018.[145]

Variasjonen i tidsbruk innenfor dette kriminalitetsområdet er stor, vel å merke. Mens politiet i 90 prosent av sakene brukte under 14 timer per sak, brukte de 570 timer på en sak registrert i første halvdel av 2018.[146] Av den totale tidsbruken gikk derfor omtrent 20 prosent av tidsbruken på ren IKT-kriminalitet registrert første halvår 2018 til denne ene saken. Dette er i tråd med politiets uttalelser om at ren IKT-kriminalitet kan være veldig krevende å etterforske, og de har bare kapasitet til å etterforske et mindretall av sakene.

[143] Riksadvokaten og Politidirektoratet (2017) *Nasjonal straffesaksinstruks*. Datert 8. mai 2020.
[144] Tidsbruk på slike saker i politidistriktene varierer mellom 0 og 15 prosent.
[145] Bare saker registrert første halvår 2018 er med i denne beregningen.
[146] Etterforskning av en datainnbruddssaker i Vest politidistrikt.

7 Oppklaring av IKT-kriminalitet

Oppklaring av sakene er et sentralt mål for politiets etterforskning. I dette kapittelet viser vi hvor stor andel av IKT-kriminaliteten som oppklares generelt og innen de tre sakstypene internettrelaterte seksuelle overgrep, økonomisk IKT-kriminalitet og ren IKT-kriminalitet, sammenlignet med annen kriminalitet som ikke er IKT-kriminalitet.

Totalt sett oppklares en mindre andel IKT-kriminalitetssaker enn andre saker som ikke er IKT-kriminalitet innen samme kategori, men oppklaringsandel varierer med sakstype. Internettrelaterte overgrep har en høy oppklaringsandel, økonomisk IKT-kriminalitet oppklares i liten grad og ren IKT-kriminalitet har den laveste oppklaringsandelen av de utvalgte sakstypene.

7.1 Oppklaringsprosent som resultatindikator

Oppklaringsprosent har vært beregnet årlig siden 1950-årene, og Politidirektoratet redegjør årlig for endringer i oppklaringsprosenten i gjennomgangen av straffesaksstatistikken.[147] Oppklaringsprosenten beregnes vanligvis med utgangspunkt i påtaleavgjorte saker i det enkelte år. Av 316 377 lovbrudd som ble påtaleavgjort i 2019, regnes 149 497 som oppklart. Det gir en oppklaringsprosent på 50,9.

Saker regnes som *oppklart* blant annet ved påtaleavgjørelse om tiltalebeslutning, forelegg eller henleggelser som følge av forhold som tilsier at saken skal frafalles. Saker regnes som *ikke oppklart* hvis de henlegges på grunn av manglende opplysninger om gjerningsperson, mangel på bevis, bevisets stilling, foreldelse eller mangel på saksbehandlingskapasitet. Hvilke påtaleavgjørelser som inngår i oppklarte og ikke oppklarte saker, er gjengitt i vedlegg 7.

Det er vanlig å skille mellom *negative* påtaleavgjørelser (henleggelser) og *positive* påtaleavgjørelser, hvor beslutningen bygger på at vilkårene for straffeansvar er til stede. De *positive* avgjørelsene består av påtaleunnlatelse, forelegg, siktelse og tiltale. De *negative* avgjørelsene er ulike former for henleggelse som kan skyldes manglende opplysninger om gjerningsperson, bevisets stilling, manglende saksbehandlingskapasitet, mangel på bevis, osv.[148]

Forskning viser at oppklaringsprosenten varerier med type lovbrudd og sakstype. Lovbrudd som avdekkes av politiet og hvor gjerningspersonen tas i det lovbruddet begås (kontrollavdekket kriminalitet), er naturligvis enklere å oppklare enn lovbrudd hvor gjerningspersonen er ukjent. Følgelig bør man være varsom med å sammenligne oppklaringsprosenten på tvers av sakstyper.

En annen utfordring ved å bruke oppklaringsprosent som indikator på resultater i etterforskningsarbeidet er at nevneren i brøken er antall anmeldte saker – en størrelse som påvirkes også av andre faktorer enn politiets effektivitet. Dersom en kriminalitetstype anmeldes i mindre grad på grunn av samfunnsmessige eller teknologiske endringer, kan det føre til en økning i oppklaringsprosent over tid uten at politiets etterforskningsarbeid endrer seg. En annen ulempe er at politiet selv kan påvirke oppklaringsprosenten for eksempel ved å unnlate å anmelde lovbrudd som det ikke er kapasitet til å etterforske.[149]

Disse utfordringene er spesielt problematiske om man vil sammenligne måloppnåelse på tvers av distrikter eller over tid. I denne undersøkelsen undersøker vi derimot resultatene av politiets etterforskningsarbeid på nasjonalt nivå for saker registrert i 2018. For det formålet kan oppklaringsprosenten, på tross av sine svakheter, være en nyttig indikator.

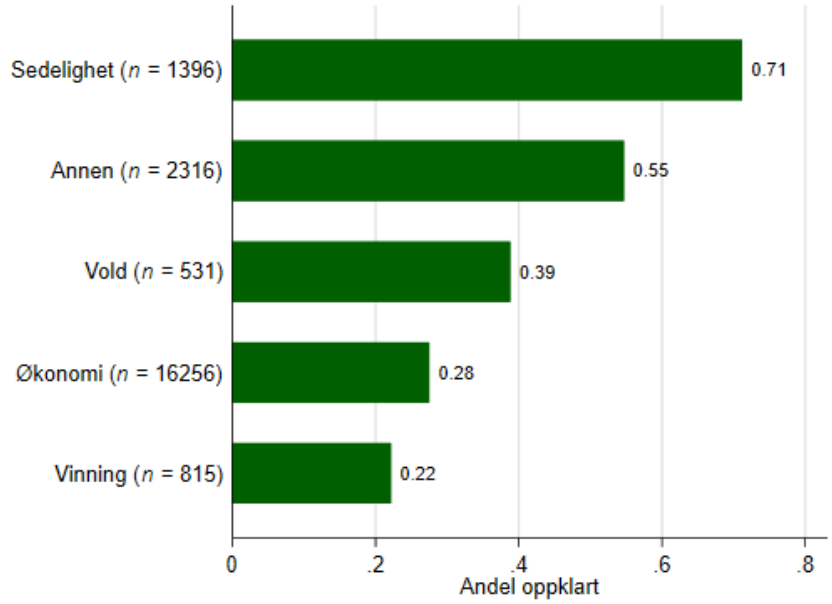
---

[147] Politidirektoratet (2020) *Strasak-rapporten – Anmeldt kriminalitet og politiets straffesaksbehandling 2019*.
[148] Riksadvokaten (2014) *Forslag til endringer i reglene om påtalekompetanse ved ikrafttredelse av ny straffelov*.
[149] En måte å unngå disse problemene på kunne vært å se på antall oppklarte saker i en tidsperiode relativt til ressursinnsats. Det er dessverre ikke mulig i denne undersøkelsen, siden det ikke finnes data på antall årsverk og andre ressurser som brukes spesifikt på IKT-kriminalitet. Se for eksempel Riksrevisjonen, 2000, *Riksrevisjonens undersøkelse vedrørende måloppnåelse i politi- og lensmannsetaten* (Dokument 3:10) og Maslov, Anton, 2015. *Measuring the Performance of the Police: The Perspective of the Public. Public* Safety Canada.

7.2 Oppklaring av IKT-kriminalitetssaker

Andelen oppklarte IKT-kriminalitetssaker har ikke vært kjent fordi politiet ikke hatt oversikt over hvilke saker som er IKT-kriminalitet. Ved å koble våre data på IKT-kriminalitet med politiets data for påtaleavgjørelser kan vi undersøke dette.

Figur 8 Oppklaringsandel for IKT-kriminalitetssaker registrert i 2018 etter kriminalitetstype*



Kilde: Politidirektoratet (STRASAK) og Riksrevisjonen
* Kriminalitetstyper med færre enn 100 IKT-kriminalitetssaker registrert i 2018 er utelatt.

Figuren ovenfor viser andel oppklarte saker innen kriminalitetstyper med minst 100 IKT-kriminalitetssaker registrert i 2018. Sakene er registrert i 2018, men kan være avgjort mellom 2018 og august 2020.[150]

Oppklaringsprosenten er høyest innen sedelighetskriminalitet. Det henger antakelig sammen med at internettrelaterte seksuelle overgrep er høyt prioritert. Som vi så i forrige kapittel brukte politiet i gjennomsnitt klart mest tid på sakene i denne kategorien. En annen mulig årsak til den høye oppklaringsprosenten er at politiet i stor grad avdekker og anmelder kriminalitet selv på dette området. Ifølge politidistriktene som er intervjuet, anmelder politiet hovedsakelig alvorligere saker hvor gjerningsperson og fornærmede er kjent, noe som bidrar til høyere sannsynlighet for oppklaring.

Oppklaringsprosenten for «annen» kriminalitet (55 prosent) er høy i forhold til den gjennomsnittlige tidsbruken, som var nest lavest av de fem kategoriene.[151] Flertallet av IKT-kriminalitetssaker innen denne kategorien dreier seg om hensynsløs atferd, brudd på kontaktforbud eller krenkelse av privatlivets fred.

Innenfor vold er 39 prosent av sakene oppklart. De aller fleste IKT-kriminalitetssakene i denne kategorien er trusler av ulike slag.

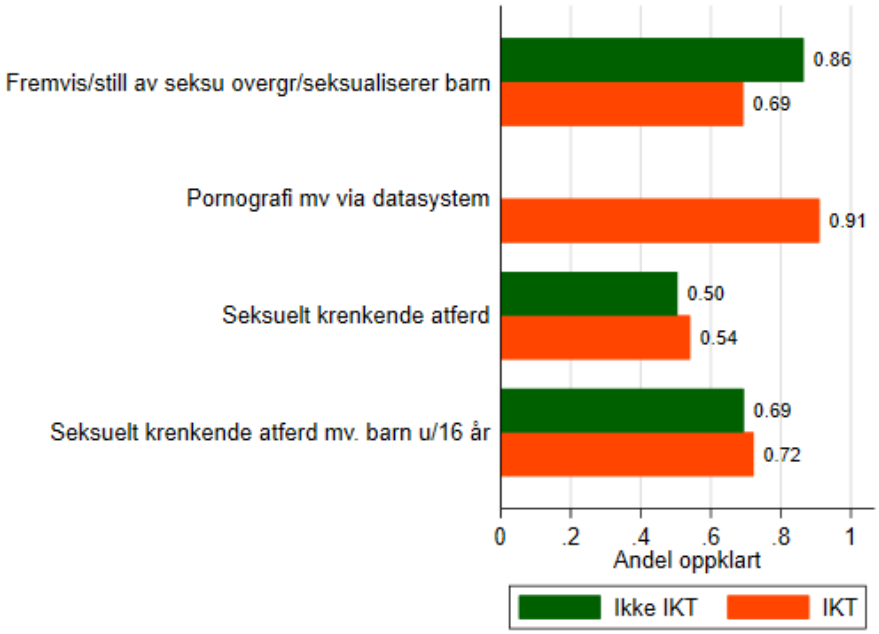
Oppklaringsprosenten er lavest innenfor økonomi (28 prosent) og vinning (22 prosent). En viktig grunn er antakelig at mange av disse sakene, som bedragerier og ID-krenkelser, er lavt prioritert og blir henlagt uten etterforskning. For IKT-kriminalitetssakene som oppklares innen disse områdene, brukes det i snitt relativt lite tid, noe som tyder på at mange av sakene ikke er veldig krevende å etterforske.[152]

[150] Under en prosent av sakene manglet avgjørelse ved tidspunktet for datauttrekket. Vi utelater disse sakene fra beregningen.
[151] Estimert gjennomsnittlige tidsbruk for IKT-kriminalitetssaker registrert og oppklart i 2018 innen disse statistikkgruppene er 10,5 timer. Til sammenligning er tilsvarende tidsbruk for oppklarte internettrelaterte seksuelle overgrep på 83,6 timer.
[152] For økonomisakene som ble registrert og oppklart i 2018, brukte politiet i snitt 16,5 timer, og for tilsvarende vinningssaker brukte de i snitt 11,4 timer.

7.2.1 Oppklaring av internettrelaterte seksuelle lovbrudd

Av alle anmeldte saker utgjorde seksuallovbruddene 2,6 prosent i 2018 og 2,2 prosent i 2019 (mot 1,6 prosent i 2015). Mange av seksuallovbruddene avdekkes og anmeldes av politiet selv. De blir også høyt prioritert: Om lag 15 prosent av politiets etterforsknings- og påtaleressurser ble brukt på disse sakene i 2017 ifølge Kapasitetsundersøkelsen. Politiet oppklarte 64 prosent av alle seksuallovbrudd i 2018 og 63 prosent i 2019.

Figur 9 Oppklaringsandel for seksuallovbrudd registrert i 2018 etter straffebestemmelse/statistikkgruppe



Kilde: STRASAK og identifiserte IKT-kriminalitetssaker fra maskinlæring.
Forklaring: Straffebestemmelser/statistikkgrupper med færre enn 100 IKT-kriminalitetssaker registrert i 2018 er ikke vist i figuren. «IKT» er IKT-kriminalitet og «Ikke IKT» er annen kriminalitet. Oppklaringsdata er trukket ut 26. august 2020. Saker som ikke var avgjort innen det tidspunktet, holdes utenfor beregningen.

Figuren over viser andelen av seksuallovbruddsakene registrert i 2018 som er oppklart for statistikkgruppene med mest IKT-kriminalitet. For fremstilling/fremvisning av seksuelle overgrep mot barn og pornografi mv via datasystem oppklares et stort flertall av sakene (henholdsvis 80 og 91 prosent). Oppklaringsprosenten er noe lavere for seksuelt krenkende atferd overfor barn (71 prosent) og lavest for seksuelt krenkende atferd (51 prosent).

Forskjellene i oppklaring gjenspeiler ikke forskjellene i gjennomsnittlig tidsbruk mellom statistikkgruppene: pornografi mv. via datasystem, som har høyest oppklaringsprosent, har lavest tidsbruk. En mulig årsak kan være at politiet i større grad mottar anmeldelser fra publikum innenfor seksuelt krenkende atferd enn innenfor statistikkgruppene som omhandler overgrepsmateriale, hvor politiet sannsynligvis selv anmelder de fleste sakene. Politiet kan derfor ha mindre mulighet til å unngå at saker som er krevende å oppklare, eller som de mangler kapasitet til å etterforske, blir anmeldt innenfor førstnevnte kategori.[153]

Generelt er det relativt små forskjeller i oppklaring mellom internettrelaterte seksuelle overgrep og andre saker innenfor samme statistikkgruppe. For seksuelt krenkende atferd (mot barn) er oppklaringsandelen veldig lik for IKT-kriminalitet (internettrelaterte seksuelle overgrep) og for andre saker. For fremstilling/fremvisning av seksuelle overgrep mot barn er oppklaringsandelen 17 prosentpoeng lavere for IKT-kriminalitet sammenlignet med andre saker.[154]

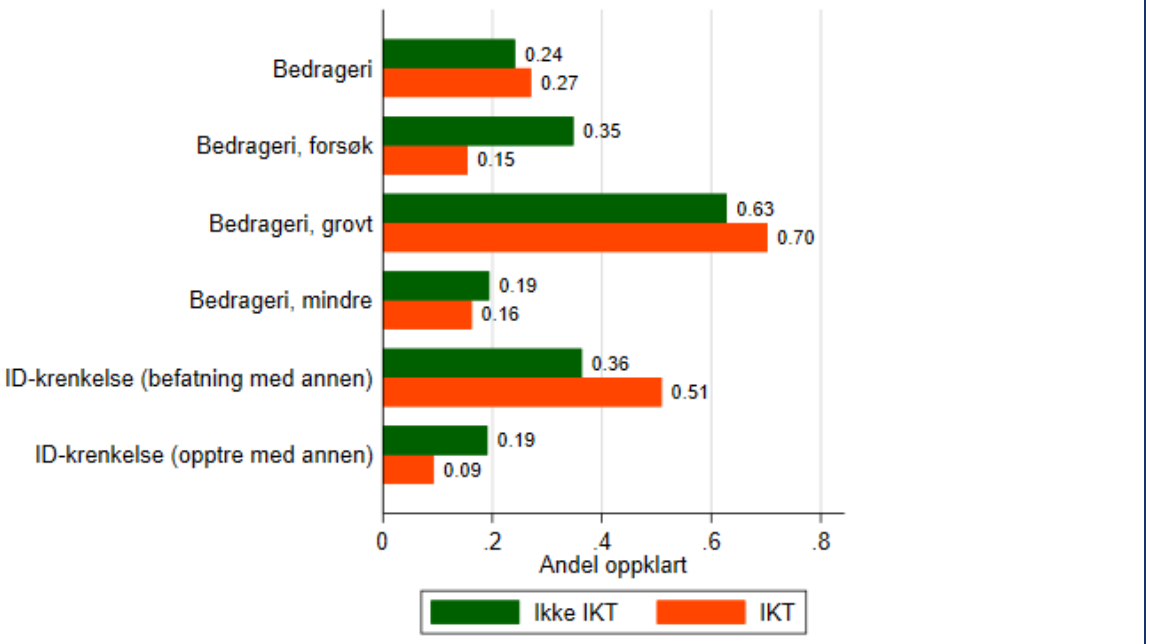
[153] Politiet registrerer ikke om anmeldelser kommer fra publikum eller fra politiet selv, så det er vanskelig å undersøke denne hypotesen grundig.
[154] Denne forskjellen er statistisk signifikant (p<0,001) i test av forskjell mellom andeler i to uavhengige grupper («prtest» i Stata). (Se vedlegg 5). Men en usikkerhet særlig knyttet til denne statistikkgruppen er muligheten for at en del faktiske ikt-kriminalitetssaker er feilklassifisert.

7.2.2 Oppklaring av økonomisk IKT-kriminalitet

Økonomisk kriminalitet utgjorde ni prosent av alle anmeldelser i 2018 og 2019. Oppklaringsprosenten er generelt lav på dette området sammenlignet med de fleste andre kriminalitetstyper. I 2018 var den på 38 prosent for økonomisk kriminalitet samlet sett.[155]

Figur 10 viser andelen økonomisaker registrert i 2018 som er oppklart etter statistikkgruppe.

Figur 10 Oppklaringsandel for økonomisk kriminalitet registrert i 2018 etter statistikkgruppe



Kilde: STRASAK og identifiserte IKT-kriminalitetssaker fra maskinlæring.
Forklaring: Straffebestemmelser/statistikkgrupper med færre enn 100 IKT-kriminalitetssaker registrert i 2018 er ikke vist i figuren. «IKT» er IKT-kriminalitet og «Ikke IKT» er annen kriminalitet. Oppklaringsdata er trukket ut 26. august 2020. Saker som ikke var avgjort innen det tidspunktet, holdes utenfor beregningen.

Oppklaringsprosenten varierer mye mellom straffebestemmelsene. Samlet sett er den klart høyest for grovt bedrageri (66 prosent), og lavest for ID-krenkelse ved opptreden med annens identitet (15 prosent). Kategorien med klart flest saker, ordinære bedragerier, har en relativt lav oppklaringsprosent på 26 prosent samlet sett. Disse forskjellene reflekterer i stor grad forskjellene i gjennomsnittlig tidsbruk på saker i de ulike statistikkgruppene. Unntaket er ID-krenkelse ved opptreden med annens identitet, hvor oppklaringsandelen er høyere enn forventet fra tidsbruksestimatet.

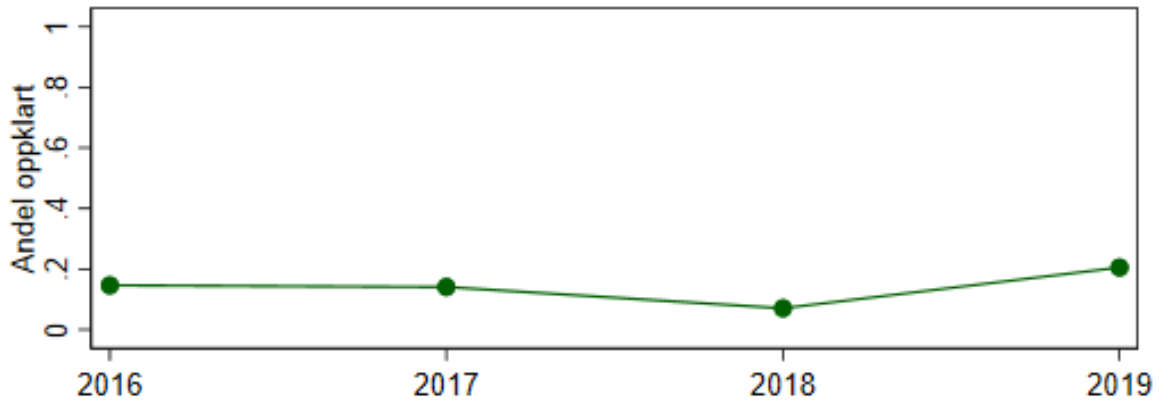
Det framkommer ikke noe tydelig mønster om vi sammenligner oppklaring for IKT-kriminalitet og andre saker innenfor samme statistikkgruppe. IKT-kriminaliteten har noe høyere oppklaringsprosent enn andre saker innenfor ordinære bedragerier (3 prosentpoeng høyere), grove bedragerier (8 prosentpoeng høyere), og ID-krenkelse ved befatning med annens identitet har (15 prosentpoeng høyere). IKT-kriminaliteten har derimot lavere oppklaringsprosent enn andre saker innenfor bedrageriforsøk (19 prosentpoeng mindre), mindre bedragerier (3 prosentpoeng mindre) og ID-krenkelse ved opptreden med annens identitet (10 prosentpoeng mindre). Forskjellene innenfor alle statistikkgruppene unntatt mindre bedragerier er signifikante på 95-prosentnivå.[156]

[155] Politidirektoratet (2019) *STRASAK-rapporten - Anmeldt kriminalitet og politiets straffesaksbehandling*, rapport utgitt 28. februar 2020.
[156] Test av forskjell mellom andeler i to uavhengige grupper («prtest» i Stata). Se Vedlegg 5.

7.2.3 Oppklaring av ren IKT-kriminalitet

Ren IKT-kriminalitet utgjør en liten andel av totalt antall anmeldte saker. I perioden 2016–2019 er det registrert til sammen 1634 saker på de to aktuelle statistikkgruppene.

Figur 11 Påtaleavgjørelser for ren IKT-kriminalitet etter registreringsår (N = 1634)*



Kilde: STRASAK, Politidirektoratet
* Oppklaringsdata er trukket ut 26. august 2020. 34 saker som ikke var avgjort innen det tidspunktet, holdes utenfor beregningen.

Figuren ovenfor viser hvor stor andel av de rene IKT-kriminalitetssakene som er oppklart etter registreringsår. Oppklaringsprosenten er gjennomgående lav sammenlignet med de fleste andre kriminalitetstyper, og varierer mellom 7 prosent (i 2018) og 21 prosent (i 2019).

Flertallet av sakene henlegges enten med henvisning til manglende opplysning om gjerningsperson (48 prosent), manglende saksbehandlingskapasitet (14 prosent) eller ikke rimelig grunn til å undersøke (12 prosent). Tiltalebeslutning forelå i seks prosent av sakene, hvorav over halvparten av disse var vedleggssaker til en større sak etterforsket av Vest politidistrikt i 2018.

8 Politiets kapasitet til å avdekke og oppklare IKT-kriminalitet

Kapitlet belyser politiets kapasitet (årsverk og antall ansatte) til etterforskning av IKT-kriminalitet i politidistrikter og særorgan. Etterforskningskapasitet er avgjørende for å kunne oppklare kriminalitet. Vi ser også på etterforskningskapasiteten innen de tre dybdeområdene. Behov for styrket kapasitet (årsverk og antall ansatte) til avdekking og etterforskning av IKT-kriminalitet er omtalt i en rekke rapporter og utredninger siden 2012. IKT-kriminalitet er ofte tid- og ressurskrevende å etterforske, og forutsetter kapasitet innen sikring og analyse av digitale beslag. Kapasiteten er styrket ved opprettelse av DPA i politidistriktene og NC3 hos Kripos, men kapasiteten utfordres av at IKT-kriminaliteten i samme periode har økt.

8.1 Kapasitet til etterforskning av IKT-kriminalitet

I perioden fra 2012 til 2020 er det pekt på et økt behov for styrket kapasitet innen etterforskning av IKT-kriminalitet i en rekke rapporter og utredninger. Økningen i ressurskrevende saker som internettrelaterte seksuelle overgrep og annen IKT-kriminalitet fører til at etterforskningen blir mer ressurskrevende. Behov for økt kapasitet som følge av økningen i IKT-kriminalitet er omtalt i en arbeidsgrupperapport fra Politidirektoratet fra 2012[157], Politidirektoratets datakrimstrategi fra 2015[158], Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet fra 2015[159], særorganutredningen fra 2017[160], Nasjonal strategi for digital sikkerhet fra 2019 og senest i Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden*. I særorganutredningen fra 2017 vises det til at ledelsen både i særorganer og politidistrikter, samt politiansatte på alle nivåer, sier det er behov for et betydelig løft i politiets kapasitet og kompetanse på området. Særorganutvalget viser til at et voksende etterslep på oppklaring av IKT-relaterte saker kan svekke tilliten til politiet og at flere velger å la være å anmelde slike saker.

I *Handlingsplan for løft av etterforskningsfeltet* fra mai 2016 ble det pekt på at etterforskningsfeltet generelt syntes å være nedprioritert som følge av oppmerksomheten om beredskap etter hendelsene 22. juli 2011.[161] Det ble derfor besluttet å gjennomføre en kapasitetsvurdering av etterforskningsfeltet. Kapasitetsvurderingen kom i 2019.[162]

Tabell 2 Sammenligning av tilgjengelige årsverk til straffesaksbehandlingen i 2013 og 2018

Rolle	Årsverk 2013	Årsverk 2018
Rendyrket etterforsker	2 380	2 248
Kriminaltekniker/dataetterforsker*	270	276
Patruljestilling / kombinert stilling	1 170	1 359
Sivil etterforsker	140	134
Sum etterforsker	3 960	4 016
Påtalejurist	759	782
Sivil straffesaksstøtte	N/A	491
Totalt	8 679	9 306

Kilde: Politidirektoratet (2019) *Kapasitetsvurdering av etterforskningsområdet*.
* - Ansatte i enheter med ansvar for kriminalteknikk og/eller e-spor.

Kapasitetsvurderingen viser at det har vært en nedgang i antall årsverk som har etterforskning som hovedoppgave fra 2013 til 2018, men at det skjer mer etterforskning fra patruljer og ansatte i kombinerte stillinger (orden/etterforskning). Utviklingen i antall årsverk for kriminalteknikere/dataetterforskere og sivile

[157] Politidirektoratet (2012) *Politiet i det digitale samfunnet – en arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på Internett.*
[158] Politidirektoratet, 2015 *Datakrimstrategien.*
[159] Justis- og beredskapsdepartementet (2015) *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, lansert 26. juni 2015.
[160] NOU 2017:11 *Bedre bistand. Bedre beredskap. Fremtidig organisering av politiets særorganer.*
[161] Politidirektoratet og Riksadvokaten (2016) *Handlingsplan for løft av etterforskningsfeltet.*
[162] Politidirektoratet (2019) *Kapasitetsvurdering av etterforskningsområdet.*

etterforskere er samlet uendret. Av stillingene norsk politi ble tilført i denne perioden, har derfor få havnet på etterforskning. Den samlede andel av ressurser til etterforskning i politiet er derfor redusert sammenlignet med andre oppgaver i denne perioden.

Det er iverksatt flere tiltak for å styrke politiets kapasitet for bekjempelse av IKT-kriminalitet. Tiltakene ble innført som følge av Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet fra 2015 og gjennom implementeringen av nærpolitireformen. Det er særlig opprettelsen av NC3 og enheter for digitalt politiarbeid i politidistriktene som trekkes fram som sentrale tiltak. Men også andre tiltak er iverksatt, blant annet:

- Fra Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet:
  - Øke antall politiutdannede fra 1,7 per 1000 innbygger til 2 per 1000 innbygger, hvor en andel av den generelle styrkingen skulle gå til å øke kapasiteten på området IKT-kriminalitet.
  - Etablere et pilotprosjekt i Oslo politidistrikt for utvikling av etterforskning og forebygging av IKT-kriminalitet som ikke faller inn under NC3.
- Nærpolitireformen:
  - Etablering av fagkontakter for digitalt politiarbeid

Hvilken betydning disse tiltakene har hatt for kapasitet til etterforskning av IKT-kriminalitet omtales i punktene under.

8.1.1 Mål om 2 politiårsverk per 1000 innbygger innen 2020

Målet om 2 politiårsverk per 1000 innbygger innen 2020 ble lansert i 2008.[163] Dette målet har ligget fast siden 2008, senest bekreftet i Meld. St. 29 (2019-2020) *Politimeldingen – et politi for fremtiden*. I Justis- og beredskapsdepartementets IKT-kriminalitetsstrategi vises det til at en andel av økningen i antall politiutdannede må brukes til å øke kapasiteten på området IKT-kriminalitet.

Tabell 3 Bemanningsutviklingen i politiet fra 2007 til 2019

År	Jurister	Politiutdannede	Administrative/sivile	Sum	Politiårsverk per 1000 innbygger
2007	628	8195	3684	12497	1,8
2019	906	10097	5976	16979	1,94
Sum endring	278	1902	2292	4482	
Prosentvis endring	**+44 %**	**+23 %**	**+62 %**	**+ 36 %**	

Kilde: Politidirektoratet, Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden*.

Den totale økningen i årsverk fra 2007 til 2019 er 4482 årsverk, flest årsverk er kommet til innen administrative og sivile stillinger. Antallet politiårsverk per 1000 innbygger er styrket til 1,94 ved utgangen av 2019. Hvor stor andel av denne styrkingen som har gått til styrking av innsatsen mot IKT-kriminalitet er vanskelig å anslå. Etterforskning av internettrelaterte seksuelle overgrep er styrket. Kapasiteten er styrket ved at kapasitet innen andre områder er overført til etterforskning av denne typen saker. I tillegg er NC3 styrket med 45 årsverk ved årsskiftet 2020/2021.

Som del av IKT-kriminalitetsstrategien (tiltak 10) fikk Politidirektoratet i oppdrag av departementet å utarbeide en plan for hvordan politiets kapasitet til å håndtere flere, større og mer kompliserte saker innen IKT-kriminalitet kunne styrkes, inkludert hvordan noe av stillingsveksten i politiet kunne disponeres for dette formålet. Planen for styrking av etterforskningskapasiteten innen IKT-kriminalitet ble oversendt Justis- og beredskapsdepartementet i februar 2016.[164] Planen skisserer en oppbemanning av Kripos, politidistriktene og Politihøgskolen med totalt 101 nye årsverk i perioden 2017–2019. Ifølge departementet var det særlig etableringen av et nasjonalt senter for å bekjempe IKT-kriminalitet (NC3) som ble framhevet i planen fra

[163] Politidirektoratet (2008) *Politiet mot 2020 – Bemannings- og kompetansebehov i politiet.*
[164] Politidirektoratet (2016) *Svar på oppdragsbrev 15/2015 - JDs strategi for å bekjempe IKT-kriminalitet*, brev til Justis- og beredskapsdepartementet 15. februar 2016.

Politidirektoratet. Slik NC3 beskrives i planen samsvarer i stor grad med NC3 slik det er under etablering per i dag ifølge departementet.

I særorganutredningen vises det til at målet om to politiårsverk per 1000 innbyggere står i konflikt med Justis- og beredskapsdepartementets strategiske mål om at Norge skal være ledende på området IKT-kriminalitet i Europa.[165] Ifølge særorganutvalget krever IKT-kriminalitetsområdet tverrfaglig kompetanse innen blant annet informatikk, inkludert dataingeniører, i tillegg til politiutdannede. Målet om to per 1000 forskyver ressursinnsatsen på bekostning av innsatsen mot IKT-kriminalitet. Det reduserte handlingsrommet dette gir politiet er også pekt på i Meld. St. 29 (2019–2020). Mål om to årsverk per 1000 er likevel opprettholdt, samtidig med en ny hovedprioritering om å rekruttere flere med annen fagbakgrunn, blant annet datateknologi og informasjonssikkerhet for å møte endringene i kriminalitetsbildet.

8.1.2 Etablering av Nasjonalt cyberkrimsenter (NC3) hos Kripos

Kripos' forslag om etablering av NC3 ble oversendt Justis- og beredskapsdepartementet 9. september 2015, og oppdraget om opprettelse ble gitt av Politidirektoratet 13. juni 2018.[166] I oppdragsbrevet ved opprettelsen skriver Politidirektoratet at senteret skal bli et nasjonalt kunnskaps- og kompetansesenter innen teknologirelaterte politioppgaver med omkring 200 medarbeidere, og skal være etablert ved utgangen av 2021. NC3 ble offisielt åpnet 25. januar 2019.[167]

Ved opprettelsen i januar 2019 ble 82 allerede ansatte i Kripos overført til senteret. Per juni 2020 er det om lag 100 ansatte. Ved utgangen av 2020 vil det være om lag 125 ansatte. Ifølge NC3 er ambisjonene om 200 ansatte innen utgangen av 2021 nedjustert til 150 ansatte innen utgangen av 2022. I intervju opplyser Politidirektoratet at dette var nødvendig på bakgrunn av den økonomiske situasjonen i etaten, justert ambisjonsnivå i flerårig virksomhetsplan og behovet for styrking av distriktenes kapasitet på dette området. Likevel påpeker direktoratet at politiet innenfor dagens rammer prioriterer styrking av NC3 med om lag 130 millioner kroner over perioden 2019-2022, på bekostning av andre oppgaver.

Ved saksinntak hos Kripos legges det vekt på om saken vil medføre utvikling av nye metoder og bruk av ny teknologi for å understøtte etaten for de mest spesialiserte og geografiuavhengige sakene. Ofte velges prinsipielle saker som er ressurs- og kompetansekrevende, ofte med omfattende internasjonale forgreininger. Dette er i tråd med mandatet som tilsier at Kripos gjennom egen etterforskning bidrar til å utvikle kompetanse og metoder som senere kommer politidistriktene til gode gjennom bistand.[168] NC3s kapasitet brukes i hovedsak til etterforskning av egne saker og til etterforskningsbistand til politidistriktene. Etterforskningskapasiteten er ifølge NC3 begrenset. I juni 2020 var størsteparten av kapasiteten satt av til to saker: bistand i etterforskning av en forsvinningssak på Lørenskog og etterforskning av datainnbruddet hos Hydro. NC3 vurderer at med nåværende antall ansatte har de kapasitet til å ta 1–1,5 Hydro-sak i året. Antall utstedte etterforskningsordre i seksjon for datakrimetterforskning hos NC3 viser også at antallet etterforskningsordre innen IKT-kriminalitet ligger på i gjennomsnitt 2 saker per år.

[165] NOU 2017:11 *Bedre bistand. Bedre beredskap.*
[166] Politidirektoratet, 2018 *Oppdragsbrev 1 – NC3, brev til Kripos* 13. juni 2018.
[167] Politiet, 2019 *Nasjonalt cyberkrimsenter (NC3)*, artikkel aksessert 29. juni 2020.
[168] NOU 2017:11 *Bedre bistand. Bedre beredskap.*

Tabell 4 Utstedte etterforskningsordre innen IKT-kriminalitet hos Kripos

År	Antall etterforskningsordre
2016	2
2017	2
2018	4
2019	2
Per andre tertial 2020	2

Kilde: Kripos, NC3.

NC3 viser til at de trenger en viss kapasitet til egne saker for læring. Økt kapasitet hos NC3 skal dekke bistand til distriktene og egne saker. Ideelt sett skal NC3 bruke 1/3 på etterforskning av saker, 1/3 på bistand til distriktene og 1/3 på etterretning og metodeutvikling. Generelt sett mener NC3 at det er et for stort gap mellom kompetanse/kapasitet og politiets behov for håndtering av IKT-kriminalitet. Intensjoner og ambisjoner er gode, men det mangler prioritering og bevilgninger for å møte endringer kriminalitetsbildet.

NC3 oppgir i intervju at all kapasitet brukes inn til å gi bistand til distrikter og etterforske egne saker. NC3 forsøker å bygge opp en kapasitet for å kunne utarbeide egne trusselvurderinger og etterretning basert på kunnskap om norsk kontekst, men foreløpig har det ikke vært kapasitet til dette. NC3 er ikke kjent med at Felles cyberkoordineringssenter (FCKS)[169] har gjennomført trusselvurderinger for IKT-kriminalitet som de fikk ansvar for fra og med 2019. Denne typen kunnskap er heller ikke etterspurt av Justisdepartementet eller Politidirektoratet fra NC3. Distriktene produserer heller ikke etterretning på dette området, hvilket er en utfordring for NC3 ved utarbeidelse av trusselvurderinger og analyser av kriminalitetsutfordringer innen IKT-kriminalitetsområdet. Politiets nasjonale trusselvurderinger har inntil nå ikke inneholdt informasjon om IKT-kriminalitet, noe NC3 mener den burde ha hatt. Det er under produksjon en ny nasjonal trusselvurdering per august 2020 som vil inneholde informasjon om IKT-kriminalitet.

Justis- og beredskapsdepartementet peker i intervju på at FCKS bidrar til felles situasjonsbilde og deling av relevant kunnskap om både trussel, risiko og ikke minst koordinering av tiltak mellom de fire deltakerne, herunder Kripos. Både Kripos og ØKOKRIM lager også egne vurderinger som også er relevante i dette bildet. Deltakerne i FCKS er også knyttet til det nasjonale cyberkoordineringssenteret (NCSC), som blant annet bidrar til kunnskap om digitale trusler (og IKT-kriminalitet) i en offentlig-privat ramme.

8.1.3 Enhet for digitalt politiarbeid (DPA) i politidistriktene

De første spesialistmiljøene for etterforskning av IKT-kriminalitet og sikring av elektroniske spor ble etablert på 2000-tallet. Hvordan kapasiteten har utviklet seg fram til dags dato er ikke mulig å fastslå eksakt. I 2012 oppgis det i en rapport fra Politidirektoratet at Oslo hadde 14 dataetterforskere med planer om å utvide til 20. Politidistrikter utenfor Oslo hadde fra ingen til tre.[170] I 2015 viser Lysneutvalget til at Oslo politidistrikts enhet for datakriminalitet hadde 20 ansatte, og Kripos hadde i underkant av 70 ansatte i seksjoner relatert til IKT-kriminalitet (125 ansatte ved utgangen av 2020).[171] I rapportene vist til over påpekes det at manglende kapasitet fører til store restanser av ubehandlede saker med elektroniske spor innen alle kriminalitetstyper og til at politiet i liten grad etterforsker IKT-kriminalitet.

I forbindelse med nærpolitireformen, som ble iverksatt 1. januar 2016, ble alle politidistrikt pålagt å etablere DPA som nå er etablert i alle politidistrikt. Dataetterforskere og andre med relevant kompetanse befinner seg i DPA. Vi har gjennomført en kartlegging av antall ansatte i DPA i 2018 og 2019, jamfør tabell 5.

[169] FCKS er et samarbeidsorgan bestående av representanter fra Nasjonal sikkerhetsmyndighet (NSM), Etterretningstjenesten, PST og Kripos, og skal blant annet bidra til at det foreligger oppdatert og helhetlig trussel- og risikobilde som grunnlag for beslutninger.
[170] Politidirektoratet (2012) *Politiet i det digitale samfunnet – en arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på Internett.*
[171] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn.*

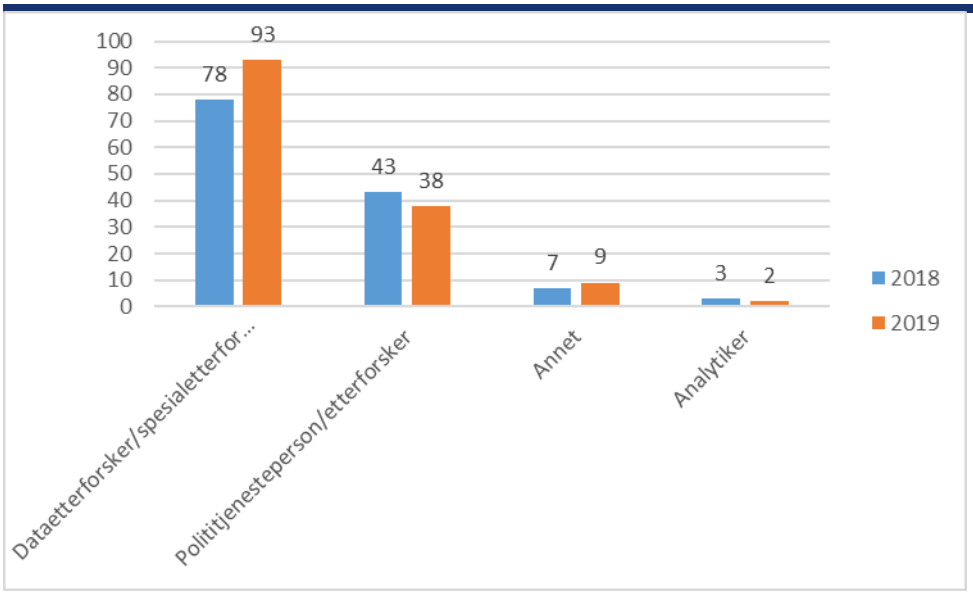
Tabell 5 Antall ansatte og stillingshjemler i DPA i politidistriktene i 2018 og 2019

Distrikt	Ansatte 2018	Ansatte 2019
Agder	3	3
Finnmark	6	6
Innlandet	7	10
Møre og Romsdal	5	9
Nordland	4	4
Sør-Vest	9	9
Sør-Øst	14	14
Troms	6	7
Trøndelag	8	8
Vest	10	9
Øst	4	9
Oslo	55	54
Sum	131	142
Totalt antall politistillinger	9904	10 132

Kilde: Riksrevisjonen

Kartleggingen viser at det var 131 ansatte i DPA i 2018 og 142 i 2019. Oslo politidistrikt er distriktet med flest DPA-ansatte (54 i 2019), Agder har færrest (3 i 2019). Fra 2018 til 2019 økte antallet ansatte med 11. I andel av det totale antallet politistillinger i politidistriktene utgjorde DPA-ansatte 1,38 prosent i 2018 og 1,46 prosent i 2019.[172] De ansatte fordeler seg på et fast sett av roller med hovedansvar som skal ivaretas av funksjonen DPA. De mest brukte er dataetterforsker/spesialetterforsker og polititjenesteperson/etterforsker. De få som er registrert under Annet er ledere for DPA. Kun enkelte distrikt har analytikere, og ingen har tatt i bruk rollen spesialist innen datakriminalitet.

Figur 12 Antallet ansatte i DPA i 2018 og 2019 fordelt på stillingskategori



Kilde: Riksrevisjonen

[172] Politidirektoratet (2019) *Ressursanalyse for 2019 – utgifter og bemanning i politiet*.

Intervjuer med politidistriktene og kartleggingsundersøkelsen til DPA-lederne viser at det har vært en betydelig økning i antall arbeidsoppgaver de senere årene uten at kapasiteten har økt tilsvarende. Ettersom elektroniske spor blir relevante på stadig flere områder, og som følge av utviklingen i IKT-kriminalitet øker behovet for bistand fra DPA. Elektroniske spor og internettrelaterte etterforskningsskritt utnyttes innen mange sakstyper, ikke bare innen IKT-kriminalitet. Det er derfor ikke mulig å sette likhetstegn mellom antall ansatte i DPA og kapasitet til etterforskning av IKT-kriminalitet ettersom en betydelig andel av kapasiteten utnyttes til etterforskning av saker som ikke er IKT-kriminalitet. De fleste politidistrikter har ikke statistikk for disse oppgavene, og kun fire av tolv distrikter rapporterer om utførte aktiviteter eller oppnådde resultater til ledelsen i eget politidistriktet. Noen distrikter har lokal statistikk, men nasjonalt mangler det oversikt over hvordan arbeidsmengden for DPA har utviklet seg.

Tabell 6 Gjennomsnittlig tidsbruk i DPA

Arbeidsoppgaver	Andel av arbeidstiden som medgår til å utføre denne oppgaven i DPA
Sikring av elektroniske spor	**28,9 %**
Teknisk analyse	**21,6 %**
Håndtering av digitale beslag (inkl. frakt av beslag)	**13,6 %**
Drift av maskinpark/utstyr/programvare, administrasjon osv.	**10,3 %**
Rådgivning	**11,6 %**
Annet (opplæring, kurs osv.)	**7,4 %**
Etterforskning av teknologikrevende IKT-kriminalitet	**6,6 %**

Kilde: Riksrevisjonen, kartleggingsundersøkelse til DPA-ledere.

I gjennomsnitt bruker DPA-ansatte nesten 75 prosent av tiden til sikring, analyse, håndtering av beslag, og drift av teknisk utstyr og programvare. Kun 6,6 prosent går til etterforskning av teknologikrevende IKT-kriminalitet. I Riksrevisjonens kartleggingsundersøkelse svarer kun 3 av 12 DPA-ledere at forebygging og etterforskning av datakriminalitet (datainnbrudd, dataskadeverk, etc.) er meget viktig. Flertallet mener andre oppgaver som sikring og gjennomgang av elektroniske spor, analyse av beslag og rådgivning er viktigere oppgaver for DPA.

Politidirektoratet har i perioden 2017–2019 gjennomført en kapasitetskartlegging av etterforskningsressursene i politidistriktene og hva de brukes til. Kartleggingen viser også hvordan dataetterforskernes tidsbruk fordeler seg på bistand til ulike sakskategorier.[173] Dataetterforskerne yter mest bistand innen seksuallovbrudd (44 %), vold (23 %), narkotika (8 %), vinning (6 %), økonomi (6 %), arbeidsmiljø, miljø, trafikk, skadeverk, og annet (7 %). Dette bekreftes i en faggrupperapport om datatekniske undersøkelser og internettrelatert etterforskning fra 2019.[174] DPA-ledere i 11 av 12 distrikter oppgir at sedelighetssaker, og saker med nedlasting av overgrepsmateriale, er høyest prioritert.

Politidirektoratet er kjent med at prioritering av DPAs kapasitet til de alvorligste sakene får konsekvenser for mindre alvorlige saker, og at det går utover for eksempel oppklaring av økonomisk kriminalitet. Dette er en kjent utfordring, og er tatt opp i satsingsforslagene til Justis- og beredskapsdepartementet i forbindelse med budsjettbehandlingen. Både DPA og etterforskning generelt må styrkes for å få gjort noe med dette.

Riksadvokaten har inntrykk av at DPAs kapasitet i stor grad benyttes til alvorlige sedelighets- og voldssaker, dette i samsvar med utviklingen innen saksporteføljen for IKT-kriminalitet. Ved knapphet på ressurser mener riksadvokaten at dette en riktig prioritering, samtidig som det er uheldig dersom «ren» IKT-kriminalitet ikke blir prioritert. Løsningen på dette er dels tilførsel av mer ressurser, og dels hvordan man håndterer de mest omfattende nettovergrepssakene. Et nytt lovforslag, som Riksadvokaten har oversendt Justis- og

[173] Politidirektoratet (2019) *Kapasitetsvurdering av etterforskningsområdet*.
[174] Politidirektoratet (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning*, faggrupperapport levert Politidirektoratet i 9. september 2019.

beredskapsdepartementet går ut på å etterforske og iretteføre de mest omfattende sakene på en smartere og mer effektiv måte. Dette vil kunne frigi ressurser, som kan brukes på andre saker.[175]

8.1.4 Pilotprosjekt om digitalt politiarbeid i Oslo politidistrikt

Et av tiltakene for å styrke kapasiteten i politidistriktene i departementets strategi har vært å etablere et pilotprosjekt i Oslo politidistrikt. Pilotprosjektet hadde som formål å vurdere hvordan politiet kan utvikle etterforskning og forebygging av IKT-kriminalitet som ikke faller inn under et nasjonalt senter. Prosjektet ble gjennomført i perioden 2015–2017 og resulterte i en sluttrapport.[176] Sluttrapporten ble sendt på høring til politidistriktene, Kripos og Politihøgskolen. Det ble laget en anbefaling som gikk via Politidirektoratet til Justis- og beredskapsdepartementet i mars 2018. [177]

Oslo politidistrikt har omorganisert sitt digitale politiarbeid slik at kapasitet innen digitalt politiarbeid nå er representert på tre nivåer i organisasjonen. Fagkontakter er tilgjengelig for bistand i førstelinje, lokale DPA er integrert i hver geografiske driftsenhet og en egen seksjon for digitalt politiarbeid og innovasjon er etablert under felles kriminalenhet. Etableringen av DPA og fagkontakter for digitalt politiarbeid ble innført før pilotprosjektet ble ferdig, slik at dette vanskelig kan ses på som et resultat av pilotprosjektet.

Prosjektet anbefalte 14 tiltak hvorav flere angår politidistriktenes kapasitet. En rekke ulike utfordringer forbundet med politidistriktenes håndtering av endringer i kriminalitetsbildet i retning mer IKT-kriminalitet omtales i sluttrapporten og i anbefalingen til departementet. Det pekes blant annet på behov for å styrke kapasitet i enheter for digitalt politiarbeid som har stor underkapasitet.

Ifølge Politidirektoratet er ikke anbefalingene fra pilotprosjektet fulgt opp spesifikt ettersom det de siste årene har vært lagt mye vekt på politireformen. Enkelte av tiltakene er vurdert som lavt prioritert, og anbefalingene må også ses i lys av faggrupperapporten om datatekniske undersøkelser og internettrelatert etterforskning som anbefalte 120 forbedringer på området. Flere av tiltakene er ifølge direktoratet også adressert gjennom andre tiltak, for eksempel gjennom politireformen.

8.2 Kapasitet til etterforskning av internettrelaterte seksuelle overgrep

Det har vært en sterk økning i antall saker innen sedelighetsområdet, og særlig innen alvorlige seksuallovbrudd mot barn under 16 år som er en høyt prioritert saksgruppe og krever betydelige ressurser til etterforskning og straffesaksbehandling.[178] Seksuallovbrudd utgjør kun 2–3 prosent av anmeldelsene politiet mottar årlig, men beslaglegger ifølge Politidirektoratets kapasitetsundersøkelse i 2018 nesten 15 prosent av etterforskningskapasiteten.

I en inspeksjon av etterforskning i Øst politidistrikt i 2018 ble det oppgitt at 2/3 av etterforskningsressursene til seksuallovbrudd hos fellesenhetene ble brukt til to store etterforskningsoperasjoner av nettovergrep.[179] Politidistriktene som er intervjuet bekrefter at nettovergrepssakene legger beslag på store deler av etterforskningskapasiteten, og etterforskningene organiseres ofte som etterforskningsoperasjoner på grunn av omfanget. For påtalemyndigheten innebærer sakene ofte et stort antall fornærmede, betydelige mengder bevismateriale og ulike typer lovbrudd i hovedsak dekket av kapittel 26 i straffeloven. Tilsvarende er arbeidet for etterforskere ressurskrevende med forberedelse av saker, gjennomføring av beslag, og avhør av gjerningsperson og fornærmede. Ettersom fornærmede ofte kan være barn under 14 år forutsetter dette gjennomføring av tilrettelagte avhør. For teknikere på enhet for digitalt politiarbeid kan ofte omfanget av beslaglagt materiale være krevende å få oversikt over og analysere.

Oslo politidistrikt behandler flest seksuallovbrudd av alle politidistriktene (14 prosent av alle seksuallovbrudd i 2019, 13 prosent i 2018). I en inspeksjonsrapport fra Oslo statsadvokatembete fra 2019 av sedelighetsetterforskning i Oslo politidistrikt omtales kapasiteten slik:[180]

> *«Det er totalt 52 årsverk på seksjonen per i dag og seksjonen har over tid opplevd en stor utskiftning av etterforskere. Etter planen skal seksjonen være 60 ansatte. Som påpekt i fjorårets rapport mistet*

[175] Riksadvokaten (2019) *Etterforsknings- og påtalepliktens grenser i omfattende nettovergrepssaker - Et nytt straffebud om serieovergrep - mulige lovendringer*, brev til Lovavdelingen, Justis- og beredskapsdepartementet, 10. september 2019.
[176] Oslo politidistrikt (2018) *Digitalt politiarbeid – Anbefaling*, datert 23. januar 2018.
[177] Oslo politidistrikt (2018) *Digitalt politiarbeid – Oppsummering etter høringsrunde*.
[178] Politidirektoratet (2019) *Kapasitetsvurdering av etterforskningsområdet*, s. 34.
[179] Oslo statsadvokatembeter (2018) Rapport etter inspeksjon/tilsyn av spesialseksjon – påtale og felles enhet for etterretning og etterforsking – Øst politidistrikt, brev til Øst politidistrikt, 14. mai 2018.
[180] Oslo statsadvokatembeter (2019) *Inspeksjonsrapport Oslo politidistrikt 2019 – Felles enhet for etterretning og etterforskning (FEE).*

seksjonen 30 medarbeidere på to 2 år. Høsten 2018 har ytterligere 9 sluttet. Dette innebærer at man i mange saker har måttet bytte etterforskere og således mistet kontinuiteten på etterforskningen. Videre medfører nyansettelser at det må brukes tid og ressurser på opplæring, samt at nødvendigvis produksjonen påvirkes. Seksjonen har imidlertid tro på at situasjonen er i ferd med å stabilisere seg og har rekruttert flere.»

Fellesenhet for etterforskning av seksuallovbrudd i Oslo politidistrikt viser til i intervju at det har vært en stor økning i nettovergrep de siste seks årene, og antallet saker som håndteres av seksjonen har økt med 75 prosent. 80 av 350 saker under etterforskning ved fellesenheten var nettovergrepssaker. Seksjonen gjør harde prioriteringer blant de prioriterte nettovergrepssakene. Saker hvor gjerningsmann har tilgang til barn prioriteres foran andre saker. Seksjonen har vært nødt til å henlegge en del prioriterte saker av hensyn til kapasitet. Det er bare få år siden antallet tilgjengelige etterforskere på disse sakene ble fordoblet. Likevel utfordres seksjonen på kapasitet og mange saker blir liggende lenge. Seksjonen har derfor vanskeligheter med å nå frister for behandling av voldtektssaker (130 dager).

Vest politidistrikt har hatt en av de største nettovergrepssakene som er etterforsket i et politidistrikt – Dark room-saken. Enheten i Vest politidistrikt som har ansvar for etterforskning av alvorlige seksuelle overgrep viser i intervju til at de ikke har kapasitet til å etterforske alle saker de gjøres kjent med. De tvinges til å prioritere de mest alvorlige sakene. Påtalejuristene som arbeider med de samme sakene har også høy arbeidsbelastning, de er få i spesialseksjonen for vold og seksuelle overgrep, og gjennomtrekken var på 26 prosent i 2018. Politidistriktet har i 2020 besluttet å styrke etterforskningskapasiteten på området med 15 nye stillinger.

Å rekruttere og beholde etterforskningskompetanse til etterforskning av alvorlige sedelighetssaker er en utfordring for flere politidistrikter. Stort arbeidspress, sviktende lønnsutvikling, høy gjennomtrekk og for lite tid til å treffe påtaleavgjørelser har vært påpekt som utfordringer med hensyn til å beholde og utvikle etterforskningskompetanse og -kapasitet.[181] Dette har vært et tema over flere år og skyldes blant annet at det er få incentiver for politiutdannede å velge en karrierevei innen etterforskning av sedelighetssaker. Dette bekreftes i intervjuer med politidistriktene. I flere distrikter utfordres i tillegg eksisterende kapasitet av andre oppgaver. Det er oppgaver som årlig obligatorisk opplæring, deltakelse på felles straffesaksinntak, avgivelse av ressurser til andre prioriterte saker på andre saksområder, osv. I enkelte distrikter har i tillegg etterforskere dobbeltroller og deltar i vakt- og turnustjeneste, og har obligatorisk opplæring for innsatsmannskaper.

8.3 Kapasitet til etterforskning av økonomisk IKT-kriminalitet

Økonomisk kriminalitet kan være skatte- og avgiftsunndragelser, korrupsjon, konkurskriminalitet, brudd på konkurranselovgivningen, økonomisk utroskap, bedrageri og underslag, brudd på regnskaps- og bokføringsbestemmelser, misbruk av offentlige støtteordninger, fiskerikriminalitet, innsidehandel, markedsmanipulasjon, osv.[182] Etterforskningskapasiteten skal med andre ord dekke en hel rekke spesialområder som dekker en rekke straffebestemmelser i straffeloven og særlovgivning på området.[183] I tillegg er antallet samarbeidspartnere med kontrollmyndighet stort og innbefatter private aktører, offentlige tilsyn/myndigheter (for eksempel Finanstilsynet, skatteetaten, tollvesenet, NAV og fiskerimyndighetene), i tillegg til bostyrere, kommune, departementer, interesseorganisasjoner, ØKOKRIM og andre kontrollorganer som er tillagt særskilt ansvar innen økonomi, arbeidsmiljø og miljø.

Politidirektoratets kapasitetsundersøkelse viser at 8,4 prosent av etterforskningskapasiteten i politidistriktene i 2018 ble brukt på etterforskning av økonomisk kriminalitet. Økonomisk kriminalitet utgjorde om lag 10 prosent av alle registrerte saker i 2018. Antallet estimerte årsverk til etterforskning av økonomisk kriminalitet i politidistriktene var 426 av totalt 5288 årsverk tilgjengelig til etterforskning i 2018.[184]

Politiets innsats mot økonomisk IKT-kriminalitet som bedragerier og ID-tyverier foretas i hovedsak av etterforskere med ansvar for økonomisk kriminalitet i geografiske driftsenheter og fellesenheter. Politidistriktene som er intervjuet, viser til at et vidt spekter av økonomisk kriminalitet skal dekkes med en

[181] Justis- og beredskapsdepartementet (2019) *Rapport fra arbeidsgruppe som har sett på saksflyt i saker som gjelder overgrep mot barn, oppnevnt av Justis- og beredskapsdepartementet 26. juli 2018*, rapport publisert 13. mars 2019.
[182] NOU 2017: 11 *Bedre bistand. Bedre beredskap.*
[183] For eksempel forurensningsloven, kulturminneloven, arbeidsmiljøloven, brann og eksplosjonsvernloven, åndsverksloven, helsepersonelloven, skattebetalingsloven, skatteforvaltningsloven, folketrygdloven, verdipapirhandelloven, aksjeloven, allmennaksjeloven.
[184] Politidirektoratet (2019) *Kapasitetsvurdering av etterforskningsområdet*.

begrenset etterforskningskapasitet. Fellesenhet for etterforskning av økonomisk kriminalitet og spesialsaker i Oslo politidistrikt peker på at saksfeltet er svært bredt, og krever spesialkompetanse på mange områder. Det er også stor forskjell på de IKT-relaterte saker som for eksempel kjærlighetssvindel, NAV-bedragerier, ID-tyverier, phishing, investeringsbedragerier, arbeidsmiljøkriminalitet, tyveri fra tidligere arbeidsgiver, skimming av bankkort osv. Fellesenheten med ansvar for økonomisk kriminalitet har ikke kapasitet og kompetanse til å etterforske mer enn noen få alvorlige IKT-kriminalitetssaker årlig, og prioriterer kun de alvorligste sakene som for eksempel rettes mot viktige institusjoner som storting og regjering. Et høyt antall saker blir henlagt på grunn av manglende kapasitet. Det forebyggende arbeidet blir derfor ansett som viktig og næringslivskontaktene har en viktig rolle her. Fra Oslo politidistrikt pekes det på at næringslivsaktører (telekomleverandører, banker og finansinstitusjoner) som mener politiet oftere må slå ned på slik kriminalitet, selv har et ansvar for å iverksette skadebegrensende tiltak.

De fire øvrige politidistriktene som er intervjuet, viser at de alvorlige bedragerisakene fellesenhetene har ansvar for er ressurskrevende å etterforske, ofte med gjerningsperson i utlandet, og kan være teknologisk krevende med kryptering og avanserte svindelmetoder. Tidlig innsats for å stoppe pengeoverføringer i samarbeid med bankene prioriteres i de fire distriktene. Når pengene er stoppet, blir sakene ofte henlagt fordi det anses som uforholdsmessig ressursbruk å oppklare sakene. Politidistriktene som er intervjuet, peker på manglende nasjonal koordinering av politiets innsats i slike saker og mener særorgan som Kripos og ØKOKRIM bør ta en større del av ansvaret her. Politidistriktene viser videre til at lav kapasitet og antallet saker som skal etterforskes tvinger politiet til å bli reaktivt og saksorientert. Det mangler også etterretning, analyser og vurderinger av bedragerifenomener som treffer mange distrikter samtidig.

En annen utfordring politidistriktene peker på, er avhengigheten av enheten for digitalt politiarbeid (DPA). Sakene inneholder som regel alltid elektroniske spor, og bistand fra DPA er avgjørende for framdrift i sakene. DPAs kapasitet er imidlertid prioritert inn i de alvorligste sakene som seksuallovbrudd, drap og andre alvorlige volds- og narkotikasaker. Bistandsanmodninger til DPA kan bli liggende i mange måneder, noe som kan påvirke etterforskningen og muligheter for oppklaring negativt.

Rekruttering av etterforskere til økonomisk kriminalitet oppgis også som en utfordring i flere av politidistriktene som er intervjuet. Ordenstjeneste og kvalifisering som innsatspersonell gir høyere lønn enn hva som tilbys i etterforskningsstillinger. Utfordringen varierer mellom politidistriktene som intervjues, men særlig de større politidistriktene opplever dette som et problem. Fellesenheten med ansvar for etterforskning av økonomisk kriminalitet i Oslo politidistrikt viser til at konkurranse fra særorgan også bidrar til utfordringer med hensyn å opprettholde en stabil etterforskningskapasitet.

Faktaboks 4 Eksempler på ressurskrevende etterforskningsoperasjoner av direktørsvindel – Operasjon Magna, Raven og Jackpot

Operasjon Magma, direktørsvindel, 2019–2020[185]

I oktober 2019 anmeldte to ansatte i det italienske energiselskapet Edison Norge direktørsvindel på 150 millioner kroner. Etterforskere ved Sør-Vest politidistrikt fulgte elektroniske spor til Israel, og ved hjelp av israelsk politi ble fire gjerningsmenn pågrepet. Parallelt med etterforskningen av denne saken i Sør-Vest ble Oljedirektoratet lurt til å utbetale en regning på 17,6 millioner kroner og tre andre bedrifter ble utsatt for direktørsvindel i millionklassen. Gjerningspersonene som utførte svindlene, var de samme i alle sakene.

Operasjon Raven, direktørsvindel, 2018–2019[186]

I mai 2018 anmeldte en ideell organisasjon et tilfelle av direktørsvindel i Oslo politidistrikt. Senere samme år ble også Regjeringsadvokaten via falske e-poster utsatt for et forsøkt på direktørsvindel fra samme gjerningspersoner. Gjennom etterforskningen som pågikk i et år fra mai 2018, oppdaget Oslo

[185] Stavanger Aftenblad, 2020 *Topplederen i et energiselskap i Stavanger og en forelsket kvinne fra Jæren havnet i det utspekulerte spillet*, publisert 21. februar 2020.
[186] Aftenposten, 2019 *Norsk politi mener å ha avslørt storsvindlere fra Nigeria*, publisert 28. juli 2019.

politidistrikt 26 forsøk på, og gjennomførte, bedragerier i Norge og oppklaring av flere hundre saker i andre europeiske land. Fire personer ble til slutt siktet i Nigeria for til sammen 12,7 millioner kroner.

Operasjon Jackpot, direktørsvindel, 2016–2017[187]

I januar 2016 anmeldte administrerende direktør for et datterselskap direktørsvindel på 500 millioner kroner i Oslo politidistrikt hvorav omtrent 100 millioner anses som tapt. Gjennom falske eposter og telefoner klarte gjerningsperson å lure en ansatt til å overføre pengene. Omfattende etterforskningssamarbeid i Oslo politidistrikt, og samarbeid med Kripos, Europol og FBI, ledet til at 12 gjerningspersoner ble identifisert og pågrepet i Israel. Gruppen hadde gjennomført lignende bedragerier i en rekke andre land og det var utstrakt samarbeid med politimyndigheter i disse landene. Det ble også samarbeidet med norske bedrifter, Cert-miljøer i Norge og Telenor.

Kilde: Stavanger Aftenblad, Aftenposten, VG.

8.4 Kapasitet til etterforskning av ren IKT-kriminalitet

Ren IKT-kriminalitet i form av datainnbrudd, befatning med tilgangsdata og andre teknologisk krevende saker blir som omtalt bl.a. i kapittel 6 og 7 i liten grad etterforsket og oppklart. Kapasiteten til etterforskning av slike saker er begrenset, og det er kun noen få distrikter og NC3 som har kapasitet til å etterforske alvorlige saker på dette området. Ren IKT-kriminalitet som har vinning som hensikt, vil i tillegg dele mange av de generelle kapasitetsutfordringene som er omtalt for øvrig i kapittel 8.

[187] VG, 2017 *Historien om «Operasjon Jackpot» – politi spilte direktør og rundlurte svindlere*, publisert 20. mars 2017.

9 Politiets kompetanse til å avdekke og oppklare IKT-kriminalitet

Dette kapittelet omhandler kompetansesituasjonen i politiet og hvordan den påvirker mulighetene for oppklaring av IKT-kriminalitet. Kapittelet beskriver flere kompetansetiltak, i tillegg til basiskompetanse i førstelinjen, spesialkompetanse hos politi og sivilt tilsatte, og påtalemyndighetens kompetanse. Det gis også en nærmere beskrivelse av kompetansen innen dybdeområdene internettrelaterte seksuelle overgrep, økonomisk og ren IKT-kriminalitet. Til tross for flere tiltak for å styrke kompetansen, er kompetanse generelt en utfordring for de som først kommer i befatning med sakene og for påtalemyndigheten. Det mangler i tillegg kompetanse innen etterforskning av teknologisk avansert IKT-kriminalitet.

9.1 Kompetanse om IKT-kriminalitet

Etterforskning og oppklaring av IKT-kriminalitet forutsetter kompetanse om kriminaliteten og metodene som brukes, for å avdekke og etterforske sakene. Det er påpekt i flere rapporter og utredninger at politiets kompetanse må styrkes, og det er iverksatt tiltak for å styrke kompetansen.

I Meld. St. 29 (2019–2020) vises det til at IKT-kriminalitet utfordrer politiets kompetanse til å analysere risikobildet, forebygge hendelser, etterforske og iretteføre straffesaker. I meldingen vises det derfor til at politiet må styrke egen kompetanse særlig på tre områder:

- **Basiskompetanse** hos operativt personell innen digitalt politiarbeid, og prinsipper for bevisintegritet, sporbarhet i beviskjeden og etterprøvbarhet.
- **Spesialkompetanse**, knyttet til oppgaver som datatekniske undersøkelser, taktisk etterforskning, digital etterretning, politiarbeid på internett mv.
- **Påtalemyndighetens kompetanse** – politiadvokater og statsadvokater har behov for kunnskap om elektroniske spor mv.

I meldingen pekes det også på at politiet i tillegg må rekruttere personer med annen faglig bakgrunn, blant annet innenfor tekniske fag og økonomi og regnskap, som kan supplere sin utdanning med elementer fra politifagene.

9.2 Basiskompetanse

I Lystadrapporten fra 2017 ble politiets kompetansebehov de neste tiårene utredet. Utvalget understreket behovet for at alle som er involvert i straffesaksbehandlingen må ha grunnleggende forståelse for hvordan datamaskiner, datasystemer og datanettverk fungerer.[188] Manglende kompetanse blant generalistene om IKT-kriminalitet og digitalt politiarbeid i politiet er påpekt i en rekke rapporter over mange år.[189] Det påpekes at det er for stor avstand mellom kompetansen og forventninger til utførelse. Dette bekreftes også av de intervjuede politidistriktene. Selv om studentene kan ha høyere digital kompetanse enn tidligere, krever etterforskning og digitalt politiarbeid mer kompetanse på området enn studentene får gjennom grunnutdannelsen fra Politihøgskolen. Flere av politidistriktene opplever det som en utfordring at det kreves betydelig med opplæring av nyutdannede etterforskere. I en fagrapport om datatekniske undersøkelser og internettrelatert etterforskning fra 2019 pekes det på at fraværet av en systematisk tilnærming til opplæring av generalisten på etterforskningsfeltet på dette området er urovekkende.[190]

Politihøgskolen er den sentrale institusjonen for utdanning i politi- og lensmannsetaten. Bachelor i politiutdanning kvalifiserer for tjeneste i norsk politi. Utdanningen bygger på at polititjenestepersoner skal være generalister. Det vil si at de skal få grunnleggende kunnskaper innen politiets forebyggende, kriminalitetsbekjempende og trygghetsskapende arbeid. I løsning av oppgavene skal generalisten ha

[188] Politidirektoratet (2017) *Politi- og lensmannsetatens kapasitets- og kompetansebehov de kommende ti-årene*, 15. desember 2017.
[189] Politidirektoratet (2012) *Politiet i det digitale samfunnet: En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett.;* Politidirektoratet (2015) *Datakrimstrategien*; Politiet, 2019, *Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning. 9. september 2019.*
[190] Politiet (2019) *Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning,* 9. september 2019.

kompetanse til å utføre politiarbeid på generalistnivå, foreta helhetsvurderinger og trekke inn relevant spesialkompetanse og samarbeidspartnere ved behov.[191]

Bachelor i politivitenskap er treårig og innebærer 180 studiepoeng. Emnet «Digitalt politiarbeid» (10 studiepoeng) ble en del av bachelorutdanningen fra august 2014.[192] Sentrale tema er grunnleggende teknologiforståelse, datasikkerhet og datakriminalitet, etterforskning på internett og etterforskning av elektroniske spor. De første studentene som tok kurset, ble uteksaminert i 2017. Fra og med 2019 er antallet studiepoeng økt til 15. Studenter som fullfører utdannelse med det nye kurset på 15 studiepoeng, vil første gang uteksamineres i 2022.[193]

9.2.1 Obligatorisk årlig opplæring innen etterforskningsfeltet

Obligatorisk årlig opplæring innen etterforskningsfeltet (OÅO) ble innført i studieåret 2018–2019 som del av etterforskningsløftet. Hensikten er økt kvalitet og effektivitet i etterforskningen, og er obligatorisk for de som deltar i etterforskningen, både for politi, påtalemyndighet og sivile. OÅO er ikke obligatorisk for politi som jobber patrulje og utfører straksetterforskning på stedet, eller de som jobber på felles straffesaksinntak (FSI). Programmet er ment å skulle være et første steg på veien mot en definert minimumsstandard for tjenesteutførelse innen etterforskning i norsk politi.[194] Politidirektoratet står fritt til å bestemme innholdet i det årlige programmet. Per i dag har digitalt politiarbeid ikke en fast plass på kursplanen.[195] Sikring av digitale spor var en del av opplæringen våren 2019. Når programmet er gjennomført skal 4500 etterforskere ha gjennomgått totalt 40 timer undervisning, hvorav 8 timer om elektroniske spor. Etter kurset i elektroniske spor skal de ha opparbeidet kunnskap og ferdigheter innen gjennomgang av databeslag. Både påtalejurister og politifaglige etterforskningsledere får kun 4 timers undervisning innen samme tematikk, med kun en teoretisk oversikt over temaet.[196]

Flere politidistrikter ble intervjuet i forbindelse med en faggrupperapport om datatekniske undersøkelser og internettrelatert etterforskning i 2019. Politidistriktene mener OÅO ikke virker å være et tilstrekkelig tiltak med tanke på å dekke avstanden mellom forventning og faktisk kompetanse.[197] Politidistriktene som er intervjuet i forbindelse med denne undersøkelsen har ulike erfaringer med OÅO. Noen distrikter mener OÅO og styrking av digitalt politiarbeid i grunnutdannelsen fra Politihøgskolen bidrar til å heve kompetansenivået på etterforskningsfeltet. Andre peker på at OÅO ikke nødvendigvis vil medføre kompetanseheving på digitalt politiarbeid og er avventende til effekten, ettersom digitalt politiarbeid ikke har en fast plass i programmet.

9.2.2 Fagkontakter

Oslo politidistrikt var det første distriktet som tok i bruk rollen fagkontakt innen digitalt politiarbeid. Formålet med å innføre fagkontakter i Oslo var videre å bidra til at elektroniske spor ble sikret også i hverdagskriminaliteten, ettersom DPAs kapasitet var forbeholdt alvorlige saker. I tillegg fikk personell utenfor spesialistfunksjonene økt kompetanse på digitalt politiarbeid. I Oslo har fagkontaktene vært bindeledd mellom DPA og førstelinje i geografiske og funksjonelle enheter. Førstelinje har kunnet henvende seg til fagkontakter for bistand og vurdering av om en sak bør løses lokalt eller av fellesenheter. Fagkontaktene avlaster enhet for digitalt politiarbeid, er en lokal, faglig støtte, og videreformidler samtidig erfaringer fra førstelinje til sentrale enheter. Fagkontaktene gjennomfører kurs ved Politihøgskolen og hospitering ved enhet for digitalt politiarbeid.[198]

Fagkontakter for digitalt politiarbeid i øvrige distrikter ble innført med politireformen. Fagkontaktrollen er beskrevet i *Rammer og retningslinjer for etableringen av nye politidistrikter* uten krav til kompetanse. Politidistriktene definerer selv krav til kompetanse. Beskrivelsen av rollen er noenlunde lik som i Oslo. I tillegg forventes det at dataetterforsker/spesialetterforskere skal delta i utviklingen og gjennomføringen av opplæring for politidistriktets fagkontakter. I faggrupperapporten om datatekniske undersøkelser og

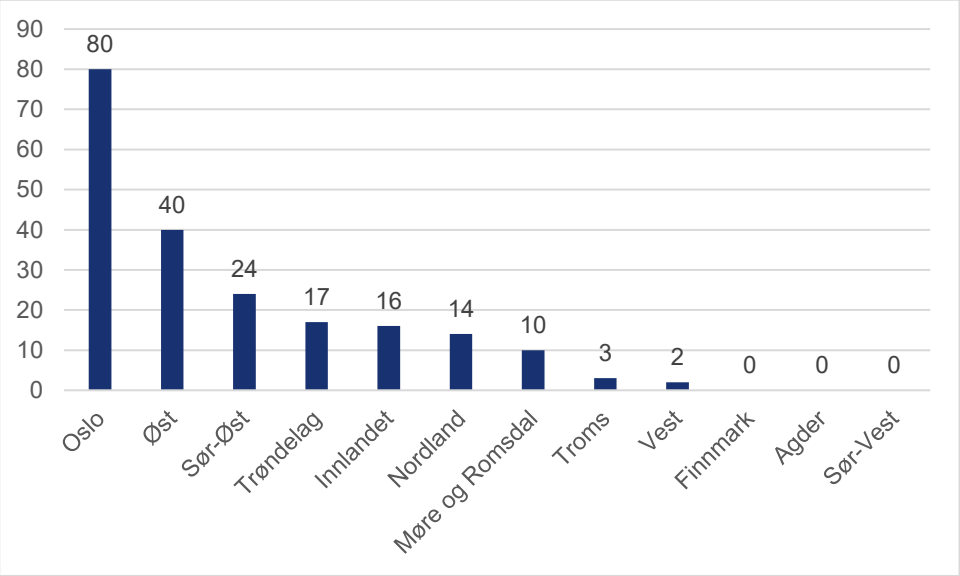
[191] Politihøgskolen (2019) *Programplan 2020-2023*.
[192] Politidirektoratet (2015) *Datakrimstrategien*.
[193] Politiet (2019) *Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning. 9. september 2019.*
[194] Politidirektoratet og Riksadvokaten (2016) *Handlingsplan for løft av etterforskningsfeltet*.
[195] Politidirektoratet (2019) *Fagforvaltning statusrapport – Status fagomr de datatekniske undersøkelser og internettrelatert etterforskning*, 9. september 2019.
[196] Politidirektoratet (2019) *Fagforvaltning statusrapport – Status fagomr de datatekniske undersøkelser og internettrelatert etterforskning*, 9. september 2019.
[197] Politiet (2019) *Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning.*9. september 2019.
[198] Politidirektoratet (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning*, faggrupperapport utarbeidet av en arbeidsgruppe på oppdrag fra Politidirektoratet, datert 9. september 2019.

internettrelatert etterforskning fra 2019 beskrives det som anses som flere utfordringer ved måten politidistriktene har tatt i bruk fagkontaktrollen for digitalt politiarbeid:[199]

- Bruken av rollen fagkontakt varierer fra ett distrikt til et annet.
- Det er ikke satt krav eller gitt råd om hvilken kompetanse fagkontaktene skal ha.
- Det er ikke satt krav eller gitt råd om hvilke oppgaver en fagkontakt kan bistå med / utføre.
- Det er uklarhet rundt hva forskjellen er på en dataetterforsker og en fagkontakt.
- Dataetterforskeren skal stå for opplæring av fagkontakt, men kompetansekravene til begge roller er like.

Riksrevisjonens kartleggingsundersøkelse til DPA-ledere fra mai 2020 viser at ni politidistrikt har fagkontakter for digitalt politiarbeid. Finnmark og Agder har ikke igangsatt ordningen per mai 2020. Sør-Vest politidistrikt har 27 ansatte i de geografiske driftsenhetene[200] som kan sikre spor fra mobiltelefon og sosiale medier. Disse fungerer ifølge Sør-vest politidistrikt foreløpig ikke som fagkontakter slik rollen er beskrevet i *Rammer og retningslinjer for etablering av nye politidistrikter*, men politidistriktet vurderer å utvide ordningen slik at den tilfredsstiller rollekravene fra Politidirektoratet.

Figur 13 Antallet fagkontakter i politidistriktene i mai 2020



Kilde: Riksrevisjonen

Distriktene har ulik praksis og ulike erfaringer med fagkontaktene.[201] Undersøkelsen til DPA-ledere viser at fagkontaktene fungerer som en buffer for enhet for digitalt politiarbeid i seks politidistrikt. De som har svart at fagkontaktene ikke fungerer etter hensikten, har enten ikke etablert fagkontaktrollen ennå, er i en etablerende fase, eller har andre utfordringer. Flere svarer at fagkontaktrollen er sårbar, kommer i tillegg til andre oppgaver og kan være krevende for DPA å følge opp, på grunn av høy gjennomtrekk, manglende økonomiske incentiver[202], og på grunn av påkrevd opplæring og oppfølging. De etterlyser derfor nasjonale retningslinjer for hvilken rolle og kompetanse fagkontaktene skal ha. De fleste politidistrikt anbefaler eller krever kurset NCFI Core ved Politihøgskolen og opplæring i programvare for sikring og gjennomgang av elektroniske beslag. Det gjennomføres i liten grad kvalitetssikring av arbeidet som utføres. Kun DPA i tre politidistrikt (Oslo, Innlandet og Troms) kvalitetssikrer fagkontaktenes arbeid.

9.2.3 Kompetanse i førstelinje

For tjenestepersonell som kommer i befatning med IKT-kriminalitet i første instans vil det være behov for tilstrekkelig kompetanse til å kunne sikre bevis og håndtere sakene riktig i de innledende faser. Lovbrudd og anmeldelser kommer politiet i hende på forskjellige måter. Noen lovbrudd oppdages av politiet i forbindelse

[199] Politidirektoratet (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning*, faggrupperapport utarbeidet av en arbeidsgruppe på oppdrag fra Politidirektoratet, datert 9. september 2019.
[200] Tidligere var politi- og lensmannskontor. Se figur 13 for nærmere beskrivelse av organisering av distrikter.
[201] Intervjuer og resultater fra kartleggingsundersøkelsen til DPA-ledere i alle politidistrikt.
[202] Ifølge politidistriktene som har vært intervjuet, fører ikke rollen som fagkontakt til lønnskompensasjon, kun flere oppgaver og større ansvarsområde.

med patruljering eller annen politiaktivitet. Andre saker anmeldes av publikum, næringsliv, offentlige virksomheter og av politiet selv. Førstelinje her vil være for eksempel patruljer, kriminalvakt, felles straffesaksinntak (FSI) og de som tar imot anmeldelser fra publikum.

I en tidlig fase i en sak er det avgjørende at saken håndteres riktig, slik at ikke bevis går tapt eller endres som følge av politiets håndtering. Det kreves også kompetanse for å forstå hva slags lovbrudd som er begått av hensyn til registrering av saken med riktig straffebestemmelser og internt kodeverk. Flere rapporter viser at kompetanse i førstelinje er en utfordring for håndteringen av IKT-kriminalitetssaker. Flere av utfordringene som ble tatt opp i en rapport fra 2012, blir fortsatt ansett som problematiske i 2019:[203, 204]

- Tilgang på riktig kompetanse som kan sikre riktig prioritering og håndtering av saker i innledende fase, er en utfordring i alle politidistrikt. Dette fører til at saker som kunne vært etterforsket og oppklart, henlegges, at digitale spor (for eksempel IP-adresser) ikke sikres tidsnok, og at det gjøres feil i etterforskningen.
- Det er ingen systematisk tilnærming til opplæring av personell som daglig møter digitale sporsteder i initialfasen (fellesstraffesaksinntak, patrulje, operasjonssentral, krimvakt, påtale).
- Personell i førstelinje søker ikke veiledning fra dataetterforskere hos enhet for digitalt politiarbeid. Terskelen for å be om råd synes å være større hos personell i geografiske driftsenheter enn for personell i fellesenheter, for eksempel hos felles straffesaksinntak. Tilgjengelighet til DPA kan også være begrenset fordi dataetterforskere ikke er tilgjengelige på kveld og helger.
- Flere av politidistriktene har erfaringer med saker som enten henlegges eller hvor det gjøres feil i etterforskningen som først oppdages når DPA blir involvert i sakene. Dette synes å være en større utfordring for etterforskning som foregår i geografiske driftsenheter, enn i fellesenhetene, hvor terskelen for å få eller be om bistand fra DPA kan være større.
- Tilgang på tilpasset støtte, veiledning og kompetanse for førstelinje understrekes som viktig. Dette varierer fra et politidistrikt til et annet. Her kan det se ut til at politidistrikter som har satset på etablering av fagkontakter, og styrking av kompetansen hos felles straffesaksinntak og operativt personell, har mindre utfordringer enn de som ikke har gjort dette.

Politidistriktene som er intervjuet, viser til at forventningene til tjenestepersonell i førstelinje er høye. Førstelinje skal på en og samme tid forholde seg til etterforskning på stedet, nye verktøy, ny organisering, osv. Politidistriktene mener derfor det ikke kan forventes at patruljene skal kunne utføre omfattende digitalt politiarbeid. Forventingene er også høye til FSI som skal prioritere, starte etterforskning, og gi råd og bistand innen de fleste sakskategorier. Tilgangen på tilpasset støtte, veiledning og kompetanse for førstelinje understrekes derfor som viktig. Enkelte av politidistriktene som er intervjuet forteller at de forsøker å bli tidlig involvert i sakene som er relevant for DPA, selv om de ofte er avhengig av å bli varslet. Når kompetansen i førstelinje er mangelfull, kan det være krevende å vurdere når DPA bør involveres. Et av distriktene kommenterer dette på følgende måte:

> *I politiet mangler det kompetanse utenfor DPA-miljøet til å vurdere når DPA bør inn i sak. Situasjonen blir da gjerne at personell uten teknisk kompetanse vurderer om teknisk kompetanse er nødvendig, noe som er uheldig.*

Oslo politidistrikt ser ut til å være blant de politidistriktene som har kommet lengst i å styrke kompetanse og støtte for førstelinje. DPA i Oslo politidistrikt viser i intervju til at avstanden mellom førstelinje og DPA tidligere var stor. Utfordringene dette skapte har ført til satsing på opplæring i digitalt politiarbeid for førstelinje, utdanning av fagkontakter, egne avsnitt for digitalt politiarbeid i geografiske driftsenheter og i fellesenheter med ansvar for etterforskning og etterretning. Dette har ifølge DPA i Oslo ført til at den samlede forståelsen for digitalt politiarbeid i distriktet er forbedret, DPA involveres tidligere i sakene og tilgangen på støtte og bistand er bedret. DPA opplever likevel fortsatt å komme for sent inn i IKT-kriminalitetssaker med stort skadepotensiale. Styrking av førstelinje løser med andre ord ikke alle utfordringer.

[203] Politidirektoratet (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning*, faggrupperapport levert Politidirektoratet i 9. september 2019
[204] Politidirektoratet (2012) *Politiet i det digitale samfunnet: En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett*;

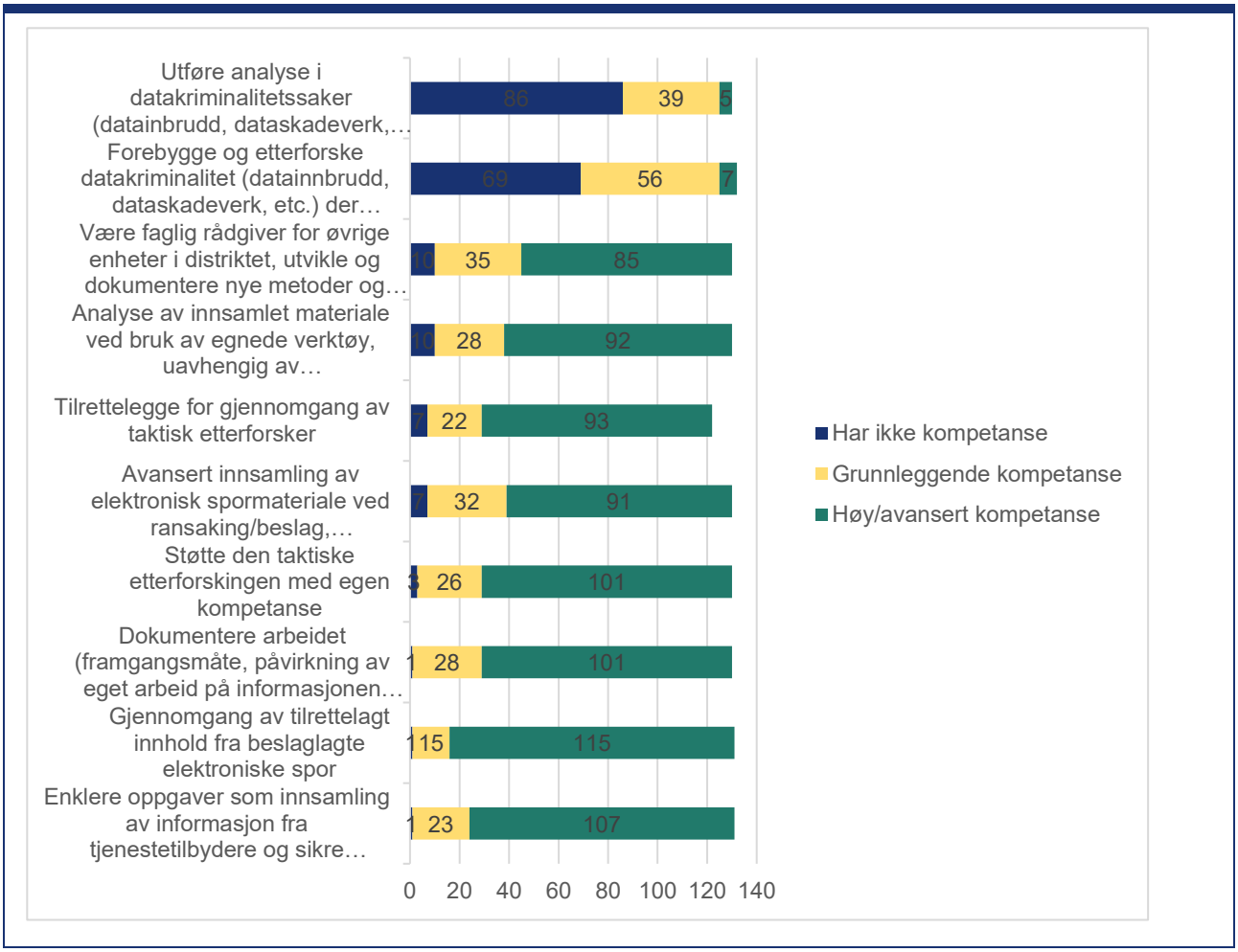
9.3 Spesialkompetanse

9.3.1 Krav til dataetterforskere

I *Rammer og retningslinjer for etableringen av nye politidistrikter* er det beskrevet hvilke oppgaver som skal løses av DPA. En av fem hovedoppgaver er å forebygge og etterforske IKT-kriminalitet der etterforskningen er teknologikrevende. I beskrivelsen av roller og hovedansvar i DPA er denne typen etterforskning tillagt rollen *Spesialist innen datakriminalitet* og *Analytiker*. Det finnes kun en spesialist og en analytiker totalt i de 12 DPA-ene i politidistriktene. For dataetterforskere er ikke IKT-kriminalitet nevnt som en særskilt oppgave de skal ivareta.

Riksrevisjonen har gjennomført en kartleggingsundersøkelse av DPA i politidistriktene. Som del av kartleggingen er DPA-lederne bedt om å klassifisere de ansatte innen kompetanseområdene enhetene skal ivareta i henhold til *Rammer og retningslinjer for etablering av nye politidistrikter*.

Figur 14 DPA-ansattes kompetanse sett opp mot hvilke oppgaver DPA skal ivareta i 2019 (N = 120–132*)



Kilde: Riksrevisjonen, kartleggingsundersøkelse til DPA-ledere.
*Som følge av at Oslo politidistrikt har et stort antall dataetterforskere med avgrenset ansvar, er det ikke fylt ut svar for alle svarkategorier. Det er fylt ut svar for færre enn 132 for enkelte av kompetanseområdene.

Figuren ovenfor viser at DPA-lederne anser at de ansatte har grunnleggende/god kompetanse innen de fleste områder, med unntak for de to øverste som gjelder forebygging, etterforskning og analyse i datakriminalitetssaker (datainnbrudd, dataskadeverk osv.). I denne kompetansekategorien er det bare noen få ansatte i politidistriktene som har høy/avansert kompetanse. Noe flere har grunnleggende kompetanse. Årsaken til at det er lav kompetanse på disse områdene kan være at DPA i liten grad bistår i etterforskning av denne typen saker fordi antall saker som anmeldes er relativt få, og fordi de ikke blir prioritert etterforsket.

Krav til dataetterforskere er beskrevet i nasjonale rollebeskrivelser[205] for ledere og medarbeidere innen etterforskningsfeltet fra 2018.[206] Dataetterforskere skal gjennomføre datateknisk etterforskning i en konkret straffesak, herunder identifisere, sikre og dokumentere de elektroniske spor som kan belyse hva som har skjedd. De skal også delta i utviklingen og gjennomføringen av opplæring for politidistriktets fagkontakter og førstelinjepersonell. Kompetansekravene er som følger:

- Formalkompetanse:
  - fullført utdanning fra Politihøgskolen eller annen relevant bachelorutdanning
  - Nordic Computer Forensic Investigators (NCFI) modul 1
  - relevant etterutdanning i etterforskning for sivile (15 studiepoeng)
- Realkompetanse
  - minst tre års erfaring innen dataetterforskning

Kravene til dataetterforskere er det samme som mange politidistrikt har valgt å stille som krav til fagkontakter. Ifølge rapport om status på fagfeltet vil NCFI Modul 1 ikke gi tilstrekkelig kompetanse til å fungere som en selvstendig dataetterforsker.[207]

Innen etter- og videreutdanning har PHS ulike kurs og studier. Ifølge Oslo politidistrikt har Politihøgskolen utviklet og tilbyr et av de mest omfattende studietilbudene i Europa innenfor fagfeltet «Computer Forensics and Cybercrime Investigations». Studiene dekker ulike fagretninger innen digitalt politiarbeid, fra sikring av elektroniske spor til mer avansert etterforskning av IKT-kriminalitet og er i utgangspunktet åpne for alle, både politiutdannede, sivile og jurister.[208]

Videreutdanning for dataetterforskere ved PHS har vært tilgjengelig siden 2010 (se vedlegg 6 for oversikt over utdanningsløp). Det er i all hovedsak politifaglig ansatte som har tatt grunnmodulen på 15 studiepoeng. I perioden 2016 til våren 2020 er totalt 301 kurs innen digitalt politiarbeid gjennomført av totalt 255 politiansatte.[209] Det er særlig ansatte i Oslo politidistrikt, Kripos og Trøndelag politidistrikt som blir sendt på kurs. Av disse var det ikke mulig å spore opp hvor 23 personer befant seg. Av de resterende har 7 av 278 sluttet i politiet, 21 prosent er ansatt i særorgan, og 79 prosent i politidistriktene.

De fleste som har gjennomført kurs innen digitalt politiarbeid, har tatt det grunnleggende kurset NCFI-1 (totalt 182 avlagte kurs). Antallet kandidater som har gjennomført dette kurset, har økt betydelig, fra 9 personer i 2016 til 67 personer i 2018 og 2019. Dette har sannsynligvis sammenheng med etableringen av fagkontaktrollen i politidistriktene, ettersom dette kurset blir brukt av mange distrikter som grunnutdanning for å kunne inneha rollen. Det er registrert 64 avlagte kurs innen modul 2 av NFCI-utdannelsen, og 40 avlagte kurs innenfor modul 3 i perioden. Disse kursene er på masternivå og inngår i den politifaglige masterutdannelsen som tilbys ved PHS.

PHS har siden 2015 samarbeidet med NTNU Gjøvik om en erfaringsbasert master i *Information Security: Digital Forensics and Cybercrime Investigation*. Denne gir en fordypning i hvordan etterforskning gjennomføres i cyberdomenet og hvordan slik etterforskning skal gjøres for å ivareta kriminaltekniske hensyn, rettsikkerhet og personvern. Tilgjengelige studieplasser har ligget på 20-30 de siste 2-3 årene. Kun en liten andel av plassene dekkes av norsk politi. Når studiet ble planlagt trodde NTNU at flere søker fra politiet skulle komme inn, men det har veldig få søkere. Det er derfor kun et lite antall kandidater fra norsk politi som har fullført masteren. Masteren må tas ved siden av full jobb og mange får heller ikke tillatelse til å delta. Høsten 2020 var 10-15 fra politidistrikter og særorgan aktivt innrullert på studiet. Tre-fire kandidater har fullført, og 6-7 er aktive i studiet ifølge NTNU.

Kripos og ØKOKRIM gjennomfører også relevante kurs for politidistriktene. Det er også vanlig at politidistriktene henter inn kursholdere eller deltar på kurs i regi av leverandører av programvare. Norsk politi deltar tar også videreutdanning og kurs utenlands, blant annet ved University College of Dublin.

---

[205] Dette er et tiltak under etterforskningsløftet som har til hensikt å sikre likt innhold og lik kompetanse i like roller på tvers av distrikter, og trygghet for at politiet kan ivareta sitt samfunnsoppdrag gjennom straffesaksbehandlingen.
[206] Politidirektoratet (2018) *Nasjonale rollebeskrivelser med kompetansekrav – etterforskningsfeltet*. Versjon 0,7, utgitt i 2018.
[207] Politidirektoratet (2019) *Fagforvaltning statusrapport – Status fagomr de datatekniske undersøkelser og internettrelatert etterforskning*, 9. september 2019.
[208] Oslo politidistrikt (2018) *Digitalt politiarbeid - Anbefaling*, rapport datert 23. januar 2018.
[209] Perioden 2016 til 2020 er valgt fordi data var lettest tilgjengelig for denne perioden. For perioden før er informasjon om gjennomførte kurs lagret på papir og sammenstilling av data ville medført betydelig ressursbruk for Politihøgskolen.

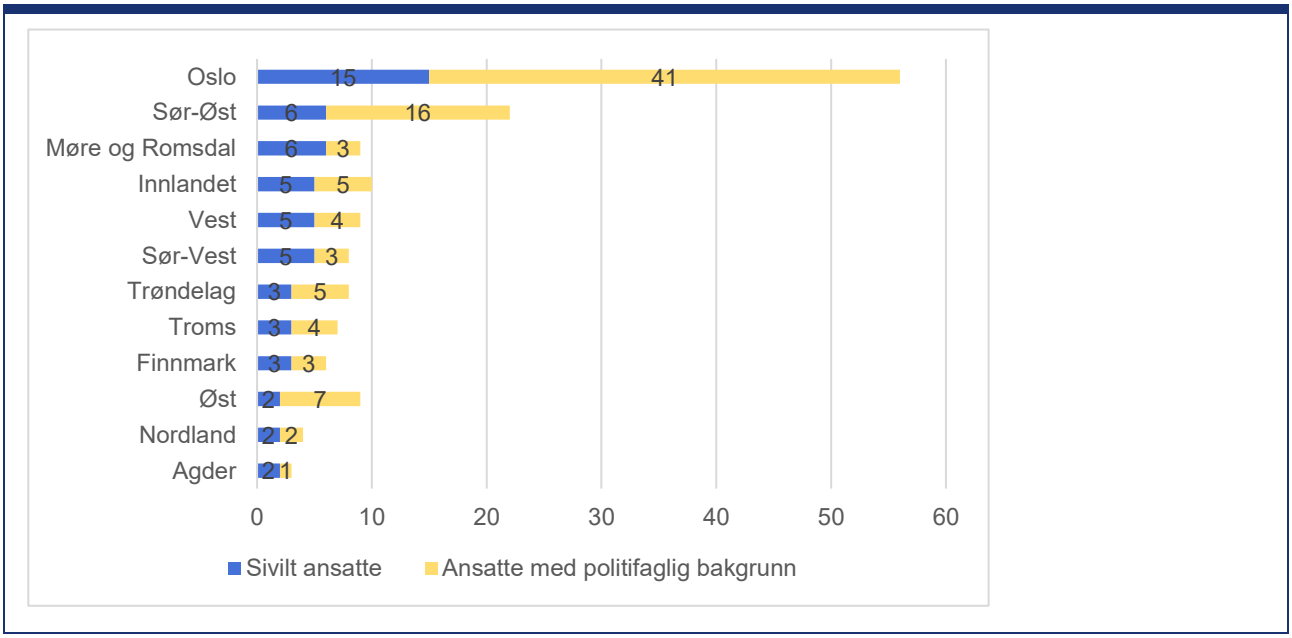
9.3.2 Sivil kompetanse

Lystadutvalget som utredet politiets kompetansebehov i 2017 viser til at bekjempelse av IKT-kriminalitet krever høy kompetanse innen informatikk og datateknikk, og fordrer en mye bredere kompetanse enn etaten har i dag. Utvalget mener derfor etaten må øke og utvide sin kompetanse gjennom rekruttering av kompetanse fra sivile utdanninger.[210]

I Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden* vises det til et særlig behov for å rekruttere folk innen blant annet datateknologi, informasjonssikkerhet og rettsinformatikk. Det vises også til at PHS må legge til rette for at disse utdanningsgruppene får tilført nødvendig tilleggskompetanse i politifag. Justis- og beredskapsdepartementet opplyser i intervju at de ser at målet om to politifolk per 1000 innbygger, som et høyt prioritert mål, gjør det vanskelig å ansette sivil kompetanse i distriktene.

I Riksrevisjonens kartleggingsundersøkelse til DPA-ledere er det kartlagt hvor mange ansatte i DPA som har sivil bakgrunn og politifaglig bakgrunn.

Figur 15 Antall ansatte med sivil og politifaglig bakgrunn i DPA 2019 (N = 151)



Kilde: Riksrevisjonens kartleggingsundersøkelse til DPA-ledere, 2020.

Figuren ovenfor viser at sivilt ansatte utgjør en stor andel av DPA-ansatte i de fleste politidistrikt. Totalt er 37 prosent av de ansatte i DPA er sivilt ansatte. I intervjuene med politidistriktene er det pekt på to hovedutfordringer når det gjelder ansettelse av sivile i DPA. Det ene er at denne typen arbeidskraft er ettertraktet og politiet har vanskeligheter med å konkurrere med privat næringsliv på lønn. Det andre er at målet om to politiårsverk per 1000 innbyggere fører til et press mot å ansette politiutdannede framfor sivile. Både Justis- og beredskapsdepartementet og Politidirektoratet uttrykker i intervju at de er kjent med at dette målet gjør det mer utfordrende å ansette sivile. Ifølge departementet har politiet behov for å rekruttere andre typer kompetanse i årene som kommer, jf. Lystadutvalgets rapport.

9.4 Påtalemyndighetens kompetanse

Påtalemyndigheten fatter beslutning om iverksettelse av etterforskning jf. påtaleinstruksens § 7-4 og er ansvarlig for straffesaksbehandlingen i politiet. Påtalemyndighetens kompetanse innen digitalt politiarbeid og IKT-kriminalitet kan være avgjørende for å ivareta rettsikkerheten på området og kan ha betydning for oppklaring av IKT-kriminalitet. Manglende kompetanse kan for eksempel føre til at saker henlegges, registreres på feil straffebud eller at feil etterforskningsskritt iverksettes.

[210] Politidirektoratet (2017) *Politi- og lensmannsetatens kapasitets- og kompetansebehov de kommende ti-årene*, 15. desember 2017.

9.4.1 Påtalemyndighetens kompetanse innen digitalt politiarbeid og IKT-kriminalitet

Påtalejurister fra politidistriktene som er intervjuet, viser til at de først og fremst opparbeider seg kompetanse gjennom erfaring. Det er lite tid til å gå på kurs og etterutdanningsmuligheter innen digitalt politiarbeid for påtalejuristene finnes i liten grad. IKT-kriminalitet krever i tillegg spisskompetanse, som er en utfordring i de mindre distriktene hvor påtalejuristene skal dekke alle typer saker. Politihøgskolen har kun tre kurs for etterutdanning av påtalejurister, men ingen av disse handler om vurdering av digitale bevis.

Påtalejurister i politidistriktene viser i intervju til at digital kompetanse er viktig for å sikre rettssikkerheten. Påtalejuristene ser helt klart et behov for å styrke kompetansen på vurdering av digitale bevis. Med bedre kompetanse kan påtalemyndigheten komme tidligere inn i sakene og se til at innhenting og vurdering av bevis skjer på en måte som gir god rettssikkerhet. Mer målstyrt etterforskning ville også ført til mer ryddig etterforskning og mindre «overetterforskning». Påtalemyndigheten i Oslo politidistrikt mener det kan settes spørsmålstegn ved om påtalemyndigheten er rigget for et framtidig kriminalitetsbilde. Det vises imidlertid til at Oslo politidistrikt har høy kompetanse tilgjengelig i organisasjonen som er til støtte i vurderingen av bevis og utforming av tiltalebeskrivelser.

Det finnes eksempler på at svakheter ved digitale bevis kan utgjøre en fare for rettssikkerheten. Et eksempel på dette er svakheter ved politiets innhenting og analyse av teledata i straffesaker i Danmark. I 2019 ble det i Danmark avdekket feil som førte til krav om gjenopptakelse av 10 000 straffesaker og en generell utfordring med tilliten til rettssystemet i det danske samfunnet. I etterkant er det i Danmark foreslått å etablere et eget uavhengig tilsyn (Bevismiddeltilsynet) med bruken av tekniske etterforskningsmidler og beviser i straffesaker.[211] I Norge har det også vist seg at det kan være utfordringer med feil i programvare for uthenting av opplysninger fra mobiltelefoner. Som følge av saken i Danmark er det oppdaget at det kan være begått feil også i Norge. Hvor mange saker det gjelder og hvilke konsekvenser dette kan ha hatt var ikke klargjort i september 2020.[212]

Enhet for digitalt politiarbeid i politidistriktene (DPA) har ansvaret for gjennomgang og analyse av digitale bevis som legges fram for påtalejuristene og som brukes videre i straffesaksbehandlingen. DPA bistår innen alle sakskategorier hvor digitale bevis forekommer. I forbindelse med politireformen viste derfor Politidirektoratet til at:

> *«Særskilt avgitt påtalekompetanse[213] for digitalt politiarbeid er avgjørende for å ivareta effektivitet, kvalitet, resultatoppnåelse og rettssikkerhet.»*

9 av 10 DPA-ledere opplyser at det ikke avsatt dedikerte politiadvokater til fagfeltet digitalt politiarbeid.[214]

9.4.2 Plan for styrking av påtalemyndighetens kompetanse innen digitalt politiarbeid

I Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet fra 2015 ble det pekt på at en generell heving av påtalemyndighetens og dommeres teknologiforståelse vil være viktig for å bedre kompetansen og evnen til å formidle og forstå digitale bevis. Justis- og beredskapsdepartementet ba derfor Riksadvokaten, i samarbeid med departementet, utarbeide en plan for å styrke påtalemyndighetens digitale kompetanse. Riksadvokatens ansvar er begrenset til kompetanseheving i Den høyere påtalemyndighet, ikke påtalejuristene i politidistriktene. Riksadvokaten tok derfor ansvar for å lage en plan for kompetanseheving for Den høyere påtalemyndighet, som også ville kunne egne seg for påtalemyndigheten i politiet.[215]

I NOU 2017: 5 *En påtalemyndighet for fremtiden* viser utvalget til at IKT-utfordringene for både påtalemyndigheten i politiet og Den høyere påtalemyndighet synes særlig å være relatert til to hovedområder:

- kompetanse/kunnskap til å forstå og håndtere IKT-kriminalitet
- kompetanse/kunnskap/utstyr til å bruke digitale arbeidsmetoder ved saksbehandlingen og formidling/presentasjon av bevis i retten

Utvalget konkluderer med at dagens kompetansetilbud til statsadvokatene og påtalejuristene i politiet generelt ikke er godt nok, og konstaterer samtidig at det ikke foreligger synlige sentrale føringer eller en

---

[211] Justitsministeriet (2020) *Justitsminister vil oprette et uafhængigt tilsyn med bevismidler*, pressemelding 22. februar 2020.
[212] Kripos (2020) *Feil i sikringer av IOS-enheter ved bruk av sikringsverktøy*, brev til den høyere påtalemyndighet 22. september 2020.
[213] Politiadvokater dedikert til fagfeltet digitalt politiarbeid.
[214] Politidirektoratet (2019) *Fagforvaltning statusrapport – Status fagomr de datatekniske undersøkelser og internettrelatert etterforskning*, 9. september 2019.
[215] Riksadvokaten (2015) *Plan for å styrke den digitale kompetansen i påtalemyndigheten*, brev til Justis- og beredskapsdepartementet, 24. september 2015.

helhetlig strategi for dette viktige arbeidet. Utvalget foreslår derfor at riksadvokaten gis det sentrale ansvaret for kompetanseutviklingen av hele påtalemyndigheten, også påtalemyndigheten i politidistriktene.

Ansvaret for kompetanseutvikling for påtalejurister og statsadvokater er delt mellom Riksadvokaten, som har ansvaret for dette i den høyere påtalemyndighet, og Justis- og beredskapsdepartementet og Politidirektoratet, som har ansvar for påtalejuristene i politidistriktene. Ifølge påtaleutvalget har ikke Politidirektoratet tatt sitt ansvar for kompetanseutviklingen for påtalejuristene i politidistriktene. Det finnes etter- og videreutdanning på Politihøgskolen som er tilgjengelig for påtalejuristene, men disse tilbudene brukes i svært liten grad.[216]

I politimeldingen fra juni 2020, Meld. St. 29 (2019–2020), vises det til at påtalejuristene har faglig krevende oppgaver, og det er gjort grundige vurderinger av påtalemyndighetens virksomhet i Påtaleanalysen (NOU 2017: 5). Påtaleanalysen peker på at systematisk kunnskapsbygging er noe av det som må til for å oppnå forbedringer. I meldingen vises det til pågående arbeid med en ny, obligatorisk grunnutdanningsmodell for nytilsatte påtalejurister. Departementet mener det er viktig med et godt kompetansetilbud på tvers av politidistriktene, som kan danne grunnlaget for høy kvalitet i arbeidet og skriver at de vil følge opp dette arbeidet. Det skal i tillegg vurderes om Riksadvokaten bør gis det sentrale ansvaret for kompetanseutviklingen også hos påtalejuristene, i tråd med forslag fra Påtaleanalysen.

9.5 Kompetanse innen etterforskning av internettrelaterte seksuelle overgrep

Nettovergrepssaker er et relativt nytt fenomen i norsk politi og i de distriktene hvor etterforskningsoperasjoner er gjennomført, har det foregått en betydelig kompetansebygging.[217] Etterforskningskompetansen varierer fra et distrikt til et annet, og metodikk som er brukt i etterforskningen i saker som gjelder seksuell utnyttelse av barn over internett har også variert.[218] Antall saker har økt, mengden beslag har økt, og evalueringer av saker viser at det har vært opp til hvert politidistrikt å avgjøre hvordan sakene håndteres med hensyn til lokale løsninger, behandling og prioritet. Alvorlige, større saker som er etterforsket, kjennetegnes ved store databeslag, behov for omfattende datatekniske undersøkelser, mange fornærmede, bruk av tilrettelagte avhør, innhenting av bevis fra utenlandske aktører osv. Sakene er store og krever samarbeid mellom spesialiserte etterforskningsressurser. Dette samarbeidet er avgjørende for å sikre god kvalitet i etterforskningen.[219]

I intervjuer med politidistriktene går det fram at det særlig tre faggrupper som er involvert i etterforskningen av nettovergrep: påtalejurister, etterforskere og dataetterforskere. Politidistriktene som er intervjuet, viser til at etterforskningen ofte blir ressurskrevende for de tre faggruppene. Det faglige arbeidet som gjennomføres av alle tre faggrupper krever spesialisert kunnskap. Kriminaliteten utvikler seg i takt med den teknologiske utviklingen, hvilket betyr at det kan være krevende for alle tre faggrupper å henge med på utviklingen. Etterforskningen av nettovergrep oppleves ofte som vanskelig. Likevel oppgir flere politidistrikter i intervju at de rekrutterer nyutdannede rett fra Politihøgskolen til etterforskning av alvorlige internettrelaterte seksuelle overgrep. Kompetansen nyutdannede har fra Politihøgskolen er ikke tilpasset den realiteten de møter på sedelighetsavsnittene ifølge distriktene. Mange av de nyutdannede ønsker seg til ordenstjeneste fordi det samsvarer bedre med hvilke forventninger de har til politiarbeid og på grunn av lønnsmessige forskjeller mellom etterforskning og orden. Flere av distriktene opplever at nyutdannede er kort tid på etterforskning før de søker seg til andre oppgaver innen ordenstjeneste eller andre etterforskningsområder. Dette fører til at kompetanse forsvinner, og det må brukes tid og krefter på å lære opp nye etterforskere.

Kripos er kjent med at det er betydelig utskifting av etterforskere i distriktene på dette området, men er usikker på om det er et større problem her enn på andre områder. Kripos er imidlertid kjent med at distriktene bruker lønn som virkemiddel for å beholde etterforskere i større grad på dette området enn på andre. Det indikerer at distriktene har vanskeligheter med å rekruttere og beholde kompetanse. Kripos mener dette kan være relatert til at etterforskning av internettrelaterte overgrep kan være belastende.

Det ble nedsatt en arbeidsgruppe i 2016–2017 (henvist til i saksflytrapporten) ledet av Kripos med deltakere fra Oslo politidistrikt, Trøndelag politidistrikt og Det nasjonale statsadvokatembetet for å se nærmere på

[216] NOU 2017: 5 *En påtalemyndighet for fremtiden – Påtaleanalysen.*
[217] Hordaland, Sogn og Fjordane Statsadvokatembeter, 2019 *Rapport etter tilsyn med Vest politidistrikt sin innsats mot vold og sedelighet/voldtekt*, rapport datert 30. oktober 2019.
[218] Justis- og beredskapsdepartementet, 2019 *Rapport fra arbeidsgruppe som har sett på saksflyt i saker som gjelder overgrep mot barn, oppnevnt av Justis- og beredskapsdepartementet 26. juli 2018*, rapport publisert 13. mars 2019.
[219] Justis- og beredskapsdepartementet, 2019 *Rapport fra arbeidsgruppe som har sett på saksflyt i saker som gjelder overgrep mot barn, oppnevnt av Justis- og beredskapsdepartementet 26. juli 2018*, rapport publisert 13. mars 2019.

utfordringene i politidistriktene. Arbeidsgruppen ga flere anbefalinger om hvordan norsk politi bør arbeide med saker som inneholder dokumentasjon på seksuelle overgrep mot barn og retningslinjer for håndtering av overgrepsmateriale med lik standard og metodikk – «Beste praksis». Løsningen er fortsatt ikke iverksatt. Implementering av metodikken forutsetter en teknisk løsning (videreutvikling av DSB-nett) som ikke er gjennomført.

9.6 Kompetanse innen etterforskning av økonomisk IKT-kriminalitet og ren IKT-kriminalitet

Kompetanse og kapasitet til etterforskning av ren IKT-kriminalitet er omtalt i Politidirektoratets datakrimstrategi fra 2015:

> *«De færreste politidistriktene har i dag tilstrekkelig kompetanse til å etterforske datainnbrudd eller andre datahendelser av en viss størrelse. Politidistriktenes dataetterforskere arbeider med sikring og analyse av databeslag og digitale spor i alle typer saker. Behovet for dataetterforskere har i lang tid vært større enn tilgjengelig kapasitet. Til tider opplever dataetterforskere en kø av ubehandlede oppdrag som skaper en flaskehals i mange etterforskningssaker.»*

Politidistriktene viser til at det er utfordringer med hvordan ren IKT-kriminalitet som datainnbrudd håndteres når det anmeldes. Enhet for digitalt politiarbeid i Vest politidistrikt opplever utfordringene slik:

> *«De som anmelder et datainnbrudd blir ofte mottatt av representanter fra politiet som ikke har relevant kompetanse til å vurdere saken. Enkelte i førstelinje tar kontakt med DPA for å få råd, men de fleste gjør ikke dette. For den som anmelder oppleves det nok derfor som om politiet ikke har kompetanse til å behandle slike saker på en god nok måte. Eventuelt får man en mangelfull anmeldelse som mangler vesentlige opplysninger og saken henlegges.»*

NC3 viser til at politiet mangler kompetanse til å etterforske den alvorlige IKT-kriminaliteten som Riksadvokaten peker på (dataangrep, datainnbrudd). Få miljøer i politiet har kompetanse til å etterforske denne typen kriminalitet. Saker av størrelse og kompleksitet, for eksempel Hydro-saken, vil ingen distrikter ha klart å ta med unntak av kanskje Oslo ifølge NC3. Selv NC3 har utfordringer med å håndtere slike saker. Kompleksiteten er høy fordi det åpner seg spor ut av landet, det kan være mange fornærmede i flere land, og det kan være organiserte kriminelle miljøer fra Norge eller andre land som står bak. Det blir store og komplekse saker med mange fornærmede som kan være krevende å etterforske.

Lignende kompetanseutfordringer forbindes med etterforskning av økonomisk IKT-kriminalitet. Politidistriktene som er intervjuet, informerer at de opplever mange ulike typer økonomisk IKT-kriminalitet som Nigeria-svindel, NAV-bedragerier, investeringsbedragerier, svindel med bankkort, finn.no-bedragerier, direktørsvindel, fakturabedragerier osv. Alle kriminalitetstypene har elektroniske spor og krever kompetanse innen digitalt politiarbeid i etterforskningen. De fleste saker henlegges, og få saker etterforskes og oppklares. Kompetanse om IKT-kriminalitet i saksmottak er en utfordring ifølge politidistriktene som er intervjuet. Manglende kompetanse til å forstå innholdet i et nettbedrageri kan for eksempel føre til at anmeldere blir avvist med henvisning til at dette ikke er noe politiet kan hjelpe med, eller at det iverksettes etterforskningstrinn som normalt ikke ville blitt iverksatt om spesialetterforskere/dataetterforskere var involvert fra starten av. Det kan også være at bedragerisaker, hvor IP-adresser foreligger, tar lang tid å registrere. Deretter skal FSI avgjøre om det skal gjennomføres etterforskning. Dersom saken skal etterforskes blir den sendt til en av de geografiske driftsenhetene eller fellesenhetene. I mellomtiden kan muligheten til å innhente IP-adresser, som er begrenset til 21 dager, være oversteget, og saken blir med en gang mer komplisert å etterforske.

10 Politiets støttesystemer til oppklaring av IKT-kriminalitet

Dette kapitlet handler om støttesystemene som er viktige i etterforskningen og for oppklaringen av saker. I prosessen med å innhente, sikre og analysere digitale bevis i politidistriktene brukes spesialiserte programmer, utstyr, lagringsmedia og infrastruktur som i hovedsak håndteres av enhet for digitalt politiarbeid (DPA).[220] Med begrepet støttesystemer forstås her både nasjonale og lokale retningslinjer, rutiner, utstyr og programvare som gir politiet støtte i det digitale politiarbeidet. Det mangler felles rutiner, standarder og retningslinjer for digitalt politiarbeid. Programvare og utstyr kjøpes inn og administreres lokalt i hvert enkelt politidistrikt uten særlig samordning fra nasjonalt hold. Det er etablert et felles beslagsnett, DSB-nett, men dette dekker ikke de behovene politidistriktene har for håndtering og analyse av digitale beslag.

Utfordringene forbundet med støttesystemer har vært kjent over lengre tid.

Flere av politiets rapporter og strategier fastslår fra 2012 at det det mangler rutiner, retningslinjer og veiledere samt nasjonal styring og kontroll med innkjøp, administrasjon og sikring av støttesystemer og verktøy til digitalt politiarbeid. En felles infrastruktur for lagring og analyse av digitale beslag har vært etterlyst. Disse utfordringene har vært påpekt i ulike rapporter og er derfor kjent for politiet.

En av de første rapportene som påpekte utfordringer på området, var en rapport fra en arbeidsgruppe nedsatt av Politidirektoratet for å se på politiets arbeid med IKT-kriminalitet i 2011:

> *«Flere politidistrikter etterlyste klarere retningslinjer fra sentralt hold med henblikk på utnyttelsen av elektroniske spor, både med hensyn til når datatekniske undersøkelser bør gjennomføres, hva slags kompetanse som kreves og hvilket utstyr distriktet bør ha. Ett distrikt ga også klart uttrykk for at det var vanskelig å prioritere området uten sentrale føringer.»*[221]

Utfordringer med infrastruktur og standarder ble også omtalt i Datakriminalitetsstrategien fra 2015 og i Justis- og beredskapsdepartementets IKT-kriminalitetsstrategi fra 2015. Departementet bestilte også en gjennomgang av tilstanden fra Politidirektoratet. I 2016 rapporterte Politidirektoratet at politiet så langt ikke hadde etablert enhetlige metoder eller løsninger for håndtering av digitale spor og sporsteder, men at dette ville bli utviklet når et strukturert system for fag- og metodeansvar var etablert. Håndteringen av digitale spor i politidistrikter og særorgan varierte både når det gjaldt kompetanse, tilgjengelige verktøy, prioritet og i hvilke sakstyper slike spor innhentes. Utfordringene ble også slått fast i en rapport fra faggruppe for datatekniske undersøkelser og internettrelatert etterforskning i 2019.[222]

10.1 Innkjøp, drift og administrasjon av utstyr og programvare

I 2012 pekte arbeidsgruppen nedsatt av Politidirektoratet på at felles løsninger for utstyr og programvare kunne bidra til å øke teknologiforståelsen i politiet og forbedre utnyttelsen av elektroniske spor.[223] Pilotprosjektet i Oslo politidistrikt om digitalt politiarbeid har framhevet at større grad av standardisering av verktøy og programmer er særlig viktig for verktøyene som skal benyttes av generalister og fagkontakter.[224]

Ifølge arbeidsgrupperapporten fra 2012 kan det være et kostnadseffektivt tiltak å etablere en sentral koordinering av innkjøps-, vedlikeholds- og oppgraderingsavtaler for det spesielle utstyret som er enhetlig for fagområdene og enhetene som arbeider med det. Et slikt tiltak ville kunne sikre politidistriktene tilgang på rett utstyr og vedlikehold og oppgradering av utstyret i tillegg til rett pris. Samkjøring av utstyrs- og programvareavtaler ville også kunne gi kvantumsrabatter i mange tilfeller. Tilsvarende ville samordning av kurs og opplæring kunne gi besparelser. Kurs kunne holdes i Norge, i stedet for at deltakere fra ulike politidistrikter enkeltvis deltok på kurs i utlandet. Felles innkjøp, vedlikehold og oppgradering av teknisk utstyr og programvare kunne gi direkte kostnadsbesparelser for etaten.[225]

---

[220] Oslo politidistrikt skiller seg noe fra de andre distriktene ved at noe av håndteringen i samarbeid med andre enheter i distriktet som enten drifter eller er avhengig av tilsvarende tjenester.
[221] Politidirektoratet (2012) *Politiet i det digitale samfunnet: En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett.*
[222] Politiet (2019) Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning.9. september 2019.
[223] Politidirektoratet (2012) *Politiet i det digitale samfunnet: En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett*.
[224] Oslo politidistrikt (Politidistrikt, 2017*) intern rapport: Foreløpig rapport fra pilotprosjekt om IKT og internett i politiarbeidet.*
[225] Politidirektoratet (2012) Politiet i det digitale samfunnet: En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett.

I statusrapporten for fagområdet datatekniske undersøkelser og internettrelatert etterforskning fra 2019 vises det til at mange av de samme utfordringene vedvarer:[226]

- DPA i de ulike distriktene benytter forskjellig utstyr og programvare.
- Det er ikke klart definert hvem som har ansvar for drift og vedlikehold av utstyr og programvare.
- Det er ingen nasjonal innkjøpsavtale som benyttes ved innkjøp og fornyelse av lisenser.
- Det er ingen føringer på hva slags utstyr det minimum skal være ved ulike enheter i politiet.
- Det er ingen krav til utskiftingstakt, standard på utstyr, programvare eller lisenser hos DPA eller geografisk driftsenheter.

Det blir også pekt på hvilke konsekvenser disse utfordringene gir:

- Stor lokal variasjon i utstyrsparken i politidistriktene.
- Mye gammelt utstyr som er modent for utskifting uten at det er planer for å skifte dette ut.
- Det brukes mye tid og ressurser til oppfølging av programvarelisenser og mange distrikter har ikke nødvendige programmer for å utføre arbeidet. Noen har begrensninger med hensyn til kapasitet i form av få lisenser på viktige verktøy på grunn av høye lisenskostnader.
- Lokalt framforhandlede priser på lisenser gir sannsynligvis høyere totalkostnader for politiet.

Flere av politidistriktene som er intervjuet mener det i større grad enn i dag burde vært tatt et nasjonalt ansvar for styring av innkjøp, administrasjon og sikring av støttesystemer og verktøy til digitalt politiarbeid. Politidirektoratet sier i intervju at de også vurderer det som en utfordring at innkjøp, drift og administrasjon i for stor grad har vært lokalt forankret, og at sentralisering av innkjøp og drift av utstyr og programvare er svaret på utfordringene på dette området.

10.1.1 Datainfrastruktur og beslagsnett

Politiet har inntil nylig ikke hatt en felles infrastruktur for håndtering av digitale beslag. Manglende felles infrastruktur har gjort det vanskelig å samarbeide både internt i politidistriktene og på tvers av distrikter. Flere steder fraktes digitale beslag fysisk fra ett sted til et annet. Utfordringene har vært tatt opp i mange år.[227]

Behovet for systemer for sikring, lagring og analyse av digitale beslag er særlig stort i nettovergrepssaker. Sakene genererer betydelige mengder beslag i form av bilder, video og andre digitale bevis som dokumenterer overgrepene. Beslagene er ofte omfattende, og det kan være utfordrende å få oversikt over innholdet. Kripos beskriver et beslag fra 2016 med 11 millioner bilder, hvorav 2,3 millioner var unike, og 56 000 filmfiler med mer enn 5800 timer samlet spilletid.[228] Mangel på verktøy for håndtering av beslag gjør at sikring og gjennomgang tar lang tid.[229] Kripos påpekte behovet for en nasjonal løsning for håndtering av overgrepsmateriale i 2016–2017 som fortsatt ikke er iverksatt. Kripos mener en nasjonal løsning kunne ha effektivisert etterforskningen, men finnes ikke per i dag. Med enhetlig metodikk og bedre verktøy ville arbeidet blitt mer effektivt og mer kunne blitt avdekket. Dette ville frigjort kapasitet til å ta nye saker.

I intervju med DPA i flere distrikter blir det pekt på ulike utfordringer knyttet til at det ikke finnes et system for lagring og deling av digitale beslag/bevis. Digitale beslag håndteres mange steder utenfor politinettet på lagringsmedia eller lokale nettverk. Ifølge Faggrupperapporten for datatekniske undersøkelser og internettrelatert etterforsking må digitale beslag forutsettes å inneholde virus og annen uønsket og skadelige programvare. Risikoen dette medfører gjør at det må håndteres utenfor politinettet. Dette bidrar imidlertid til at både bistand og samhandling blir vanskeligere. Faggrupperapporten bekrefter at manglende infrastruktur for håndtering av digitale beslag er et av de viktigste problemområdene for fagfeltet digitalt politiarbeid.[230]

Ifølge intervjuer med politiet er det, med unntak av i Oslo, DPA-personellet selv som drifter utstyr og nettverk som ikke er en del av politinettet. Det brukes betydelig med ressurser på drift av maskinpark som, med noen unntak, gjøres lokalt av DPA-personell. Inntil ett til to årsverk på drift i flere distrikter. Drift av maskinpark kunne vært overlatt til ansatte med slik fagbakgrunn, for å frigjøre kapasitet til etterforskning. Dette vil også

[226] Politiet (2019) *Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning.9. september 2019.*
[227] Politiet (2019),, *Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning. 9. september 2019.*
[228] Kripos (2019) *Seksuell utnyttelse av barn og unge over internett*.
[229] Hordaland, Sogn og Fjordane Statsadvokatembeter (2019) Rapport etter tilsyn med Vest politidistrikt sin innsats mot vold og sedelighet/voldtekt, rapport datert 30. oktober 2019.
[230] Politiet (2019) *Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning.9. september 2019.*

kunne sikre bedre kontroll på utskifting av utstyr for å unngå risiko som nedetid og tap av data forbundet med gammelt utstyr.[231]

Flere av de intervjuede politidistriktene peker på at det brukes betydelige ressurser til transport av beslag og reiser for gjennomgang av digitalt materiale hos geografiske driftsenheter. I dag reiser for eksempel etterforskere fra de ulike geografiske driftsenhetene i Vest politidistrikt til Florø eller Bergen for å avlevere og senere igjen for å gjennomgå digitalt innhold i sakene.

Politidirektoratet peker i intervju på at politiet har behov for en egen og bedre tilrettelagt IKT-infrastruktur, systemer og verktøy for å håndtere kriminalitetsutfordringene i det digitale rom. Det innebærer uakseptabel risiko for politiet å behandle digitalt materiale fra kriminell virksomhet i det ordinære politinettet og i lokale løsninger. Denne infrastrukturen er for mangelfull i dag, og DPA-enhetene har i stor grad vært nødt til å etablere lokale løsninger for å behandle sakene. Dette er utilfredsstillende. Det ville vært en stor forbedring om sentraliserte løsninger kunne ha erstattet lokale løsninger ifølge direktoratet.

10.1.2 Prosjekt Digitale spor og beslag (DSB)

Politiets IKT-tjenester (PIT) påbegynte utvikling av et felles beslagsnett i 2016 kalt Digitale spor og beslag (DSB). DSB-prosjektet hadde som formål å levere to tjenester:

- Et adskilt uavhengig nettverk for transport av data internt i politiet mellom enheter og distrikter – DSB-NETT.
- Et langtidslager for oppbevaring av digitalt beslagsmateriale – DSB-Arkiv

Håndtering av beslag fra saker vedrørende overgrep mot barn er gitt prioritet i prosjektet. I første omgang ble prosjektet begrenset til arkivering av digitale beslag fra avgjorte saker og en mulighet til å utveksle data mellom brukere av nettet.[232] Noen distrikter har fått anledning til internt i distriktet å benytte politinettet som bærer for et eget lokalt beslagsnett. Dette gir tilgang til distriktets digitale bevis fra flere steder.

Kartleggingsundersøkelsen til DPA-lederne viser at ti av tolv politidistrikter har tatt i bruk DSB-nett/DSB-arkiv. Flere peker på at det er for lite lagringsplass tilgjengelig og at nettet ikke er tilkoblet alle steder som har behov for det. Åtte av distriktene mener at DSB-nett og DSB-arkiv ikke, eller bare i noen grad, dekker det faktiske behovet DPA har for transport, oppbevaring og arkivering av elektronisk bevismateriale.

Før DSB-prosjektet ble igangsatt av PIT i 2016, hadde Oslo politidistrikt utviklet et eget beslagsnett fra 2010 som høsten 2019 fortsatt var i bruk. Ifølge Oslo politidistrikt overtok PIT ansvaret for dette nettet med IKT-ansatte og all infrastruktur i 2015, men har i ettertid ikke utviklet tjenesteinnholdet, kun lagringsplass og nødvendig drift. Konsekvensen for Oslo politidistrikt har vært at det lokale beslagsnettet omgås, beslag lagres lokalt, lastes over til system som har funksjonene som trengs for så å lastes opp igjen til det lokale beslagsnettet. Dette er arbeidskrevende og tungvint ifølge Oslo politidistrikt. DSB-prosjektet bygger ifølge Oslo politidistrikt, ikke på de erfaringer politidistriktet har og vil heller ikke svare ut det behovet Oslo politidistrikt har. Muligheter for gjenbruk eller utvidelse av Oslos beslagsnett synes heller ikke å ha vært vurdert av PIT. Funksjonene i det nye beslagsnettet er begrenset til lagring/filutveksling og er ikke tilrettelagt for analyse ifølge Oslo politidistrikt.

DPA i Vest politidistrikt har brukt øremerkede midler til innkjøp av datautstyr til utvikling av et lokalt beslagsnett som rulles ut i 2020.[233] Vest politidistrikt planlegger å bruke transportnettet i DSB-nett, men tilføre en analysedel som bygges kun for distriktet. Etterforskere vil da få tilgang til sin sak og veiledning til innholdsanalyse gjennom systemet. Sakene kan da ferdigstilles i den geografiske driftsenheten. Med et lokalt beslagsnett opplyser DPA i distriktet at de raskere og mer effektivt vil kunne gjennomgå en sak, og DPA vil kunne bruke tid på andre oppgaver. DPA samarbeider med PIT om etableringen av denne løsningen. PIT har ikke hatt ressurser til å bidra. DPA har derfor satt en av sine egne operative etterforskere til å arbeide fulltid med etableringen av tjenesten. DPA i Vest politidistrikt mener at dette er en dårlig utnyttelse av spesialistkompetanse. Vest politidistrikt mener tjenesten som etableres for fjerngjennomgang av sakene burde være av interesse også for andre distrikter, og burde gått på tvers av distriktsgrenser. Dette er kommunisert til PIT. Andre distrikter har meldt sin interesse for å utvikle lignende løsninger.

[231] Politiet (2019) *Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning.9. september 2019.*
[232] Politiet, 9. september 2019, Unntatt offentlighet, *Fagforvaltning statusrapport: Status fagområde datatekniske undersøkelser og internettrelatert etterforskning.*
[233] Politidistriktene fikk i 2018 øremerkede midler til bekjempelse av IKT-kriminalitet. Bruken av disse midlene rapporterte politidistriktene på i sine årsrapporter for 2018.

NC3 uttaler i intervju at de mener DSB-nett er en begrenset løsning som ikke møter det faktiske behovet politiet har. Politidistrikter og særorgan bruker egenutviklede løsninger. Konsekvensen av at norsk politi ikke har klart å gå sammen om å utvikle et system som løser distrikter og særorganers behov er akkumulert risiko for at det gjøres feil. Ettersom eksisterende løsninger fungerer til en viss grad, kommer man ikke i gang med en helhetlig tilnærming. Det burde ha vært utviklet en løsning sentralt som dekker alles behov. Dette medfører økte kostnader i noen år, men på lang sikt er det potensiale for å spare betydelige med ressurser på en mer sentralisert og systematisk tilnærming. Dette krever økte bevilgninger og prioritering ifølge NC3.

ØKOKRIM opplever at kapasiteten og funksjonaliteten i dagens DSB-nett er svært begrenset. ØKOKRIM har tilgang, men benytter det kun til utveksling av databeslag med politidistrikter og Kripos. DSB-nett er utviklet for å håndtere digitale beslag fra overgrepssaker. Implementeringen, arkitekturvalg og linjekapasitet tilsier at DSB-nett ikke vil løse ØKOKRIMs prosesserings- og lagringsbehov i nær framtid. ØKOKRIM mener likevel at prosjektet bør videreføres (med friske midler) for massesaker hvor det i dag knapt benyttes elektroniske spor for å avhjelpe kapasitetsutfordringer hos DPA.

Politidirektoratet påpeker i intervju at det har tatt for lang tid å få på plass sentrale løsninger, for eksempel DSB-nett. Det foreligger et forslag om videreutvikling av DSB-nett, men det er foreløpig ikke tatt beslutning om dette. Direktoratet er kjent med at DSB-nett foreløpig har begrensninger, og at distriktene fortsatt bruker betydelige med ressurser fordi det sentrale nettet mangler analysemuligheter. Politidirektoratet ser at det er potensial for å samordne beslagshåndtering og -gjennomgang i politidistriktene for å utnytte etterforskningskapasiteten på en bedre måte. Videreutvikling av blant annet DSB-nett vil kunne bidra til å løse utfordringer på dette området.

10.1.3 Retningslinjer, rutiner og standarder for sikring av digitale bevis

Sikring og analyse av digitalt bevismateriale gjøres i de fleste tilfeller av dataetterforskere i politidistriktene ved hjelp av avansert spesialverktøy og programvare som kan kreve omfattende opplæring. Tidligere rapporter og strategier peker på utfordringer på dette området. Kartleggingen som ble gjennomført i 2012 peker på at det kunne være hensiktsmessig å gi sentrale føringer på hvilke verktøy, metoder og retningslinjer som skal gjelde innen dette tekniske og kompliserte saksområdet. I rapporten hevdes det at dette vil kunne gi effektiviseringsgevinster, bidra til bedre rettssikkerhet og gjøre det enklere å imøtegå eventuelle innvendinger til politiets kompetanse på området.[234]

I faggrupperapporten om datatekniske undersøkelser og internettrelatert etterforskning fra 2019 vises det til at det ikke finnes noen enhetlig strategi eller systematikk knyttet til utforming, forankring, deling og oppbevaring av støttedokumenter. Selv om det er mye god metodeutvikling som skjer lokalt, blir denne i liten grad delt med resten av politiet og er ikke tilgjengelig for alle som trenger det. Dette hemmer læring og utvikling innen faget digitalt politiarbeid, medfører risiko for utvikling av ulik praksis, og medfører trolig store effektivitetstap ifølge rapporten. Forankring og kvalitetssikring av eksisterende støttedokument/retningslinjer er fraværende, og gode løsninger blir dermed forankret lokalt uten ekstern evaluering eller gjennomgang. Faggruppen anbefaler at Politidirektoratet gjennomgår rutiner og retningslinjer for å sikre at de er oppdatert og dekkende for det digitale politiarbeidet.[235]

I intervjuene med politidistriktene etterlyses det mer retningslinjer og standarder for digitalt politiarbeid. Utarbeidelse av rutiner og veiledere blir i for stor grad opp til det enkelte distrikt og det etterlyses tydeligere nasjonale føringer på hvilke digitale bevis som skal innhentes og etterforskes.

Kartleggingsundersøkelsen blant DPA-ledere i politidistriktene viser at retningslinjer og rutiner mangler i mange politidistrikt, og mange politidistrikt savner støttesystemer i arbeidshverdagen.

- Seks av tolv DPA peker på at de savner nasjonale retningslinjer på eget fagområde.
- Fem av tolv DPA har ikke utarbeidet egne rutiner, retningslinjer eller veiledninger for digitalt politiarbeid/sikring av elektroniske bevis som gjøres av andre enn DPA.
- To av tolv DPA har utviklet retningslinjer for digitalt politiarbeid/sikring av elektroniske bevis for alle politifunksjoner. Flere svarer at de har rutiner for fagkontakter og etterforskere.
- Åtte av tolv DPA svarer at de savner støttesystemer for å utføre oppgavene funksjonen har ansvar for på noen eller alle områder.

[234] Politidirektoratet (2012) *Politiet i det digitale samfunnet: En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett.*
[235] Politidirektoratet (2012) *Politiet i det digitale samfunnet. En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett*, 10.

- I politidistrikter der det er etablert rutiner, retningslinjer eller veiledninger for digitalt politiarbeid/sikring av elektroniske bevis som gjøres av andre enn DPA, er det ulikt hvordan DPA følger opp bruken av disse.

Kripos' forslag til nasjonal løsning for håndtering av overgrepsmateriale fra 2016–2017 er et eksempel på forsøk på utrulling av nasjonale retningslinjer. Anbefalingene Kripos ga er ikke gjennomført fullt ut i distriktene. Politidirektoratet sier i intervju at det burde vært utarbeidet nasjonale retningslinjer på dette området. Det er derfor gitt et oppdrag til faggruppen for datatekniske undersøkelser og internettrelatert etterforskning om å utarbeide retningslinjer for politiets håndtering og gjennomgang av digitale beslag for ulike brukergrupper, med fokus på initialfasen. Her er politipatruljer og FSI de primære brukergruppene. Retningslinjene vil utarbeides i samarbeid med Riksadvokaten og omhandle politiets håndtering og gjennomgang av digitale beslag for ulike brukergrupper, med vekt på initialfasen (patruljen, FSI).

10.2 Utvikling og bruk av støttesystemer i Kripos/NC3 og ØKOKRIM

Kripos/NC3 og ØKOKRIM viser i intervju til at behovet for støttesystemer for lagring og håndtering av digitale beslag er økende. De to særorganene har utviklet og tatt i bruk egne løsninger for å håndtere behovene de har.

NC3 viser til at det er et stadig økende behov for lagring av store mengder informasjon og økt prosesseringskraft i alle straffesaker. For å håndtere en økende mengde digitale beslag har Kripos blant annet inngått samarbeid med nederlandske politi om bruk av programvareløsningen «Hansken». «Hansken» er utviklet av nederlandsk politi og benyttet i mer enn 700 straffesaker i Nederland. Løsningen er utviklet for å håndtere saker med mange og store beslag samtidig på en effektiv måte, og er avhengig av avansert teknisk infrastruktur som krever spesialistkompetanse for drift og videreutvikling.[236]

Faktaboks 5 Programvareløsningen «Hansken»

I 2017 og 2018 gjennomførte Kripos i samarbeid med ØKOKRIM, og Oslo og Øst politidistrikter en pilot på sentralisert prosessering av digitale beslag ved bruk av «Hansken». Løsningen ble testet ut på saker innen økonomisk kriminalitet, narkotika, vold, sedelighet, datakrim, drap, mv. i 2017 og 2018. Sluttrapport for utprøving av løsningen ble oversendt Politidirektoratet 20. juni 2018.[237]

I et intervju med Politiforum sier en etterforsker fra Kripos som testet løsningen følgende:[238]

> *«Mens mange etterforskere i dag trenger hjelp fra spesialetterforskere for å tolke databeslag, kan Hansken gjøre at flere vanlige etterforskere kan bruke dataene og finne fram selv. Det er bra for rettssikkerheten i de sakene som ikke når opp eller må stå i kø hos spesialetterforskere med begrenset kapasitet.»*

NC3 bruker Hansken i Hydro-saken og programvaren er veldig nyttig i etterforskningen. NC3 tester ut løsningen, og betaler foreløpig ikke noe for bruken. Hansken kan sees på som infrastruktur/konsept/verktøy/system i løpende utvikling. Kripos ønsker å fortsette å bruke Hansken, og må da betale for lisenser. Kripos er partner med NFI i Nederland som har laget programvaren, og skal være med og bidra til videreutvikling av Hansken både som verktøy og konsept på vegne av politiet.

ØKOKRIM kjenner også konkret til Hansken gjennom besøk hos NFI og samarbeid med forskere bak konseptet. Løsningen er foreløpig tilpasset håndtering av overgrepssaker med bilde og videomateriale, og er foreløpig ikke like god for håndtering av tekst og bedriftssystemer som ØKOKRIM ofte forholder seg til. Designet og arkitekturen til Hansken er ifølge ØKOKRIM bra og kan skaleres til også å håndtere ØKOKRIMs saker. Men funksjonaliteten gjør at den på nåværende tidspunkt ikke er et egnet alternativ

[236] Politidirektoratet (2019) *Faggrupperapport datatekniske undersøkelser og internettrelatert etterforskning*.
[237] Kripos (2018) *Kripos 2018 2. Tertial*, tertialrapport 2. kvartal 2018 til Politidirektoratet.
[238] Politiforum (2018) Nederlandsk big-data-program analyserer store mengder data på rekordtid. Nå anbefaler Kripos at norsk politi får ta det i bruk. Artikkel publisert 8. juni 2018.

for ØKOKRIM. Dette er verifisert gjennom samarbeid med FIOD (Toll/Skatt Nederland) som har saker med tilsvarende utfordringer som ØKOKRIM.

I styringsdokumentet for DSB-prosjektet fra august 2019 fastslås at prosjektet ikke skal vurdere eller realisere samhandlings- og verktøybehov utover en minimums verktøykasse basert på dagens mest anvendte programvare.[239] Men det kan gjøres unntak for vurdering av Hansken, slik at en mulig framtidig anskaffelse av dette verktøyet vil kunne gjennomføres uten større arkitekturendringer i det framtidige DSB-konseptet.

Kilde: Tekst endres

ØKOKRIM viser til at sakene de har ansvar for kjennetegnes av svært store databeslag med mye tekstlig informasjon fra bedriftsmiljøer, og at volumutfordringene på dette området traff ØKOKRIM før det traff Kripos og politidistriktene. ØKOKRIM har derfor gjennom 15 år har vi satt sammen et sett av kommersielle verktøy med spesialtilpasset infrastruktur for å håndtere stadig økende datamengder. ØKOKRIM mener dette er veien å gå og har aktivt støttet etatens arbeid med sentralisert lagring og prosessering av digitale beslag. Systemet er på mange måter sammenlignbart med Hansken.

Ifølge Politidirektoratet har ulike aktører i politiet utviklet egne løsninger. Direktoratet har bevilget penger til blant annet oppbygging av meget gode beslagshåndteringssystemer både hos ØKOKRIM og Kripos. Hansken kommer i tillegg til andre systemer Kripos har etablert for beslagslagring og gjennomgang, og er bedre enn de politidistriktene har. Årsaken til dette er at Merverdiprogrammet ble vedtatt stanset i 2016. Merverdiprogrammet skulle levere løsninger for beslagshåndtering, men når programmet ble stanset, har det heller ikke kommet sentrale løsninger. Resultatet av dette er at særorgan og distrikter utvikler egne løsninger for å dekke eget behov. Dette burde ha vært løst med sentraliserte løsninger.

[239] Politidirektoratet (2019) *Styringsdokument - Digitale Spor og Beslag (DSB)*, godkjent av styringsgruppen 22. august 2019.

11 Organisering og samarbeid

Dette kapitlet omhandler betydningen av organisering og samarbeid for oppklaring av IKT-kriminalitet. IKT-kriminaliteten har det kjennetegnet at den kan utøves samtidig mot mange fornærmede på tvers av politidistriktene. Organisering av saksmottak og enheter for digitalt politiarbeid er viktig i denne sammenhengen. I tillegg er samarbeid mellom politidistrikter, mellom politidistrikter og særorgan, og med næringslivet avgjørende for å oppklare denne typen saker.

11.1 Organiseringen av mottaket av anmeldelser

Hvordan politiet håndterer innkommende saker, har betydning for det videre etterforskningsarbeidet og mulighetene for å oppklare sakene. Politireformen har lagt opp til en mer enhetlig og standardisert organisering av saksmottaket. Felles straffesaksinntak (FSI) er etablert i hvert politidistrikt for mottak av alle straffesaker for å sikre befolkningen så lik behandling som mulig, uavhengig av hvor de utsettes for kriminelle handlinger. FSI har i de fleste politidistrikt integrert påtaleledelse og politifaglig etterforskingsledelse for å styrke kvaliteten på den innledende straffesaksbehandlingen. FSI gjør en innledende vurdering av sakene og prioriterer om etterforskingsskritt skal iverksettes, henlegges eller overlates andre myndigheter. FSI har også en viktig rolle i å fordele saker til rett etterforskningsenhet i politidistriktene og er fortsatt under utvikling.

Kripos/NC3 og flere politidistrikter oppgir i intervju at evnen til å se sammenheng i saker er en utfordring. I saker som forekommer hyppig er det grunn til å tro at det foregår kriminalitet på tvers av politidistrikter hvor gjerningspersoner forsøker seg på mange ofre, ofte med økonomisk formål. Utbyttet i hver enkelt sak kan være lavt, men samlet kan det nasjonalt være snakk om store summer. I de fleste distrikter håndterer FSI store saksmengder og har ikke kapasitet til å analysere sammenheng i sakene. Det er heller ingen som ser på sammenhenger i saker nasjonalt. Evne til å fange opp trender og sammenhenger i kriminalitetsbildet mangler. Når politiet ikke har systemer for å fange opp sammenhenger mellom saker, eller vektlegger å lete etter slike saker, fører det til at for eksempel organiserte kriminelle som utøver IKT-kriminalitet mot mange ofre samtidig i liten grad avdekkes. Dette bekreftes av større næringslivsaktører som er intervjuet i forbindelse med undersøkelsen.

Ifølge politidistriktene er det også utfordringer ved den tidlige håndteringen av anmeldelser av alvorlig IKT-kriminalitet med stort skadepotensial. Det forekommer at saker ikke blir registrert, at de ikke blir overlevert videre raskt nok, at saker ikke blir ikke oppfattet som alvorlig nok, og/eller at etterforsker som får ansvar for saken ikke har kompetanse til å sette i gang formålstjenlige etterforskningsskritt. Politidistriktene peker på at politiet har for dårlig kompetanse i mottakssiden, og at kapasiteten til å behandle sakene videre inn i systemet er for lav.

I en rapport til Politidirektoratet høsten 2019 vises det til at FSI, i motsetning til intensjonen, ikke er organisert likt i distriktene. Ingen FSI var organisert i henhold til rutinebeskrivelse fra Politidirektoratet.[240] Ifølge rapporten gir dette utfordringer med hensyn til å utvikle nasjonale rutinebeskrivelser for hvordan FSI skal driftes. Hensikten med tiltaket, som var å sikre befolkningen så lik behandling som mulig uavhengig av hvor man utsettes for kriminelle handlinger, blir ikke optimalt fordi polititjenestene som leveres i initialfasen er ulike.[241] Det er ikke etablert rutiner for å fange opp sammenhenger i mengdesakene ved FSI.[242] I en faggrupperapport om operativ kriminalanalyse pekes det på at det hadde vært nyttig for FSI og politiet å ha kontroll på endringer i kriminalitetsbildet og ha rutiner for å undersøke modus, se etter fellestrekk, og innrette tiltak og forebyggende innsats deretter. Rapporten peker også på at det hadde vært nyttig å se kriminaliteten på tvers av distrikter for å fange opp kriminelle som begår lovbrudd i flere distrikter.[243]

---

[240] Formål, organisasjonstilhørighet, hovedoppgaver, organisering av arbeidet og roller med tilhørende ansvar er beskrevet i Rammer og retningslinjer for etablering av nye politidistrikter fra Politidirektoratet. Politidirektoratet har i tillegg utarbeidet veiledere som beskriver hvordan FSI er tenkt å fungere: *Forberedelse av varetektsfengsling - FSI, Kommunikasjon og samhandling- FSI/OPS/PPS, Mottak og registrering av anmeldelser, Veileder for etterforskningsledelse i FSI, Vurdering og fordeling av saker- FSI, Påtaleavgjørelser og beslutninger om tvangsmidler- FSI,* og *Bruk av BL - Rollebeskrivelser- FSI.*

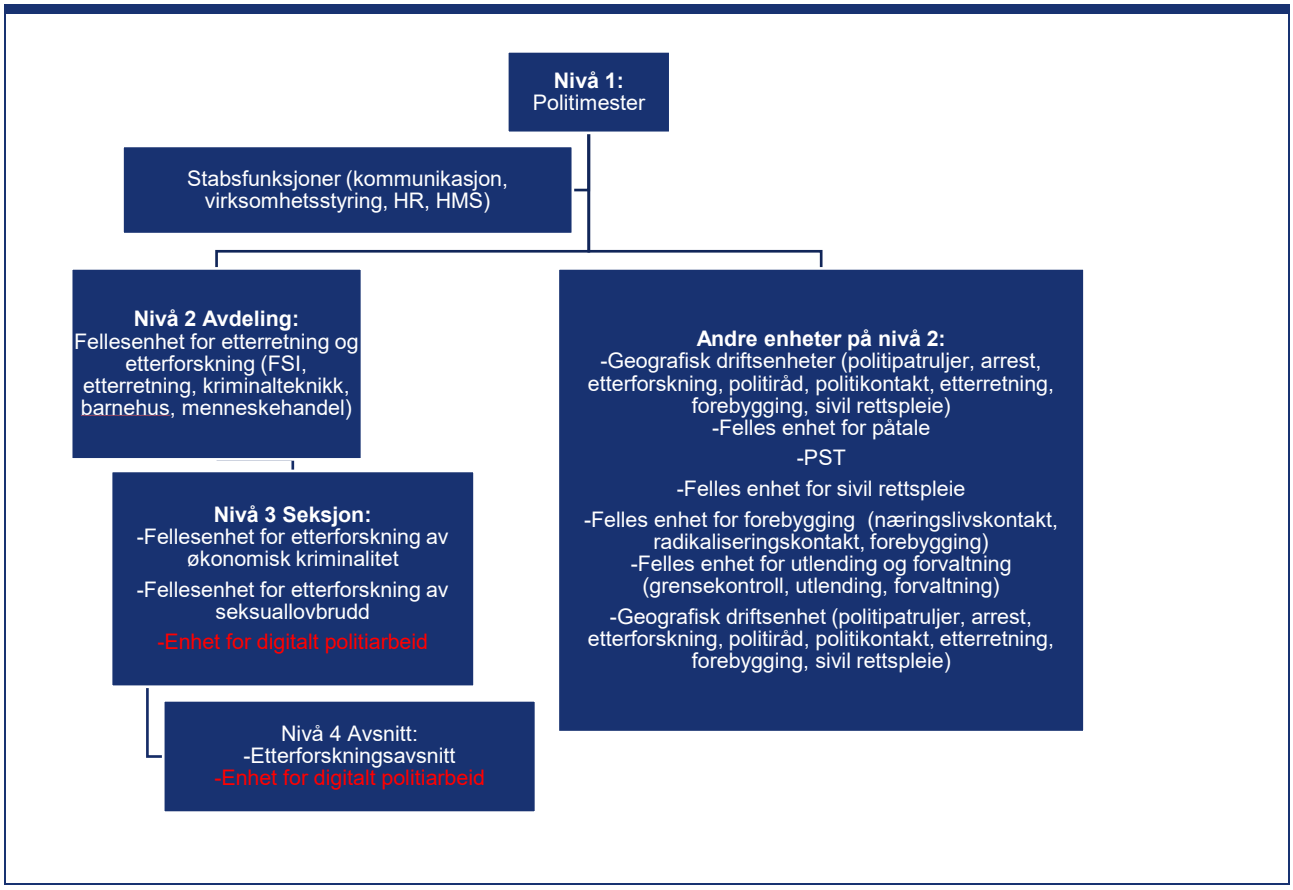
[241] Politidirektoratet (2019) *Status fagområde etterforskningsledelse*, faggrupperapport levert Politidirektoratet i september 2019.

[242] Se Faggrupperapporten om operativ krimanalyse, s. 17.

11.2 Organiseringen av DPA i politidistriktene

Politidirektoratet har i forbindelse med politireformen lagt føringer om at enhet for digitalt politiarbeid (DPA) skal organiseres under Felles enhet for etterretning og etterforskning (FEE).[244] Deler av funksjonen kan være lokalt plassert der det er hensiktsmessig.[245] I en faggrupperapport til Politidirektoratet hevdes det at DPA i politidistriktene bærer preg av å være ulikt organisert, og på ulike nivå i politiorganisasjonen.[246] Ifølge rapporten preger dette flere av politidistriktene negativt, og skaper mål- og interessekonflikter. Dette understøttes av intervjuer med politidistriktene og kartleggundersøkelsen til politidistriktene. Det er særlig DPA i politidistriktene hvor DPA er organisert på et lavt nivå som er opptatt av denne problemstillingen.

Figur 16 Organisering av DPA i distriktene



Kilde: Riksrevisjonen

Figuren over viser hvilke nivåer i organisasjonen enhet for digitalt politiarbeid er organisert på. I noen distrikter er DPA organisert på nivå tre under politimester som seksjon, i andre politidistrikt på nivå fire som avsnitt.

Tabell 7 Organisering av enhet for digital politiarbeid i politidistriktene

Distrikt	Seksjon, nivå 3	Avsnitt, nivå 4	Som seksjon utenfor FEE/FEFE
Vest		DPA er organisert som avsnitt under seksjon for kriminalteknikk og digitalt politiarbeid, under FEE.	
Innlandet		X	

[244] I mindre distrikter er også forebygging lagt til enheten som da heter Felles enhet for etterretning, forebygging og etterforskning (FEFE).
[245] Politidirektoratet (2017) *Rammer og retningslinjer for etablering av nye politidistrikter,* versjon 1.2, 16. juni. 2017
[246] Politidirektoratet (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning*, faggrupperapport utarbeidet av en arbeidsgruppe på oppdrag fra Politidirektoratet, datert 9. september 2019.

Oslo			**Seksjon under Felles kriminalenhet**
Sør-Øst	X		
Øst	X		
Finnmark		Sammen med kriminalteknisk, uten dedikert DPA-leder.	
Agder		X	
Nordland		Sammen med kriminalteknisk, uten dedikert DPA-leder.	
Sør-Vest	X		
Trøndelag		X	
Troms		Sammen med kriminalteknisk, uten dedikert DPA-leder.	
Møre og Romsdal		**X**	

Kilde: Organisasjonskart fra politidistriktene.

Tabellen over viser at kun fire av tolv politidistrikter har DPA organisert som seksjon. Fire DPA er i tillegg organisert sammen med kriminalteknisk. Det er hovedsakelig de distriktene hvor DPA er organisert som avsnitt eller sammen med kriminalteknikk som melder om ulemper med organiseringen. DPA i tre av disse distriktene oppgir også i kartleggingsundersøkelsen at forebygging og etterforskning av teknologikrevende datakriminalitet er mindre viktig. To politidistrikt oppgir i intervju at ulik organisering av DPA gir utfordringer med hensyn til kunnskapsdeling og kompetanseutvikling. Det vises også til at det mangler nasjonale rammeverk, fagstyring og føringer for organisering av funksjonen. Digitalt politiarbeid blir for lite synlig nasjonalt, og det gir ikke nødvendig framdrift i arbeidet med å omstille politiet til endringene i kriminalitetsbildet med mer IKT-kriminalitet.

11.3 Samarbeid innad i politiet

Flere av politidistriktene som er intervjuet, peker på manglende incentiver for samarbeid mellom politidistriktene. Etterforskningen av internettrelaterte seksuelle overgrep og nettbedragerier medfører at en gjerningsperson kan ramme mange hundre ofre over hele landet i løpet av kort tid med samme metode. Å avdekke og etterforske slike saker forutsetter derfor samarbeid mellom politidistriktene. Flere av politidistriktene som er intervjuet mener det bør større grad av nasjonal koordinering til i disse sakene. Et av politidistriktene sier følgende om situasjonen:

> *«Samarbeid på tvers av distriktsgrenser er utfordrende. Distriktene har ulik organisering og ulik ansvarsdeling på sakstrekk. Alle distrikter har mange saker å etterforske. Ettersom incentiver for å bistå andre distrikter er fraværende, blir samarbeid ofte nedprioritert. Det samme gjelder overtagelse av saker fra andre distrikt. Man gir heller fra seg saker enn å ta de selv. Å ta over en sak kan også innebære å begynne på nytt med etterforskningen, og ettersom digitale spor er flyktige kan dette ha negativ påvirkning på muligheter for oppklaring. For saker som berører flere politidistrikter samtidig er dette en utfordring.»*

Ifølge Kripos er en av de viktigste utfordringene norsk politi har innen etterforskning av internettrelaterte seksuelle overgrep, mangel på samordning og muligheter for å dele etterforskningsresultater. I dag gjennomgås bilder/video i hvert enkelt distrikt uten samordning. En nasjonal løsning, som beskrevet i kapitlet om støttesystemer, kunne bidratt til kvalitetsheving, mer treffsikkerhet, ville forenklet identifiseringsarbeidet og spart etterforskerne for mye arbeid. Kripos peker også på at kunnskap om hvor mange saker som gjelder internettrelaterte overgrep som finnes i politiets systemer, hvem de fornærmede er, og hvem gjerningspersonene er, har ikke politiet god nok kontroll på. Per i dag foreligger en betydelig mengde informasjon i form av registrerte anmeldelser og straffesaker i politiets saksbehandlingssystem BL, i etterretningssystemet Indicia og i form av tips som kunne vært utnyttet bedre. Dette er informasjon som burde vært systematisert og analysert for å avdekke pågående overgrep. For å få til dette trengs personell som har dette som sin oppgave og som støtter opp om informasjonsbehovet politiet har.

Tilsvarende utfordringer finnes innen etterforskningen av økonomisk IKT-kriminalitet. I en rapport fra Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) vises det til at fornærmede i hele landet utsettes for systematiske bedrageri. Saker med fellesnevnere registreres i hvert enkelt politidistrikt og

likhetstrekk mellom politidistriktene avdekkes ikke. Både NTAES og politidistriktene som er intervjuet peker på manglende nasjonal koordinering av politiets innsats i slike saker. Ifølge NTAES-rapporten tvinger lav etterforskningskapasitet politidistriktene til å bli reaktive og saksorienterte. Det mangler etterretning, analyser og vurderinger av bedragerifenomener som treffer mange distrikter samtidig. Politidistriktene viser til at det er behov for at noen ser sakene i sammenheng nasjonalt, ikke bare fordi gjerningspersoner kan stå bak flere saker i flere distrikter, men også fordi det kan være at etterforskning gjennomføres flere steder uten koordinering. I NTAES-rapporten anbefales det å sikre at anmeldelser registreres med riktig straffesakskode og at næringsliv og andre aktører deler informasjon om modus og trender med politiet slik at denne typen saker fanges opp.[247]

Samtidig finnes det eksempler på at politidistriktene lykkes med samarbeid. Eksempler er samarbeid om etterforskning av «Olga-svindel»[248] og direktørsvindel. Næringslivskontakter og bankene har bidratt til at saker ses i sammenheng, i tillegg er det opprettet samarbeid mellom distriktene som følge av etterforskning av enkelt saker.

Anmodning om sentralisering av etterforskning kan fremmes av politimestrene, sjef Kripos eller statsadvokatene, og riksadvokaten treffer beslutning etter å ha rådført seg med Politidirektoratet.[249] NC3 viser til at enhetens kapasitet utnyttes best ved å gi råd og bistand inn i et større antall saker som håndteres av distriktene lokalt. På den måten kan NC3s kapasitet og kompetanse utnyttes i et langt større antall saker enn hvis all kapasitet skulle gå med til å etterforske sakene fra start til slutt. Distriktene kan etterforske med bistand fra Kripos selv om sakene kan være kompliserte å etterforske. NC3 mener samarbeid mellom distrikter er vanskelig å få til, og Kripos kan bli flinkere til å drive fram dette. Der det er behov for samarbeid spør distriktene gjerne Kripos om å overta saken. Kripos mener de kanskje kunne hatt en rolle her, med tanke på å se sammenhenger og koordinere innsats. Samtidig understreker Kripos at det er viktig at de er en støttefunksjon i å få til koordinering og samarbeid, og overtar ikke ansvaret fordi en sak treffer flere distrikter.

Politidirektoratet viser i intervju til at gjennom politireformen har politiet gått fra 27 til 12 politidistrikter. Hvert distrikt har større nedslagsfelt, er mer robust og vil kunne koordinere større saker. Enkelte politidistrikter har opprettet prosjekter der de prioriterer en sakstype for en periode. Operasjon Dark Room i Vest politidistrikt er et slikt eksempel. Når utspringssaker sendes andre politidistrikter kan det forekomme at mottaker distrikter ikke prioriterer saken like høyt. Politidirektoratet peker på at Kripos bistår politidistriktene i enkelt saker og i saker på tvers av politidistrikter.

11.4 Samarbeid med næringslivet

Politiet samarbeider med Næringslivets sikkerhetsråd (NSR). I tillegg har næringslivskontaktene i politidistriktene god dialog med NSRs regionale kontakter. For eksempel arrangerte politiet i samarbeid med NSR og PST i 2018 og 2019 flere åpne møter både nasjonalt og lokalt, hvor offentlige og private aktører fikk kjennskap til det aktuelle trusselbildet i Norge.

Politidistriktene og Kripos har nylig innført en ordning med næringslivskontakter (NLK) som skal sørge for samarbeid mellom politi, næringsliv, sikkerhetsmyndigheter og andre aktører. I de større distriktene er rollen plasser under fellesenhet for forebygging, i de mindre under fellesenhet med ansvar for forebygging, etterretning og etterforskning.

Politidirektoratet viser til at NKL er sentral i utviklingen av politiets primærstrategi, kriminalitetsforebygging, i samarbeid med andre.[250] Alle NLK samles fem ganger per år og utveksler erfaringer og kompetanse. Ifølge Politidirektoratet er NLKs viktigste oppgave innen digital sikkerhet å bidra til å øke private virksomheters evne og bevissthet til å beskytte seg mot uønskede digitale hendelser, gjennom blant annet formidling av trusselvurderinger fra PST, E-tjenesten, NSM, Kripos, Europol og andre relevante rapporter. NLK henviser ofte til relevante aktører og hjemmesider tilhørende NSM og NorSIS. Det foregår også samarbeid med akademia om digital sikkerhet, styrking av NLKs kompetanse på IKT-kriminalitet og foredrag/seminarer for næringslivet, blant annet i samarbeid med Næringslivets sikkerhetsråd og Politiets sikkerhetstjeneste.

[248] Kriminelle tar kontakt med eldre, enslige offer og utgir seg for å representere vedkommendes bank. Bedrageriene kommer i perioder, og hadde i løpet av første halvår 2020 en aktiv periode.
[249] Meld. St. 7 (2010–2011) *Kampen mot organisert kriminalitet*.
[250] Politidirektoratet (2019) *Næringslivskontaktenes rolle - forebygging av IKT-kriminalitet*, notat til Riksrevisjonen, 1. oktober 2019.

Kunnskap om trusselbildet formidles også i sosiale medier, og det gjennomføres dialogmøter med virksomheter som ønsker kontakt.

NLK i Sør-Øst politidistrikt tok i 2018 initiativ til en rapport om kriminalitet som rammer næringslivet.[251] I rapporten er fire av de seks mest aktuelle truslene for næringslivet IKT-kriminalitet omtalt: direktørsvindel, løsepengevirus, dataskadeverk/sabotasje og informasjonstyveri. Rapporten er delt med NLK i alle politidistrikter. NLK i Oslo politidistrikt og Møre og Romsdal politidistrikt viser i intervju til at mange av sakene næringslivet melder fra om dreier seg om bedragerier i forskjellige former, ofte alvorlige bedragerisaker. Bare i 2019 er NLK i Oslo gjort kjent med flere større bedragerisaker rundt omkring i landet hvor den største innebar et tap på 150 millioner kroner. NLK i Møre og Romsdal peker på at sakene ofte er krevende å etterforske, og vanskelig å oppklare fordi gjerningspersoner befinner seg i utlandet. Rask innsats og stopping av pengeoverførsler blir derfor prioritert.

NLK i Oslo politidistrikt opplever at rollen som NLK er positivt mottatt av næringslivet, og kunnskapsdelingen som foregår styrker kompetansen begge veier. En generell utfordring NLK i både Oslo og Trøndelag opplever er at næringslivet har liten tillit til politiets kompetanse, kapasitet og ressurser til å håndtere IKT-kriminalitet. NLK i Trøndelag politidistrikt forteller at mange bedrifter som utsettes for IKT-kriminalitet får beskjed når de ringer om at dette ikke er noe politiet kan bistå med. Dette fører til at mange bedrifter lar være å anmelde saker.

Ifølge NLK i Oslo politidistrikt har politiet et svakt kunnskaps- og situasjonsbilde på området fordi næringslivet ikke anmelder og fordi det er vanskelig å lese ut av anmeldelsesstatistikken hva som foregår. Politiet mangler kunnskap og etterretning for å kunne se bedragerisaker i sammenheng både lokalt og nasjonalt. Samme gjerningsperson er ofte involvert i saker på tvers av distriktene og landegrenser, og det er også flere store kriminelle nettverk som utøver denne type kriminalitet. Større grad av samarbeid om analyse og etterretningskompetanse er ønsket fra næringslivet uten at politiet så langt har klart å møte denne invitasjonen. Fra politiets side gjøres det framskritt, større saker er etterforsket og gjerningspersoner er dømt, blant annet i Oslo politidistrikt og utenlands, men det er fortsatt en vei å gå på dette området, ifølge NLK.

[251] Sør-Øst politidistrikt (2018) *Kriminalitet i og mot næringslivet – Trusler og trender*, rapport utarbeidet av to medarbeidere i Sør-Øst politidistrikt.

12 Bruker politiet internasjonalt samarbeid til å avdekke og oppklare IKT-kriminalitet?

IKT-kriminalitet kjennetegnes ved at det enkelt kan begås på tvers av landegrenser. IKT-verktøy gjør det mulig å angripe mange mål samtidig eller dele ulovlig overgrepsmateriale globalt, ofte med lav oppdagelsesrisiko. Internasjonalt samarbeid er derfor ofte avgjørende for oppklaring av sakene særlig der hvor gjerningspersonen befinner seg i utlandet. Norge er et velstående, digitalisert land og derfor attraktivt for svindlere og personer som driver med utpressing. I 2018 ble det hevdet at Norge var et av landene i verden hvor datakriminelle så størst muligheter til å gjennomføre en vellykket svindel via e-post (phishing).[252] Etterforskning utenlands er ofte tidkrevende og komplisert. Ulikheter i nasjonal lovgivning og tungvinte prosesser rundt rettsanmodninger fører til at politiet ofte nedprioriterer oppklaring av saker med gjerningsperson utenlands.

12.1 Norsk politi er ikke alene om utfordringer forbundet med internasjonalt samarbeid

I 2019 publiserte Eurojust og Europol en rapport om hvilke utfordringer IKT-kriminalitet skaper for politi og påtalemyndigheten i europeiske land.[253] I rapporten grupperes utfordringene i fem kategorier:

1. Manglende tilgang til data – datalagringsdirektivet, GDPR-lovgivningen, kryptering og kryptovaluta gjør det vanskelig å avdekke og etterforske lovbrudd og identifisere gjerningspersoner.
2. Manglende opplysninger om åsted og IKT-verktøy – kryptering, anonymiseringsverktøy, kryptovaluta, Dark Web og skyløsninger gjør det vanskelig å identifisere gjerningspersoner, avgjøre jurisdiksjon og finne ut hvor lovbruddet fant sted, og avdekke hvilke metoder som er brukt.
3. Forskjeller i nasjonal lovgivning – selv om det finnes internasjonale avtaler på området er disse i varierende grad gjennomført på nasjonalt nivå, og forskjeller i lovgivning, straffer og politiets mandat til å etterforske kriminalitet på internett varierer og skaper utfordringer.
4. Hindringer for internasjonalt samarbeid – det mangler systemer for effektiv deling av bevis og politisamarbeid. Samarbeidet tar ofte tid og krever involvering av juridiske myndigheter og rettsanmodninger, og gjør det også vanskelig å respondere på større, koordinerte dataangrep som rammer mange virksomheter på tvers av land, jf. Wannacry- og NotPetya-virusene.
5. Utfordringer i samarbeidet mellom offentlige og private virksomheter – juridiske utfordringer for samarbeid, lovgivning for personvern og informasjonssikkerhet, jurisdiksjon for tjenesteleverandører med tilstedeværelse i mange land og teknologiutviklingen i næringslivet skaper utfordringer.

I Meld. St. 29 (2019-2020) vises det til at Norge deltar i Europarådets utarbeidelse av en tilleggsprotokoll til Budapestkonvensjonen om samarbeid om cyberkriminalitet og tilgang til elektroniske bevis. Norge følger også EUs arbeid om forenklet prosedyre for å innhente og sikre elektroniske bevis over landegrensene, og om tiltak for forenkling av rettslig bistand i straffesaker. Norge bidrar også i arbeidet med IKT-kriminalitet i FN, blant annet i samarbeidet mellom FN og Interpol.

12.2 Norsk politis utnyttelse av internasjonalt samarbeid i innsatsen mot IKT-kriminalitet

I en nylig gjennomført gjennomgang av internasjonalt straffesaksarbeid oppgir de tre seksjonene hos Kripos med ansvar for internasjonalt samarbeid at det generelt er mangelfullt eller varierende nivå på norsk politi når det gjelder internasjonalt straffesaksarbeid. Politidistrikter og Kripos er også enig i at KO:DE, politiets fagportal, bør forbedres og gjøres mer brukervennlig.[254]

[252] Symantec 2019 *Internet Security Threat Report*, Volume 24, February 2019.
[253] Eurojust and Europol, 2019 *Common challenges in combating cybercrime – As identified by Eurojust and Europol*, Joint report, June 2019.
[254] Politidirektoratet (2019) *Fagforvaltning statusrapport - Status fagområde Internasjonalt straffesaksarbeid*, 2. oktober 2019.

Norsk politi deltar på en rekke samarbeidsarenaer internasjonalt, i Norden, under EU, Europol[255], Eurojust[256], Interpol, FN, osv. Kripos er det nasjonale kontaktpunktet for internasjonalt politisamarbeid og har den faste kontakten med de fleste internasjonale samarbeidsorganer. Kripos brukte ca. 10 prosent av et budsjett på 551 millioner kroner i 2017 på internasjonalt politisamarbeid.[257] ØKOKRIM er det nasjonale kontaktpunktet for finansielle etterretningsopplysninger mens riksadvokaten er Eurojusts kontaktpunkt.

Faktaboks 6 Internasjonale organisasjoner norsk politi utnytter i innsatsen mot IKT-kriminalitet

Eurojust er etablert av EU, og Norge har hatt en samarbeidsavtalesiden 2005. Eurojust er samarbeidsorgan for medlemslandenes påtalemyndigheter. Samarbeidet gjør det enklere å etterforske og oppklare større straffesaker med forgreninger i flere land innen EU.

Europol er EUs organisasjon for politisamarbeid mellom medlemslandene. Norge har deltatt i Europol siden 2001. Europol har særlig oppmerksomhet mot kriminelle grupper som opererer på tvers av landegrenser, og etablerte i 2013 et europeisk datakrimsenter (EC3) som er navet i medlemslandenes innsats mot IKT-kriminalitet.

Interpol er en internasjonal politiorganisasjon med 194 medlemsland. Interpol åpnet i 2015 et nytt cyberkrimsenter Interpol Global Complex for Innovation (IGCI) i Singapore.

Kripos er nasjonalt kontaktpunkt for internasjonalt politisamarbeid, herunder kontakt med Interpol og Europol sine kompetansesentre for bekjempelse av IKT-kriminalitet.

Kilde: Regjeringen

Kripos har flere roller innen internasjonalt politisamarbeid. De har blant annet etterforskningsansvar for internasjonale straffesaker. Kripos er også kontaktpunkt for sikring av elektroniske spor ved henvendelser fra utlandet og utveksling av personopplysninger som del av Schengen-samarbeidet. Kripos viser i intervju til at det internasjonale etterretningssamarbeidet er betydelig enklere enn straffesakssamarbeidet som følge av at virkemidlene for utveksling av straffesaksopplysninger er krevende. Kripos peker videre på at samarbeidet er enklere når det gjelder internettrelaterte seksuelle overgrep. I «Operasjon Duck» samarbeidet Trøndelag politidistrikt og Kripos tett. Dette bidro til at informasjon av relevans for utenlandsk politi ble delt og gjerningspersoner utenlands ble etterforsket. I andre etterforskninger kan det skje at opplysninger som burde blitt delt internasjonalt ikke blir det, og norsk politi konsentrerer seg kun om etterforskning av norske gjerningspersoner.

12.2.1 Etterforskningsskritt i utlandet – bistands- og rettsanmodninger

Når man ønsker bistand fra et annet lands politi eller judisielle myndigheter til å gjennomføre etterforskingsskritt eller utføre tvangsmidler, vil mange land kreve en rettsanmodning. Der Norge har avtale med gjeldende land kan rettsanmodning sendes direkte til kompetent myndighet. I andre tilfeller må anmodning enten sendes via Kripos til Interpol i hastesaker, eller via Justis- og beredskapsdepartementet i andre saker.[258] Norge har en rekke avtaler med andre land, og lovverket for rettsanmodninger kan være ulikt innen Norden, EU og utenfor.[259]

Politidistriktene som er intervjuet, sier at IKT-kriminalitetssakene med spor eller gjerningsperson utenlands ofte henlegges av hensyn til tids- og ressursbruken som ofte medgår i slike saker. Dette funnet støttes av kartleggingen av internasjonalt politiarbeid fra 2019 som også viser at dette arbeidet er tids- og

[255] Europol etablerte et europeisk datakrimsenter (EC3) i 2013 og gir hvert år ut publikasjonen Internet Organised Crime Threat Assessment (IOCTA).
[256] Eurojust består av representanter fra påtalemyndigheten i hvert EU-land og ble i sin tid opprettet for å effektivisere etterforsking og påtale i straffesaker som gjelder grenseoverskridende og organisert kriminalitet. Norge inngikk samarbeidsavtale med Eurojust i april 2005. Relasjonene og oppgavefordelingen mellom Europol og Eurojust reguleres i en egen avtale av 9. juni 2004. Organene utfyller hverandre faglig ved at de representerer ulike sider og aspekter ved det europeiske politi- og straffesakssamarbeidet. Norge har en statsadvokat fast utplassert ved Eurojusts hovedkvarter i Haag i Nederland.
[257] NOU 2017:11, *Bedre Bistand. Bedre beredskap. Fremtidig organisering av politiets særorganer*.
[258] Forskrift om internasjonalt samarbeid i straffesaker, *§ 10. Oversendelse*.
[259] De nordiske landene har en egen samarbeidsavtale av 12. august 2012, revidert 01. april 2016. For anmodning om politibistand som enten kommer fra eller skal til Danmark, Finland, Island eller Sverige, gjelder denne avtalen. Nordisk overenskomst 26. april 1974 gjelder direkte oversendelse av anmodninger om forkynning og bevisopptak. Norge er også tilknyttet EUs konvensjon om gjensidig hjelp i straffesaker (2000-konvensjonen).

ressurskrevende.[260] Ifølge intervjuer må en sak være høyt prioritert for at samarbeid med andre land igangsettes. Sakene er ikke nødvendigvis vanskeligere å etterforske, men selve prosessen for bistands- og rettsanmodninger oppleves som kompleks, og det kan ta mange måneder eller år før svar eller bistand kommer. Tilsvarende gjelder rettsanmodning for å få vite eier av IP-adresser i andre land. Det kan i tillegg være komplisert å vurdere om politiet har det rettslige grunnlaget for å kunne innhente nødvendig informasjon fra et annet land.

Kartleggingen av internasjonalt politiarbeid fra 2019 viser at det er store forskjeller mellom politidistriktene når det gjelder forfølging av spor og etterforskningskritt utenlands.[261] Distriktene har ikke rutiner eller sjekklister for dette utover at noen rutinemessig bruker den nordiske politisamarbeidsavtalen. Kompetansen er i stor grad personavhengig innen de forskjellige kriminalitetstypene som går igjen i det internasjonale samarbeidet (organisert kriminalitet, økonomisk kriminalitet, IKT-kriminalitet, seksuallovbrudd osv.). Mange av respondentene i kartleggingen sier de kan for lite om hva som kreves i en rettsanmodning, de er kjent med at det tar lang tid å motta svar, og de lar derfor være. Dette gjelder både politiforespørsler og rettsanmodninger til utlandet.

12.2.2 Innhenting av informasjon fra tjenesteleverandører

Informasjon fra digitale tjenesteleverandører og sosiale medier som for eksempel Microsoft, Google, Facebook og Snapchat kan være avgjørende som bevis i straffesaker. Anmodninger til andre lands myndigheter og samarbeid med internasjonale tjenesteleverandører er utfordrende og tidkrevende.[262] Prosedyrer for informasjonsutveksling og innsynsbegjæringer er basert på tradisjonell praksis for utlevering av fysiske bevis mellom land og dårlig tilpasset den teknologiske utviklingen. Politiet har i utgangspunktet ikke tilgang til brukerdata eldre enn 21 dager. Dette betyr at innhenting av IP-adresser brukt for pålogging hos utenlandske tjenester må skje innen 21 dager, men innhenting av IP-adresser fra for eksempel Facebook og Google tar ofte mer enn 21 dager.[263] Dette fører til ressurskrevende leting etter alternative beviskilder som kan føre til at flere enn nødvendig kommer i politiets søkelys.

Kripos mottar daglig informasjon fra aktører i andre land om norske brukere som har lastet ned eller delt overgrepsmateriale hvor barn og unge er offer. I USA har tjenesteleverandører plikt til å melde fra dersom de oppdager overgrepsmateriale eller seksualisert materiale av barn som blir lagret eller distribuert via tjenestene deres. Rapporteringsplikten omfatter norske brukere som benytter tjenestene. Flere andre land har lignende bestemmelser, og rapporteringsplikten gjelder også norske brukere av tjenestene som er omfattet av disse. Som følge av rapporteringsplikten i USA mottok Kripos 10 500 tips i 2018 fra National Center for Missing and Exploited Children (NCMEC) og National Child Exploitation Coordination Center (NCECC) i USA. Flere større nettovergrepssaker er rullet opp i Norge som følge av slike tips.[264] Norske internettleverandører er ikke pålagt tilsvarende rapportering når deres tjenester brukes til oppbevaring eller distribusjon av seksualisert materiale av barn. Kripos anbefalte i 2019 at også norske tjenesteleverandører bør bidra i arbeidet med å avdekke nettovergrep.[265]

I faggrupperapporten om datatekniske undersøkelser og internettrelatert etterforskning vises det til at etterforskere i noen tilfeller kvier seg for å sende anmodninger om utlevering av informasjon til tjenestetilbydere, eller at disse er utformet på en måte som gjør at en ikke får riktig informasjon tilbake fra tilbyderen. Det anbefales derfor i rapporten å etablere et nasjonalt Singel-Point-Of-Contact (SPOC) politidistriktene kan rette henvendelsene sine til for å senke terskelen for å sende, og kvaliteten på, henvendelser til tjenestetilbydere. Kripos har SPOC for henvendelser som skal til Interpol og Europol, og ansvar for sambandstjenesten som brukes innen Norden. Kripos mener det mangler en SPOC for rettsanmodninger og for kontakt med de store, internasjonale tjenesteleverandørene. Det har vært diskutert om SPOC skal opprettes på samme måte som de har i Sverige og Danmark. Blant annet har Facebook ytret et ønske om dette, og Politidirektoratet vurderer for tiden om en SPOC-funksjon skal opprettes på dette området fra 2022.

Politidistriktene som er intervjuet, bekrefter i stor grad inntrykket fra rapportene som er gjengitt ovenfor. Innen Norden er det ikke noe problem å ta kontakt med tjenesteleverandører, men utenfor oppleves det som vanskelig. Innen økonomisk kriminalitet kan det bety at etterforskningsarbeidet blir tids- og krevende, penger

[260] Politidirektoratet (2019) *Fagforvaltning statusrapport - Status fagområde Internasjonalt straffesaksarbeid*, 2. oktober 2019.
[261] Politidirektoratet (2019) *Fagforvaltning statusrapport - Status fagområde Internasjonalt straffesaksarbeid*, 2. oktober 2019.
[262] NOU 2017:11 *Bedre Bistand. Bedre beredskap. Fremtidig organisering av politiets særorganer*.
[263] Politidirektoratet (2017) *Trusler og utfordringer innen IKT-kriminalitet (2017)*.
[264] Kripos (2019) *Seksuell utnytting av barn og unge over internett*.
[265] Kripos (2019) *Seksuell utnytting av barn og unge over internett*.

og spor er borte før politiet kommer på banen, og sakene henlegges. I alvorlige prioriterte saker, for eksempel nettovergrep, går prosessene raskere. Politidistriktene peker på mangel på etablerte rutiner for internasjonalt samarbeid som fører til at sporsikring ikke skjer raskt nok, og behov for et felles kontaktpunkt i norsk politi når det gjelder dialogen med internasjonale tjenesteleverandører. Flere peker på at personlig nettverk og kontakter utenlands kan føre til fortgang i sakene.

12.2.3 Støttedokumenter, veiledere og rutiner for internasjonalt samarbeid

Det finnes begrenset med nasjonale støttedokumenter når det gjelder internasjonalt politi- eller rettslig samarbeid.[266] Det som finnes, ligger på KO:DE, som administreres av Kripos. I en rapport fra 2019 ble det hevdet at innholdet som gjelder internasjonalt samarbeid ikke er godt nok systematisert og at det kan være utfordrende å raskt finne fram relevant informasjon. Ifølge Kripos er KO:DE basert på en foreldet teknisk løsning som gjør den tungvint å bruke, oppdatere og vedlikeholde. Mange distrikter lager derfor sine egne støttedokumenter. I faggrupperapporten om digitalt politiarbeid er spekteret av utfordringer dekket. Mange spesielle behov og ønsker har ført til at KO:DE framstår uoversiktlig og lite tilgjengelig.

12.2.4 Politidistriktenes oppfølging av saker fra Europol

I en inspeksjonsrapport fra det nasjonale statsadvokatembetet høsten 2018 ytres det bekymring rundt manglende oppfølging av saker initiert gjennom samarbeid med Europol.[267] Når Kripos mottok disse sakene ble det opprettet anmeldelser og det ble foretatt innledende undersøkelser i sakene før sakene ble overført til lokalt politidistrikt med tilbud om bistand fra Kripos. Data som er inkludert i disse sakene er ofte gamle og 21 dagers fristen for lagring av IP adresser var derfor en hindring. Kripos erfaring var at politidistriktenes oppfølging av sakene var mangelfull, blant annet grunnet manglende kompetanse, ressurser og ulik prioritering. Resultatet var at kun noen få av sakene ble etterforsket. Ifølge Statsadvokaten må det forventes at politidistriktene håndterer slike saker bedre, særlig sett i lys av politireformen. Kun et fåtall av sakene som sendes distriktene fra Europol via Kripos ble etterforsket. Tettere samarbeid mellom Kripos og distriktene i slike saker er foreslått som en løsning fra nasjonalt statsadvokatembete.

[266] Politidirektoratet (2019) *Fagforvaltning statusrapport - Status fagområde Internasjonalt straffesaksarbeid*, 2. oktober 2019.
[267] Det nasjonale statsadvokatembetet (2018) *Inspeksjon av seksjon for datakriminalitet*, brev til sjef Kripos datert 28. september 2018.

13 Styring og oppfølging av politi- og påtalemyndighetens oppfølging av IKT-kriminalitet

Dette kapitlet omhandler styringen av politiets innsats mot IKT-kriminalitet. Justis- og beredskapsdepartementet og Politidirektoratet har ansvar for den faglige og ressursmessige styringen av politiet, men i straffesaksbehandlingen er politidistrikter og særorgan underlagt Riksadvokaten. Aktørene som styrer norsk politi, har over lengre tid vært klar over hvilke utfordringer IKT-kriminalitet har skapt for norsk politi. Dette er likevel et område som i liten grad er prioritert i en periode hvor budsjetter og årsverk har økt betydelig.

13.1 Ansvaret for den nasjonale styringen av politiet

Ansvarsforholdene er todelt. I straffesaksbehandlingen er politiet underlagt påtalemyndigheten i form av den integrerte påtalemyndigheten i distriktene, distriktenes statsadvokater og Riksadvokaten. For øvrige oppgaver er politiet underlagt Politidirektoratet og Justis- og beredskapsdepartementet. Riksadvokatens overordnede ansvar er å fastsette prioriteringene for straffesaksbehandlingen, lede det faglige påtalearbeidet på straffesaksområdet og fastsette kvalitetskrav til behandlingen av straffesaker. Justis- og beredskapsdepartementet og Politidirektoratet har ansvar for å legge til rette for at Riksadvokatens krav realiseres på en effektiv og hensiktsmessig måte gjennom disponering av ressurser, organisering, kompetanse, mv.[268]

Den overordnede og fortløpende styringen med politiets aktiviteter skjer i hovedsak i to spor:

1. Riksadvokatens prioriteringer og føringer for straffesaksbehandlingen
   a. Årlig mål- og prioriteringsrundskriv
   b. Øvrige rundskriv og direktiver
   c. Behandling av straffesaker
2. Mål- og resultatstyring
   a. Justis- og beredskapsdepartementets etatsstyring av Politidirektoratet og instruks for Politidirektøren
   b. Politidirektoratets resultatavtaler og instrukser for politimester og sjefer for særorganene

Utover de formelle rammene for styringen som nevnt over, styres politiet av strategier og handlingsplaner på ulike nivåer. Justis- og beredskapsdepartementet og regjeringen har strategier som legger rammene for satsingen på IKT-kriminalitet og digital sikkerhet. Politidirektoratet og Riksadvokaten har flere strategier og handlingsplaner som også legger rammer for politiets innsats på dette området.

a. Nasjonale handlingsplaner og strategier, blant annet
   i. Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet
   ii. Nasjonal strategi for digital sikkerhet
b. Politidirektoratets og Riksadvokatens strategier:
   iii. Handlingsplan for løft av etterforskning (Etterforskningsløftet)
   iv. Politiet mot 2025 − politiets virksomhetsstrategi
   v. Kriminalitetsforebygging som primærstrategi 2018−2020

Samlet legger disse føringene grunnlaget for politiets prioriteringer generelt, og innsatsen mot IKT-kriminalitet spesielt.

13.2 Riksadvokatens prioriteringer og føringer for politiets innsats mot IKT-kriminalitet

Riksadvokaten har i det årlige mål- og prioriteringsskrivet hvert år siden 2005 understreket at alvorlig IKT-kriminalitet skal etterforskes. I mål- og prioriteringsskrivet for 2020 skriver Riksadvokaten at etterforskning av alvorlige dataangrep, datainnbrudd og annen IKT-kriminalitet skal intensiveres.[269] Riksadvokaten antar at denne kriminaliteten er økende i omfang og kompleksitet, men konstaterer at relativt få lovbrudd straffeforfølges. Sakene krever høy teknologisk kompetanse. Riksadvokaten skriver videre at det er

[268] NOU 2017: 5 *En påtalemyndighet for fremtiden – Påtaleanalysen*.
[269] Riksadvokaten (2020) *Mål og prioriteringer for straffesaksbehandlingen i 2020*. Rundskriv 1/2020.

nødvendig å legge til rette for mer samarbeid mellom politidistriktene, Kripos og næringslivet for å avdekke flere alvorlige straffbare forhold.

I ulike sammenhenger er det påpekt at Riksadvokatens prioritering av alvorlig IKT-kriminalitet synes å være uklar og er mangelfullt fulgt opp. Politirektoratet omtaler prioriteringen slik i 2015:

> *«Selv om Riksadvokaten i prioriteringsrundskriv har sagt at alvorlig datakriminalitet skal prioriteres, er prioriteringen i praksis uklar og varierer betydelig mellom distriktene.»*[270]

Politidistriktene som er intervjuet, opplever ikke at IKT-kriminalitet blir prioritert. Flere peker på utfordringer knyttet til de mange prioriteringene som skal tas hensyn til. Justis- og beredskapsdepartementet kommenterer at hvert politidistrikt må finne en krevende balanse mellom de saker som Riksadvokaten forutsetter blir prioritert og mengden av ressurser som står til rådighet.[271] Politidirektoratets kapasitetsundersøkelse viser at 30 prosent av etterforskningsressursene brukes på de 3 prosent alvorligste sakene som drapssaker, grov vold, grove narkotikalovbrudd og alvorlige seksuelle overgrep. Dette er også saker som legger beslag på dataetterforskernes og DPAs kapasitet.

En betydelig andel av ØKOKRIM porteføljе er saker der de mulige straffbare forholdene er begått ved hjelp av IKT-verktøy. ØKOKRIM anser ikke IKT-kriminalitet som et eget uavhengig kriminalitetsområde. ØKOKRIM vurderer det slik at de aller fleste forbrytelser i dag i større eller mindre grad blir foretatt ved hjelp av IKT-verktøy. Å anse IKT-kriminalitet som et eget kriminalitetsområde treffer derfor ikke kriminalitetsbildet ifølge ØKOKRIM.

NC3 viser i intervju til at det ikke er tallfestet et krav til antall saker som skal etterforskes og iretteføres på dette feltet, og politiet har i praksis aldri reelt prioritert IKT-kriminalitet i sin styring. En av årsakene til dette kan være at det er vanskelig å relatere seg til kriminalitet som ikke begås i det fysiske rom. Dette er saker som ses på som IKT-sikkerhetsutfordringer eller et «IKT-problem». Politiet mangler i tillegg kompetanse til å etterforske den alvorlige IKT-kriminaliteten som Riksadvokaten peker på (dataangrep, datainnbrudd). Selv om politiets kompetanse er forbedret har også teknologien utviklet seg. Gapet mellom kompetanse og teknologisk utvikling har vært der over lang tid. NC3 viser til at politiet forholder seg til mange prioriteringer fra ulike hold. I tillegg til føringer fra Riksadvokaten, forholder politiet seg til føringer fra Justis- og beredskapsdepartementet og Politidirektoratet. Politidistriktene viser til at de selv må prioritere blant prioriterte saker. Dette medfører at mange saker må henlegges.

Politidirektoratet viser til at politiet må prioritere, det er ikke ressurser til å etterforske alt. Politiets samfunnsoppdrag er å forhindre, avdekke, etterforske og straffeforfølge kriminalitet. Politiet må henlegge mange saker fordi etterforskningskapasiteten er begrenset og må forbeholdes de alvorligste sakene. Politidirektoratet er klar over at det er utfordringer på området, men grunnet manglende muligheter til å prioritere området innenfor tilgjengelige midler vedvarer utfordringene.

Riksadvokaten viser til at resultatene i kriminalitetsbekjempelsen på dette området ikke er tilfredsstillende. Det gjelder både for de alvorlige lovbruddene som omfattes av Riksadvokatens prioriteringer, men også for de mindre alvorlige sakene. Riksadvokaten opplever at det er for få saker som blir anmeldt, og for få av de anmeldte sakene som blir etterforsket. Riksadvokaten er også bekymret over at det er et lavt antall positive påtaleavgjørelser innenfor IKT-kriminalitetsfeltet.

Årsakene til at kriminalitetsbekjempelsen på området ikke er tilfredsstillende, er ifølge Riksadvokaten sammensatt. Kapasitet på etterforskningsfeltet er en av utfordringene, men er ikke alene årsaken til de dårlige resultatene. Riksadvokaten mener, som Riksrevisjonens undersøkelse underbygger, at også kompetansen på IKT-kriminalitetsfeltet i politiet ikke er god nok. Feltet har heller ikke fått den oppmerksomheten fra den høyere påtalemyndighet som kriminalitetsutviklingen tilsier. Organiseringen av arbeidet i politidistriktene, ved manglende samlokalisering av fagmiljøene, liten grad av tverrfaglighet og manglende skjerming av spesialistene, er også årsaker til de dårlige resultatene. Dette har også vært et problem i bekjempelsen av økonomisk kriminalitet. Mangel på en felles definisjon av IKT-kriminalitet er en utfordring, og når dette ikke er på plass vanskeliggjør det arbeidet med å utarbeide treffsikre analyser. Uten å ha dette på plass, vil det ifølge Riksadvokaten, være vanskelig å oppnå en tilfredsstillende innsats på IKT-kriminalitetsfeltet.

---

[270] Politidirektoratet (2015) *Datakrimstrategien*, s. 137.
[271] Justis- og beredskapsdepartementet (2020) *Tilbakemelding på utkast til forvaltningsrevisjonsrapport om politiets arbeid med IKT-kriminalitet*, brev til Riksrevisjonen 11. november 2020.

13.3 Mål- og resultatstyring på området IKT-kriminalitet

13.3.1 Justis- og beredskapsdepartementet styring av Politidirektoratets innsats mot IKT-kriminalitet

Justis- og beredskapsdepartementet har det overordnede ansvaret for politi- og lensmannsetaten og etatsstyringsansvaret for Politidirektoratet. Dette innebærer å fastsette overordnede mål og hovedstrategier, og påse at direktoratet gjennomfører fastsatte mål og prioriteringer. Departementet har også ansvar for å føre kontroll med direktoratet, og sikre seg at alle virksomheten har tilfredsstillende internkontroll.[272] Styringen skjer hovedsakelig gjennom hovedinstruks for politidirektøren og årlige tildelingsbrev som utformes på grunnlag av den årlige budsjettproposisjonen til Stortinget.

Hovedmålene for justissektoren ble endret i 2015. For straffesakskjeden er de overordnede målene i perioden 2015–2020:

- redusere alvorlig kriminalitet
- styrke forebyggingen av kriminalitet
- en mer effektiv straffesakskjede

Med utgangspunkt i Stortingets budsjettvedtak og de mål, prioriteringer og økonomiske rammer som ligger til grunn her, utarbeider Justis- og beredskapsdepartementet tildelingsbrev til Politidirektoratet der de økonomiske rammene for etaten det kommende budsjettåret presenteres. I tildelingsbrevet konkretiseres hvilke målsettinger som gjelder for Politidirektoratet og underliggende enheter.

Siden 2018 er målene for politiets virksomhet følgende:

1. Befolkningens trygghet og sikkerhet ivaretas
2. Redusere kriminalitet gjennom effektiv forebygging
3. Effektiv straffesaksbehandling med høy kvalitet
4. Alle som oppholder seg i Norge, har avklart identitet og lovlig opphold
5. Tilgjengelige tjenester med god service

Under de fem målene er det listet opp 16 styringsparametere og 12 oppdrag i tildelingsbrevet for 2020. Det understrekes også at politiet har en viktig rolle i en rekke strategier og handlingsplaner som gjelder for politiets virksomhet. I tillegg til disse gjelder målene for nærpolitireformen og det politiske målet om to politiårsverk per 1000 innbyggere innen 2020.[273]

IKT-kriminalitet er nevnt som en voksende utfordring i tildelingsbrevene for perioden 2016–2019, men er ikke nevnt som en utfordring i tildelingsbrevet for 2020. I perioden 2016-2020 er det gitt flere styringssignaler som berører IKT-kriminalitet. Eksempler på styringssignaler som er gitt i perioden, er

- føring om styrking av innsatsen mot internettrelaterte seksuelle overgrep mot barn, inkludert alvorlig integritetskrenkende kriminalitet som vold og overgrep mot barn og unge
- føring om styrking av innsats mot alvorlig profittmotivert kriminalitet, med særlig vekt på økonomisk kriminalitet og IKT-kriminalitet.
- føring om oppfølging av tiltakene i departementets strategi for å bekjempe IKT-kriminalitet og om rapportering på gjennomføring av tiltak.
- føringer om at Politidirektoratet må tilrettelegge for at politiet omstiller seg til å møte de kriminalitetsutfordringene som digitaliseringen av samfunnet fører med seg

I tildelingsbrevene er det i liten grad resultatkrav eller styringsparametere som gjelder IKT-kriminalitet. Politidirektoratet bekrefter i intervju at IKT-kriminalitet får liten plass i styringen. Unntaket er et mål som gjelder forebygging av IKT-relatert kriminalitet i tildelingsbrevene for 2019 og 2020. Målet her er å redusere kriminalitet gjennom effektiv forebygging. Politidirektoratet er bedt om å gi en kvalitativ vurdering av arbeidet på disse områdene i sin årsrapportering. I årsrapporten for 2019 rapporterer Politidirektoratet i hovedsak om pågående arbeid som etablering av næringslivskontakter, etablering av tilstedeværelse på internett, etablering av NC3 og om det forebyggende arbeidet som skjer i regi av Kripos/NC3. I 2020 vil direktoratet prioritere standardisering av politiets tilstedeværelse på nett og kvalitetsheving av arbeidet med å forebygge kriminalitet på nett, og videre arbeid med å etablere forebygging som primærstrategi.

[272] Justis- og beredskapsdepartementet (2018) *Hovedinstruks til politidirektøren*, fastsatt av Justis- og beredskapsdepartementet, 16. januar 2018.
[273] Justis- og beredskapsdepartementet (2020) *Tildelingsbrev 2020 Politidirektoratet*.

I henhold til samfunnssikkerhetsinstruksen, kapittel IV. *Krav til departementenes arbeid med samfunnssikkerhet* har Justis- og beredskapsdepartementet ansvar for å utarbeide og vedlikeholde systematiske risiko- og sårbarhetsanalyser (ROS-analyser) for justis- og beredskapssektoren. ROS-analysen fra 2019 har blant annet økt IKT-kriminalitet og digitalt bankran som scenario. Generelt sett ble det pekt på at alle aktører hadde for liten kompetanse og mørketallene ble anslått å være store. For justismyndighetene og politiets del ble det pekt på manglende beredskapsplaner, dårlig kunnskap om IKT-sikkerhet, manglende tilstedeværelse på nett, uklarhet om politiets rolle vs. andre myndigheter, manglende etterforskningskapasitet og digitale etterforskningsmetoder. Det ble pekt på at flere tiltak i *Nasjonal strategi for digital sikkerhet* vil kunne adressere de identifiserte utfordringene. Det ble blant annet pekt på behov for å styrke politi- og påtalemyndighetens kompetanse og evne til bekjempelse av IKT-kriminalitet. Det ble også pekt på styrking av NC3 og samhandlingen mellom politidistriktene.[274]

I et styringsmøte mellom Justis- og beredskapsdepartementet og Politidirektoratet sent i 2019 erkjente departementet at styringen av politiet er preget av et stort antall mål, føringer og resultatkrav. Det erkjennes at det neppe lar seg gjøre for politiet innenfor gjeldende ressursrammer å levere på alle krav og føringer samtidig. Departementet presiserer samtidig at POD sannsynligvis har større frihetsgrader enn det som er direktoratets utgangspunkt i dag og at dette kan og bør utnyttes.[275] Styringsutfordringene er også omtalt i den siste politimeldingen. Justis- og beredskapsdepartementet sier i intervju at departementet er i løpende dialog med direktoratet om hvilket handlingsrom direktoratet har til å løse sitt samfunnsoppdrag. Denne dialogen bidrar til å sikre at direktoratet utnytter eget myndighetsområde.

I perioden 2017–2020 peker Politidirektoratet på i sine årsrapporter at en stadig større andel av kriminaliteten er IKT-relatert, og at dette er et utfordrende område for politiet. I årsrapportene for 2018 og 2019 viser Politidirektoratet til at politiet utfordres på kompetanse og kapasitet som følge av at kriminaliteten blir mer digital og grenseoverskridende. Det vises til at alvorlig kriminalitet øker, flere saker flytter seg til det digitale rom og ressurser og kapasitet strekker ikke til. Under kapitlet om framtidsutsikter i Politidirektoratets årsrapport for 2019 vises det til at politiet har et betydelig utviklingsbehov. Eksisterende og nye tjenester skal ivaretas parallelt med at samfunns- og kriminalitetsutviklingen utfordrer politiet på nye områder. Kriminalitet i det digitale rom er ett av fire områder som har betydelig utviklingsbehov.[276]

> *«Politiet har et stort behov for å utvikle bedre evne til å møte data- og IKT-relatert kriminalitet. Dette krever både styrket kapasitet, kompetanse og teknologi, både i distriktene og ved politiets datakrimsenter (NC3), og må sees i sammenheng med andre etaters kapasiteter. Investeringsbehovet er betydelig, og politiet vil i mindre grad kunne møte utfordringene uten særlig styrking på dette området.»*

Politidirektoratet sier i intervju at IKT-kriminalitet er et økende problem. Det har ifølge direktoratet vært vanskelig å prioritere dette området i en situasjon hvor andre oppgaver har vært høyere prioritert. Politidirektoratet har levert satsingsforslag til departementet de tre siste årene for å styrke innsatsen mot IKT-kriminalitet. Det har ikke vært mulig å løfte dette området utover de tiltakene som allerede er igangsatt når det gjelder NC3, etablering av DPA i distriktene og styrking av grunn-, etter- og videreutdanningstilbudet på området ifølge Justis- og beredskapsdepartementet. Direktoratet viser til at kravene til politiet er høyere på en rekke områder enn det er kapasitet til. En strategisk satsing på IKT-kriminalitet har ikke vært mulig. Ifølge direktoratet vil man derfor kun i begrenset grad kunne møte de kravene samfunns- og kriminalitetsutviklingen stiller innenfor dagens økonomiske rammer.

Justis- og beredskapsdepartementet viser i intervju til at Politidirektoratet innenfor tildelte bevilgninger har betydelig rom og fullmakter til å prioritere slik det synes hensiktsmessig for å nå målene. Politidirektoratet får oppdrag og bevilgninger gjennom tildelingsbrevet. For øvrig vil ikke departementet kommentere regjeringens interne budsjettprosesser.

13.3.2 Politidirektoratets styring av politidistrikters og særorgans innsats mot IKT-kriminalitet

Politidirektoratet styrer politidistrikt og særorgan gjennom instruks og årlige resultatavtaler som tar utgangspunkt i tildelingsbrevet fra departementet, flerårig virksomhetsplan for politiet og etatens virksomhetsstrategi «Politiet mot 2025».[277] I perioden fram til og med 2019 videreformidlet Politidirektoratet

[274] Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen), 1. september 2017.
[275] Justis- og beredskapsdepartementet (2019) *Referat fra styringsdialogmøte mellom Justis- og beredskapsdepartementet og Politidirektoratet 25. oktober 2019*.
[276] De andre områdene er utvikling av nye ID-tjenester/grense- og territorialkontroll, IKT-sikkerhet/-infrastruktur og digitalisering av tjenester og arbeidsprosesser.
[277] Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden.*

styringssignaler fra Justis- og beredskapsdepartementet i et årlig disponeringsskriv til politidistrikter og særorgan. Fra og med 2020 styrer Politidirektoratet gjennom årlige resultatavtaler.

Politidirektørens prioriterte resultatområder og tiltak er angitt i resultatavtalene med politidistriktene for 2020. Prioriterte resultatområder er å styrke innsatsen mot alvorlige kriminalitetstyper, redusere straffesaksrestanser, innfri responstidskrav og retur av personer uten lovlig opphold. Blant de seks prioriterte tiltakene er ett knyttet til IKT-kriminalitet: «Utvikle etatens evne innen digitalt politiarbeid gjennom videre oppbygging av nasjonalt datakrimsenter (NC3) ved Kripos».

For perioden 2017–2020 har Politidirektoratet gjennom virksomhetsstrategien definert fire strategiske temaer, 12 strategiske mål og en rekke delmål. De strategiske temaene og målene tar opp i seg departementets overordnede mål og prioriteringer. Delmål som berører arbeidet med IKT-kriminalitet er listet under strategisk tema *3: Trygghet i det digitale rom*.

Tabell 8 Politidirektoratets virksomhetsstrategi «Politiet mot 2025» - Tema 3 Trygghet i det digitale rom

Strategisk tema	Strategiske mål	Delmål
3 Trygghet i det digitale rom	• **Styrke tilstedeværelse på nett** • **Styrke håndtering av datakrim og elektroniske spor**	Tilstedeværelse på nett: **1** Vi setter innbyggerne og virksomheter i stand til å beskytte seg selv og avdekker, forhindrer og etterforsker effektivt i det digitale rom **2** Vi har utført systematisk kartlegging av internettrelatert kriminalitet **3** Vi har oppdatert regelverket for enhetlig praksis i tjenesteutøvelsen på internett - for åpen og skjult tilstedeværelse Håndtering datakrim/espor: **4** Vi har etablert et nasjonalt datakrimsenter med sentrale oppgaver innen metodeutvikling, etterretning og straffeforfølgning av krevende og komplekse former for datakriminalitet, og med analyse av digitale spor **5** Vi arbeider systematisk på tvers i politiet og utnytter både lokal og sentral kompetanse og kapasitet **6** Vi har aktivt samarbeid med andre aktører for å sikre tilgang til oppdatert teknologi og kompetanse, og vi får løpende informasjon om relevante hendelser

Kilde: Politidirektoratet, 2016 *Politiet mot 2025*, Politidirektoratets virksomhetsstrategi for perioden 2017–2020.

I styringen av distriktene er det operasjonalisert to mål som begge berører området IKT-kriminalitet:

- styrke tilstedeværelse på nett
- bedre forebygging og bekjempelse av datakriminalitet

Politidistriktene gjennomfører en risikovurdering av måloppnåelse for alle strategiske mål, inkludert de som gjelder IKT-kriminalitet, og rapporterer om dette i tertial- og årsrapporteringen.[278] En gjennomgang av rapporteringen fra samtlige politidistrikter per 31. desember 2019 viser at risikovurderingene gjøres på litt ulike måter. Oppsummert viser rapporteringen følgende:

- 2 politidistrikter har ikke rapportert risikovurderinger.
- 7 politidistrikter rapporterer om kritisk risiko for at mål om bekjempelse av IKT-kriminalitet ikke nås.
- 1 politidistrikt rapporter om høy risiko for at mål om bekjempelse av IKT-kriminalitet ikke nås.
- 2 politidistrikter rapporterer om lav risiko for at mål om bekjempelse av IKT-kriminalitet ikke nås.

Årsaker til at risiko for manglende måloppnåelse på dette området vurderes som høy eller kritisk, er gjennomgående manglende kompetanse, kapasitet og tilgang på utstyr.

Politidistriktene som er intervjuet, peker på at det i styringen legges stor vekt på kvantitative mål og frister for straffesaksbehandlingen og andre områder. Rapporteringen om dette gjenspeiler i liten grad hvilke utfordringer politidistriktene har. Et av politidistriktene som er intervjuet, beskriver situasjonen slik:

[278] I 2020 ble det ikke gjennomført risikovurderinger for strategiske mål som gjelder IKT-kriminalitet. Politidistriktene er bedt om å risikovurdere kun ti utvalgte styringsparametere i resultatavtalene for 2020. Mål som gjelder IKT-kriminalitet er ikke blant disse.

«Foreløpig er politidistriktet overveldet av antallet saker som må etterforskes og restansene som hoper seg opp. Det betyr at det er lite tid og oppmerksomhet til omstilling til det nye kriminalitetsbildet.»

Ifølge politidistriktene blir IKT-kriminalitet og utfordringene innenfor etterforskning av internettrelaterte seksuelle overgrep mot barn og unge i liten grad synliggjort. Sakene utfordrer distriktene på kapasitet både når det gjelder etterforskning, tiltaleutforming og rettsbehandling.[279] Fire av fem politidistrikter som er intervjuet, er i tillegg kritiske til Politidirektoratets styring av innsatsen mot IKT-kriminalitet. Den faglige styringen oppleves som svak. Et av politidistriktene peker også på at man for kriminalitetstypen internettrelaterte seksuelle overgrep overser at mange saker er initiert av politiet selv, og at det bidrar til den høye oppklaringsprosenten. Hvis politiet i en periode reduserer egengenererte anmeldelser, kan man få inntrykk av at kriminaliteten er dalende, uten at den nødvendigvis er det. Kunnskap om kriminalitetsbildet utover anmeldelses- og oppklaringsstatistikk er derfor avgjørende.

13.4 Strategier for bekjempelse av IKT-kriminalitet

Justis- og beredskapsdepartementet og Politidirektoratet har utarbeidet flere strategier med tilhørende tiltak som gjelder IKT-kriminalitet i perioden 2015–2019:

- Politidirektoratets *Datakrimstrategi* fra 2015[280]
- *Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet* fra 2015.[281]
- *Nasjonal strategi for digital sikkerhet*, som ble lagt fram av regjeringen 30. januar 2019

Dokumentene gir et godt bilde av utfordringene forbundet med digitalt politiarbeid og IKT-kriminalitet.

13.4.1 Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet

Politidirektoratets datakrimstrategi fra 2015 var bredt anlagt med en visjon og mer enn 50 foreslåtte tiltak. Tiltakene foreslått i datakrimstrategien ble ikke satt i verk. I stedet laget Justis- og beredskapsdepartementet en egen strategi for bekjempelse av IKT-kriminalitet samme år. Departementets strategi beskriver hovedutfordringer og strategier for å møte utfordringene innen seks områder:

1. Felles kunnskaps- og analysegrunnlag
2. Kompetanse
3. Kapasitet
4. Tilgjengelig teknologi
5. Nasjonalt og internasjonalt samarbeid
6. Et godt og oppdatert lov- og regelverk

I strategien foreslås det også 15 tiltak som ifølge Justis- og beredskapsdepartementet skal bidra til å forebygge at IKT-kriminalitet skjer. Tiltakene Politidirektoratet har hatt ansvar for, ble rapportert som gjennomført i direktoratets årsrapport for 2018.[282]

Tabell 9 Tiltak i Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet

Tiltak	Ansvarlig	Status*
Tiltak 1 – Foreta en løpende revidering av strategien mot IKT-kriminalitet	Justis- og beredskapsdepartementet	Status ukjent.
Tiltak 2 – Utarbeide en særskilt, felles, årlig trusselvurdering for IKT-kriminalitet	Politidirektoratet	Utført i 2016 og 2017, overlatt til FCKS fra 2019.
Tiltak 3 – Etablere en sentralisert statistikkrapportering og ordning for selvrapportering fra fornærmede	Politidirektoratet	Innført IKT-moduskoder fra 1.1.2018
Tiltak 4 – Sikre mørketallundersøkelsen	Politidirektoratet	Bidratt med finansiering i 2018.

[279] Riksadvokaten (2019) *Etterforsknings- og påtalepliktens grenser i omfattende nettovergrepssaker - Et nytt straffebud om serieovergrep - mulige lovendringer*, brev til Lovavdelingen, Justis- og beredskapsdepartementet, 10. september 2019.
[280] Politidirektoratet (2015) *Datakrimstrategien*,
[281] Justis- og beredskapsdepartementet (2015) *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, lansert 26. juni 2015.
[282] Politidirektoratet (2019) *Direktoratets rapportering på Justis- og beredskapsdepartementets IKT-kriminalitetsstrategi i forbindelse med årsrapporteringen for 2019*. Rapportering 3. tertial, R10: Rapportere på strategier og handlingsplaner.

Tiltak 5 – Etablere et nasjonalt senter for å forebygge og bekjempe IKT-kriminalitet	Politidirektoratet	NC3 etablert 1.1.2019
Tiltak 6 - Utarbeide en strategi for digital og politifaglig kompetanseheving	Politidirektoratet	Oversendt JD i september 2016.
Tiltak 7 – Utarbeide en plan for å styrke den digitale kompetansen hos påtalemyndigheten	Riksadvokaten/Justis- og beredskapsdepartementet	Ifølge Riksadvokaten er det ikke iverksatt særskilte tiltak på området. Arbeidet med nettovergrepssaker har bidratt til kompetanseheving, og denne typen kompetanse vil kunne styrkes gjennom årlig obligatorisk opplæring og andre generelle kompetansetiltak i tiden framover.
Tiltak 8 - Etablere et pilotprosjekt i Oslo politidistrikt	Politidirektoratet	Gjennomført og avsluttet i desember 2017.
Tiltak 9 - Utarbeide en forskningsstrategi for å forebygge og bekjempe IKT-kriminalitet	Politidirektoratet	Oversendt JD i september 2016.
Tiltak 10 - Utarbeide en plan for styrking av etterforskningskapasiteten	Politidirektoratet	Oversendt plan i februar 2016.
Tiltak 11 – Kartlegge teknologiske løsninger	Politidirektoratet	Oversendt fra POD til JD i februar 2016.
Tiltak 12 – Styrke nasjonalt samarbeid i samarbeid med Næringslivets sikkerhetsorganisasjon	Justis- og beredskapsdepartementet	Justis- og beredskapsdepartementet delfinansierer Mørketallsundersøkelsen som kommer ut hvert annet år.
Tiltak 13 – Styrke internasjonalt samarbeid	Justis- og beredskapsdepartementet og Politidirektoratet	Pågår. Løpende arbeid.
Tiltak 14 – Forenkle og standardisere samarbeidet med andre land	Justis- og beredskapsdepartementet	Pågår. Løpende arbeid.
Tiltak 15 – Vurdere behovet for å foreta endringer i straffelovgivningen	Justis- og beredskapsdepartementet	Pågår. Løpende arbeid.Se bl.a. kapittel 13.5 om lovmessige endringer.

Kilde: Politidirektoratets årsrapport 2019.
* - Basert på Politidirektoratets rapportering

Flere av tiltakene i strategien gikk ut på å utarbeide rapporter, planer og strategier, vurdere tiltak eller kartlegge tilstand (tiltakene 2, 4, 6, 7, 9, 10, 11, 12, 15). Disse dokumentene er utarbeidet, men det er vanskelig i ettertid å spore hvilke faktiske resultater disse dokumentene har gitt utover generell kunnskapsheving på feltet. De mest konkrete tiltakene som er mulig å etterprøve er etablering av sentralisert statistikkrapportering (tiltak 3), etableringen av et nasjonalt senter for IKT-kriminalitet (tiltak 5) og etableringen av et pilotprosjekt i Oslo politidistrikt (tiltak 8). Tiltakene er gjennomført, men om tiltakene har bidratt til å innfri strategiens formål, er mer usikkert. Den sentraliserte statistikkrapporteringen bidro i begrenset grad til å gi oversikt over IKT-kriminaliteten. Et nasjonalt kriminalitetssenter er etablert i form av NC3. Ambisjonene er for NC3 er redusert, og NC3 viser til at kapasiteten er begrenset. Pilotprosjektet i Oslo politidistrikt er gjennomført og ga innsikt i utfordringene. Om foreslåtte tiltak fra pilotprosjektet er gjennomført, er mer uklart.

Politidirektoratet viser i intervju til at departementets strategi bygger på Politidirektoratets Datakrimstrategi fra 2015, men inneholder færre tiltak som har vært mindre ressurskrevende å sette i verk enn andre. Direktoratet viser til at Datakrimstrategien inneholdt mange tiltak, og direktoratets satsingsforslag til departementet bygger på disse. Det er imidlertid ikke bevilget midler til gjennomføring av satsingsforslagene, og store deler av direktoratets strategi er derfor ikke gjennomført.

Justis- og beredskapsdepartementet viser til at strategien (departementets) er fem år gammel, og at det har vært stor utvikling på området. Det er ikke gitt at alle tiltak i strategien er de riktige i dag. Tema behandlet i strategien er også behandlet i politimeldingen. Andre tiltak er kvittert ut andre steder. Departementet viser for øvrig til at flere av tiltakene er gjennomført, blant annet etablering av NC3, enheter for digitalt politiarbeid i distriktene og den nye strategien for digital sikkerhet behandler også dette temaet.

13.4.2 Nasjonal strategi for digital sikkerhet

I Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar* og Innst. 187 S (2017–2018) anmodet Stortinget regjeringen om å legge fram en plan som synliggjør politiets arbeid med IKT-kriminalitet og hvordan dette skal finansieres. I Prop. 1 S (2019–2020) rapporterte departementet at vedtaket er fulgt opp ved åpning av NC3 og etableringer av enheter for digitalt politiarbeid i politidistriktene. Det vises også til at politiet er mer til stede på internett, og at det i januar 2019 ble lagt fram en nasjonal strategi for digital sikkerhet, der arbeidet med å nedkjempe IKT- og datarelatert kriminalitet er ett av fem prioriterte områder.

Nasjonal strategi for digital sikkerhet ble lagt fram av regjeringen 30. januar 2019. Ett av fem prioriterte områder er å bekjempe datakriminalitet og IKT-relatert kriminalitet. Overordnet mål på dette området er å

styrke politiets evne til å bekjempe denne typen kriminalitet. To delmål er etablert for å nå det overordnede målet:

- Politiets kompetanse og kapasitet til å bekjempe data- og IKT-relatert kriminalitet er styrket
- Samfunnet har tillit til at politiet kan bekjempe data- og IKT-relatert kriminalitet.

Kapasitet og kompetanse står sentralt i regjeringens satsing i tillegg til etableringen av NC3. Tiltak som er listet opp under denne delen av strategien er:

- Stortingsmelding om politiets kapasitet og kompetanse – meldingen ble framlagt for Stortinget i juni 2020.
- Politiets sikkerhetstjeneste (PST) – det vises til at PSTs bevilgning ble økt med 25 mill. kroner i 2019 for å styrke arbeidet med hybride trusler og cybertrusler. Midlene skal brukes til anskaffelse av personell og teknologi som gir bedre kapasitet i det digitale rom til å avdekke, forhindre, håndtere og etterforske de mest alvorlige forsøkene på spionasje, sabotasje, påvirkningsoperasjoner og sammensatte (hybride) trusler. Bevilgningen vil blant annet gi grunnlag for videre utvikling av PSTs samarbeid med E-tjenesten, NSM og Kripos i FCKS.
- Støtte FNs innsats for å bekjempe data- og IKT-relatert kriminalitet globalt – økonomisk støtte til FNs kontor for narkotika og kriminalitet (UNODC) for bekjempelse av data- og IKT-relatert kriminalitet. I hovedsak støtte til å styrke utviklingslandenes kompetanse og kapasitet på området.
- Nasjonalt elektronisk identitetsbevis (eID) – nasjonale ID-kort skal lanseres i 2020 og vil styrke sikkerhetsnivået for elektronisk identifisering.
- Internasjonalt samarbeid om data- og IKT-relatert kriminalitet – deltakelse i internasjonale fora hvor det pågår arbeid med relevans for norsk forebygging og bekjempelse av data- og IKT-relatert kriminalitet, bl.a. FN, Europarådet og EU.
- Politiets nasjonale innbyggerundersøkelse − gjennomføre den årlige innbyggerundersøkelsen som måler befolkningens tillit til politiet, også på dette området.

Det er meget få av disse tiltakene som tar tak i utfordringene som er forbundet med kompetanse, kapasitet og støttesystemer i politidistriktene som håndterer IKT-kriminalitet i det daglige. Justis- og beredskapsdepartementet viser i intervju til ulike tiltak som er gjennomført for å nå målene. Politiets Nasjonale cyberkrimsenter (NC3) er etablert. Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden* omhandler både endringer i kriminalitetsbildet og konsekvenser for politiets oppgaver og kompetanse. I tillegg deltar departementet i internasjonale fora. Politiets evne og kapasitet må også ses i sammenheng med andre aktørers arbeid, blant annet Felles cyberkoordineringssenter (FCKS) og Nasjonal sikkerhetsmyndighet (NSM).

13.5 Lovmessige utfordringer som bidrar til lavere effektivitet i etterforskning og oppklaring av IKT-kriminalitet

Det er allment kjent at flere lovmessige utfordringer bidrar til en lavere effektivitet i etterforskning og oppklaring av IKT-kriminalitet. Den mest omtalte utfordringen som hindrer politiets arbeid, er begrensninger i muligheter til å lagre IP-adresser utover 21 dager. Denne bestemmelsen innebærer i praksis at saker hvor IP-adresser ikke sjekkes før fristen på 21 dager, ofte henlegges. Dette er påpekt som et problem gjentatte ganger over mange år. En annen kjent utfordring er større, nettovergrepssaker med mange hundre fornærmede som skaper kapasitetsutfordringer innen digitalt politiarbeid, generell etterforskning, påtale og i domstolsbehandlingen. Disse og flere andre lovmessige endringer er tatt opp med Politidirektoratet og Riksadvokaten, og forslag til lovendringer er oversendt Justis- og beredskapsdepartementet.

Strafferammene for datainnbrudd og flere andre typiske IKT-krimsaker (med unntak av seksuallovbrudd) har lave strafferammer. Dette fører ifølge intervjuer med flere politidistrikter til lavere prioritering og henleggelse av saker med lave strafferammer som datainnbrudd, som kan vise seg å være alvorlige hvis det gjennomføres etterforskning. Se kapittel 5.2 for mer utfyllende informasjon.

Faktaboks 7 Lovmessige utfordringer for etterforskning og oppklaring av IKT-kriminalitet

- **Begrenset lagringstid for IP-adresser utover 21 dager.**
  Tatt opp gjentatte ganger over mange år, blant annet i Kripos' høringsutkast til innføringen av datalagringsdirektivet 12. april 2010, hvor Kripos viser til at Norge har med dagens praksis for lagring av IP-logger inntil 21 dager gir meget begrenset mulighet for å kunne avdekke både overgripere og personer som sprer overgrepsmateriale med base i Norge. Norge er i ferd med å bli en frihavn for denne typen kriminelle. Dette er omtalt i ulike sammenhenger, blant annet i en rapport fra Kripos om seksuelle overgrep mot barn og unge fra 2019 og senest i Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden*. Forslag til lovendringer ble sendt på høring 9. oktober 2020 med frist for innspill i januar 2021.
- **Kapasitetsmessige utfordringer i nettovergrepssaker med mange fornærmede.**
  Lovforslag fra Riksadvokaten med forslag til løsninger ble oversendt til Justis- og beredskapsdepartementet 10. september 2019. Forslag til lovendringer ble sendt på høring 31. august 2020 med frist for innspill 1. desember 2020.
- **IP-adresser – manglende krav til lagring av abonnementsinformasjon for IP-adresser.**
  Samordningsorganet tilrådet en lovendring for dette området i 2018, og Kripos stilte seg bak forslaget i sin rapport om seksuelle overgrep mot barn og unge i 2019. Forslag til lovendringer ble sendt på høring 9. oktober 2020 med frist for innspill 11. januar 2021.
- **Manglende regulering av VPN-leverandører.**
  VPN-løsninger brukes i økende grad av seksualforbrytere for å skjule nettaktivitet og sin identitet. VPN-leverandørene er ikke forpliktet til å utlevere opplysninger om brukere av deres tjenester om politiet ber om dette. Samordningsorganet foreslo å utrede et påbud i 2018, og Kripos stilte seg bak dette forslaget i sin rapport om seksuelle overgrep mot barn og unge i 2019.
- **Manglende regulering av kryptovaluta.**
  Kryptovaluta brukes for å skjule identitet ved kjøp av for eksempel bestillingsovergrep. Forskrift om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften) trådde i kraft i oktober 2018. Om dette nye regelverket kan anvendes for å avdekke norske gjerningspersoner som bruker virtuelle valutaer for kjøp av overgrep, er ifølge Kripos uvisst.
- **Manglende meldeplikt for tjenesteleverandører ved funn av overgrepsmateriale.**
  I USA er det lovregulert at tjenestetilbydere skal melde fra om overgrep mot barn; dette er ikke tilfellet i Norge. NC3 peker på at de som utsettes for nettrelaterte overgrep i liten grad melder fra selv og politiet har ikke ressurser til å avdekke og følge med på alt som foregår på internett. At tjenesteleverandørene har varslingsplikt anses derfor som viktig og kan være en viktig kilde til informasjon om overgrep. I Norge er det en generell anmeldelses- og avvergingsplikt som også påligger tjenesteleverandørene å følge, men leverandørene har ikke varslingsplikt ved mistanke eller avdekking av overgrep. Lovreguleringen i USA og Canada er mer eksplisitt på dette området enn det norsk lovgivning er.
- **Andre forslag fra Kripos for å styrke innsatsen mot internettrelaterte seksuelle overgrep mot barn og unge:**
  – Avklare prosessuelle rettigheter for fornærmede i utlandet med hensyn til erstatning – for eksempel de som er utsatt for overgrep bestilt eller gjennomført av nordmenn.
  – Forlenge foreldelsesfristen for straffeloven § 305 b.[283]
  – Øke strafferammen for straffeloven § 311 *Fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn* som i dag har en ramme på 3 års fengsel, som er lavere enn strafferammene i for eksempel Sverige og Danmark, som er seks år.
  – Innføre avvergingsplikt for straffelovens § 310 *Fremvisning av seksuelle overgrep mot barn eller fremvisning som seksualiserer barn* og § 311 *Fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn*.
  – Inngå gjensidig avtale med USA om bistand i straffesaker ettersom dagens praksis er komplisert og utilfredsstillende for utveksling av IP-adresser mellom USA og Norge. Foreslått endret av samordningsorganet i 2018.
  – Styrke samarbeidet med internasjonale politimyndigheter.

[283] I Prop. 66 L (2019-2020) er det foreslått å heve strafferammen etter § 305 fra 1 til 2 år. Endringen medfører at foreldelsesfristen forlenges fra to til fem år. Proposisjonen ble behandlet i Stortinget 3. november 2020.

Kilde: Kripos (2010) *Datalagringsdirektivet – høringssvar fra Kripos*, brev til Samferdselsdepartementet 12. april 2020; Kripos, 2019 *Seksuell utnyttelse av barn og unge over internett;* Riksadvokaten, 2019 *Etterforskings- og påtalepliktens grenser i omfattende nettovergrepssaker – et nytt straffebud om serieovergrep – mulige lovendringer*, brev til Justis- og beredskapsdepartementet 10. september 2019.

Justis- og beredskapsdepartementet opplyser i intervju at rapporten Kripos utarbeidet i 2019 om internettrelaterte seksuelle overgrep mot barn og unge, i sin helhet er meldt som et innspill fra Politidirektoratet til departementet i forbindelse med utviklingen av en tverrdepartemental strategi mot internettrelaterte overgrep mot barn. En tverrdepartemental strategi mot internettrelaterte overgrep skal legges fram i 2020. Departementet peker videre på at det per november 2020 pågår flere andre arbeider:

- Endringer i ekomloven (lagring av IP-adresser mv.). Høringsnotatet er utarbeidet i samarbeid med Kommunal- og moderniseringsdepartementet (KMD) som har ansvaret for ekomloven. Fristen for høringsinnspill er 11. januar 2021.[284]
- Endringer i straffeloven (bilder som er særlig egnet til å krenke privatlivets fred). Forslag til lovendringer har vært på høring (2018). Departementet arbeider med oppfølging av høringen.

Departementet har i tillegg, på bakgrunn av innspill fra Riksadvokaten og politiet, foreslått endringer i reglene om adgangen til å avgrense etterforsking og påtale i omfattende straffesaker (tilskjæring).[285] Formålet er å legge til rette for bedre utnyttelse av ressursene i straffesakskjeden. Departementet tror det er en bedre løsning på utfordringene enn å tilføre enda mer ressurser. Høringen inneholder også forslag om en ny bestemmelse som rammer omfattende seksuallovbrudd som et sammenhengende straffbart forhold.

[284] Kommunal- og moderniseringsdepartementet og Justis- og beredskapsdepartementet (2020) *Høring – endringer i ekomloven*, 9. oktober 2020.
[285] Endringer i straffeprosessloven og straffeloven (etterforsknings- og påtaleplikt i store straffesaker, nytt straffebud om serierovergrep mv.). Høringsfrist er 1. desember 2020.

14 Vurderinger

Politiets hovedoppgave er å bekjempe kriminalitet og å fremme og befeste borgernes sikkerhet, trygghet og alminnelige velferd. Utviklingen og økningen av alvorlig kriminalitet i samfunnet kan bidra til at borgerne opplever større utrygghet.[286]

Politiet har vært gjennom en omfattende evaluering etter 22. juli-hendelsene og en påfølgende politireform for å styrke forebygging, etterforskning og påtale av kriminelle handlinger, og sikre innbyggernes trygghet. Politiet står overfor et annet kriminalitetsbilde enn for bare få år tilbake. Det har vært en generell nedgang i den anmeldte kriminaliteten samtidig som nye digitale kriminalitetsformer har kommet til. Kriminalitet flytter seg til internett i takt med at samfunnet og økonomiske verdier digitaliseres. Politidistrikter og særorgan rapporterer om store utfordringer i sin håndtering av disse endringene. Kunnskapen om forekomsten av IKT-kriminalitet er svak ettersom tilbøyelighet til å anmelde er lavere her enn for den tradisjonelle kriminaliteten som begås i det fysiske rom. Næringslivets og befolkningens tillit til politiets innsats er i tillegg mindre når det gjelder IKT-kriminalitet.

Det er vesentlige svakheter i politiets arbeid for å etterforske og oppklare ren IKT-kriminalitet og økonomisk IKT-kriminalitet. Politidirektoratets faglige styring av innsatsen mot IKT-kriminalitet har vært svak. Undersøkelsen viser at politiet i enkelte saker som organiseres som etterforskningsoperasjoner, har oppnådd positive resultater i innsatsen mot internettrelaterte seksuelle overgrep mot barn og unge. Men det er fortsatt betydelige utfordringer i politiets innsats også mot denne kriminalitetstypen. Enheter for digitalt politiarbeid er opprettet i alle politidistrikter, NC3 er opprettet hos Kripos, og utdanningstilbudet ved Politihøgskolen innen digitalt politiarbeid er utvidet. Det er likevel store utfordringer i form av manglende oversikt over kriminalitetsbildet, manglende kapasitet og kompetanse, og utfordringer innen organisering, støttesystemer og etterforskning av grensekryssende kriminalitet. Politidirektoratet og Justis- og beredskapsdepartementet har vært klar over utfordringene, men har i for liten grad evnet å omstille politiets innsats til å håndtere denne typen kriminalitet på en bedre måte. Manglende innsats på området utgjør en fare for borgernes trygghet og velferd, og for tilliten til norsk politi.

14.1 Effektiv bekjempelse av IKT-kriminalitet forutsetter et kunnskaps- og analysegrunnlag politiet mangler

Effektive forebyggende og kriminalitetsbekjempende tiltak forutsetter et kunnskapsbasert politiarbeid som vektlegger analyse og etterretning. Dette er vektlagt i politiets etterretningsdoktrine, i nærpolitireformen og i den siste politimeldingen. Dette er også vektlagt i Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet fra 2015 hvor det heter at «*en effektiv og målrettet innsats mot IKT-kriminalitet krever et godt kunnskaps- og analysegrunnlag*».

Kunnskaps- og analysegrunnlaget departementet etterlyste i 2015 er fortsatt ikke på plass. Store mørketall, begrenset oversikt over anmeldt IKT-kriminalitet og mangel på etterretning og systematisk kunnskapsbygging innebærer at politiet i liten grad evner å være i forkant av kriminaliteten. Politiet utnytter i liten grad tilgjengelig kunnskap i egne saksbehandlingssystemer og fra andre kilder for å innrette etterforskningskapasiteten effektivt.

Da strategien ble vedtatt i 2015, manglet politiet en oversikt over IKT-kriminaliteten. For å utvikle et kunnskapsgrunnlag for trusselvurderinger på området, innførte Politidirektoratet moduskoder for IKT-relatert kriminalitet fra 2018. Moduskodene er praktisert ulikt i politidistriktene. De har bidratt til å gi politiet en viss innsikt i forekomst, men underestimerer omfanget. Omfanget av spesielt økonomisk IKT-kriminalitet er større enn det som går fram av statistikk utviklet med grunnlag i modusregistrering. En viktig forutsetning for å kunne etablere et kunnskapsgrunnlag for bekjempelse av IKT-kriminalitet, er å ha oversikt over både den IKT-kriminaliteten som anmeldes, og den som ikke anmeldes.

Mørketallene på området er store som følge av at næringsliv, offentlige virksomheter og befolkningen i liten grad anmelder IKT-kriminalitet. Omfanget av mørketall varierer med kriminalitetstype. Innen internettrelaterte seksuelle overgrep har man kommet lengre i å kartlegge mørketallene, men på andre områder har politiet

[286] Innst. 326 S (2016–2017), jf. Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn.*

mindre oversikt over mørketall. Samlet bidrar manglende oversikt over både mørketall og den anmeldte IKT-kriminaliteten til å gjøre området uoversiktlig.

Uklarhet rundt begrepet IKT-kriminalitet har dessuten skapt utfordringer. Fenomenet omtales med ulike begreper som datakriminalitet, cyberkriminalitet, digital kriminalitet og IKT-relatert kriminalitet. Begrepet IKT-kriminalitet tolkes forskjellig av distrikter, særorgan og nasjonale myndigheter, og antallet lovbestemmelser som kun omhandler eller bruker begrepet IKT-kriminalitet, er ytterst få. Uklarheten har bidratt til at andre forhold, som digitalisering av politiet og annen kriminalitet med elektroniske spor, sammenblandes med IKT-kriminalitet. Uklarheten bidrar til liten oversikt over omfanget av IKT-kriminalitet og kan også ha medvirket til mangel på effektive strategier og tiltak på området.

Etterretning og systematisk kunnskapsbygging som grunnlag for strategier og metodeutvikling har ikke vært tilstrekkelig prioritert. Kripos har hatt ansvar for IKT-kriminalitet over lang tid, men NC3 oppgir at det så langt etter opprettelsen av senteret ikke har vært kapasitet til å samle etterretning for ren IKT-kriminalitet og økonomisk IKT-kriminalitet. Større næringslivsaktører har tilbudt seg å dele etterretningsinformasjon med politiet, men politiet mangler kapasitet og systemer for å motta denne typen kunnskap. Innen internettrelaterte seksuelle overgrep finnes det etterretningskunnskap, men tilgjengelig kunnskap fra pågående saker og tipstjenester blir i for liten grad sammenstilt og analysert for å effektivisere innsatsen i politidistrikter og særorgan. Politidistriktene har heller ikke samlet etterretningsinformasjon eller systematisert tilgjengelig kunnskap på disse områdene. All kapasitet går i hovedsak til etterforskning av relativt få, alvorlige og komplekse saker. Politiet blir reaktive og kapasiteten innen digitalt politiarbeid brukes der behovet er størst, som er å sikre elektroniske spor i de alvorligste vold-, narkotika og sedelighetssakene. Det finnes kunnskap om organisert kriminalitet og annen kriminalitet på dette området i næringslivet og hos andre offentlige aktører og internasjonalt. Men kunnskapen blir ikke innhentet, systematisert og utnyttet godt nok. Mangel på etterretning har bidratt til at politiet mangler det informasjonsgrunnlaget som er nødvendig for å iverksette effektive, kriminalitetsbekjempende tiltak på området.

14.2 Politiet prioriterer i liten grad etterforsking og oppklaring av ren IKT-kriminalitet

Riksadvokaten har siden 2005 sagt at alvorlig IKT-kriminalitet som datainnbrudd skal prioriteres, i tillegg til flere andre alvorlige kriminalitetstyper, blant annet alvorlig vold, narkotika og seksualforbrytelser.

Gjennomsnittlig tidsbruk for ren IKT-kriminalitet, som omfatter straffebestemmelser Riksadvokaten har sagt skal prioriteres, er lav. Ren IKT-kriminalitet har i tillegg den laveste oppklaringsandelen av de utvalgte sakstypene. Det er imidlertid variasjon i tidsbruk, som er høy i noen få saker. Enhetene for digitalt politiarbeid (DPA) bruker også lite tid på etterforskning av teknologikrevende kriminalitet, som ren IKT-kriminalitet.

Tidsbruken for etterforskning av internettrelaterte seksuelle overgrep er generelt høy, og innenfor flere straffebestemmelser brukes det mer tid på internettrelaterte overgrep enn saker som ikke er IKT-kriminalitet. Internettrelaterte overgrep har også en høy oppklaringsandel. Samtidig er det kjent at mange av sakene anmeldes av politiet selv. Dette er i hovedsak alvorlige saker med høy sannsynlighet for oppklaring.

Innenfor økonomisk kriminalitet er det marginalt lavere tidsbruk på IKT-kriminalitetssaker sammenlignet med saker som ikke er IKT-kriminalitet. Oppklaringsprosenten for økonomisk kriminalitet er samlet sett lav. En sannsynlig årsak til dette er at flertallet av saker er mindre alvorlige saker (bedragerier og ID-krenkelser) som henlegges. Det framkommer ikke noe tydelig mønster ved sammenligning av oppklaringsprosent mellom IKT-kriminalitet og saker som ikke er IKT-kriminalitet innenfor samme straffebestemmelse.

14.3 Manglende kompetanse hindrer avdekking og oppklaring av IKT-kriminalitet

Iht. Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar* er regjeringen opptatt av at digital kompetanse må bygges i alle politidistrikt, slik at politiet har tilstrekkelige forutsetninger for å bekjempe IKT-kriminalitet. At politiet mangler kompetanse for å bekjempe IKT-kriminalitet, er slått fast i en rekke rapporter, utredninger og strategier helt tilbake til 2012. Senest i årsrapporten for 2019 skriver Politidirektoratet at det mangler kompetanse til å møte utfordringene på dette området. Regjeringen peker også i Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden* på at IKT-kriminalitet og digitalisering av kriminaliteten utfordrer politiets kompetanse.

Politiets kompetanse til å avdekke og etterforske IKT-kriminalitet er avgjørende for å bekjempe IKT-kriminalitet. Kompetansen er mangelfull på flere nivåer. Basiskompetansen hos personell ansatt i ordenstjeneste/patruljer, kriminalvakt og saksmottak har generelt sett vært svak. Det har ført til at lovbrudd som anmeldes, eller avdekkes på åsted eller ved pågripelse, kan håndteres feil i den viktige initiale fasen. Det forekommer derfor at saker avvises, at spor ikke sikres på riktig måte, at feil etterforskningsskritt tas, at saker registreres feil, og at saker som kunne vært oppklart, henlegges. Oppmerksomhet om digitalt politiarbeid varierer fra ett politidistrikt til et annet. Enkelte politidistrikt har kommet lengre enn andre i å styrke kompetansen på dette nivået.

Spesialistkompetanse ivaretas hovedsakelig av enhet for digitalt politiarbeid (DPA) i distriktene, av NC3 og ØKOKRIM. Spesialistkompetansen i politidistriktene brukes per i dag hovedsakelig til å sikre elektroniske spor i alvorlige saker som seksuallovbrudd, grov vold og alvorlig narkotikakriminalitet. Det er kun NC3 og i noen grad Oslo politidistrikt som bruker spesialistkompetanse til å etterforske alvorlig IKT-kriminalitet utover internettrelaterte seksuelle overgrep. Både Oslo politidistrikt og NC3 har begrensede ressurser med kompetanse til å etterforske teknologisk krevende IKT-kriminalitet.

Politiet vil i tiden framover være avhengig av å rekruttere informatikere og dataingeniører for å bekjempe alvorlig, teknologisk krevende IKT-kriminalitet. Justisdepartementet erkjenner at målet om to politiårsverk per 1000 innbygger gjør det vanskelig å ansette sivile i distriktene. I tillegg er den kompetansen politiet har behov for også attraktiv på arbeidsmarkedet, noe som gjør det krevende å for politiet å tiltrekke seg nødvendig arbeidskraft.

Påtalemyndighetens kompetanse er viktig for kvaliteten på etterforskningen av IKT-kriminalitet. Det har over flere år vært påpekt at påtalemyndigheten mangler kompetanse innen digitalt politiarbeid og IKT-kriminalitet. Påtalejuristene tar i liten grad etter- og videreutdanning, og baserer seg i hovedsak på erfaringsbasert læring. Påtalejuristene tar påtaleavgjørelser om henleggelse og tiltalebeslutning. Manglende oppmerksomhet om styrking av påtalekompetansen i politidistriktene er derfor en utfordring både for bekjempelsen av IKT-kriminalitet generelt, men også for ivaretakelse av rettssikkerheten for fornærmede og tiltalte i IKT-kriminalitetssaker hvor digitale bevis er avgjørende. Dette forsterkes ytterligere ved det økte omfanget av IKT-kriminalitet og digitale bevis i straffesaksbehandlingen.

14.4 Tiltakene for å styrke politiets kapasitet til etterforskning av IKT-kriminalitet har gitt få resultater og holder ikke tritt med utfordringene

I Meld. St. 29 (2011–2012) *Samfunnssikkerhet* ble det slått fast at IKT-kriminaliteten var i kraftig vekst, og at politiet stod overfor store utfordringer på dette området. I perioden fra denne stortingsmeldingen ble lagt fram i 2012, til utgangen av august 2020 er det totale antallet årsverk i politiet (unntatt PST) økt med 24 prosent (3392 årsverk).[287] Politidirektoratets kapasitetsundersøkelse fra 2019 viser at nesten ingen av disse årsverkene har havnet innen etterforskning. Etterforskningsarbeidet er likevel styrket etter politireformen ved at sakene håndteres mer enhetlig i felles straffeinntak i distriktene, og ved at kvaliteten på straffesaksarbeidet er bedret etter etterforskningsløftet. Men kapasiteten er fortsatt en utfordring. Dette er særlig synlig på området IKT-kriminalitet.

Det er iverksatt flere tiltak for å styrke politiets kapasitet til å etterforske IKT-kriminalitet og sikre elektroniske spor. Opprettelsen av enheter for digitalt politiarbeid (DPA) i alle politidistrikt i forbindelse med politireformen og NC3 ved Kripos fra januar 2019 er to av de viktigste tiltakene. Undersøkelsen viser imidlertid at det er kapasitetsutfordringer. Digitale spor kan være avgjørende bevis i alvorlige straffesaker. Undersøkelsen viser at politidistriktenes kapasitet innen digitalt politiarbeid og etterforskning av IKT-kriminalitet i all hovedsak brukes til å sikre elektroniske spor i alvorlige straffesaker som drap, grov vold, narkotika og sedelighetssaker. Annen IKT-kriminalitet enn seksuallovbrudd blir i mindre grad prioritert etterforsket. Ambisjonene for NC3, som er frontet som en stor satsing innen bekjempelsen av IKT-kriminalitet, er nedjustert fra en ambisjon om 200 ansatte innen utgangen av 2021, til 150 ansatte innen utgangen av 2022.

Mange politidistrikter har utfordringer med å sikre kontinuiteten i kompetanse og kapasitet til etterforskning av de alvorligste sakene – for eksempel internettrelaterte seksuelle overgrep. Mange saker skal etterforskes, og det er stor gjennomtrekk av etterforskere, som blant annet skyldes at mange av lønnsmessige årsaker

[287] Oversikter over antall ansatte fra Politidirektoratet viser at det totalt var 13 907,5 årsverk 31. desember 2012, og 17 299,7 årsverk 31. august 2020.

ønsker seg til ordenstjeneste framfor etterforskning. Begrenset kapasitet fører til krevende prioriteringer mellom de sakstypene Riksadvokaten framhever som prioriterte i sitt årlige mål- og prioriteringsskriv.

Som det slås fast i den siste politimeldingen, er det grunn til å anta at økningen i IKT-kriminalitet og digitalisering av kriminalitetsbildet vil fortsette. Behovet for etterforskningskapasitet er økende. Utfordringen er at dataetterforskere skal sikre elektroniske spor i et vidt spekter av saker samtidig som de skal bistå i etterforskning av IKT-kriminalitet. Sikring av elektroniske spor i de prioriterte, alvorlige straffesakene fører til at IKT-kriminalitet på andre områder nedprioriteres, for eksempel den økonomiske IKT-kriminaliteten og ren IKT-kriminalitet. Undersøkelser fra Næringslivets sikkerhetsråd og politiets innbyggerundersøkelse viser også at næringslivet og befolkningen har lavere grad av tillit til politiet på dette området, og at saker i mange tilfeller ikke anmeldes. Det er en fare for at dette fører til at IKT-kriminalitet som rammer enkeltpersoner og næringslivet ikke anmeldes og etterforskes. En konsekvens av dette er at virksomheter og privatpersoner henvender seg til private aktører for bistand når de utsettes for IKT-kriminalitet, for eksempel et løsepengevirusangrep.

14.5 Svakheter ved støttesystemer fører til lavere effektivitet, lite effektiv ressursbruk og manglende oppklaring av IKT-kriminalitet

I Innst. 306 S (2014–2015) viser justiskomiteen til at riktig bruk av digitale verktøy er avgjørende for politiets evne og mulighet til å løse sitt samfunnsoppdrag. Arbeidsmetoder og arbeidsprosesser må sikre effektiv disponering av politiressursene og legge til rette for raskere etterforskning med høyere kvalitet. I Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar* vises det til at verktøyene for å håndtere digitale spor må være oppdatert i tråd med den teknologiske utviklingen, og politiets etterforskningsmetoder må holde tritt med de kriminelles bruk av moderne teknologi.

Utfordringer ved støttesystemer har vært kjent over mange år. Innkjøp og drift av programvare og utstyr er i stor grad overlatt til det enkelte politidistrikt, og dataetterforskere bruker betydelig med tid og ressurser på å kjøpe inn, drifte og utvikle programvare og utstyr. Dette bidrar til en ineffektiv ressursbruk i en etat som fra før opplever et hardt press på ressursene. Mangel på utstyr og utdatert utstyr er en utfordring i en del distrikt. Og det foregår liten eller ingen samordning av dette arbeidet nasjonalt. Flere politidistrikter etterlyser nasjonal styring av innkjøp, administrasjon og sikring av støttesystemer og verktøy til digitalt politiarbeid. Det mangler i tillegg retningslinjer, standarder og veiledning for det digitale politiarbeidet. Dette er en potensiell risiko for at det utvikler seg måter å arbeide på som ikke er i tråd med faglig beste praksis.

Politiet mangler en tilfredsstillende infrastruktur for håndtering av digitale beslag. Politiets IKT-tjenester har brukt lang tid på å utvikle et lagringsnett for digitale beslag som i løpet av 2019 og 2020 er tatt i bruk av alle politidistrikt med unntak av Oslo politidistrikt. Det nye beslagsnettet tilfredsstiller i liten grad anbefalingene fra Kripos, møter ikke behovene distriktene har, og har vært preget av manglende brukerinvolvering. En stor utfordring for politiet i etterforskning av internettrelaterte seksuelle overgrep mot barn og unge, og annen IKT-kriminalitet, er omfanget av digitale beslag. Enheter for digitalt politiarbeid i distriktene bruker en stor andel av sin tid til gjennomgang av denne typen beslag. Kripos foreslo en nasjonal løsning for håndtering av overgrepsmateriale i 2016–2017 som fortsatt ikke er iverksatt. I dag gjennomgås digitale beslag i hvert enkelt distrikt uten særlig samordning. Politiet mangler en nasjonal løsning som kan bidra til å samordne etterforskningen på tvers av politidistrikter og gjøre informasjon mer tilgjengelig for analyse og etterforskning. Uten en nasjonal løsning blir politiets arbeid mindre effektivt. En videreutvikling av lagringsnettet slik at det i større grad kan imøtekomme de behovene politidistriktene har, er foreslått av fagmiljøet, men ikke prioritert av Politidirektoratet. Manglende prioritering og leveranser på dette området fra Politidirektoratet og Politiets IKT-tjenester fører til at utfordringene på dette området vedvarer.

14.6 Manglende samordning av etterforskningen av IKT-kriminalitet gir utfordringer for oppklaring av sakene.

Det går fram av Innst. 306 S (2014–2015) en forventning om at større organisatoriske enheter og en mer helhetlig organisering av politidistriktene vil styrke forutsetningene for systematisk kunnskapsutvikling og kunnskapsdeling.

IKT-kriminalitet skiller seg fra annen kriminalitet ved at det kan ramme mange offer på tvers av politidistrikter. Gjerningspersoner som står bak internettrelaterte seksuelle overgrep og nettbedragerier, utnytter denne

muligheten. Samordning mellom politidistriktene vil derfor i mange tilfeller være avgjørende for å avdekke og effektivt etterforske denne typen kriminalitet. Incentivene for samarbeid mellom distrikter er få. Manglende samordning og koordinering av politiets innsats mot internettrelaterte seksuelle overgrep er påpekt av Kripos, og tilsvarende er påpekt innen økonomisk IKT-kriminalitet av næringslivet som foreslår tettere samarbeid om deling av informasjon og etterretning uten at politiet har kunnet møte denne invitasjonen så langt. I påvente av bedre nasjonal samordning handler politiet reaktivt på innkommende saker, utvikler egne løsninger og metoder lokalt, og evner i liten grad å se kriminalitetsbildet nasjonalt og sette inn effektive tiltak for å forhindre eller effektivt bekjempe kriminaliteten. Nasjonal styring og samordning av innsatsen mot alvorlig kriminalitet på dette området er svak.

Manglende kompetanse og rutiner for å se sammenheng i saker i saksmottaket i distriktene fører til svakheter i den tidlige behandlingen. Felles straffesaksinntak (FSI) etablert i forbindelse med politireformen skal sikre befolkningen så lik behandling som mulig uavhengig av hvor man utsettes for kriminelle handlinger.[288] Undersøkelsen viser at det generelt er lite fokus på digitalt politiarbeid ved FSI i de fleste distrikter. Det er også generelt en utfordring med tilgang på riktig utstyr, programvare og kompetanse som kan sikre riktig prioritering og håndtering av saker i innledende fase. Undersøkelsen viser videre at FSI mangler rutiner og evne til å se sammenheng i saker som kommer inn. I de fleste distrikter håndterer FSI store saksmengder og har ikke kapasitet til å analysere sakene. Dette betyr at man mangler evnen til å fange opp trender og sammenhenger i kriminalitetsbildet i distriktet. Dette fører det til at for eksempel organiserte kriminelle som utøver IKT-kriminalitet mot mange ofre samtidig, i liten grad avdekkes. Dette bekreftes av større næringslivsaktører som er intervjuet i forbindelse med undersøkelsen.

Den viktigste ressursen for oppklaring av IKT-kriminalitetssaker, enhet for digitalt politiarbeid (DPA), bærer preg av å være ulikt organisert på ulike nivå i politiorganisasjonen. Dette preger flere av politidistriktene negativt, og skaper mål- og interessekonflikter.[289] Politidistriktene har organisert DPA noen steder som egen seksjon, andre steder som avsnitt, og enkelte steder sammen med kriminalteknikk i avsnitt eller seksjon. Ulik organisering av DPA gir utfordringer med hensyn til kunnskapsdeling og kompetanseutvikling. Det mangler nasjonale rammeverk, fagstyring og føringer for organisering av funksjonen. Digitalt politiarbeid blir for lite synlig nasjonalt og det gir ikke nødvendig framdrift i arbeidet med å omstille politiet til endringene i kriminalitetsbildet med mer IKT-kriminalitet. Fagkontakter kan være en viktig ressurs for oppklaring av IKT-krimsaker, men brukes i varierende grad. DPA i flere distrikter etterlyser nasjonale retningslinjer for hvilken rolle og kompetanse fagkontaktene skal ha.

14.7 Utfordringer ved internasjonalt samarbeid bidrar til lav oppklaring av IKT-kriminalitet

I Prop. 1 S (2018–2019) for Justis- og beredskapsdepartementet presiseres det at lovbrudd ofte har internasjonale koblinger og gjennomføres av kriminelle nettverk som ikke følger landegrensene. Dette vil i mange saker bety at et godt internasjonalt samarbeid er en forutsetning for bekjempelse av grenseoverskridende kriminalitet. Fra 2016 har Riksadvokaten sagt at internasjonalt samarbeid må vektlegges i oppfølgingen av IKT-kriminalitet.

For politiet er internasjonalt samarbeid i mange sammenhenger avgjørende for oppklaring, men politiet utfordres av ulikheter i landenes lovgivning som gjør det krevende å opprettholde en effektiv kriminalitetsbekjempelse og straffeforfølgning.[290] Politidistriktene som er intervjuet sier at IKT-kriminalitetssakene med spor eller gjerningsperson utenlands ofte henlegges av hensyn til tids- og ressursbruken som ofte medgår i slike saker. En sak må være høyt prioritert for at samarbeid med andre land igangsettes. Dette gjelder både ved behov for gjennomføring av avhør utenlands eller ved innhenting av bevis fra tjenesteleverandører i utlandet. Flere politidistrikter peker på mangel på rutiner og et felles kontaktpunkt når det gjelder dialogen med internasjonale tjenesteleverandører.

[288] Politidirektoratet (2019) *Status fagområde etterforskningsledelse*, faggrupperapport levert Politidirektoratet i september 2019.
[289] Politidirektoratet (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning*, faggrupperapport utarbeidet av en arbeidsgruppe på oppdrag fra Politidirektoratet, datert 9. september 2019.
[290] NOU 2017:11 *Bedre bistand. Bedre beredskap. Fremtidig organisering av politiets særorganer*.

Det er også store forskjeller mellom politidistriktene når det gjelder forfølging av spor og etterforskningsskritt utenlands.[291] Videre er det begrenset med nasjonale støttedokumenter når det gjelder internasjonalt politi- eller rettslig samarbeid.[292]

Utfordringene i det internasjonale politisamarbeider bidrar til at kriminelle unnslipper rettsforfølging ved å operere på tvers av landegrenser. Disse svakhetene utnyttes av kriminelle nettverk. Slik det internasjonale samarbeidet er i dag, er forutsetningene for effektiv bekjempelse av kriminalitet med internasjonale forgreninger ikke til stede. Vi kan heller ikke se at det internasjonale samarbeidet er vektlagt i politiet.

14.8 IKT-kriminalitet har i liten grad vært prioritert av Politidirektoratet og Justis- og beredskapsdepartementet

I henhold til reglement for økonomistyring i staten § 7 skal ansvarlige departementer fastsette mål, styringsparametere og krav til rapportering for underliggende virksomheter. Styring, oppfølging, kontroll og forvaltning må tilpasses virksomhetens egenart, risiko og vesentlighet, jf. § 4.

Riksadvokaten viser til at resultatene i kriminalitetsbekjempelsen på dette området ikke er tilfredsstillende. Det gjelder både for de alvorlige lovbruddene som omfattes av Riksadvokatens prioriteringer, men også for de mindre alvorlige sakene. Riksadvokaten opplever at det er for få saker som blir anmeldt, og for få av de anmeldte sakene som blir etterforsket. Riksadvokaten er også bekymret over at det er et lavt antall positive påtaleavgjørelser innenfor IKT-kriminalitetsfeltet. Årsakene til at kriminalitetsbekjempelsen på området ikke er tilfredsstillende, er sammensatt ifølge Riksadvokaten. Manglende kapasitet og kompetanse på etterforskningsfeltet er en utfordring. Riksadvokaten mener feltet ikke har fått den oppmerksomheten som kriminalitetsutviklingen tilsier, verken fra Justis- og beredskapsdepartementet, Politidirektoratet, de enkelte politidistriktene eller den høyere påtalemyndighet. Mangel på en felles definisjon av IKT-kriminalitet er en utfordring, og vanskeliggjør arbeidet med å utarbeide treffsikre analyser. Uten å ha dette på plass, vil det ifølge Riksadvokaten, være vanskelig å oppnå en tilfredsstillende innsats på IKT-kriminalitetsfeltet.

Fagmiljøene innen etterforskning av IKT-kriminalitet opplever Politidirektoratets styring av innsatsen mot IKT-kriminalitet som svak. Politidirektoratet har bestilt rapporter og utredninger som gjentatte ganger de siste ti årene fastslår utfordringene på dette området. I den samme perioden har både bemanning og budsjetter økt betydelig i politietaten. Likevel fastslår direktoratet, senest i årsrapporten for 2019, at utfordringene på dette området i mindre grad vil kunne nås uten særlig styrking av kapasitet, kompetanse og teknologi. Politidirektoratet viser til at det gjentatte ganger er bedt om ressursmessig styrking uten at dette er prioritert, og at dette har gjort det vanskelige å ta tak i utfordringene.

Justis- og beredskapsdepartementet skal ivareta en rekke prioriteringer når det gjelder politiet. Det er ikke revisjonens oppgave å overprøve disse prioriteringene. Vi konstaterer imidlertid at departementet har vært klar over utfordringen på området IKT-kriminalitet over mange år. Det ble blant annet derfor iverksatt en strategi i 2015 og bekjempelse av IKT-kriminalitet er også sentralt i regjeringens nasjonale strategi for digital sikkerhet for 2019. Justis- og beredskapsdepartementet mener at Politidirektoratet har hatt mandat og handlingsrom til å prioritere dette området. Når departementet er kjent med utfordringene, og Politidirektoratet ikke har prioritert området, er det vår vurdering at Justis- og beredskapsdepartementet i større grad burde hatt en tettere og tydeligere styring, jf. kravet om at styringen skal tilpasses risiko og vesentlighet. At begrepet IKT-kriminalitet har vært uklart både for Politidirektoratet og departementet, i tillegg til den manglende oversikten over omfanget av IKT-kriminalitet, synes å ha bidratt til styringsutfordringene.

[291] Politidirektoratet (2019) *Fagforvaltning statusrapport - Status fagområde Internasjonalt straffesaksarbeid*, 2. oktober 2019.
[292] Politidirektoratet (2019) *Fagforvaltning statusrapport - Status fagområde Internasjonalt straffesaksarbeid*, 2. oktober 2019.

15 Vedlegg

Vedlegg 1: Manuell gjennomgang

Gjennomgang av saker

Tabell 10 gir en oversikt over hvordan vi gikk fram for å kode sakene i de utvalget.

Tabell 10 Oversikt over framgangsmåte for manuell gjennomgang av saker

Antall saker	Antall personer som kodet	Formål
30 saker (ikke med i utvalget)[293]	4 personer på hver sak	For sjekk av samsvarsrate mellom kodere
100 saker (med i utvalget)	4 personer på hver sak	For ytterligere sjekk av samsvarsrate og oppstart av utvalget for manuell koding
898 saker (med i utvalget)	4 personer totalt (2 ulike personer gjennomgikk hver sak)	For manuell klassifisering
74 saker (med i utvalget)	3 personer totalt (2 ulike personer gjennomgikk hver sak)	Datasett for test av maskinlæringsmodell. Ble også brukt inn i den manuelle klassifiseringen

Kilde: Riksrevisjonen

Som tabellen viser, ble 30 saker fra 2018 gjennomgått som pilotering og for å sørge for omforent kodepraksis. Disse var ikke en del av utvalget vårt. Disse sakene ble gjennomgått av alle fire kodere, for å sørge for omforent kodepraksis. Deretter ble 100 saker *fra utvalget* gjennomgått av alle fire koderne. Saker der ikke alle sammen hadde kodet identisk ble gjennomgått. De neste 898 sakene ble delt i to, hvor to kodere gikk gjennom de samme sakene. Der kodingen ikke var identisk ble saken gjennomgått av alle kodere i fellesskap. I etterkant ble datasettet supplert med 74 saker, som skulle brukes for å teste maskinlæringsmodellen. Siden disse sakene ble trukket med samme utvalgskriterier som de andre sakene, ble disse sakene inkludert i den manuelle klassifiseringen. Alle sakene ble gjennomgått av to personer. Der sakene ikke var blitt identisk kodet, ble de gjennomgått i fellesskap.

Samsvarsrate mellom kodere

De 100 første gjennomgåtte sakene, som ble kodet av alle fire kodere, ble brukt for å beregne samsvar på tvers av de fire koderne. Tabellen under viser resultatene i form av samsvarsrate og fem andre mål som justerer for tilfeldig samsvar. Koeffisientene for de siste fem målene ligger mellom 0,70 og 0,84, og indikerer enten «betydelig» grad av samsvar (mellom 0,61 og 0,80) eller «nesten perfekt» samsvar (mellom 0,81 og 1).[294]

Tabell 11 Samsvarsestimater for 100 saker kodet av alle fire koderne

			95 % konfidensintervall	
Mål for samsvar	**Samsvar**	**Standardfeil**	**Nedre**	**Øvre**
Samsvarsrate	0,87	0,03	0,82	0,92
Brennan and Prediger	0,81	0,04	0,73	0,89
Cohen/Conger's Kappa	0,70	0,05	0,60	0,80
Scott/Fleiss' Kappa	0,70	0,05	0,60	0,80

[293] Ble brukt i utviklingen av maskinlæringsalgoritmen, der det ikke er viktig at utvalget er representativt.
[294] Klein, Daniel (2018) *Implementing a general framework for assessing interrater agreement in Stata*. Stata Journal 18(4): 871-901.

Gwet's AC	0,84	0,03	0,77	0,91
Krippendorff's Alpha	0,70	0,05	0,60	0,80

Kilde: Riksrevisjonen

Ser vi nærmere på uoverensstemmelsene, finner vi at de i hovedsak gjelder koding av saker som «vet ikke». Av de 21 sakene med uoverensstemmelse mellom én eller flere av koderne er det bare i 4 saker at én eller flere har kodet «IKT-kriminalitet», mens andre har kodet «ikke IKT-kriminalitet». Dette tyder på at uoverensstemmelsene hovedsakelig dreier seg om hvor mye informasjon man må ha for å kunne klassifisere en sak. I saker med tilstrekkelig informasjon er det veldig liten uoverensstemmelse i klassifiseringen.

Hjelp fra referansegruppe

Flertallet av anmeldelsene var enkle å kategorisere, basert på beskrivelsen av det anmeldte lovbruddet. I enkelte tilfeller var det imidlertid vanskeligere å avgjøre. For fem utvalgte sakstyper hvor det var tvil om klassifisering. Tre av disse forekom relativt hyppig.[295] Det ble derfor innhentet synspunkter fra en referansegruppe bestående av fem påtalejurister, fem dataetterforskere og to fra Politidirektoratet. Seks av gruppens medlemmer ga tilbakemelding på hver enkelt kategori, en ga en generell tilbakemelding. Basert på tilbakemeldingene fra gruppen ble kun én av fem tvilstilfeller klassifisert som IKT-kriminalitet. For nærmere beskrivelse se vedlegg 1.

Tabell 12 Medlemmer i referansegruppens innspill til klassifisering av 5 ulike sakstyper

Sakstype, statistikkgruppe	Hvor hyppig forekommer saken i utvalget?	Ja, kan klassifiseres som IKT-kriminalitet	Nei, ikke IKT-kriminalitet	Endelig klassifisering
1. **Narkotika, narkotikaovertredelse.** Anmeldelse fra Tollvesenet av forsøk på ulovlig import av narkotika via brevpost. Det går ikke fram om vedkommende har bestilt dette på nettet. Lignende saker forekommer ved forsøk på ulovlig import av våpen og dopingpreparater.	Hyppig	3	3	Ikke IKT-kriminalitet
2. **Økonomi, Identitetskrenkelse, befatning med annens identitetsbevis/ID-tyveri/bedrageri** Anmeldelser av ukjente transaksjoner fra bankkonto eller misbruk av betalingskort. Kortet oppgis å være stjålet eller mistet, men kan ha blitt brukt for eksempel i nettbutikker, fysisk i butikk eller for bestilling av telefonabonnement.	Hyppig	1	5	Ikke IKT-kriminalitet
3. **Økonomi, bedrageri.** Anmeldt av NAV for inngivelse av uriktige opplysninger i elektroniske meldekort.	Hyppig			IKT-kriminalitet – basert på opplysninger fra en rapport fra NTAES hvor det heter at elektroniske meldekort behandles automatisk og digitalt, og handlingen er derfor å anse som et databedrageri.[296]
4. **Annet, hensynsløs atferd.** Det er eksempler på saker hvor trusler formidles til fornærmede via telefonsamtale.	Mindre hyppig	2	4	Ikke IKT-kriminalitet
5. **Annet, dokumentfalsk.** Anmeldelse fra apotek for forfalskning av resept. Det framgår ikke hvordan resepten har blitt produsert.	Mindre hyppig	2	3	Ikke IKT-kriminalitet

Kilde: Riksrevisjonen

[295] Sakstyper som forekom relativt hyppig, var ID-krenkelser/bedragerier hvor svindel med kort var involvert, svindel med elektronisk meldekort til NAV og narkotikaovertredelser – forsøk på import av narkotika via brevpost.
[296] Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) (2019) *Bedrageri mot næringslivet*, februar 2019.

Resultater fra koding

Resultatet av den manuelle gjennomgangen er vist i tabellen nedenfor. Totalt ble 148 saker klassifisert som IKT-kriminalitet, 11 saker ble klassifisert som usikre, av totalt 1072 saker. Resultatene viser at politiet underestimerer omfanget av IKT-kriminalitet ved å basere seg på statistikk som tar utgangspunkt i koding av IKT-modus i sakene.

Tabell 13 IKT-kriminalitet etter kriminalitetstype

Kriminalitetstype	Utvalg	IKT-kriminalitet	Vet ikke	Andel IKT-kriminalitet	Andel saker med IKT-modus registrert av politiet
Annen	150	12	5	8,6 %	**7 %**
Narkotika	148	2	-	1,4 %	**-**
Seksuallovbrudd	150	36	-	24,3 %	**19 %**
Skadeverk	88	-	-		**-**
Trafikk	86	-	-		**-**
Vinning	150	3	-	2,1 %	**0,7 %**
Vold	150	6	-	3,6 %	**0,9 %**
Økonomi	150	89	6	58,6 %	**36 %**
Totalt	**1072**	**148**	**11**		

Kilde: Riksrevisjonens manuelle identifisering av IKT-kriminalitet fra et tilfeldig valgt utvalg på 998 saker fra 2018

Samsvar mellom vår manuelle klassifisering av IKT-kriminalitetssaker og politiets moduskoding kan også framstilles ved hjelp av en konfusjonsmatrise (Confusion Matrix). I tabellen under (tabell 14) er samsvar vist med utgangspunkt i 1061[297] av de 1072 sakene som er manuelt gjennomgått.

Tabell 14 Konfusjonsmatrise (confusion matrix) for den manuelle kodingen og politiets registrering

		Politiets registrering		Sum
		Ikke IKT	IKT	
Manuell koding	Ikke IKT	902	11	**913**
	IKT	64	84	**148**
Sum	**966**	**95**	**1061***	

Kilde: Riksrevisjonen
* 11 av de 1072 sakene som ble gjennomgått manuelt, ble kodet som «vet ikke». De kan derfor ikke brukes til å sammenligne den manuelle kodingen og politiets koding.

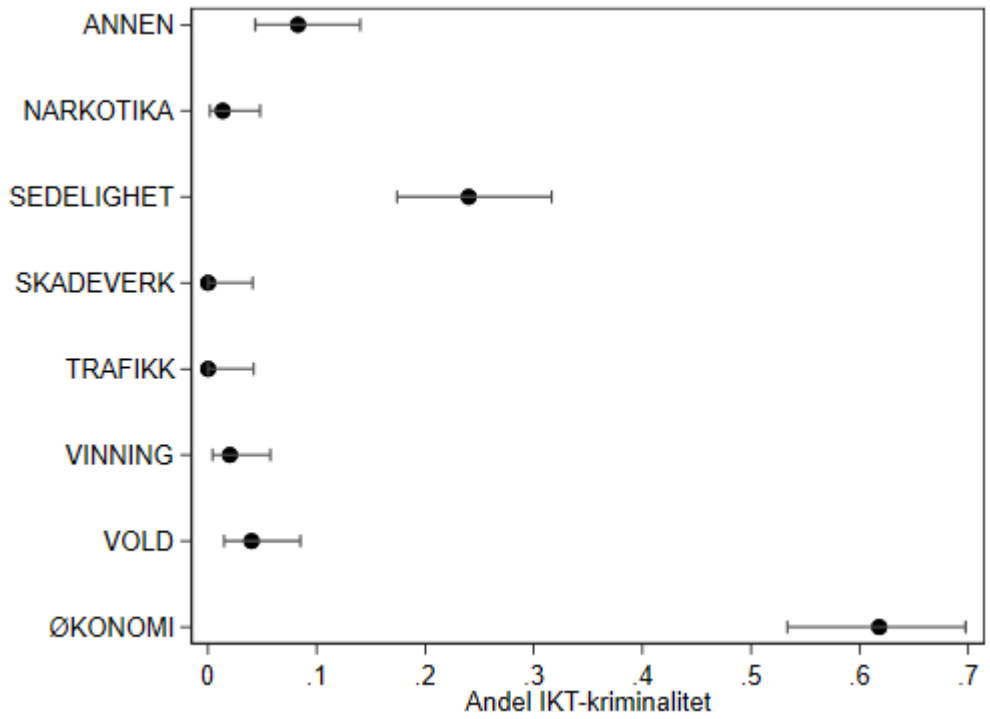
Tabellen viser at Politiet underestimerer IKT-kriminalitet. Ved å anvendte politiets IKT-moduskoding vil kun 84 av 148 saker klassifiseres som IKT-kriminalitet.

Figur 17 viser estimatene for IKT-kriminalitet med konfidensintervaller.

[297] 11 av de 1072 sakene som ble gjennomgått manuelt, ble kodet som «vet ikke». De kan derfor ikke brukes til å sammenligne den manuelle kodingen og politiets koding.

Figur 17 Andel IKT-kriminalitet innenfor anmeldte saker i 2018 etter kriminalitetstype

[Bilder eller grafikk endres etter behov]



Kilde: Riksrevisjonen.
Forklaring: Data: Manuell koding av stratifisert utvalg på 1072 saker. Prikkene viser punktestimatet for andel IKT-kriminalitet, mens utstikkerne viser 95 % konfidensintervall (Exact Binomial Clopper-Pearson).

Konfidensintervaller for saker som er manuelt klassifisert, viser at de reelle tallene kan være både høyere og lavere. Gitt at en konservativ tolkning av hva som er IKT-kriminalitet er lagt til grunn, kan det være grunnlag for å anta at antallet IKT-kriminalitetssaker kan være betydelig høyere enn det vi har anslått, særlig innen kriminalitetstypene sedelighet og økonomi.

Vedlegg 2: Maskinlæringsmodell for klassifisering av IKT-kriminalitetssaker

Datagrunnlag for trening av maskinlæringsmodellen – dataomfang og andel IKT-kriminalitet

Av totalt 334 544 saker med tekst har 286 726 anmeldelsestekst, for 47 814 saker består teksten bare av saksbeskrivelse og modussammendrag, og 4 har bare modussammendrag. 1081 saker er merket (labelled) med klassifisering fra den manuelle gjennomgangen.

Data inkluderer ulike kriminalitetstyper som har ulik frekvens. Til modellbyggingen, er kriminalitetstype dikotomisert etter hvorvidt det er IKT-kriminalitet, eller ikke er IKT-kriminalitet. Disse gruppene er ikke jevnt fordelt i populasjonen. Andelen predikert IKT-kriminalitet i den totale populasjonen er 6 prosent. På grunn av denne skjevfordelingen, er utvalget av kodede (labelled) saker for utvikling av modellen valgt med en fordeling av kriminalitetstyper som har en større andel IKT-kriminalitetssaker, slik som vist i tabell 16.

Tabell 15 Antall anmeldelser og prosent IKT-kriminalitet per kriminalitetskategori

Krimtype	Antall anmeldelser	% IKT-krim*	Antall anmeldelser	% IKT-krim
ANNEN	40 003	5.8	139	**9.4**
ARBEIDSMILJØ	863	0.1	2	**0.0**
MILJØ	1985	1.1	6	**0.0**
NARKOTIKA	36 292	0.2	147	**1.4**
SEDELIGHET	8438	16.6	152	**24.3**
SKADEVERK	17 068	0.1	91	**0.0**
TRAFIKK	54 275	0.0	88	**0.0**
UNDERSØKELSESSAKER	12 017	0.5	0	**0.0**
VINNING	100 854	0.8	153	**2.0**
VOLD	33 171	1.6	152	**3.9**
ØKONOMI	29 578	55.0	151	**64.2**
Totalt	334 544	-	1081	-

Kilde: Riksrevisjonen
* IKT-andel i hele populasjonen estimert fra ML-prediksjon.

Det merkede utvalg på total 1081 saker blir delt i to. Et datasett for trening og validering av modellen på 944 saker, og et datasett på 137 saker som blir holdt tilbake for test av endelig modell.

Ytelsesmål (*performance measure*)

Det er flere mål for å vurdere en modells ytelse (performance). På grunn av skjevfordelingen av klasser i treningsdata og i populasjonen, er modellene evaluert ved å se på *Matthew's correlation coefficient* (MCC). Denne er definert ved:

$$MCC = \frac{TP \cdot TN - FP \cdot FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

hvor sanne positive TP (true positives), falske positive FP (false positives), sanne negative TN (true negatives) og falske negative FN (false negatives) hentes fra konfusjonsmatrisen.

MCC er standard mål for binær klassifisering og ble valgt fordi den er symmetrisk mellom positiv og negativ klasse, og derfor håndterer ulik klassefordeling godt. Det betyr at det er uproblematisk at det finnes mindre antall IKT-krim enn ikke-IKT-krim. Høyere MCC indikerer en bedre modell, med høyeste score 1, som indikerer perfekt klassifisering.

I tillegg til MCC beregnes spesifisitet, sensitivitet og presisjon:

- Spesifisitet: $(spes = \frac{TN}{TN+FP})$ måler andel av ikke-IKT saker som er riktig klassifisert.
- Sensitivitet: $(sens = \frac{TP}{TP+FN})$ måler andel av IKT-skaker som er riktig klassifisert.
- Presisjon: $(pres = \frac{TP}{TP+FP})$ måler andel av IKT-klassifiseringer som er riktig.

Alle disse målene er interessante, men det er knyttet stor usikkerhet til både sensitivitet og presisjon fordi de er sterkt avhengig av IKT-klasser som har få observasjoner. Derfor legges det mer vekt på høy spesifisitet, det vil si færre falske positive. I avveiing av falske positive mot falske negative er sistnevnte dessuten mer akseptabel i vår kontekst for å teste om politiets modusklassifisering tilstrekkelig fanger opp IKT-kriminalitet.

Variabler (feature engineering)

Det benyttes to typer variabler (kalt features) i modellen:

1. Variabler som er konstruert fra den relative frekvensen av bestemte ord i teksten (satt sammen av anmeldelsestekst, saksbeskrivelse og modussammendrag)
2. Variabler basert på metadata

For den siste typen er det konstruert fire variabler:

- Dikotom variabel om teksten er på engelsk eller ikke (*is_english*).
- Dikotom variabel om informasjon om gjerningsbydel finnes eller ikke (*has_gb*).
- To diktotome variabler for om kriminalitetstype er enten økonomi (*kt_oko*) eller sedelighet (*kt_sedan*). Disse kriminalitetstypene har høyest andel av IKT-kriminalitet.

Alle andre, av de totalt 75 variablene, beskriver frekvensen av ord i teksten.

Fra tekst til numeriske variabler

Teksten er vasket og delt opp i ord (tokens).[298] Frekvensen av hvert ord i en tekst er da beregnet relativ til frekvensen i alle tekster (det vil si av alle saker i hele populasjonen, inklusive ikke-merkede saker med ukjent klasse).

Fordi ulike ord kan brukes for lignende forhold, gjør det stor forskjell for klassifiseringen hvilke ord som er slått sammen til synonymer. For kontekst av IKT-kriminalitet er det meningsfylt å definere synonymer, for eksempel for nettsider, sosiale medier eller verb som beskriver handlinger knyttet til IKT-kriminalitet. I tillegg brukes synonymer for å slå sammen ord som forekommer sjelden, men som er en klar indikator på hvorvidt en sak gjelder IKT-kriminalitet eller ikke, slik at disse ikke vil plukkes opp av en maskinlæringsmodell. For eksempel inneholder det genererte «synonymet» *rare_it* ord som domene, hacke, datasystem, mens «synonymet» *rare_not_it* inneholder ord som regnskapsovertredelse, bokføring og kreditorbegunstigelse.

Tekst fra standardskjema

Et spesielt «synonym» er utviklet for det vi kaller et standardskjema brukt ved anmeldelse. «Synonymet» slår sammen mange sammensatte ord (compounds) som gjenspeiler setninger fra ulike versjoner av et standardskjema. Før trening av modellen er variable konvertert til en dikotom variabel, som viser om et standardskjema ble brukt eller ikke.

Standardskjema fylles av og til ut for hånd og håndskrift er ikke mulig å lese inn til maskinlesbar skrift med optisk tegngjenkjenning (optical character recognition, OCR). Teksten som leses inn, blir da kun den standardteksten som er del av skjemaet. Ordene fra denne teksten vil ikke nødvendigvis ha noe med saken å gjøre, og kan gi modellen dårligere ytelse. Når et slik skjema er benyttet, blir derfor teksten som hører til skjemaet fjernet, og bare de setningene som er skrevet i selve skjemaet blir beholdt.

I tillegg forsøkes det i analysen av standardskjema å identifisere om en fysisk gjenstand med sensitiv informasjon er mistet eller stjålet. Bakgrunnen for denne analysen er anmeldelser av uautoriserte kontooverføringer (identitetstyverier, bedragerier). Når bankkort eller andre fysiske gjenstander er mistet eller stjålet, regnes saken ikke som IKT-kriminalitet. Funksjonen som analyserer standardskjema, legger da til *fysisk_tap_ja* eller *fysisk_tap_nei* til korpuset. Det er kun *fysisk_tap_ja* som blir brukt i modellbyggingen, som

[298] Denne delen av prosessen er dokumentert i dokumentet «Dokumentasjon Text Mining», men på grunn av sensitivt datamateriale vil dette ikke deles i rapporten.

en del av synonymet *rare_not_it*. *fysisk_tap_nei* blir ikke brukt, da den gir for mange falske negative, det vil si tilfeller hvor noe som var frastjålet, ikke kunne identifiseres i analysen av skjemaet.

Valg av variabler

Relative ordfrekvenser i treningsdata er brukt i utvelgelse av variabler (features) til modellen. Følgende tilnærming er fulgt:

- Ord er rangert etter relativ hyppighet separat for de to klassene IKT-krim og ikke-IKT-krim, hvor det mest hyppig brukte ordet rangeres høyest.
- De 150 hyppigste ordene fra de to klassene er så valgt.
- Ord som er i begge lister og har en forskjellig rangering, som er lavere enn 100, er fjernet for å unngå at ord som forekommer hyppig for alle typer saker blir inkludert.
- Listen over ord er så korrigert med en manuell liste over ord som skal ekskluderes eller inkluderes (denne er i hovedsak satt sammen av prosjektteamet).
- Deretter er de 70 ordene som har størst forskjell i gjennomsnittlig *logcount (mean(1+log(tf_{ij})))* mellom IKT- / ikke-IKT-saker, valgt ut.
- De 15 ordene med neststørst ordfrekvens (etter de 70 er tatt ut), er kombinert inn i nye synonymer (*extra_it* og *extra_not_it*).

Bare disse ordene er brukt som variabler, vektet med skjemaet *logave* med naturlig logaritme:

$$\frac{1 + ln(tf_{ij})}{1 + ln(\sum_j tf_{ij}/N_i)}$$

Synonymer *rare_it* og *rare_not_it* er i tillegg vektet med en faktor 3, og synonym *other_not_it_1* med en faktor 2. Sistnevnte synonym inneholder på samme måte som *rare_not_it* ord som er enkeltvis ikke hyppige, men ikke helt så uvanlig som ord i *rare_not_it*.

Treningsprosedyre

Siden ytterligere deling av treningsdata i faste trenings- og valideringsdata fører til store endringer i MCC avhengig av hvilket *seed* som settes for delingen (pseudo-tilfeldig utvalg), benyttes 4-foldet kryssvalidering. På denne måten benyttes hele datasettet til trening og validering, og det tas et gjennomsnitt av MCC på testdata for å evaluere modellene. I tillegg til de klassiske *hyperparametrene*[299] som bestemmer modellen, må også de parametrene som er brukt for å velge ut variablene til modellen (slik som antall ord, type vekting mv.) anses som en form for hyperparametre, da disse har stor påvirkning på den endelige modellen.

Følgende modelltyper ble testet:

- Naive Bias
- Random Forest (RF)
- XGBoost
- Support Vector Machine (SVM)

Tidlig i prosessen (dvs. uten mye optimering av hyperparameter) ble Naive Bias utelukket fordi MCC var lavere enn for de andre (0,6 mot omtrent 0,7 for de tre andre), og RF og XGBoost ble utelukket fordi de var sterkt overtrent (MCC på treningsdata var nesten 1). SVM var derfor i utgangspunkt mest lovende, og ble videre optimert.

Resultat

Den endelige modellen er trent på alle kodede observasjoner (uten inndeling i trenings- og testdata). For å estimere ytelse på hele populasjonen blir i tillegg kjørt en 5-foldet kryssvalidering med ulike kriminalitetskategori-fordeling i trenings- og testdel av data, samt at modellen er trent på datautvalg tilsvarende den kodede populasjonen, mens ytelse er beregnet på datautvalg med kriminalitetskategorier som tilsvarer andelen i hele populasjonen. MCC er estimert til 0,79, sensitivitet til 0,79, spesifisitet til 0,99 og presisjon til 0,84. Merk at det kan forventes at ytelse er bedre for kriminalitetskategorier som har flere

[299] Hyperparametre er parametre som blir satt før modellen kjøres, og som kan ha betydning for ytelsen til modellen. For eksempel er antall grener i et beslutningstre, eller antall beslutningstrær i en Random Forest-modell hyperparametre.

eksempler i treningsdata enn for kriminalitetskategorier som er mindre representert i treningsdata. Tabell 17 viser konfusjonsmatrise for alle merkete saker for både ML modellen og politiets moduskoding.

Tabell 16 Konfusjonsmatrise av politiets moduskoding vs. prediksjon av ML model

	Ikke IKT	IKT	Ikke IKT	IKT
Ikke-IKT-kriminalitet	902	11	891	**22**
IKT-kriminalitet	**64**	**84**	**23**	**125**

Kilde: Riksrevisjonen.

Merk at for den endelig ML modellen er dette tilsvarende treningsytelse, det vil si litt bedre enn tallene ovenfor. Samtidig vises det at modellens absolutte antall falske positive og falske negative er ganske likt, så total predikert omfang av IKT-saker er ganske pålitelig. Politiets moduskoding viser derimot mange flere falske negative enn falske positive.

Modellen er ikke brukt for klassifisering av enkelte saker. Dersom det var ønskelig å utvikle en modell for klassifisering av enkeltsaker, anbefales det at et betydelig større utvalg av saker hadde blitt kodet for trening, og eventuelt at separate modeller hadde blitt trent for ulike kriminalitetskategorier.

Vedlegg 3: Sammenligning av tidsbruksestimater

Vi har brukt Stata for å beregne tidsbruk per straffesak, siden det tillot en effektiv behandling av de store datamengdene og dokumentasjon av alle operasjoner i et repliserbart skript. I korte trekk gjennomførte vi følgende steg:

1. Import (til Stata), omstrukturering og sammenslåing av rutinetabellene
2. Import og sammenslåing av tidsbrukstabellene
3. Gjennomgang og skriving av formler for tidsbruk for hver rutine i Stata-skript
4. Utregning av tidsbruk per rutine
5. Sammenslåing til en samlet tabell med tidsbruksestimater for hver straffesak
6. Kobling av tabellen med tidsbruksestimater per sak og tabellen med vår klassifisering av IKT-Kriminalitet for saker registrert i 2018.

For å sjekke prosessen vår sammenlignet vi tidsbruksestimatene våre med aggregerte estimater fra Kapasitetsundersøkelsen. Vi gikk tilbake og gjorde endringer inntil avvikene var små. For å kontrollere vår bearbeiding av tidsbruksdataene aggregerte vi våre estimater opp til gjennomsnittlig antall timer per sak etter sakskategori. Denne statistikken ble også utregnet av Kapasitetsundersøkelsen (vedlegg tilsendt Riksrevisjonen).

Tabellen under viser gjennomsnittlig antall timer etter undergruppe fra Kapasitetsundersøkelsen og Riksrevisjonen. Prosentvis feil er beregnet med utgangspunkt i at Kapasitetsundersøkelsens estimater er riktige.

Den gjennomsnittlige feilen på tvers av undergrupper er veldig liten (0,6 %). Feilen er på under +/– 10 prosent for 18 av 21 undergrupper. Den klart største prosentvise feilen er for annen økonomisk kriminalitet (–24,2 %). Men siden denne undergruppen har relativt lav tidsbruk så er feilen liten i absolutte tall (2 timers forskjell).

Tabell 17 Gjennomsnittlig antall timer per undergruppe fra Kapasitetsundersøkelsen og Riksrevisjonen

	Timer per sak (estimert)		
Undergruppe	**Kapasitets-undersøkelsen**	**Riksrevisjonen**	**Feil (%)**
Annen økonomisk kriminalitet	8,6	10,6	-24,2
Trafikk	9,6	10,9	-13,5
Annen	12,1	13,0	-7,7
Doping-/narkotikaovertredelse	10,0	10,6	-6,7
Skadeverk	5,7	6,0	-5,5
Annen vinningskriminalitet	4,4	4,6	-4,6
Undersøkelsessaker	20,9	21,6	-3,4
Hatkriminalitet	14,9	15,2	-2,4
Annen vold	38,4	38,8	-1,1
Orden	7,8	7,9	-0,9
Forfalskning / uriktige oppl. / unndragelser	7,6	7,7	-0,4
Arbeidsmiljø/miljø	23,3	22,8	2,3
Grovt tyveri	18,3	17,8	2,7
Ran	99,1	95,4	3,8
Voldtekt	149,5	143,7	3,8
Drap	1344,3	1282,6	4,6

Mishandling i nære relasjoner	131,0	124,1	5,2
Seksuell omgang og voldtekt av barn u. 16 år	149,7	140,3	6,2
Grov doping-/narkotikaovertredelse	612,9	556,9	9,1
Alvorlig økonomisk kriminalitet	42,7	38,6	9,8
Andre seksuallovbrudd	32,3	29,0	10,5
Gjennomsnitt	130,6	123,7	-0,6

Kilde: Politidirektoratet og Riksrevisjonen.

Vedlegg 4: T-tester av forskjeller i tidsbruk

Tabell 18 T-tester av forskjell i tidsbruk mellom IKT-saker og ikke-IKT saker innen sedelighetsområdet

Statistikkgruppe	Differanse (timer)^	t-verdi	N
Framvis/still av seks. overgr./seksualiserer barn	-38.10***	(-7.28)	834
Seksuelt krenkende atferd	-0.405	(-0.10)	367
Seksuelt krenkende atferd mv. barn u. 16 år	-26.47*	(-1.99)	322

Kilde: ^ Differanse: gjennomsnittlig tidsbruk på ikke-IKT-saker minus gjennomsnittlig tidsbruk på IKT-saker
* p < 0.05, ** p < 0.01, *** p < 0.001

Tabell 19 T-tester av forskjell i tidsbruk mellom IKT-saker og ikke-IKT saker innen økonomiområdet

Statistikkgruppe	Differanse (timer)	t	N
Bedrageri	1.341**	(2.58)	7294
Bedrageri, forsøk	5.534***	(3.84)	538
Bedrageri, grovt	6.252	(1.02)	881
Bedrageri, mindre	0.685	(1.55)	1224
ID-krenkelse (befatning med annen)	-1.125	(-0.60)	244
ID-krenkelse (opptre med annen)	0.134	(0.13)	1583

Kilde: ^ Differanse: gjennomsnittlig tidsbruk på ikke-IKT-saker minus gjennomsnittlig tidsbruk på IKT-saker
* p < 0.05, ** p < 0.01, *** p < 0.001

Vedlegg 5: Tester av forskjeller i oppklaringsandel

Tabell 20 Tester av forskjell mellom andel oppklart for IKT-saker og ikke-IKT-saker innen økonomiområdet

Statistikkgruppe	Differanse	t	N
Bedrageri	-0.0289***	(-3.53)	12399
Bedrageri, forsøk	0.194***	(7.00)	943
Bedrageri, grovt	-0.0755**	(-3.03)	1430
Bedrageri, mindre	0.0337	(1.63)	1780
ID-krenkelse (befatning med annen)	-0.146***	(-3.70)	641
ID-krenkelse (opptre med annen)	0.0985***	(7.31)	2579

Kilde: Resultat fra test av forskjell mellom andeler i to uavhengige grupper («prtest» i Stata).
^ Differanse: Andel oppklart for ikke-IKT-saker minus andel oppklart for IKT-saker
* p < 0.05, ** p < 0.01, *** p < 0.001

Tabell 21 Tester av forskjell mellom andel oppklart for IKT-saker og ikke-IKT-saker innen sedelighetsområdet

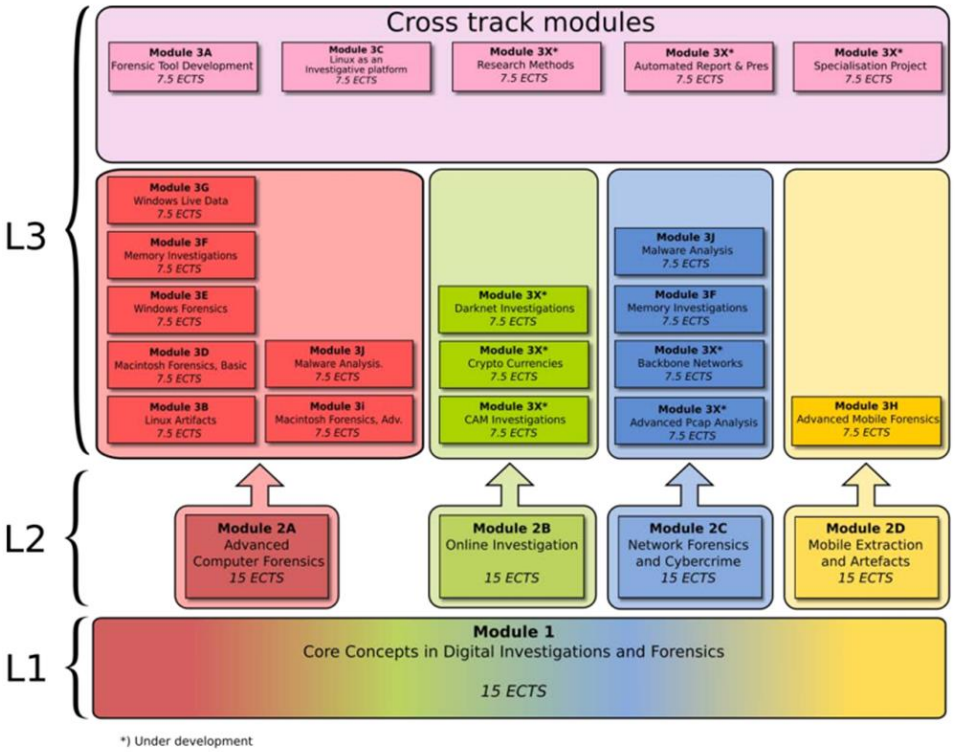
Statistikkgruppe	Differanse	t	N
Framvis/still av seks. overgr./seksualiserer barn	0.174***	(6.96)	1190
Seksuelt krenkende atferd	-0.0346	(-0.77)	712
Seksuelt krenkende atferd mv. barn u. 16 år	-0.0282	(-0.72)	538

Kilde: Resultat fra test av forskjell mellom andeler i to uavhengige grupper («prtest» i Stata).
^ Differanse: Andel oppklart for ikke-IKT-saker minus andel oppklart for IKT-saker
* p < 0.05, ** p < 0.01, *** p < 0.001

Vedlegg 6: Utdanning innen digitalt politiarbeid ved Politihøgskolen

Figuren nedenfor gir en oversikt over ulike kurs ved Politihøgskolen som er tilgjengelige for dataetterforskere som ønsker videreutdanning. Ifølge fagforvaltningsrapporten om datatekniske undersøkelser og internettrelatert etterforskning dekker studiene ulike fagretninger innen digitalt politiarbeid, fra tradisjonell «Digital Forensics» til «Internettetterforskning», «Cybercrime» og avansert mobil-telefon analyse/undersøkelse. Rapporten viser til at i henhold til «Nasjonale rolledefinisjoner med kompetansekrav - etterforskningsfeltet» er det kun NCFI Module 1, eller tilsvarende, som er satt som krav til dataetterforsker.[300]

Figur 18 Ny modell for videreutdanning av data etterforskere ved Politihøgskolen fra 2019



Kilde: Politidirektoratet, 2019 *Faggrupperapport om datatekniske undersøkelser og internettrelatert etterforskning*.
Forklaring: L1, L2 og L3 skisserer nivåene i utdanningen og tilsvarer det som tidligere ble kalt Module1, Module 2 og Module 3. L1 har 15 studiepoeng, L2 har 4 spor hver på 15 studiepoeng, til sammen 60 studiepoeng, L3 har per september 2019 foreløpig 9 godkjente studieplaner på til sammen 67,5 studiepoeng.

[300] Politidirektoratet (2019) *Fagforvaltning statusrapport – Status fagomr de datatekniske undersøkelser og internettrelatert etterforskning*, 9. september 2019.

Vedlegg 7: Påtaleavgjørelser som medfører oppklaring, ikke oppklaring og saker som trekkes ut før oppklaringsprosent beregnes

Oppklaring av sakene håndterer skjer ved påtaleavgjørelse. I hovedsak skilles det mellom oppklarte saker og ikke oppklarte saker. I tillegg er det en gruppe saker som ikke inngår i beregningen av oppklaringsprosent. Hvilke påtaleavgjørelser som inngår i de ulike kategoriene av oppklaring, ikke oppklaring og saker som trekkes ut før oppklaring beregnes, er gjengitt i tabellen nedenfor.

Oppklarte saker – positive påtaleavgjørelser

Påtaleavgjørelser som regnes som positive:

- siktelse med forslag til tilståelsesdom
- tiltalebeslutning
- forelegg
- overføring til konfliktråd
- påtaleunnlatelse

Mange av de positive påtaleavgjørelsene forekommer innenfor det som kalles kontrollavdekket kriminalitet. Det vil saker som avdekkes i det lovbruddet begås, og hvor politiet avdekker gjerningsperson og lovbrudd fysisk. Dette er derfor også saker som normalt sett er enklere å oppklare. Positive påtaleavgjørelser forekommer i stor grad innen kriminalitetstyper hvor kontrollavdekkete lovbrudd forekommer hyppigst – trafikk, narkotika, annen (ordensforstyrrelser), vinning og vold.

Oppklarte saker – negative påtaleavgjørelser

Påtaleavgjørelser som regnes som negative, er i hovedsak henleggelser:

- fordi mistenkte var under 15 år
- fordi mistenkte var under 15 år og saken oversendes barnevernet
- fordi allmenne hensyn ikke krever påtale mot anmeldte
- fordi anmeldtes forhold ikke er straffbart
- fordi foretaksstraff ikke anses hensiktsmessig
- fordi gyldig påtalebegjæring mangler
- fordi påtalebegjæringen er for sent framsatt
- fordi påtalebegjæringen er trukket tilbake
- på grunn av foreldelse
- på grunn av jevnbyrdighet i alder og utvikling
- på grunn av mistenktes død
- av andre lovbestemte grunner
- åpenbar grunnløs sak
- strl. (1902) § 228 tredje ledd / strl. (2005) § 271 andre ledd
- strpl. § 62a unnlatt påtale, ikke allmenne hensyn
- intet straffbart forhold bevist
- tvil om gjerningsmannens tilregnelighet
- kjennelse på rettergangsbot
- sak påtaleavgjort

Det er betydelig færre saker i denne kategorien. Her er det også i stor grad kontrollavdekket kriminalitet som dominerer, som trafikklovbrudd, vold, vinning og trafikk.

Ikke oppklarte saker

Påtaleavgjorte saker som regnes som ikke oppklarte er henleggelser som følge av

- manglende opplysninger om gjerningsmannen
- bevisets stilling
- foreldelse
- mangel på bevis
- manglende saksbehandlingskapasitet

To tredjedeler av de ikke oppklarte sakene er henleggelser som følge av manglende opplysninger om gjerningsperson. Dette forekommer i høy grad innen vinning hvor sykkeltyverier er det hyppigst forekommende lovbruddet. Andre kriminalitetstyper som har en høy andel av ikke oppklarte saker, er økonomi (bedragerier) og skadeverk.

Saker som trekkes ut før oppklaringsprosenten beregnes

Påtaleavgjorte saker som trekkes ut før oppklaringsprosenten beregnes, er saker som er

- avgjort utenfor straffesak
- avvist hos Spesialenheten – påtaleinstruksen § 34-5
- avvist hos ØKOKRIM – påtaleinstruksen § 34-5
- henlagt ikke rimelig grunn til å undersøke om det foreligger straffbart forhold
- henlagt ikke rimelig grunn til å undersøke om det er et straffbart forhold
- henlagt fordi allmenne hensyn ikke krever påtale henlagt fordi forholdet ikke er straffbart
- henlagt fordi forholdet ikke er straffbart
- henlagt fordi gyldig påtalebegjæring mangler
- henlagt fordi påtalebegjæringen er trukket tilbake
- henlagt som åpenbart grunnløs
- henlagt strpl. § 62a unnlatt påtale, ikke allmenne hensyn
- henlagt, intet straffbart forhold bevist
- sendt utlandet som rette vedkommende
- stillet i bero etter strpl. § 250
- stillet i bero etter strpl. § 251
- utenlands dom

Henleggelser som følge av at saken regnes som ikke rimelige å undersøke, er kategorien som forekommer hyppigst blant de påtaleavgjorte sakene som trekkes ut før oppklaringsprosenten beregnes. I tillegg er det en stor andel av undersøkelsessakene som avgjøres utenfor straffesak.

16 Referanseliste

Lover og forskrifter

- *Lov om politiet (politiloven) av 1. oktober 1995*
- *Lov om straff (straffeloven) av 1. oktober 2015*
- *Lov om rettergangsmåten i straffesaker (straffeprosessloven) av 1. oktober 1986*
- *Forskrift om ordningen av påtalemyndigheten (påtaleinstruksen) av 1. januar 1986*

Internasjonale avtaler

- *Europarådets konvensjon om datakriminalitet* av 23. november 2011, trådte i kraft i Norge 1. oktober 2006.

Stortingsdokumenter

Innstillinger til Stortinget

- Innst. 326 S (2016–2017), jf. Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*
- Innst. 306 S (2014–2015), jf. Prop. 61 LS (2014−2015) *Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen)*
- Innst. 187 S (2017–2018), jf. Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar*
- Innst. 6 S (2018−2019), jf. Prop. 1 S (2018–2019) *Justis- og beredskapsdepartementet*
- Innst. 6 S (2017–2018), jf. Prop. 1 S (2017–2018) *Justis- og beredskapsdepartementet*
- Innst. O. nr. 53 (2004–2005), jf. Ot.prp.nr. 40 (2004–2005)
- Innst. 199 S (2015−2016), jf. Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom*

Proposisjoner til Stortinget

- Ot.prp. nr. 40 (2004–2005) *Om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet)*
- Prop. 61 LS (2014–2015) *Endringer i politiloven mv (trygghet i hverdagen – nærpolitireformen)*
- Prop. 1 S (2017–2018) Justis- og beredskapsdepartementet
- Prop. 1 S (2018–2019) *Justis- og beredskapsdepartementet*.
- Prop. 1 S (2019–2020) *Justis- og beredskapsdepartementet*

Meldinger til Stortinget

- Meld. St. 29 (2019–2020) *Politimeldingen – et politi for fremtiden*
- Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*
- Meld. St. 38 (2016–2017) *IKT-sikkerhet – Et felles ansvar*
- Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom*
- Meld. St. 7 (2010–2011) *Kampen mot organisert kriminalitet*.

Reglement og rutiner

- *Bevilgningsreglementet* av 26. mai 2005
- *Reglement for økonomistyring i staten* (økonomireglementet) (kgl.res. 2003).

Instrukser

- Oslo politidistrikt (2017) *Straffesaksbehandlingen ved Oslo politidistrikt (straffesaksinstruksen)*, datert 1. mai 2017.
- Riksadvokaten og Politidirektoratet (2017) *Nasjonal straffesaksinstruks*, 5. desember 2017
- Riksadvokaten og Politidirektoratet (2020) *Nasjonal straffesaksinstruks*, 8. mai 2020.
- Justis- og beredskapsdepartementet (2018) *Hovedinstruks til politidirektøren*, fastsatt av Justis- og beredskapsdepartementet, 16. januar 2018.

- *Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen)*, 1. september 2017.

Rundskriv

- Riksadvokaten (2018) *Kvalitetskrav til straffesaksbehandlingen i politiet og ved statsadvokatembetene mv. (kvalitetsrundskrivet),* Rundskriv 3/2018.
- Riksadvokaten (2019) *Mål- og prioriteringer for straffesaksbehandlingen i 2019 – politiet og statsadvokatene,* rundskriv 1/2019.
- Riksadvokaten (2020) *Mål og prioriteringer for straffesaksbehandlingen i 2020*, rundskriv 1/2020, 15. februar 2020.

Strategier

- Politidirektoratet (2015) *Overordnet nasjonal strategi for bekjempelse av datakriminalitet – Datakrimstrategien.* Utredning fra gruppe oppnevnt av Politidirektoratet etter oppdrag fra Justis- og beredskapsdepartementet i brev av 1. november 2013. Avgitt til Justis- og beredskapsdepartementet 12. mai 2015.
- Justis- og beredskapsdepartementet (2015) *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, lansert 26. juni 2015.
- Politidirektoratet (2018) *Innspill til revisjon – strategi for bekjempelse av IKT-kriminalitet*. 15. januar 2018.

Styringsdokumenter

- Justis- og beredskapsdepartementet (2020) *Tildelingsbrev 2020 Politidirektoratet*.
- Justis- og beredskapsdepartementet (2019) *Referat fra styringsdialogmøte mellom Justis- og beredskapsdepartementet og Politidirektoratet 25. oktober 2019*, referat fra styringsdialogmøte mellom Justis- og beredskapsdepartementet og Politidirektoratet 25. oktober 2019.
- Politidirektoratet (2019) *Direktoratets rapportering på Justis- og beredskapsdepartementets IKT-kriminalitetsstrategi i forbindelse med årsrapporteringen for 2019*. Rapportering 3. tertial, R10: Rapportere på strategier og handlingsplaner.
- Oslo politidistrikt (2019) *Regler om saksansvar ("trekkregler") i Oslo politidistrikt*, sist justert 9. desember 2019.
- Politidirektoratet (2018) *Oppdragsbrev 1 – NC3, brev til Kripos* 13. juni 2018.
- Politidirektoratet (2017) *Rammer og retningslinjer for etablering av nye politidistrikter*, Versjon 1.2, 16. juni 2017.
- Politidirektoratet (2017) *Trusler og utfordringer innen IKT-kriminalitet.*

Offentlige utredninger (NOU)

- NOU 2017: 5 *En påtalemyndighet for fremtiden – påtaleanalysen*
- NOU 2017:11 *Bedre bistand. Bedre beredskap*
- NOU 2015:13 Digital sårbarhet – sikkert samfunn

Inspeksjonsrapporter

- Hordaland, Sogn og Fjordane statsadvokatembeter (2019) *Rapport etter tilsyn med Vest politidistrikt sin innsats mot vold og sedelighet/voldtekt*, rapport datert 30. oktober 2019.
- Det nasjonale statsadvokatembetet (2018) *Inspeksjon av seksjon for datakriminalitet*, brev til sjef Kripos datert 28. september 2018.
- Oslo statsadvokatembeter (2018) *Rapport etter inspeksjon/tilsyn av spesialseksjon – påtale og felles enhet for etterretning og etterforsking – Øst politidistrikt*, brev til Øst politidistrikt, 14. mai 2018.

Rapporter, fagartikler

- DNB (2020) *Trusselvurdering 2020*, offentliggjort 13. mai 2020.
- Eurojust og Europol (2019) *Common challenges in combating cybercrime – As identified by Eurojust and Europol*, Joint report, June 2019.
- Europol (2019) Eurojust and Europol, 2019 *Common challenges in combating cybercrime, as identified by Eurojust and Europol*, June 2019.
- Europol, 2019 *INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019*, 9. oktober 2019.
- Finanstilsynet (2020) *Risiko- og sårbarhetsanalyse 2020*.
- KANTAR TNS (2020) *Politiets innbyggerundersøkelse 2019.*
- Kripos, 2019 *Seksuell utnyttelse av barn og unge over internett*, rapport fra Kripos, mars 2019.
- Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES), 2019 *Bedrageri mot næringslivet*. Utgitt i februar 2019.
- Justis- og beredskapsdepartementet (2019) *Rapport fra arbeidsgruppe som har sett på saksflyt i saker som gjelder overgrep mot barn, oppnevnt av Justis- og beredskapsdepartementet 26. juli 2018*, rapport publisert 13. mars 2019.
- NOVA (2018) *Nettovergrep mot barn i Norge 2015-2017*, NOVA-rapport 10/18.
- NSM (2019) *Årsrapport 2018*.
- NSM (2019) *Helhetlig digitalt risikobilde 2019*.
- Næringslivets sikkerhetsråd (2018) *Mørketallsundersøkelsen*.
- Næringslivets sikkerhetsråd (2019) *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2019*. Gjennomført av Opinion AS for Næringslivets Sikkerhetsråd
- Olaussen, Leif Petter (2004) *Oppklaringsprosenten - en indikator på hva?* Lov og Rett 07-08, 2004 (Volum 43).
- Oslo politidistrikt (2018) *Trender i kriminalitet 2018−2021. Digitale og Globale utfordringer*.
- Oslo politidistrikt (2018) *Digitalt politiarbeid – Anbefaling.* Rapport til Politidirektoratet datert 23. januar 2018.
- Oslo politidistrikt (2018) *Digitalt politiarbeid – Oppsummering etter høringsrunde*.
- Oslo politidistrikt (2018) *Datakriminalitet rettet mot næringslivet*, internt notat datert 9. april 2018.
- Oslo politidistrikt (2017) *Intern rapport: Foreløpig rapport fra pilotprosjekt om IKT og internett i politiarbeidet.*
- Politidirektoratet (2020) *Strasak-rapporten 2019 - Anmeldt kriminalitet og politiets straffesaksbehandling*, rapport utgitt i februar 2019.
- Politidirektoratet (2019) *STRASAK-rapporten 2018 - Anmeldt kriminalitet og politiets straffesaksbehandling*, rapport utgitt 28. februar 2020.
- Politidirektoratet (2019) *Ressursanalyse for 2019 – utgifter og bemanning i politiet*.
- Politidirektoratet (2019) *Kapasitetsvurdering av etterforskningsområdet*, rapport utarbeidet av Accenture på oppdrag fra Politidirektoratet.
- Politidirektoratet (2019) *Status fagområde Operativ kriminalanalyse*, Fagforvaltning statusrapport, 28. august 2019.
- Politidirektoratet (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning*, Fagforvaltning statusrapport, 9. september 2019.
- Politidirektoratet (2018) *Nasjonale rollebeskrivelser med kompetansekrav – etterforskningsfeltet*. Versjon 0,7.
- Politidirektoratet (2017) *Trusler og utfordringer innen IKT-kriminalitet*.
- Politidirektoratet (2017) *Politi- og lensmannsetatens kapasitets- og kompetansebehov de kommende ti-årene*, 15. desember 2017.
- Politidirektoratet (2016) *Handlingsplan for løft av etterforskningsfeltet*, rapport fra Politidirektoratet og Riksadvokaten 31. mai 2016.
- Politidirektoratet (2012) *Politiet i det digitale samfunnet: En arbeidsgrupperapport om elektroniske spor, ikt-kriminalitet og politiarbeid på internett.*
- Politidirektoratet (2008) *Politiet mot 2020 – Bemannings- og kompetansebehov i politiet*.
- Politiet (2020) *STRASAK-rapporten 2019: Anmeldt kriminalitet og politiets straffesaksbehandling*
- Politiet (2019) *STRASAK-rapporten 2018: Anmeldt kriminalitet og politiets straffesaksbehandling*. 15. februar 2019.
- Politihøgskolen (2019) *Programplan Bachelor – Politiutdanning 2020-2023*. Fastsatt av Justis- og beredskapsdepartementet 11. juli 2018.
- Symantec 2019 *Internet Security Threat Report*, Volume 24, February 2019

- Sør-Øst politidistrikt (2018) *Kriminalitet i og mot næringslivet – Trusler og trender*, rapport utarbeidet av to medarbeidere i Sør-Øst politidistrikt.

Brev og notater

- Politidirektoratet (2019) *Næringslivskontaktenes rolle - forebygging av IKT-kriminalitet*, notat til Riksrevisjonen, 1. oktober 2019.
- Riksadvokaten (2019) *Etterforsknings- og påtalepliktens grenser i omfattende nettovergrepssaker - Et nytt straffebud om serieovergrep - mulige lovendringer*, brev til Lovavdelingen, Justis- og beredskapsdepartementet, 10. september 2019.
- Politidirektoratet (2018) *Etablering av statistikk og innføring av tvungen modus for IKT-kriminalitet*, brev til politidistrikt og særorgan, 8. januar 2018.
- Riksadvokaten (2015) *Plan for å styrke den digitale kompetansen i påtalemyndigheten*, brev til Justis- og beredskapsdepartementet, 24. september 2015.
- Riksadvokaten (2014) *Forslag til endringer i reglene om påtalekompetanse ved ikrafttredelse av ny straffelov*.

Internettsider og -artikler

- Aftenposten (2019) *Norsk politi mener å ha avslørt storsvindlere fra Nigeria*, artikkel datert 28. juli 2019.
- Aftenposten (2012) *Dømt for nettangrep mot DNB, bloggtjenester og PST*, artikkel publisert 14.12.2013 [24.3.2020].
- Justitsministeriet i Danmark (2020) *Justitsminister vil oprette et uafhængigt tilsyn med bevismidler*, pressemelding 22. februar 2020.
- Politiet (2019) *Nasjonalt cyberkrimsenter (NC3)*, artikkel aksessert 29. juni 2020.
- Politiforum (2017) *Norsk politi sakker akterut på nett*, artikkel i Politiforum 26. juni 2017.
- SSB (2019) *Flere personer utsatt for bedrageri*, artikkel 2. september 2019.
- VG (2017) *Historien om «Operasjon Jackpot» – politi spilte direktør og rundlurte svindlere*, artikkel datert 20. mars 2017.
- ØKOKRIM (2018) *Bedrageri*, artikkel oppdatert 1.november 2018.
- Norsk senter for informasjonssikring (2020) *Fersk undersøkelse: 100 000 har vært utsatt for ID-tyveri*, 09. mars.2020.
- NRK (2013) *Flere pågrepet for overgrepsbilder*, artikkel publisert 5.12.2013.
- Bergens tidende, (2016) *Nå må de skille fantasier fra ekte overgrep*, artikkel publisert 25.11.2016.