Digitale bevis
– Sjekkliste som støtteverktøy for dommere

På Oslo tingretts fagdag om straffesaker 17. januar 2025 holdt politioverbetjent, PhD, Nina Sunde ved Politihøgskolen et innlegg med tittelen *Mulige fallgruver i vurderingen av digitale bevis*. Som ledd i oppfølgingen av fagdagen har Sunde på forespørsel fra tingretten i samarbeid med dommer Martin Eiebakke utarbeidet en sjekkliste som støtteverktøy for dommerne ved vurderingen av digitale bevis.

Formålet med sjekklisten er å gjøre dommere bedre rustet til å foreta vurderinger av digitale bevis. Den er ment som et støtteverktøy som den enkelte dommer selv kan velge å benytte dersom det anses nyttig, og brukes på eget ansvar.

Sjekklisten er ikke ment å legge føringer på rettens bevisvurdering. Prinsippet om fri bevisvurdering gjelder også ved vurderingen av digitale bevis. Som Høyesterett har uttrykt det i HR-2025-458-A avsnitt 24-26, er det opp til den dømmende rett å vurdere hvilken vekt som skal legges på de enkelte bevisene som er ført og hvilken fremgangsmåte som skal velges i den enkelte sak. Det må også ved digitale bevis gjøres en samvittighetsfull, forstandig og rasjonell vurdering av bevisene.

Som innlegget til Sunde på fagdagen illustrerte, kan det i alle fall tidvis være utfordrende for dommere å foreta en slik fornuftsbasert vurdering av digitale bevis. Det vises her til hennes gjennomgang av mulige fallgruver i hennes presentasjon

Sjekklisten kan forhåpentligvis bidra til økt bevissthet, gjøre det lettere å stille relevante spørsmål og ta opp mulige problemstillinger knyttet til digitale bevis før eller underveis i forhandlingene, samt være en støtte for dommeren i etterkant.

Denne første versjonen av sjekklisten er publisert i april 2025. Flere dommere ved Oslo tingrett har gitt innspill, og det tas sikte på å revidere den når det har vært i bruk over noe tid. Dersom du har innspill til sjekklisten eller er villig til å dele erfaringer fra vurderingen av digitale bevis, kan du kontakte Eiebakke på martin.eiebakke@domstol.no og Sunde på nina.sunde@phs.no

Versjon 1 (April 2025)

Sjekkliste - digitale bevis

Om sjekklisten: *Denne sjekklisten er ment å støtte dommere i vurderingen av digitale bevis i straffesaker. Den er aktuell både ved gjennomgang av rapporter om digitale bevis og ved muntlige forklaringer fra politivitner.* *Digitale bevis kan stamme fra ulike datakilder, som for eksempel mobiltelefoner, datamaskiner, navigasjonssystemer, smartklokker eller skytjenester og sosiale medier.* *Sjekklisten er særlig rettet mot to typer rapporter:* ***- gjennomgangsrapport**, skrevet av taktiske etterforskere etter gjennomgang av beslag,* ***- teknisk undersøkelsesrapport/rapport om teknisk analyse,** utarbeidet av dataetterforskere med høyere teknisk kompetanse.*	
1. KOMPETANSE	
- Har politivitnet/dataetterforsker relevant og tilstrekkelig kompetanse til å: - gjøre rede for påliteligheten av beviset? - trekke kvalifiserte slutninger om hva funnene forteller, som utførte aktiviteter og hvem som har gjort det? - identifisere og gjøre rede for relevante usikkerhetsmomenter ved beviset? <u>Politibetjenter uten spesialistkompetanse</u> har som regel ikke tilstrekkelig kompetanse til å trekke selvstendige slutninger og gjøre sannsynlighetsvurderinger av digitale bevis, og slike vitnemål bør være avgrenset til **beskrivelse av funn ved gjennomgang av databeslag basert på gjennomgangsrapporter, se punkt 5**. Gjennomgang gjøres typisk i dataverktøy som for eksempel Cellebrite, XRY, Magnet Axiom eller Griffeye. <u>Dataetterforskere med utdanning og erfaring innen datatekniske undersøkelser</u> har som regel tilstrekkelig kompetanse til å gjennomføre systematiske observasjoner, tester og eksperimenter som kan danne grunnlag for **tolkninger, vurderinger, slutninger og konklusjoner, se punkt 6.**	
2. KVALITETSKONTROLL	
- Er rapporten kvalitetskontrollert? (dette bør fortrinnsvis gjennomføres av noen med lik eller bedre kompetanse enn rapportskriver) - Er sentrale funn presentert i rapporten verifisert med et annet dataverktøy, eller ved manuell sjekk av personell med tilstrekkelig kompetanse? Alle **gjennomgangsrapporter** om digitale beslag med funn av betydning for straffesaken skal kvalitetssikres ved gjennomlesning av personell med høyere teknisk kompetanse eller fra etterforskningsledelsen. Alle **tekniske undersøkelsesrapporter/rapport om teknisk analyse** med funn av betydning for straffesaken bør som hovedregel kvalitetssikres. Dette skjer ved gjennomlesning av rapporten av personell med lik eller høyere teknisk kompetanse.	

Sentrale funn i begge rapport-typer skal som hovedregel **verifiseres** av dataetterforskere. Det bør rettes særskilt oppmerksomhet mot dette når: - beviset er særlig sentralt - beviset er sikret ved nye metoder - beviset er sikret av tredjeparter eller av politi i andre land	
3. GRUNNLEGGENDE PÅLITELIGHET	
- Datagrunnlagets **integritet**: Har datagrunnlaget blitt endret etter at det ble sikret av politiet? (integritet handler om at dataene er uendret og intakte siden innsamling) - **Ubrutt beviskjede**: - Er beviset sikret av politiet, eller av en tredjepart? - Har politiet dokumentert hvem som har hatt tilgang til bevismaterialet gjennom etterforskningsprosessen? - Er det entydig dokumentert hvilken databærer de relevante funnene stammer fra?	
4. UNDERSØKELSESPROSESSEN	
- Er undersøkelsen basert på et tydelig **mandat/oppdrag** med et klart formål, og med avgrensninger til det som er nødvendig og forholdsmessig? - Framgår det tydelig hvilken informasjon man har **søkt** etter i undersøkelsen? - Er undersøkelsen utført på en **objektiv** måte, ved å lete etter informasjon som styrker/svekker både tiltalte og fornærmedes forklaringer, f.eks.: - Er det aktivt søkt etter informasjon i det digitale beslaget som kan kontrollere (styrke/svekke) fornærmedes forklaring? - Er det aktivt søkt etter informasjon som støtter tiltaltes forklaring eller som på annen måte styrker tiltaltes side av saken – og ikke kun det som taler mot tiltalte?	
5. PRESENTASJON AV FUNN	
5.1 Beskrivelser av innhold (f.eks. bilder, video, meldinger) - Gjøres det rede for funnenes opprinnelige kontekst? - Dersom det hevdes av innholdet er manipulert/endret – er det gjort undersøkelser for å utelukke dette?	
5.2 Beskrivelser av kommunikasjon (epost, meldinger, chat, kommentarer på sosiale medier) - Er det gjort tilstrekkelige undersøkelser for å verifisere at kommunikasjonen er fullstendig og gir et dekkende bilde av relevant innhold i samtalen? - Presenteres tilstrekkelig kontekst slik at innholdet i kommunikasjonen ikke lett kan feiltolkes? (ikke enkeltmeldinger tatt ut av sammenheng)	

5.3 Beskrivelser av <u>steder, bevegelser eller bevegelsesmønster</u> (f.eks. lokasjonsdata (latitude/longitude), kartposisjoner, kjøreruter, loggede skritt/distanser/ trappetrinn) - Har vitnet kunnskap om hvor nøyaktig slike data blir logget? - Er det gjort undersøkelser for å verifisere at funnene omkring hendelser og aktiviteter er tolket riktig – f.eks. ved systematisk observasjon, testing eller rekonstruksjon?	
5.4 Beskrivelser av <u>tidspunkter</u> - Er tidspunktene verifisert? - Presenteres de i norsk tid?	
5.5 Beskrivelser av <u>aktiviteter og handlingsmønster</u> (f.eks. søk og nedlasting fra internett, lading av mobil, åpnet melding, spilt av video) - Hvilke undersøkelser er gjort for å verifisere at funnene omkring hendelser og aktiviteter er tolket riktig? - Er det undersøkt om aktivitetene kan ha en annen forklaring enn brukergenerert aktivitet, for eksempel at de er systemgenererte (f.eks. resultat av systemoppdatering)? - Dersom det hevdes at sporene er resultat av hacking - er det gjort undersøkelser for å utelukke hacking?	
5.6 Beskrivelser av <u>knytning mellom innhold/aktiviteter/bevegelser/kommunikasjon og person</u> - Er det gjort undersøkelser for å utelukke at andre enn siktede knyttes til innhold og/eller har utført aktiviteter/bevegelser/kommunikasjon? - Er det utelukket at det aktuelle innholdet eller de observerte aktivitetene kan skyldes automatisert systemaktivitet snarere enn brukergenererte handlinger? (f.eks. loggføring etter systemoppdateringer, automatiske sletteprosesser, bakgrunnsprosesser osv.)	
6. VURDERING OG TOLKNING AV FUNN	
Om vitnets **kompetanse** til å vurdere og tolke funn, se punkt 1. <u>Politibetjenter uten spesialistkompetanse</u> - Holder politibetjenten seg til å beskrive funn? - Dersom politibetjenten presenterer tolkninger, vurderinger, slutninger og konklusjoner – se spørsmålene nedenfor	
<u>Dataetterforskere med utdanning og erfaring innen datatekniske undersøkelser</u> - Kan dataetterforsker gjøre rede for hvordan han/hun har kommet fram til sine tolkninger, vurderinger, slutninger og konklusjoner? - Er alternative forklaringer på sporene undersøkt? - Beskrives begrensninger og usikkerhetsmomenter knyttet til undersøkelser og funn? - Gir funnene tilstrekkelig støtte dataetterforskers tolkninger, vurderinger og konklusjoner? - Har tolkninger, vurderinger og konklusjoner vært gjenstand for kvalitetskontroll av en annen dataetterforsker med lik eller bedre kompetanse?	