DEN HØYERE
PÅTALEMYNDIGHET

CYBERUNDERSØKELSE 2024

En gjennomgang av avgjorte saker i perioden september 2023 – august 2024.

Innholdsfortegnelse

Forord

Riksadvokaten presenterer med dette rapporten fra cyberundersøkelsen – tilsyn av politiets etterforskning av cyberrettet kriminalitet.

Statsadvokatene har et lovpålagt ansvar for å føre tilsyn med straffesaksbehandlingen i politiet, og tilsynsarbeidet er en sentral del av Den høyere påtalemyndighets fagledelse. Virksomheten er viktig for å identifisere og synliggjøre avvik der det foreligger mangler ved politiets innsats. Uten slik synliggjøring, vil vi ikke kunne legge grunnlag for forbedringstiltak som fremmer kvalitet og målrettet oppfølging av straffesaksarbeidet.

Rapporten representerer noe nytt i vår tilsynspraksis. Undersøkelsen er i hovedsak gjennomført av et begrenset antall ressurser ved Riksadvokatembetet og Det nasjonale statsadvokatembetet. Undersøkelsen har i liten grad medført ressursuttak fra politidistriktene. Arbeidsformen viser at det kan gjennomføres tilsyn som ikke er særlig omfattende, men som likevel gir god og pålitelig informasjon. Riksadvokaten har videre hatt god støtte av spesialistmiljøet ved Kripos, som har bidratt med dyktige medarbeidere. Deres særskilte kompetanse og innsikt på området har vært avgjørende for kvaliteten i gjennomgangen og vurderingene, og riksadvokaten benytter anledningen til å takke Kripos for bistanden.

Cyberrettet og cyberstøttet kriminalitet er et område med betydelig alvor og potensielt stor samfunnsrisiko. Det er derfor avgjørende at førstelinjen i politiet har tilstrekkelig innsikt og kompetanse til å identifisere saker som krever rask og målrettet oppfølging. Undersøkelsen viser at det er behov for kompetanseheving for å møte dette behovet.

Undersøkelsen synliggjør også andre forhold som i sum viser at politiets innsats på området ikke er god nok. Når anmeldelsestallene er lave og om lag 97 prosent av sakene henlegges, gir undersøkelsen et tydelig grunnlag for tiltak både på kort og lang sikt.

Gjennomgangen viser også at tradisjonelle indikatorer som kort saksbehandlingstid og oppklaringsprosent i begrenset grad sier noe om måloppnåelsen på feltet. Dette understreker behovet for en resultatoppfølging, både lokalt og nasjonalt, som gir et mer presist bilde av hvordan vi lykkes i kriminalitetsbekjempelsen. Et arbeid mellom riksadvokaten og Politidirektoratet for å utvikle treffende styringsindikatorer for oppfølgingen av resultatene på straffesaksfeltet, herunder cyberkriminalitet, er allerede igangsatt. Sakene i utvalget gjelder forhold frem til medio 2024. Det er grunn til å anta at politidistriktene i tiden frem til nå har lagt ned en innsats for å forbedre resultatene på området. En er også kjent med at Politidirektoratet over tid har rettet oppmerksomhet mot cyberkriminalitet, og har iverksatt flere tiltak. Rapporten, funnene og anbefalingene må leses i lys av dette.

Avslutningsvis vil riksadvokaten understreke at Den høyere påtalemyndighet ikke bare skal utøve tilsynsvirksomhet og påpeke avvik; innenfor vårt ansvarsområde skal vi også være en konstruktiv bidragsyter i arbeidet med å heve kvaliteten i politiets arbeid. Vi vil derfor følge opp funnene med ytterligere tiltak og dialog i tiden som kommer, for å bidra til at arbeidet på dette viktige kriminalitetsområdet styrkes.

Oslo, 20. november 2025

Jørn Sigurd Maurud
sign.

1 Innledning

1.1 Konklusjon

Undersøkelsen viser at politiets innsats mot cyberkriminalitet ikke er i tråd med riksadvokatens føringer. Mange saker om cyberrettet kriminalitet blir ikke etterforsket, og politiet evner ikke i tilstrekkelig grad å prioritere de alvorlige sakene. Det er avdekket lav kunnskap og kompetanse om digitale spor. Gjennomgående trekkes manglende kompetanse og tilgjengelige ressurser frem som hovedårsaker til hvorfor sakene ikke blir etterforsket eller prioritert.

Funnene er alvorlige, og riksadvokaten vurderer at det er behov for kortsiktige tiltak for å sørge for at saker blir behandlet i tråd med riksadvokatens føringer om prioritering og kvalitet i etterforskningen. Videre er det behov for mer langsiktige tiltak som sikrer at etterforskere og politiadvokater har tilstrekkelig kompetanse om digitale spor og sporsteder.

1.2 Om cyberrettet kriminalitet og bakgrunnen for undersøkelsen

Omfanget av cyberkriminalitet har økt de siste årene. Likevel har antall anmeldelser til politiet vært synkende siden 2018, med kun 281 saker anmeldt i 2024. Det antas å være betydelige mørketall, og antallet anmeldelser gjenspeiler ikke det reelle omfanget.

I vurderingen av alvorsgraden ved cyberrettede lovbrudd, kan det i mange tilfeller ha mindre betydning om gjerningspersonene lykkes i å gjennomføre lovbruddet eller opererte på forsøksstadiet. For eksempel vil koordinerte forsøk på angrep på systemer som er en del av kritisk infrastruktur, være svært alvorlig selv om gjerningspersonene ikke lykkes. Ofte vil det være vanskelig å vurdere sakens alvor innledningsvis, uten at det gjøres noen undersøkelser eller ved å se ulike saker i sammenheng.

I 2024 påbegynte Den høyere påtalemyndighet et langsiktig arbeid for å heve innsatsen mot cyberkriminalitet gjennom økt kompetanse i Den høyere påtalemyndighet, og økt kvalitet i politiets straffesaksbehandling. Politidirektoratet har siden 2023 arbeidet med å øke politiets kompetanse og kapasitet til å håndtere denne type kriminalitet. Resultatene fra undersøkelsen gir et godt grunnlag for det videre arbeidet, og vil også være nyttige for politimestrene i styringen av innsatsen i distriktene.

Bakgrunnen for undersøkelsen er at statistikk og annen kunnskap om cyberkriminalitet indikerte at politiets innsats mot de alvorlige sakene på kriminalitetsområdet ikke var i tråd med riksadvokatens sentrale føringer. For å styrke kunnskapsgrunnlaget i det videre arbeidet med å heve innsatsen på området, gjennomførte derfor Riksadvokatembetet og Det nasjonale statsadvokatembetet høsten 2024 en nasjonal undersøkelse i samarbeid med Kripos. Det ble både undersøkt hvordan sakene ble prioritert i distriktet, og om politiet og påtalemyndigheten har tilstrekkelig kunnskap om digitale spor, sporsteder og andre sentrale etterforskingsskritt i saker innenfor cyberkriminalitet. Denne rapporten redegjør for hovedfunnene fra undersøkelsen.

2 Saksutvalg, metode og statistikk

2.1 Innledning

I dette kapittelet redegjøres det kort for saksutvalget, samt hvilke metoder som er benyttet i undersøkelsen. Metodene kombinerer kvantitative data fra politiets systemer (statistikk), en spørreundersøkelse rettet til de påtaleansvarlige og kvalitative vurderinger fra statsadvokater og tjenestepersoner med spisskompetanse innenfor området (saksgjennomgang).

2.2 Saksutvalg

Saksutvalget i undersøkelsen omfatter alle påtaleavgjorte saker kodet som «Ren IKT-kriminalitet» i politiets straffesakssystem i perioden 1. september 2023 til 31. august 2024.[1] Dette utgjorde 298 saker.[2]

Undersøkelsen er avgrenset til cyberrettet kriminalitet,[3] som gjelder saker om overtredelser av straffeloven §§ 201 (*Uberettiget befatning med tilgangsdata, dataprogram mv*), 204 (*Innbrudd i datasystem*) og 206 (*Fare for driftshindring*). Bakgrunnen for avgrensningen er dels begrensningene i mulighetene til å gjøre saksuttrekk,[4] og dels at mengden saker i de valgte kategoriene muliggjorde en gjennomgang av alle registrerte saker. I tillegg er det lagt vekt på at det sentrale i etterforskingen av disse sakene er digitale spor. Funnene fra undersøkelsen antas derfor å ha stor overføringsverdi til saker innen cyberstøttet kriminalitet og saker hvor digitale spor er sentrale.

2.3 Spørreundersøkelse

For hver sak i utvalget har den som påtaleavgjorde saken besvart en spørreundersøkelse med om lag 30 spørsmål.[5] Spørreundersøkelsen berørte temaer knyttet til registrering av sak, etterforskingen og påtaleavgjørelsen.

2.4 Den høyere påtalemyndighets saksgjennomgang

Riksadvokatembetet og Det nasjonale statsadvokatembetet har gjennomgått 127 saker som enten var avgjort med positiv påtaleavgjørelse eller henlagt med begrunnelsene *ikke rimelig grunn til å etterforske* (kode 106 og 022), *manglende ressurser eller kapasitet* (kode 025 og

[1] «Ren IKT-kriminalitet» innbefatter statistikkgruppene «355 Innbrudd i datasystem», «351 Uberettiget befatning med tilgangsdata, dataprogram mv.» og «607 Inntrenging i dataanlegg/system (§ 145, 2. ledd)».

[2] Riksrevisjonen gjennomførte en undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT, se Dokument 3:5 (2020-2021). Undersøkelsen viste at uklarhet rundt begrepet IKT-kriminalitet har skapt utfordringer, som at begrepet tolkes forskjellig av blant annet distrikter og særorganer. Dette gjør det vanskelig å skaffe oversikt over kriminaliteten. IKT-kriminalitet sammenblandes også med kriminalitet med elektroniske spor og digitalisering.

[3] Cyberkriminalitet omfatter både saker som gjelder kriminalitet mot datasystemer og kriminalitet utført i datasystemer (cyberrettet kriminalitet) og kriminalitet begått med datasystemer og kriminalitet supplert av datasystemer (cyberstøttet kriminalitet). Dette er utfyllende beskrevet i Kripos' årlige rapport om cyberkriminalitet: «*Cyberkriminalitet 2025 – Politiets årlige rapport om cyberrettet og cyberstøttet kriminalitet*», s. 29.

[4] For en del lovbrudd som i dag både kan begås fysisk og ved bruk av teknologi (cyberstøttet), skiller ikke opplysningene i saksbehandlingssystemet mellom disse på en måte som gjør det mulig å hente ut en komplett oversikt over kun de cyberstøttede sakene.

[5] Hvert spørreskjema knyttet seg til ett unikt saksnummer, hvilket innebar at påtalejurister som hadde avgjort flere saker innenfor saksutvalget måtte besvare undersøkelsen flere ganger. For det tilfelle at den aktuelle påtalejuristen ikke lenger jobbet i politiet ble undersøkelsen besvart av nærmeste leder.

078), *manglende opplysninger om gjerningsperson* (kode 014), *ikke straffbart forhold* (kode 010), *avgjort utenfor straffesak* (kode 016), *åpenbart grunnløs* (kode 026), *mistenkte under 15 år* (kode 051), *fordi allmenne hensyn ikke tilsier påtale* (kode 062) eller *sendt utlandet som rette vedkommende* (182).

2.5 Kripos' saksgjennomgang

Ved vurdering av sakens oppklaringspotensial, er det viktig at påtalejuristen har en riktig forståelse av mulige digitale spor i saken. En uriktig forståelse, kan medføre at saken henlegges til tross for potensial for oppklaring. Kripos gjennomgikk derfor saker hvor påtalejuristen i spørreundersøkelsen hadde vurdert at videre etterforsking av digitale spor og sporsteder *ikke* kunne gitt relevante funn.[6] Kripos undersøkte om det var flere spor i saken, og om mulige spor var relevante med tanke på oppklaring. Videre vurderte de om det ville vært hensiktsmessig å bruke ressurser på etterforsking av de mulige sporene i lys av sakens alvor[7] og mulige resultat av etterforskingsskrittene.

2.6 Statistikk

Kriminalitet rettet mot datasystemer dekkes av lovbruddskategorien «Ren IKT-kriminalitet» i politiets saksbehandlingssystem. I perioden 2018 til 2024 fordeler påtaleavgjørelsene seg slik:

	2018	2019	2020	2021	2022	2023	2024	Totalsum	Andel av total
Oppklart	27	122	23	49	23	76	9	329	12 %
42 Tiltalebeslutning	11	68	5	17	16	5	2	124	5 %
41 Siktelse (tilståelsesdom)	2	38	5	21	1	7	2	76	3 %
104 Henlagt som åpenbar grunnløs			1			57		58	2 %
Øvrige avgjørelseskoder	14	16	12	11	6	7	5	71	3 %
Ikke oppklart	345	303	294	253	259	207	195	1 856	68 %
14 Henlagt grunnet mangel på opplysninger om gjerningspersonen	231	225	161	159	172	145	126	1 219	45 %
25 Henlagt - ikke forholdsmessig ressursbruk	81	44	68	53	58	34	40	378	14 %
58 Henlagt på grunn av bevisets stilling	15	20	43	24	13	13	13	141	5 %
78 Henlagt - ikke forholdsmessig ressursbruk	16	11	19	12	11	14	15	98	4 %
Øvrige avgjørelseskoder	2	3	3	5	5	1	1	20	1 %
Trekkes ut før oppklaringsprosenten beregnes	97	74	71	63	85	99	62	551	20 %
22 Henl ikke rim gr til å undersøke om det forel str bart forh	73	56	46	54	69	62	48	408	15 %
106 Henl ikke rim grunn undersøke om det er straffbart forhold	21	14	19	6	14	22	9	105	4 %
Øvrige avgjørelseskoder	3	4	6	3	2	15	5	38	1 %
Totalsum	**469**	**499**	**388**	**365**	**367**	**382**	**266**	**2 736**	**100 %**

Antall anmeldte saker har sunket i perioden, til tross for at omfanget av kriminaliteten har økt[8].

Flesteparten av de anmeldte sakene (60%) avgjøres ved FSI (Felles straffesaksinntak), mens de øvrige (27% og 12%) avgjøres ved en GDE (Geografisk driftsenhet) og FDE (Felles

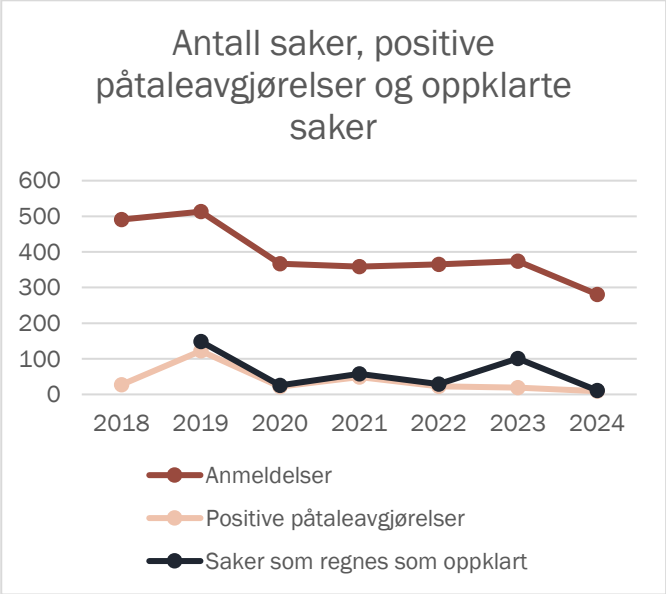
[6] Spørsmålet var som følger: «Vurderer du at (videre) etterforsking av noen av de aktuelle sporstedene eller potensielle digitale spor i saken, kunne ha gitt relevante funn?» Av 298 saker er det registrert 265 svar. 33% svarte «ja», 15% svarte «usikker» og 52% svarte «nei». Kripos gjennomgikk de sistnevnte sakene.

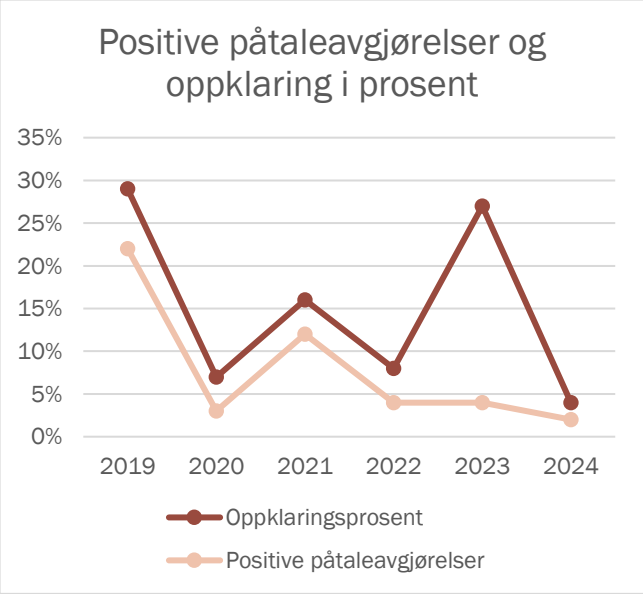
[7] Kripos har klassifisert alvorlighetsgraden på sakene etter en matrise basert på det britiske National Cyber Security Centre (NCSC) sin klassifiseringsmatrise. Kripos gjennomgikk totalt 132 saker.

[8] Kripos, *Cyberkriminalitet 2025 – Politiets årlige rapport om cyberrettet og cyberstøttet kriminalitet, s. 30-33.*

driftsenhet)[9]. Om lag 62% av sakene er avgjort innen 14 dager, 73% innen 30 dager og hele 84% innen 90 dager. Saksbehandlingstiden er med andre ord kort, men dette må ses i sammenheng med at majoriteten av sakene ikke etterforskes.

Tabellene nedenfor viser forholdet mellom antall saker, saker med positive påtaleavgjørelser og oppklarte saker:





Den høyere oppklaringsprosenten i 2019 og 2021 skyldes at henholdsvis 85 og 17 saker knyttet til tre sakskompleks ble påtaleavgjort med *Tiltalebeslutning* (kode 042) eller *Siktelse, tilståelsesdom* (kode *041).* Den høyere oppklaringsprosenten i 2023 skyldes ett sakskompleks hvor 57 saker ble henlagt med begrunnelsen *Henlagt som åpenbar grunnløs (kode 026 eller 104),* som regnes som oppklart.

Av totalt antall påtaleavgjørelser i perioden 2018–2024 ble omtrent 45% av sakene henlagt grunnet *mangel på opplysninger om gjerningsperson* (kode 014).

Det anmeldes flest saker til Oslo politidistrikt, som har avgjort rundt 36% av sakene, mens de øvrige distriktene hadde en andel på mellom 1–11%.

[9] De resterende sakene er avgjort ved særorgan eller annen enhet.

3 Rettslige utgangspunkter

Etterforsking av cyberkriminalitet er underlagt samme generelle krav til etterforsking og kvalitet som øvrige kriminalitetsområder. I undersøkelsen har særlig følgende direktiver vært sentrale:

- Riksadvokatens årlige mål- og prioriteringsrundskriv for 2023 og 2024 (nr. 1/2023 og nr. 1/2024).
- Riksadvokatens rundskriv nr. 3/2018 «Kvalitetskrav til straffesaksbehandlingen i politiet og ved statsadvokatembetene mv.».
- Riksadvokatens rundskriv nr. 3/2016 «Henleggelse på grunn av manglende saksbehandlingskapasitet mv.».
- Riksadvokatens rundskriv nr. 3/1999 «Etterforsking».

Etterforsking er en formålsstyrt virksomhet hvor målet som regel er å avdekke om noe straffbart har funnet sted, og om noen eventuelt kan stilles til ansvar. For all cyberkriminalitet er det imidlertid viktig å være bevisst på at et sentralt formål med etterforsking også er å *avverge eller stanse* straffbare handlinger, jf. straffeprosessloven § 226 første ledd bokstav d. Etterforskingen av cyberrettet kriminalitet kan for eksempel avdekke spor som peker mot andre fornærmede som er eller vil bli kompromittert, slik at disse kan varsles og det kan iverksettes mottiltak. Ved å etterforske cyberrettet kriminalitet vil politiet også kunne identifisere modus og fremgangsmåter som kan brukes i politiets forebyggende virksomhet, herunder for å tette sårbarheter som har blitt utnyttet. Samhandling og deling av informasjonen med andre aktører, både nasjonalt og internasjonalt, vil være sentralt.

Straffeprosessloven § 224 bestemmer at politiet skal igangsette etterforskning når det «er rimelig grunn til å undersøke om det foreligger [et] straffbart forhold». Dersom anmeldelsen og/eller det beskrevne forholdet ikke gir rimelig grunn til å igangsette etterforskning, kan saken henlegges *fordi det ikke er rimelig grunn til å iverksette etterforsking* (kode 022 eller 106). Riksadvokaten har i rundskriv nr. 3/2016 punkt IV[10] gitt føringer for hvilke vurderinger som skal gjøres før en sak kan henlegges med denne begrunnelse, og hvordan koden skal praktiseres sammenlignet med kapasitetshenleggelser og *henleggelser på grunn av manglende opplysning om gjerningsperson* (014). Det er normalt ikke gjennomført etterforsking i saker som henlegges av disse grunner.

Riksadvokaten har i prioriteringsrundskrivet som gjaldt på tidspunktet for undersøkelsen, samt tidligere år, gitt anvisning på at alvorlig kriminalitet rettet mot datasystemer skal gis prioritet og at innsatsen på området skal intensiveres. Digitale spor er flyktige, og det har vært fremhevet at påtalemyndigheten må sørge for rask iverksettelse av etterforsking, sporsikring og informasjonsdeling.

Det fremgår av riksadvokatens kvalitetsrundskriv (rundskriv nr. 3/2018) at det innenfor de sentralt prioriterte kriminalitetsområder hvor det ofte ikke inngis anmeldelser fra en fornærmet, er viktig at politiet selv avdekker og etterforsker lovbrudd. Av samme rundskriv følger at saker skal kodes korrekt ved registrering, og oppdateres dersom etterforskingen gir grunnlag for det – samt at henleggelsesgrunn skal være korrekt og i samsvar med den reelle begrunnelsen for at etterforskingen avsluttes.

[10] Riksadvokatens har utgitt nytt rundskriv om henleggelser av straffesaker (nr. 2/2025), som trer i kraft 1.1.26.

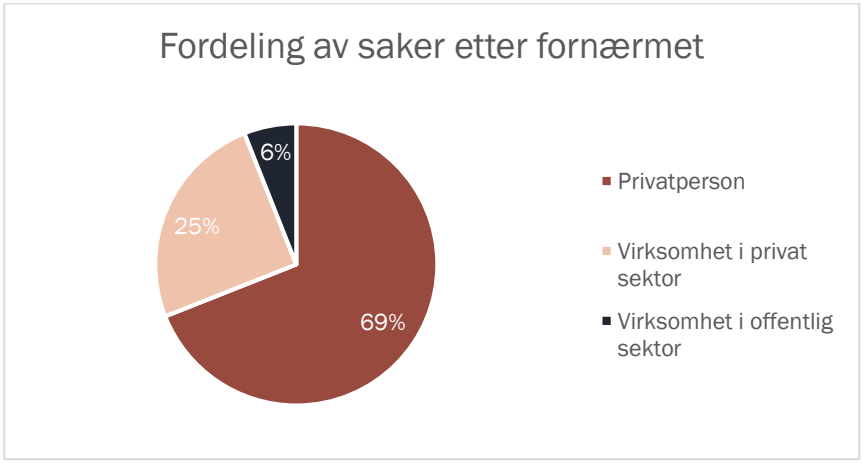
4 Funn

4.1 Innledning

Cyberundersøkelsen omhandler politiets innsats mot cyberrettet kriminalitet basert på en gjennomgang av påtaleavgjorte saker gjennom et helt år. Både i tiden før og etter dette finnes det eksempler på godt arbeid som er gjort i enkeltsaker. I lys av riksadvokatens føringer om at innsatsen mot de alvorlige sakene skal styrkes, må politidistriktene sørge for jevn og målrettet etterforskingsinnsats, og sikre at resultatene ikke er en følge av sporadisk eller tilfeldig enkeltsaksbehandling.

4.2 Anmeldte saker

Av de 265 sakene som er omfattet av undersøkelsen, er fornærmede en privatperson i 69% av sakene, mens virksomheter er fornærmet i de resterende 31% av sakene.



En stor andel av sakene som anmeldes av privatpersoner, omhandler tap av kontroll over kontoer på sosiale medier eller mistanke om overvåkning eller hacking. Selv om alvorsgraden isolert sett er lav, vil denne type lovbrudd kunne ha stor betydning for den enkelte. Samtidig viser saksgjennomgangen at det i mange av disse sakene mangler konkrete holdepunkter for at det er begått en straffbar handling. I vurderingen av om etterforsking skal iverksettes, må det også tas hensyn til at anmeldelser av denne type lovbrudd kan skyldes manglende teknisk kompetanse hos anmelder eller en feilaktig oppfatning av å være overvåket eller forfulgt. I noen saker vil det være åpenbart at det ikke er begått en straffbar handling, mens det i andre saker vil være mer krevende å skille anmeldelser av *reelle* lovbrudd og de som er en følge av manglende teknisk kompetanse eller feilaktige oppfatninger.

I alle anmeldelsene som var inngitt på vegne av en virksomhet, var det holdepunkter for at det objektivt sett var begått en straffbar handling.

I de fleste sakene (66%) foreligger det kun en helt enkel anmeldelse, hvor fornærmede ikke har foretatt noen undersøkelser for å fremskaffe opplysninger om saken. Slike enkle anmeldelser er i hovedsak inngitt av privatpersoner. I de resterende sakene har fornærmede

selv foretatt undersøkelser (24% av disse sakene) eller latt seg bistå av en profesjonell aktør som eksempelvis et hendelseshåndterings-selskap (10%).

Av sakene som er gjennomgått, er det kun syv som er initiert av politiet basert på etterretningsopplysninger, opplysninger fra andre straffesaker eller offentlige tilgjengelige opplysninger. De øvrige sakene er avdekket som følge av anmeldelse fra fornærmede eller ved at forholdet er nært beslektet med et annet forhold under etterforsking og avdekkes som følge av denne; eksempelvis når en eks-kjæreste anmeldes for plagsom eller hensynsløs adferd, og denne adferden også omfatter urettmessig innlogging på fornærmedes kontoer på sosiale medier.

Sakene er i hovedsak (82%) opprettet på bakgrunn av skriftlig anmeldelse fra fornærmede, enten ved bruk av politiets anmeldelsesskjema eller ved at fornærmede har innlevert en mer omfattende skriftlig redegjørelse med dokumentasjon. Politiet har ikke en digital anmeldelsesløsning for datakriminalitet, og både privatpersoner og virksomheter må derfor møte fysisk hos politiet og ta med dokumentasjon for å anmelde lovbrudd.[11]

4.3 Politiets etterforskingsinnsats

Det ble det truffet positiv påtaleavgjørelser i kun syv saker. Dette utgjør i underkant av tre prosent av saksutvalget.

Flesteparten av sakene med positiv påtaleavgjørelse omhandlet uberettiget tilgang til nettkontoer mellom parter med en forutgående relasjon, og saken inngikk stort sett i et sakskompleks mellom disse partene. I tillegg ble én gjerningsperson under 18 år ilagt påtaleunnlatelse for å ha installert skadevare på skolens datasystemer, og to saker gjaldt bl.a. phishing-bedragerier.

De øvrige 97% av sakene ble henlagt med ulike begrunnelser:

Begrunnelse	Andel
Manglende opplysning om gjerningsperson (kode 014)	47,5%
Manglende kapasitet (025 eller 078)	23,0%
Ikke rimelig grunn til å iverksette etterforsking (022 eller 106)	19,6%
Bevisets stilling (017 eller 058)	4,5%
Øvrige henleggelseskoder	2,6%

Henleggelsesgrunnen *bevisets stilling* benyttes i saker hvor det har vært gjennomført etterforsking. De øvrige henleggelsesgrunner benyttes normalt i saker hvor det ikke har vært gjennomført etterforsking. I saker henlagt på grunn av *manglende opplysning om gjerningsperson*, var det gjennomført etterforsking i 15 saker.

Samlet sett innebærer det at om lag 87 % av sakene ikke var gjenstand for etterforsking.

[11] https://www.politiet.no/rad/datakriminalitet/#slik-anmelder-du, besøkt 1. juli 2025.

Ved gjennomgangen er det avdekket *minst* åtte alvorlige saker om datainnbrudd hvor det ikke ble iverksatt etterforsking til tross for at melder – virksomheter i privat eller offentlig sektor – enten hadde en samfunnskritisk funksjon, forvaltet viktig infrastruktur eller anførte at angrepet medførte konsekvenser eller fare for konsekvenser for slike funksjoner eller infrastrukturer. Flere av disse sakene ble henlagt med begrunnelsen *ikke rimelig grunn til å iverksette etterforsking* (kode 022 eller 106). I det følgende nevnes to eksempler:

I. I én av sakene var det konkret mistanke om at noen hadde skaffet seg uberettiget tilgang til styringssystemer for kritisk infrastruktur og foretatt endringer som fikk store konsekvenser. Det fremkommer av de interne arbeidsloggene i politiets saksbehandlingssystem at politiet vurderte forholdet som alvorlig, men at man ikke iverksatte etterforsking fordi det var et «tynt mistankegrunnlag», den angrepne virksomheten hadde endret passord på den misbrukte brukerkontoen og det ville være vanskelig å komme i mål med etterforskingen.

II. I en annen sak anmeldte en virksomhet et datainnbrudd med etterfølgende phishing-angrep ved misbruk av virksomhetens navn. Angrepet var rettet mot flere tusen norske innbyggere. Av interne arbeidslogger i politiets saksbehandlingssystem fremkommer det at en politiadvokat vurderte at det er tale om et profesjonelt angrep hvor det forelå mye dokumentasjon som burde innhentes. Likevel – og bare knappe tre timer senere – henlegges saken av en annen politiadvokat. Av de interne loggene fremkommer det at den da ble «vurdert som overordnet», og at man heller «avventet enkeltstående anmeldelser».

Av fritekstfeltene i spørreundersøkelsen til de påtaleansvarlige, ble det gjennomgående trukket frem at det manglet ressurser og kompetanse til å etterforske denne type saker, og at sakstypen ikke reelt sett ble prioritert i politidistriktet.

Den høyere påtalemyndighets saksgjennomgang avdekket uriktig bruk av henleggelseskode i 23 av de 114 sakene som var henlagt *på grunn av manglende kapasitet*, *ikke rimelig grunn til å iverksette etterforsking* eller *avgjort utenfor straffesak*.

I spørreundersøkelsen til de påtaleansvarlige i politiet, fremkom at påtalemyndigheten vurderte at det ikke var flere relevante spor i 132 av sakene som var henlagt. Kripos har gjennomgått disse sakene, og konkludert med følgende:

- I 83 av sakene var det spor som kunne gitt relevante funn i retning av oppklaring.
- I 25 av disse 83 sakene ville det også vært hensiktsmessig å bruke ressurser på å etterforske. I 24 av disse var fornærmede en virksomhet, og 13 av de 25 sakene ble klassifisert som alvorlige.

5 Vurderinger

5.1 Mørketall og årsaker til få anmeldte saker

Det er sannsynlig at flere alvorlige lovbrudd innenfor kriminalitetsområdet ikke blir anmeldt til politiet. Det kan være flere og sammensatte årsaker til dette.

Mange angrep oppdages ikke. Sivile mottiltak som en følge av økt bevissthet i befolkningen og næringslivet om behovet for å forebygge denne type hendelser, kan bidra til reduksjon i anmeldelser. Videre kan det være at virksomheter i økende grad benytter seg av private hendelseshåndterings-firmaer med fokus på gjenoppretting fremfor etterforsking – i kombinasjon med et ønske om å unngå publisitet og tilhørende risiko for omdømmetap.

Det kan også være at publikum har lave forventninger til mulighetene for å kunne oppklare saker med internasjonale forgreninger. Videre kan det være at straffbare forsøk ikke anmeldes på grunn av en uriktig antakelse om at dersom lovbruddet ikke er vellykket, er ikke forholdet alvorlig. Det lave anmeldelsestallet kan imidlertid også være et uttrykk for lav tillit til politiets håndtering av sakene.

Internasjonalt samarbeid har blitt viktigere, og mulighetene for oppklaring gjennom samarbeid med andre land er større enn før.[12] Det antas at det kan foreligge manglende bevissthet om dette, noe som kan påvirke både omfanget av saker som blir anmeldt og hvilke saker politiet iverksetter etterforsking i.

Uavhengig av årsak, er det bekymringsfullt at politiet ikke mottar flere anmeldelser, når det samtidig foreligger kunnskap om at cyberkriminalitet er økende. Politiets håndtering av sakene som anmeldes, kan bidra til ytterligere svekkelse av tilliten til politiets evne til å etterforske disse sakene – som i seg selv er alvorlig. Når f.eks. virksomhetsledere anmelder åpenbart alvorlige lovbrudd, men møtes med umiddelbare henleggelser med begrunnelsen om at det ikke er rimelig grunn til å iverksette etterforsking, er det lite sannsynlig at disse pånytt vil oppsøke politiet ved nye og alvorlige lovbrudd.

Som det fremgår av kvalitetsrundskrivet (rundskriv nr. 3/2018), er det nødvendig at politiet også selv avdekker og etterforsker forhold innenfor kriminalitetsområder med store mørketall. Det fremgår også særskilt av riksadvokatens prioriteringsrundskriv (rundskriv nr. 1/2024). Gjennomgangen viser at politiet ikke i nevneverdig grad evner å initiere saker på eget initiativ basert på eksisterende kunnskapsgrunnlag innenfor dette kriminalitetsområdet, noe som også er med på å forklare hvorfor antall saker er lavt.

5.2 Manglende etterforskning og prioritering

Flesteparten av sakene henlegges. Gjennomgangen av de forholdene som blir anmeldt til politiet, viser at det blant de cyberrettede sakene er overvekt av saker av mindre alvorlig

[12] Eksempelvis har både Europol og Interpol gjennomført koordinerte aksjoner mot cyberkriminelle i både Europa og Vest-Afrika i nyere tid, herunder gjennom Operation Endgame (Europol) og Operation Jackal III (Interpol).

karakter. Det er imidlertid også slik at politiet mottar et ikke ubetydelig antall anmeldelser som gjelder alvorlige forhold, og som etter riksadvokatens føringer skulle vært etterforsket.

I lys av dagens sikkerhetspolitiske situasjon som preges av sammensatte trusler og fare for sabotasje fra fremmede stater, er det særlig viktig at politiet etterforsker mulige digitale skadeverk eller innbrudd hos virksomheter med viktig infrastruktur eller samfunnskritiske funksjoner. Undersøkelsen har avdekket manglende etterforsking i flere slike saker. Det er således på det rene at politiets håndtering av alvorlig kriminalitet rettet mot datasystemer er mangelfull.

Brorparten av sakene er isolert sett ikke alvorlige, og det kan være riktig at disse ikke gis prioritet. Det er imidlertid ikke mulig å fastslå om resultatet er utslag av en kunnskapsbasert og aktiv prioritering i tråd med riksadvokatens føringer, eller først og fremst sammenfall med manglende kompetanse om elektroniske spor og/eller at området ikke gis prioritet. De øvrige funn trekker i retning av sistnevnte.

Gjennomgangen av sakene med positiv påtaleavgjørelse viser at utvelgelsen av saker hvor det iverksettes etterforsking, er tilfeldige forhold avdekket i sakskompleks om eksempelvis hensynsløs eller plagsom adferd, og ikke utslag av en prioritering av cyberrettet kriminalitet.

Det er videre avdekket at flere alvorlige saker som fikk eller kunne fått alvorlige konsekvenser for samfunnskritiske funksjoner eller viktig infrastruktur, ble henlagt uten etterforsking.

At politiet ikke i tilstrekkelig grad prioriterer denne type kriminalitet, understøttes av fritekstsvar fra politiadvokatene i spørreundersøkelsen. Det underbygges også av at de fleste sakene avgjøres umiddelbart ved FSI, uten å settes ut til etterforskingsmiljøene.

Kripos' gjennomgang viser at politiets vurdering av om det var relevante spor i de henlagte sakene, er uriktig i *flesteparten* av tilfellene. Videre viser gjennomgangen at det henlegges en ikke ubetydelig andel saker som skulle vært etterforsket. Dette gjelder også for saker som faller innenfor kategorien «alvorlig IT-kriminalitet» og som skulle vært gitt prioritet i tråd med riksadvokatens dagjeldende prioriteringsrundskriv (nr. 1/2024).

Saksgjennomgangen til Den høyere påtalemyndighet avdekket også at politidistriktene i om lag 20% av sakene anvender feil henleggelsesgrunnlag, hvilket er for høyt.

Den manglende etterforskingen av de prioriterte sakene gir grunn til bekymring. Både Kripos' gjennomgang og fritekst-svar i spørreundersøkelsen, gir holdepunkter for at politiet mangler nødvendig kompetanse til å etterforske sakene. Etterforsking av cyberrettet kriminalitet kan kreve både spesialistkompetanse og spisskompetanse. For å forstå alvorsgraden av enkelte av lovbruddene kan også en viss fenomenforståelse være nødvendig.

Mangelen på slik kompetanse og fenomenforståelse kan påvirke hvordan sakene prioriteres og avgjøres i politidistriktene. Det kan likevel ikke fullt ut forklare funnene i undersøkelsen. Dette gjelder særlig de alvorlige sakene med fare for samfunnskritiske funksjoner og viktig infrastruktur, hvor det ikke ble identifisert at det skulle iverksettes etterforsking. I disse sakene

var det åpenbart – selv uten særskilt opplæring og fenomenforståelse – at saken var omfattet av riksadvokatens sentrale prioriteringer for hva som skal etterforskes.

Gjennomgangen av interne arbeidslogger i politiets saksbehandlingssystem etterlater er klart inntrykk av at det er mangel på ressurser i distriktet, herunder *tilgjengelig* kompetanse, som er en vesentlig årsak til at sakene henlegges.

Sakstypen har vært prioritert i mange år. Viktigheten av innsats på området forsterkes ytterligere av den sikkerhetspolitiske situasjonen. Funnene i undersøkelsen tyder på at riksadvokatens føringer om intensivering av innsats på kriminalitetsområdet, i det vesentlige ikke har blitt implementert og operasjonalisert i politidistriktene.

5.3 Andre forhold

Riksadvokaten bemerker at fornærmedes manglende muligheter til å anmelde cyberrettet kriminalitet digitalt, fremstår som uheldig. Det skaper en hindring som kan innebære at fornærmede avstår fra å anmelde, vanskeliggjør deling av digitale bevis som fornærmede har tilgang til, og medfører i mange tilfeller en unødig forsinkelse før politiet får anmeldelsen og tilgang til bevis. Den gammeldagse og papirbaserte tilnærmingen til anmeldelse av digital kriminalitet, kan i seg selv medføre lave forventinger og tillit til politiets evne til å etterforske slik kriminalitet.

6 Anbefalinger

6.1 Overordnede anbefalinger

Det er nødvendig å iverksette tiltak innenfor både organisering, ressurssetting og kompetanse.

Kriminalitetsområdet har vært prioritert i en årrekke, uten at det har ført til særlig gode resultater. Det er ikke tilstrekkelig å «fortsette som før». Det kreves særskilt oppmerksomhet fra både Politidirektoratet, som har det nasjonale ansvaret for at føringene gitt av riksadvokaten realiseres i politidistriktene gjennom ressursallokering, organisering og kompetansehevende tiltak, og den enkelte politimester, som har det tilsvarende ansvaret for at føringene realiseres i eget distrikt. Videre krever det fortsatt oppmerksomhet fra Den høyere påtalemyndighet i fagledelsen av politiet.

Det er behov for kortsiktige tiltak for å sørge for at politiet etterforsker de alvorlige og prioriterte sakene. Videre er det behov for å styrke innsatsen med mer langsiktige tiltak. Dette innebærer også å legge til rette for at politiet mottar flere anmeldelser enn i dag og sørge for at politiet har et tilstrekkelig kunnskapsgrunnlag til å kunne iverksette etterforsking på eget initiativ der det er grunn til det.

Noen politidistrikter har allerede påbegynt et forbedringsarbeid, og politimestrene i de aktuelle distriktene må nøye vurdere endringsarbeidet i lys av denne rapporten og anbefalingene.

6.2 Kortsiktige tiltak

På kort sikt vil det for politidistriktet være viktig å gjennomføre umiddelbare tiltak som sørger for at etterforsking iverksettes i de alvorligste sakene som blir anmeldt. Erfaringene fra undersøkelsen er at dette som oftest er saker som anmeldes av virksomheter. Nasjonalt er det tale om mindre enn 100 saker i løpet av ett år. Ettersom disse sakene ofte henlegges ved FSI, bør tiltak være rettet mot ledelse, etterforskere og påtalejurister ved denne enheten. Tiltak rettet mot FSI vil være viktig for å sikre rask iverksettelse av etterforsking og sporsikring.

For å sikre riktig håndtering av sakene, bør det fra ledelsesnivå være målrettet oppfølging av distriktets henleggelser av anmeldelser av cyberrettet kriminalitet fra virksomheter.

Dersom distriktet ikke selv har spesialistkompetanse til å etterforske sakene, bør Kripos rutinemessig konsulteres.

Politidirektoratet bør også vurdere tiltak på kort sikt, for å sørge for at distriktene påbegynner arbeidet med å styrke innsatsen. Det må vurderes om allerede iverksatte tiltak er tilstrekkelig, sammenholdt med funnene i denne rapporten.

Videre bør Politidirektoratet sørge for at det raskt åpnes for digitale anmeldelser av kriminalitet rettet mot datasystemer, som ventelig vil bidra til flere og bedre anmeldelser.

For Den høyere påtalemyndighet vil det være en utfordring å komme i posisjon til å drive fagledelse av politiet i disse sakene, fordi sakene sjelden sendes inn til statsadvokatene. Når

sakene eventuelt kommer til behandling vil det som oftest være på et tidspunkt hvor avgjørende spor kan ha gått tapt. Statsadvokatene bør vurdere om foreleggelesplikt skal benyttes i en periode, for å sikre at det iverksettes etterforsking i saker hvor det er grunn til det. Basert på erfaringene fra undersøkelsen, vil en slik foreleggelsesplikt kunne innrettes mot saker som er anmeldt av virksomheter. En slik foreleggelsesplikt bør inntre allerede ved mottak av anmeldelse for å sikre at det raskt iverksettes etterforsking og sporsikring dersom det er grunn til det, samt at eventuell etterforsking får et hensiktsmessig omfang og at innsatsen rettes mot de alvorligste sakene.

Statsadvokatene bør også vurdere en målrettet oppfølging av distriktets egeninitierte saker i en begrenset periode. Innsatsen på området bør vies særskilt oppmerksomhet i resultatoppfølgingen og dialogen mellom embetsleder og politidistriktets ledelse.

6.3 Langsiktige tiltak

For Politidirektoratet er det nødvendig å iverksette langsiktige tiltak for å sørge for at riksadvokatens prioriteringer på kriminalitetsområdet realiseres. Det synes særlig å være behov for kompetansehevende tiltak.

Riksadvokaten er kjent med at Politidirektoratet har gjennomført kartlegging av distriktenes evne til å håndtere kriminalitetsområdet, og ser på ulike modeller for organisering og kompetansefordeling. Det synes helt nødvendig at dette langsiktige arbeidet fortsetter og intensiveres.

Det er i flere inspeksjonsrapporter fra Den høyere påtalemyndighet trukket frem at høy turn-over er en hovedårsak til manglende kvalitet og etterlevelse av riksadvokatens føringer på straffesaksfeltet. En plan for langsiktige tiltak bør også adressere denne utfordringen.

Politiet mangler teknologiske løsninger for å effektivt etterforske denne type saker, og denne kriminalitetstypen vil ikke kunne bekjempes uten at politiet har tilgang til adekvate teknologiske verktøy. Dette innebærer løsninger som blant annet kan bidra til rask informasjonsinnhenting og analyse av saksinformasjon, effektiv informasjonsdeling og lett tilgjengelig fagkunnskap som kan bidra til kompetanseheving og høyere kvalitet i enkeltsaker. Politidirektoratet har påbegynt et arbeid med å utvikle et nytt saksbehandlingssystem med målsetting om at løsningen skal erstatte dagens løsning innen 2030. Politidirektoratet bør vurdere om arbeidet med disse løsningene prioriteres og utvikles raskere.

Riksadvokaten og Politidirektoratet har allerede påbegynt et arbeid for å få bedre indikatorer for oppfølgingen av resultatene på straffesaksfeltet, herunder cyberkriminalitet. Dette arbeidet bør gis prioritet for å understøtte politimestrenes og statsadvokatenes oppfølging av kriminalitetsområdet.