STORTINGET

Innst. 360 S

(2020–2021)

Innstilling til Stortinget
fra kontroll- og konstitusjonskomiteen

Dokument 3:5 (2020–2021)

Innstilling fra kontroll- og konstitusjonskomiteen om Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT

Til Stortinget

1. Sammendrag

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.

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 Riksrevisjonens dokument.

1.1 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.

1.2 Riksrevisjonens merknader

1.2.1 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 holder 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 pst. 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.

1.2.1.1 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 etterforskingsskritt 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.

1.2.1.2 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 pst. (3 392 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. For politi-

utdannede 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.

1.2.1.3 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. 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.

1.2.1.3.1 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:

- 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.
- 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.

1.2.1.3.2 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.

1.2.1.3.3 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 av 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.

1.2.1.4 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. 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.

1.2.1.5 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.

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, 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.

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. 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.

1.2.2 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. 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 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.

1.2.3 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. Figur 1 i rapporten viser tips Kripos mottok om internettrelaterte seksuelle overgrep i perioden 2015–2020.

Av den totale mengden tips Kripos mottar, velges det ut et antall tips for videre oppfølging (gule søyler). Dette er tips der det foreligger mistanke om straffbare forhold. Figur 1 i rapporten viser at Kripos opparbeider seg stadig økende restanser (grønne søyler) blant sakene som velges ut for videre oppfølging. Mer enn 40 pst. 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 pst. av alle seksuallovbrudd i 2018 og 63 pst. 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 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. 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 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.

1.2.4 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. 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.

1.2.5 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 identifisert anmeldt IKT-kriminalitet i 2018. Figur 2 i rapporten viser andel IKT-kriminalitet innenfor ulike sakskategorier, basert på ulike metoder for registrering.

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, 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 pst.), sedelighet (24 pst.) og kategorien annen (9 pst.). 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 po-

litiet 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.

1.2.6 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.

Politiets primæroppgave i henhold til politiloven § 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 ut over 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.

1.3 Riksrevisjonens anbefalinger

Riksrevisjonen anbefaler Justis- og beredskapsdepartementet

- å tydeliggjøre rutiner og ansvar for etterforskning av IKT-kriminalitet
- å 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 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

1.4 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 fore-

bygge, 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 etterforskning 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 Budapestkonvensjonen 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 å 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.

2. Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, lederen Dag Terje Andersen, Eva Kristin Hansen og Magne Rommetveit, fra

Høyre, Svein Harberg og Bente Stein Mathisen, fra Fremskrittspartiet, Solveig Horne, fra Senterpartiet, Nils T. Bjørke, fra Sosialistisk Venstreparti, Freddy André Øvstegård, fra Venstre, Terje Breivik, og uavhengig representant Ulf Isak Leirstein, viser til Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT, Dokument 3:5 (2020–2021).

Politiets viktigste oppgaver er å sørge for lov og orden i samfunnet ved å sørge for rettssikkerhet, trygghet og alminnelig velferd for borgerne. Politiet skal forebygge og forhindre straffbare handlinger og avdekke, stanse og forfølge lovbrudd og straffbare forhold.

Komiteen viser til at økende digitalisering av samfunnet også øker kriminaliteten som skjer på digitale flater. Kort fortalt så flytter kriminaliteten seg «fra gata til data». Mens vi ser en nedgang av de tradisjonelle kriminalitetstypene, har det skjedd en eksplosiv økning av kriminalitet på IKT-området. Særlig gjelder dette nettovergrep mot barn og unge, datainnbrudd og nettbedragerier.

Målet med undersøkelsen har vært å vurdere om politi- og påtalemyndigheten har oversikt over, etterforsker og oppklarer datakriminalitet i samsvar med føringer gitt av Stortinget. Riksrevisjonen har sett på tre utvalgte områder: internettrelaterte seksuelle overgrep, økonomisk datakriminalitet (bedragerier og identitetskrenkelser) og «ren» datakriminalitet (datainnbrudd og uberettiget befatning med tilgangsdata).

Riksrevisjonens undersøkelse viser at politiets evne til å avdekke og oppklare datakriminalitet har klare svakheter, som samlet sett er alvorlige. Politiet mangler for det første kompetanse på etterforskning av datakriminalitet. I tillegg holder ikke politiet tritt med utfordringene. En stadig større andel av kriminaliteten utføres på nett, uten at politiet har klart å holde følge med utviklingen. Dette til tross for at politiet har vært budsjettvinnere de siste årene med en økning på cirka 10 mrd. kroner siden 2010 og over 3 300 årsverk siden 2012. For det andre fører svakheter ved støttesystemene til ineffektiv ressursbruk og manglende samordning mellom distrikter. I tillegg er det utfordringer ved internasjonalt samarbeid. Samlet sett bidrar dette til lav oppklaring av datakriminalitet.

Komiteen viser til at politiet over flere år har prioritert etterforskning og oppklaring av internettrelaterte seksuelle overgrep, men at politiets etterforskningskapasitet utfordres av store omfattende nettovergrepssaker med mange fornærmede. Komiteen finner det alarmerende at politiet får en økende mengde tips, som det ikke finnes kapasitet til å gjennomgå. Komiteen viser til at konsekvensene for barn, unge, privatpersoner og virksomheter som utsettes for datakriminalitet, kan være dramatiske.

Komiteen viser til at det er bred politisk enighet om at vold i nære relasjoner og seksuelle overgrep mot barn skal ha høyest prioritet. Komiteen er bekymret over funnene Riksrevisjonen har gjort hva gjelder koordinering og styring av arbeid mot nettovergrep. Som Riksrevisjonen skriver, bruker enheter for digitalt politiarbeid (DPA-enhetene) en stor andel av tiden til å gjennomgå denne typen beslag. Komiteen vil vise til at Kripos i 2016/2017 foreslo en nasjonal løsning for håndtering av overgrepsmateriale som fortsatt ikke er iverksatt. Norsk politi har derfor ikke en enhetlig måte å behandle internettrelaterte seksuelle overgrep som omfatter bildedeling, -distribusjon og -produksjon. Komiteen merker seg at digitale beslag gjennomgås i hvert enkelt distrikt uten særlig samordning, og at 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. Komiteen vil vise til at Riksrevisjonen har konkludert med at politiets arbeid blir mindre effektivt uten en nasjonal løsning på dette.

Komiteen er bekymret for at lovbrytere som opererer på tvers av landegrensene, i praksis slipper unna. Riksrevisjonen har uttalt følgende:

«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.»

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, er enige i denne kritikken.

Komiteen viser til at som følge av kompetanse- og kapasitetsproblemer har politiet i liten grad prioritert etterforskning og oppklaring av ren datakriminalitet som datainnbrudd og løsepengevirus. Det samme gjelder økonomisk datakriminalitet. En sannsynlig årsak til dette er at flertallet av sakene anses som mindre alvorlige. Dette gjelder særlig bedragerier og ID-krenkelser.

Komiteen fremhever at det over mange år har vært kjent at basiskompetansen i politidistriktene har vært svak innenfor området IKT-kriminalitet. Komiteen er overrasket over hvor store mangler som er avdekket.

Komiteen vil vise til at 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. Riks-

revisjonen skriver at dette punktet ennå ikke har ført til konkrete tiltak, noe komiteen påpeker må følges opp.

Komiteen understreker at etterforskningen av IKT-kriminalitetssakene i all hovedsak må skje i distriktene. Riksrevisjonen fremholder i rapporten at politiet ifølge statsbudsjettet har fått tilført ekstra ressurser i forbindelse med politireformen, og at bemanningen skal ha økt med over 20 pst. Samtidig stadfester de at dette i liten grad er utnyttet til å styrke politiets evne til å håndtere IKT-kriminalitet.

Komiteen viser til at samlet sett mener Riksrevisjonen at svakhetene i politiets evne til å avdekke og oppklare datakriminalitet er alvorlige. Komiteen deler denne oppfatningen.

Konsekvensen av den manglende prioriteringen er at alvorlig kriminalitet ikke etterforskes og oppklares, og at norske borgere og virksomheter mister tillit til politiet og lar være å anmelde lovbrudd.

Komiteen viser til at et av målene med politireformen er å vri ressursbruken over mot etterforskning og straffeforfølging av vinningskriminalitet. Nesten all kriminalitet har i dag et digitalt element i seg. Ofte fordi svindel eller overgrep skjer på nett, andre ganger fordi målet i seg selv er å angripe en datamaskin eller et nettverk. Selv tradisjonell kriminalitet har ofte digitale spor som kan følges, for eksempel telefonbruk, bompasseringer mv.

I tråd med digitaliseringen av økonomien og samfunnslivet øker insentivene for potensielle lovbrytere til å vri vinningskriminalitet over til digitale plattformer. På samme måte som formålet med tradisjonell vinningskriminalitet er å skaffe seg ulovlige inntekter, er også formålet med digital vinningskriminalitet å skaffe seg ulovlige inntekter.

Mange av sakene er også mer omfattende og kompliserte enn før, hvor én gjerningsperson kan være ansvarlig for mange hundre ofre for nettovergrep, svindel og andre former for digital kriminalitet. Videre befinner ofre og gjerningsperson seg gjerne ulike steder i landet, om ikke også i ulike land. Det gjør etterforskningen mer arbeidskrevende enn før, og vi må sikre oss at vi har et politi med kapasitet og kompetanse til å håndtere denne utviklingen.

Komiteen vil vise til gjentatte bekymringer rundt kapasiteten generelt i våre politidistrikter, samt at etterforskningsløftet henger etter. Komiteen merker seg videre at Riksrevisjonen mener at Politidirektoratet burde har sørget for en nasjonal samordning av innkjøp, drift og administrasjon av utstyr og programvare som brukes av DPA-enhetene. Rapporten viser til at bedre støttesystemer kunne gjort samordningen mellom politidistriktene enklere og effektivisert politiets arbeid. Komiteen stiller seg undrende til at dette ikke er gjennomført.

Komiteen viser til at Riksrevisjonen mener det er sterkt kritikkverdig at det ikke er tatt høyde for denne utviklingen i gjennomføringen av politireformen.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, viser til statsrådens svar til Riksrevisjonens rapport, der statsråden minner om at politiet har gjennomført en omfattende reform i den perioden Riksrevisjonen har undersøkt (2016–2019). Arbeidet med reformen har vært ressurskrevende, men har ifølge statsråden hevet kvaliteten på politiets arbeid. Flertallet viser også til statsrådens svar om at politiet daglig står i en krevende situasjon hvor flere prioriterte saksområder skal løses med begrensede ressurser.

Flertallet viser til Innst. 248 S (2020–2021), der flertallet i justiskomiteen viser til at de gjentatte ganger har advart mot å gjennomføre en stor reform uten å sørge for tilstrekkelig finansiering. Forliket om «nærpolitireformen» slo fast at det ikke skulle bli en sparereform, men at den skulle finansieres. Flertallet reagerer derfor på at regjeringen har som foreløpig svar på den alvorlige rapporten at arbeidet med reformen har vært svært ressurskrevende. Riksrevisjonens funn, konklusjoner og anbefalinger viser at løftet om finansiering av nærpolitireformen ikke er fulgt opp. De funn som fremkommer i Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT (Dokument 3:5 (2020–2021)), står i sterk kontrast til regjeringens budskap om at politiets innsats mot IKT-kriminalitet er betydelig styrket gjennom nærpolitireformen. Flertallet understreker at det er statsrådens ansvar å vurdere risikoen for politiets oppgaveløsning ved gjennomføring av reformer.

Flertallet merker seg at Riksrevisjonen konkluderer med at datakriminalitet i liten grad har vært prioritert av Politidirektoratet og Justis- og beredskapsdepartementet, og at det ifølge Riksrevisjonen er lite som tyder på IKT-kriminalitet har blitt prioritert, ut over at politidistriktene og Kripos har brukt betydelige ressurser på seksuelle overgrep på nett.

Flertallet understreker at 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. Flertallet støtter Riksrevisjonens vurdering av at når departementet har vært kjent med utfordringene, og Politidirektoratet ikke har prioritert området, burde Justis- og beredskapsdepartementet hatt en tettere og tydeligere styring. I lys av at Politidirektoratets trusselvurdering av 18. mars 2021 fremhever stor fare for datainnbrudd, stiller flertallet spørsmål ved hvorfor IKT-kriminalitet i liten grad har vært prioritert tidligere.

Flertallet vil særlig fremheve Riksrevisjonens påpekning av at 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 regjeringen. Flertallet understreker at den samlede kritikken i rapporten er så alvorlig at politiets evne til å avdekke og oppklare IKT-kriminalitet bør inngå som en del av Justis- og beredskapsministerens redegjørelse for hvordan politiet skal fylle sitt samfunnsoppdrag i fremtiden.

Komiteen støtter Riksrevisjonens anbefalinger til Justis- og beredskapsdepartementet:

- tydeliggjøre rutiner og ansvar for etterforskning av datakriminalitet
- bedre kapasiteten på etterforskning av datakriminalitet og sikring av elektroniske spor
- styrke den nasjonale samordningen på datakrim mellom involverte politidistrikt og særorgan (Kripos og Økokrim)
- styrke kunnskapsgrunnlaget om datakriminalitet og framtidige utfordringer
- styrke etterforskningskompetansen på området
- samordne innkjøp og administrasjon av programvare og utstyr som brukes av enheter for digitalt politiarbeid og særorgan
- utvikle sentralt lagringsnett slik at det i større grad kan brukes for å analysere innsamlet bevismateriale og støtte etterforskningen

Komiteen har merket seg at Politidirektoratet (POD) har satt i gang flere tiltak i politiet som vil bidra til å følge opp Riksrevisjonens anbefalinger, og at statsråden vil følge opp dette arbeidet i den løpende styringsdialogen med POD. Komiteen har også merket seg at statsråden vil gå i dialog med Riksadvokaten om behov for tiltak hos Den høyere påtalemyndighet.

Komiteen forventer/legger til grunn at politiets innsats mot datakriminalitet blir betydelig styrket i årene som kommer. Datakriminalitet er en økende trussel for norske borgere og virksomheter. Da må man kunne forvente at nasjonale politimyndigheter har kapasitet til å møte utviklingen innenfor hele spekteret av datakriminalitet, og ikke bare når det gjelder seksuelle overgrep på nett.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet understreker at de samlede funnene i Riksrevisjonens rapport avdekker så grunnleggende mangler i politiets evne til å løse sitt samfunnsoppdrag at oppfølgingen vil kreve mer fra statsråden enn å følge opp arbeidet i den løpende styringsdialogen med Politidirektoratet. Disse medlemmer viser til at Boston Consulting Group (BCG) på oppdrag fra Justis- og beredskapsdepartementet og Finansdepartementet har gjennomført en områdegjennomgang av politi- og lensmannsetaten i desember 2020. Gjennomgangen peker på at styringen er preget av detaljorientering og mangel på god styringsinformasjon, og at bred oppgaveportefølje vanskeliggjør effektiv ressursutnyttelse og bidrar til økt detaljfokus i styringen. Områdegjennomgangen viser at Justis- og beredskapsdepartementet i for liten grad utøver strategisk styring med vekt på forutsigbare rammebetingelser og langsiktige planer. BCGs vurdering er at styringen i langt større grad kan bidra til at etatens ressurser brukes best mulig for å løse oppgavene Gjennomgangen anbefaler at politisk styring må dreies mer i retning av mål for kriminalitetsbekjempelse og prioriterte kriminalitetsområder, og at Justis- og beredskapsdepartementet må bidra til en dreining mot strategisk styring i samspillet med Politidirektoratet. Disse medlemmer ser derfor behov for at statsråden vurderer formen på departementets styring av Politidirektoratet når Riksrevisjonens anbefalinger skal følges opp.

3. Komiteens tilråding

Komiteen har for øvrig ingen merknader, viser til rapporten og råder Stortinget til å gjøre følgende

vedtak:

Dokument 3:5 (2020–2021) – Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT – vedlegges protokollen.

Oslo, i kontroll- og konstitusjonskomiteen, den 27. april 2021

Dag Terje Andersen
leder

Solveig Horne
ordfører

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets grafiske seksjon