

Artikkelen er publisert under modellen grønn åpen tilgang (green open access). Det betyr at utgiver tillater forfatter å arkivere sin artikkel i åpne institusjonelle arkiv (egenarkivering) eller på eget eller arbeidsgivers nettsted, i den versjon og det format som ble godkjent av tidsskriftets redaksjon (akseptert versjon/tekstversjonen).

Sitering av artikkelen i APA (6<sup>th</sup>):

Sunde, N. (2020). Digitale bevis i norske gjenåpningsbegjæringer: Kan vi utelukke systematiske feil?. *Tidsskrift for strafferett*, 20(1), 18-37. <https://doi.org/10.18261/issn.0809-9537-2020-01-03>

Dette er siste tekstversjon av artikkelen, den kan inneholde ubetydelige forskjeller fra forlagets pdf-versjon.

## Digitale bevis i norske gjenåpningsbegjæringer – kan vi utelukke systematiske feil?

Nina Sunde, politioverbetjent ved Politihøgskolen og doktorgradsstudent ved Universitetet i Oslo.

Nina Sunde er politiutdannet fra Politihøgskolen i 1998. Hun har mastergrad i informasjonssikkerhet og cybercrime fra NTNU i 2017. Hun underviser nå ved Politihøgskolen, og er i doktorgradsløp ved Universitetet i Oslo. Hun har tidligere jobbet ved Oslo politidistrikt og Kripos, og har i hovedsak arbeidet med etterforskning av alvorlige voldslovbrudd og datakriminalitet.

[nina.sunde@phs.no](mailto:nina.sunde@phs.no)

Politihøgskolen, Postboks 2109 Vika, 0125 Oslo

### Sammendrag

Digitale bevis betraktes gjerne som objektive og pålitelige bevis. I denne artikkelen settes søkelyset på hvor gyldig slutningen egentlig er. Vet vi egentlig nok til å kunne utelukke systematiske feil i vurderingen av noen bevistyper som f.eks. digitale bevis ved behandlingen av gjenåpningsbegjæringer? En analyse av Gjenopptakelseskommissjonens gjenåpnede saker fram til august 2019, samt et utvalg av 100 ikke gjenåpnede saker, viser at digitale bevis er tatt i betraktning i 6 av de 307 gjenåpnede sakene. Analysen av de ikke gjenåpnede sakene viser en langt større forekomst av digitale bevis, og at begrunnelsen domfelte oftest gjør gjeldende i gjenåpningsbegjæringen, er at retten har misforstått eller feilvurdert det digitale beviset.

**Nøkkelord:** justisfeil, systematiske feil, gjenopptakelseskommissjonen, dataetterforskning, digitale bevis, kvalitet, bevisbedømmelse

### Introduksjon og bakgrunn<sup>1</sup>

---

<sup>1</sup> Takk til Helene O.I. Gundhus, Johanne Yttri Dahl, Eivind Kolflaath og Inger Marie Sunde for verdifulle kommentarer til tidligere utkast av artikkelen.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegi\\_aeringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegi_aeringer_kan_vi_ute)

I en ytring i dette tidsskriftet skriver professor Ulf Stridbeck at i perioden 2004–2011 ble ca. 15 % av avsluttede saker gjenåpnet, men at andelen er i overkant av 5 % når man trekker fra utilregnelighet, domfellelse av feil person, ankesiling og feil juss.<sup>2</sup> Dette kom som et tilsvar til stortingspolitiker Jenny Klinges uttalelse om at det muligens var for få gjenåpninger i Norge. Stridbeck konkluderte med at gjenåpningsprosenten i Norge er høy sammenlignet med andre land.

I artikkelen «Prevention of Wrongful Convictions: Norwegian Legal Safeguards and the Criminal Cases Review Commission» argumenterer Stridbeck og professor Svein Magnussen for at hovedproblemet i norsk straffesakskjede *ikke er feil på systemnivå*, og trekker f.eks. fram en rekke sider ved det norske strafferettssystemet som underbygger dette, bl.a. utnevnte (og ikke valgte) dommere og påtalejurister, anklagerprinsipp (til forskjell fra inkvisitorisk prinsipp) i straffeprosessen og nøytrale rettsoppnevnte sakkyndige. De peker på at problemet med uriktige domfellelser i Norge heller knytter seg til at man ikke lykkes med å finne eller presentere bevis som ville påvirket utfallet i den opprinnelige rettssaken.<sup>3</sup>

## **Kan vi utelukke systematiske feil?**

Danmark er rammet av det de omtaler som «teledataskandalen», hvor det våren 2019 ble oppdaget feil i teledata helt tilbake til 2012.<sup>4</sup> I skrivende stund er det påvist feil i form av manglende data, feil i basestasjonsopplysninger og feil i rådata, og minst 10 700 straffesaker skal gjennomgås for å avgjøre om teledata har hatt betydning for utfallet, og om saken derfor må gjenåpnes. Mange av feilene har oppstått i programmet Raven, som dansk politi har benyttet for å innhente teledata fra de ulike teleleverandørene og konvertere dataene til ett felles format. I Norge brukes ikke dette programmet, men det fundamentale problemet med teledata deles likevel med Danmark: Kvaliteten på teledataene er dimensjonert til behovet teleleverandøren selv har, f.eks. til faktureringsformål. Det påhviler ingen krav til teleleverandørene om at dataene de lagrer, skal holde noen bestemt kvalitet. Dette har aldri vært noen hemmelighet, og utfordringene danskene nå strir med, kommer på toppen av denne

---

<sup>2</sup> Tidsskrift for strafferett 2/2018.

<sup>3</sup> Stridbeck, U. & Magnussen, P.S. (2011), «Prevention of wrongful convictions: Norwegian legal safeguards and the criminal cases review commission», *University of Cincinnati Law Review* 80, 1373.

<sup>4</sup> Se f.eks. omtale her: <https://nrkbeta.no/2019/08/23/over-10-000-rettssaker-ma-gjennomgas-etter-teledataskandale-hos-dansk-politi/>

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegjæringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegjæringer_kan_vi_ute)

usikkerheten. Det er derfor grunn til å stille spørsmål om slike bevis har «gått under radaren» i Norge på grunn av manglende kritiske spørsmål eller fravær av kritisk vurdering.

I Baneheia-saken var trafikkdata og basestasjonsopplysninger gjenstand for etterforskning, og man lyktes aldri å oppnå kontakt mellom åstedet og basestasjonen hvor domfelte Viggo Kristiansens telefon hadde slått inn på et tidspunkt som var nær opptil det man mente måtte være tidspunkt for ugjerningen.<sup>5</sup> Det som gjensto som en *teoretisk mulighet* for kontakt med basestasjonen, ble til slutt lagt til grunn som bevis for at Kristiansen hadde vært på åstedet i tiden hvor drap og voldtekt av to unge jenter ble begått, selv om sannsynligheten ifølge journalist Bjørn Olav Jahr er 0,000001 prosent.<sup>6</sup> Til sammenligning – sannsynligheten for å vinne førstepremien i lotto er 0,000019 prosent.<sup>7</sup> Andre tekniske bevis som knytter Kristiansen til åstedet, finnes angivelig ikke.

Spørsmålet jeg stiller i denne artikkelen er: Kan vi med den kunnskapen vi har i dag, slå fast at vi ikke, eller i liten grad, er rammet av systematiske feil i norsk straffesakskjede? Kan det være at noen bevis blir betraktet som mer objektive og pålitelige enn andre, og at de faktiske usikkerhetsmomentene systematisk ikke blir undersøkt eller tatt i betraktning? Jeg har forsøkt å kaste lys over dette ved å undersøke hvordan en type bevis – nærmere bestemt *digitale bevis* – blir behandlet i Gjenopptakelseskomisjonens saker. Jeg vil underveis trekke fram noen eksempler fra saker hvor digitale bevis har blitt gjort gjeldende i domfeltes gjenåpningsbegjæringer.

Min definisjon av digitale bevis bygger på professor Ørnulf Øyens<sup>8</sup> mer generelle definisjon av bevis: Digitale bevis forstås som digitalt lagret informasjon som direkte eller indirekte kaster lys over sakens bevistemaer, påliteligheten av slik informasjon eller troverdigheten til informasjonskilden. Digitale bevis kan derfor være innholdsdata (bilder, film, dokumenter, kommunikasjon) eller metadata (data om dataene, som f.eks. tidsstempler, lokasjonsdata etc.).<sup>9</sup>

---

<sup>5</sup> LA-2001-980-1

<sup>6</sup> Jahr, B.O. (2018), *Drapene i Baneheia. To historier, en sannhet*, Oslo: Pitch forlag, s. 342.

<sup>7</sup> Ibid.

<sup>8</sup> Øyen, Ø. (2013), «Rettens kontroll med bevisføringens omfang i straffesaker», *Tidsskrift for strafferett* 13(02), s. 199–236, s. 211.

<sup>9</sup> Definisjonen og analysen som presenteres i denne artikkelen, avgrenser mot kommunikasjon som er innhentet gjennom kommunikasjonskontroll. Bevis innhentet på denne måten regnes ikke for å falle inn under definisjonen av digitalt bevis, selv om opptakene lagres digitalt.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegi\\_aeringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegi_aeringer_kan_vi_ute)

Formålet med artikkelen er å begrunne behovet for en kvalitativ gjennomgang av Gjenopptakelseskommisjonens saker, som kan gi svar på om det i Norge – i likhet med flere andre land – kan finnes en sammenheng mellom justisfeil og enkelte typer bevis. Formålet er således ikke å vurdere eller kritisere Gjenopptakelseskommisjonens avgjørelser.

Jeg gjør først rede for noen sentrale begreper og relevant forskning, og beskriver så tidligere evalueringer av Gjenopptakelseskommisjonens saker og arbeid. Så presenteres metoden som er benyttet til denne studien, etterfulgt av en presentasjon og diskusjon av resultatet. Her gjør jeg først rede for de gjenåpnede sakene hvor digitale bevis ser ut til å ha hatt betydning for gjenåpningen. Jeg tar så for meg de ikke gjenåpnede sakene, og gjør rede for hvilke typer digitale bevis som oftest er involvert, og fellestrekk domfeltes argumentasjon for gjenåpning. Avslutningsvis diskuterer jeg behandlingen av digitale bevis i straffesakskjeden opp imot kvalitet og kompetanse, og konkluderer med at vi mangler kunnskap om sammenhengen mellom justisfeil og bevistyper i norske straffesaker.

## **Digitale bevis og andre bevistyper som årsak eller medvirkende årsak til justisfeil**

Digitale bevis inngår i de fleste typer straffesaker og er ofte av helt avgjørende betydning for å bevise et hendelsesforløp. I mitt doktorgradsarbeid om dataetterforskning og digitale bevis ser jeg bl.a. på menneskelige feil i dataetterforskningsprosessen. Jeg undersøker hvorvidt databaseslag blir behandlet på en måte som ivaretar kvalitet, og hvorvidt bevisene blir presentert i tråd med bevisenes relevans og pålitelighet. Som et ledd i dette arbeidet har jeg forsøkt å få en bedre oversikt over i hvor stor grad digitale bevis er årsak eller medvirkende årsak til feilaktige domfellelser.

Når begrepet «justisfeil» benyttes, så henviser det til begrepet *errors of justice* som omfatter ethvert avvik av sakens optimale utfall.<sup>10</sup> Justisfeil kan føre til uriktige domfellelser og dermed få alvorlige konsekvenser i form av at skyldige går fri eller at uskyldige blir dømt.

Flere kriminaltekniske disipliner under samlebetegnelsen *forensic science* har vært satt under press etter tallrike avsløringer av saker hvor uskyldige er dømt for alvorlige straffbare forhold. I USA har Innocence Project over tid arbeidet med å få gjenåpnet slike saker. I arbeidet med å

---

<sup>10</sup> Forst, B. (2004), *Errors of Justice: Nature, Sources and Remedies*, Cambridge: Cambridge University Press, s. 4. Se også Rachlew, A. (2009), *Justisfeil ved politiets etterforskning: Noen eksempler og forskningsbaserte mottiltak* (doktorgradsavhandling), Oslo: Det juridiske fakultet, Universitetet i Oslo.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegieringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegieringer_kan_vi_ute)

identifisere de bakenforliggende årsakene har man avdekket at kriminaltekniske bevis har vært årsak eller medvirkende årsak i 45 % av de feilaktige dommene som er blitt oppklart gjennom DNA-bevis.<sup>11</sup> Ifølge National Registry of Exonerations er feilaktige eller villedende kriminaltekniske bevis årsak eller medvirkende årsak i 23 % av tilfellene hvor uskyldige ble dømt, når også andre bevis enn DNA er grunnlaget for frifinnelsen.<sup>12</sup> En gjennomgang av 71 feilaktige domfellelser i Australia fra 1922 til 2015 viste at andelen her var 31 %.<sup>13</sup> I en omfattende studie av 235 saker gjenåpnet etter anke i England og Wales ble kriminaltekniske bevis identifisert som direkte eller medvirkende årsak til feilaktig dom i 32 % av sakene.<sup>14</sup> De kriminaltekniske bevisene kom fra mange ulike kategorier, som DNA, dyreblod, dokumenter, digitale bevis, narkotika, fingeravtrykk, fottøyavtrykk, glass, håndskrift, medisin, våpen og patronavfyringsrester. I disse studiene har man gravd dypere i årsakene til feil, og gjort noen viktige funn: Noen ganger knytter feilene seg til ikke-testede eller upålitelige kriminaltekniske metoder. Men feilen ligger ofte ikke i det bevisende objekt, men heller i *presentasjonen* av beviset, som kan lide av overdrivelser av bevisverdi og sannsynlighet.<sup>15</sup>

I forordet i sin bok *Åsted – på innsiden av Kripas* sier den erfarne kriminalteknikeren Håvard H. Arntzen at kriminalteknikerne jobber på vegne av de «tause vitnene», og at disse forteller sannheten om hva som skjedde, siden «de tause vitnene lyver aldri».<sup>16</sup> Det er lett å si seg enig med Arntzen i at de tause vitnene aldri lyver, men det er simpelthen fordi vitnene *er tause*. Når de tause vitner ikke kan fortelle, så kan de i alle fall ikke fortelle «sannheten». Den må formidles av en kriminaltekniker, dataetterforsker eller sakkyndig.

---

<sup>11</sup> Innocence Project. Tilgjengelig på <https://www.innocenceproject.org/overturning-wrongful-convictions-involving-flawed-forensics/> (besøkt 5.9.2019).

<sup>12</sup> National Registry of Exonerations (2015), *The First 1600 exonerations*. Tilgjengelig på [https://www.law.umich.edu/special/exoneration/Documents/1600\\_Exonerations.pdf](https://www.law.umich.edu/special/exoneration/Documents/1600_Exonerations.pdf) (besøkt 5.9.2019). Tabellen på s. 11 viser at det er en variasjon innenfor lovbruddskategoriene fra 5 til 32 %.

<sup>13</sup> Dioso-Vila, R. (2012), «Without legal obligation: Compensating the wrongfully convicted in Australia», *Albany Law Review* 75(3), s. 1329-1372, og Dioso-Vila, R. (2015), «A repository of wrongful convictions in Australia: First steps toward estimating prevalence and causal contributing factors», *Flinders Law Journal* 17, s. 163–202.

<sup>14</sup> Smit, N.M., Morgan, R.M. & Lagnado, D.A. (2018), «A systematic analysis of misleading evidence in unsafe rulings in England and Wales», *Science & Justice* 58(2), s. 128–137.

<sup>15</sup> Dioso-Vila, R. (2012), «Without legal obligation: Compensating the wrongfully convicted in Australia», *Albany Law Review* 75(3), s. 1329-1372, og Dioso-Vila, R. (2015), «A repository of wrongful convictions in Australia: First steps toward estimating prevalence and causal contributing factors», *Flinders Law Journal* 17, s. 163–202., og Smit, N.M., Morgan, R.M. & Lagnado, D.A. (2018), «A systematic analysis of misleading evidence in unsafe rulings in England and Wales», *Science & Justice* 58(2), s. 128–137. Se også Garrett, B.L. (2011), *Convicting the innocent*, Harvard University Press, og Garrett, B.L. & Neufeld, P.J. (2009), «Invalid forensic science testimony and wrongful convictions», *Virginia Law Review*, s. 1–97.

<sup>16</sup> Arntzen, H.H. (2018). *Åsted. På innsiden av Kripas. En kriminalteknikers jakt på sannheten*, Oslo: Kagge, s. 9.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegi\\_aeringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegi_aeringer_kan_vi_ute)

Det er svært få eller kanskje ingen bevis som kan presenteres for retten uten at de er beheftet med en eller annen grad av usikkerhet. Hvilken verdi bevisene skal tillegges, bør henge sammen med hvorvidt etterforskningen er gjennomført av kompetent personell, med god og vitenskapelig forankret metodikk, og hvorvidt beviset blir dokumentert og presentert i tråd med bevisets relevans og pålitelighet.

Beviset – i form av et dataspor, en bloddråpe eller en sotflekk – har liten bevisverdi i seg selv før det blir fortolket, beskrevet og plassert i en kontekst av et menneske. Først da kan retten danne seg en oppfatning av beviset og gjøre sin egen vurdering av relevans og pålitelighet. Det er derfor større kvalitative likheter mellom vitnebevis og kriminaltekniske bevis i forhold til objektivitet enn man intuitivt kanskje kan tenke seg. Antakelsen om et objektivt og pålitelig bevis kan oppstå ved at man glemmer eller feilvurderer den menneskelige faktors betydning for fortolkningen og formidlingen av beviset.

Antakelsen om bevisenes objektivitet og pålitelighet kan også henge sammen med mangel på *vitenskapelig kapital*.<sup>17</sup> Vitenskapelig kapital (eng.: «science capital») kan forstås som et mål på en persons erfaring med og kunnskap om vitenskap. Denne betinger evnen til å stille spørsmål om det vitenskapelige fundamentet beviset bygger på og metoden som er benyttet for å produsere beviset. Men forutsetningen om objektivitet og pålitelighet kan også henge sammen med mangel på det man kan kalle *digital kapital*, altså en persons erfaring med og kunnskap om informasjons- og kommunikasjonsteknologi.<sup>18</sup> Denne vil på samme måte som vitenskapelig kapital betinge evnen til å utfordre de digitale bevisenes betydning og pålitelighet, slik at feil og usikkerhetsmomenter kan bli belyst.

## **Evalueringer av Gjenopptakelseskommisjonens saker og arbeid**

For å besvare spørsmålet jeg stiller i denne artikkelen, har jeg lest evalueringer av Gjenopptakelseskommisjonens saker og arbeid og søkt etter svar i dens arkiv på Lovdata. Det er gjort evalueringer av Gjenopptakelseskommisjonens saker for årene 2004–2009<sup>19</sup> og for

---

<sup>17</sup> Dahl, J.Y. (2012), «Overdreven tro på og tillit til bruk av DNA-bevis i strafferettspleien?», *Sosiologi i dag*, 42(2), s. 29–47, og Dahl, J.Y. (2015), «DNA-beviset i retten – de profesjonelle aktørene i rettsvesenets erfaringer og oppfatninger», *Tidsskrift for Rettsvitenskap* 128(3–4), s. 364–386.

<sup>18</sup> Bakken, S.A. & Demant, J. (2019), «Narkotikamarkedene på nett. En begrepsutvikling av digital kapital», *Norsk sosiologisk tidsskrift* 3(03), s. 209–227.

<sup>19</sup> Dullum, J. (2010), *Justisfeil i straffesaker. En analyse av saker behandlet av Kommisjonen for gjenopptakelse av straffesaker (Gjenopptakelseskommisjonen) i perioden 2004–2009*, Oslo: Institutt for kriminologi og retts sosiologi, Universitetet i Oslo.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegj\\_aeringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegj_aeringer_kan_vi_ute)

årene 2004–2011.<sup>20</sup> Gjenopptakelseskommissjonens avgjørelser er tilgjengelig i referats form på deres hjemmesider og i mer utfyllende form på Lovdata. Jeg kjenner ikke til noen fullstendig gjennomgang som inkluderer saker etter 2011.

Dr. Jane Dullum gjennomførte i 2009 en evaluering av 120 av Gjenopptakelseskommissjonens saker fra årene 2004 til mai 2009. 68 saker var gjenåpnede saker, og 52 var tilfeldig utvalgte saker blant dem som ikke var blitt tatt til følge. Formålet var å kartlegge realitetsbehandlede saker for å se etter mønstre i sakstyper, informasjon om dem som søkte gjenåpning, gjenåpningsgrunnlag, dokumentasjon og utfall. I dette arbeidet stilte Dullum en rekke spørsmål, bl.a. om på hvilket grunnlag var sakene gjenåpnet, hva partenes anførsler var, om noen feil ble påberopt oftere enn andre, om noen feil oftere endte med gjenåpning, og om det var anførsler fra domfeltes side som sjelden eller aldri førte til gjenåpning.

Etter gjennomgang av gjenåpninger etter strpl. § 391 nr. 3 (nye omstendigheter/nye bevis) kom Dullum fram til at en stor del av sakene handlet om tilregnelighet og nye sakkyndigerklæringer, men hun så ingen klare mønstre i de gjenåpnede sakene utover dette. I sakene som ble avvist, var det vanligst at domfelte anførte nye bevis / nye omstendigheter som grunnlag for gjenåpning. Dullum fant ingen fellestrekk eller mønstre i bevisene/omstendighetene som ble anført av domfelte, men trakk fram at det er oppnevnt sakkyndige i færre av sakene som ikke er tatt til følge, enn i sakene som er gjenåpnet av kommisjonen.

Arbeidsgruppen for etterkontroll av Gjenopptakelseskommissjonen, under ledelse av Ulf Stridbeck, gjennomgikk samtlige realitetsbehandlede gjenåpningsbegjæringer for perioden 2004–2011 (428 begjæringer) med sikte på å undersøke den statistiske forekomsten av ulike forhold av interesse for evalueringen.<sup>21</sup> Arbeidsgruppen gjennomførte ingen systematisk gjennomgang og evaluering av kommisjonens arbeid i enkeltsaker. Parallelt med dette arbeidet gjennomførte Stridbeck og psykologspesialist Pål Grøndahl en studie av 49

---

<sup>20</sup> Justis- og beredskapsdepartementet (2012), *Etterkontroll av kommisjonen for gjenopptakelse av straffesaker. Rapport fra arbeidsgruppe for etterkontroll av Gjenopptakelseskommissjonen*. Justis- og beredskapsdepartementet.

<sup>21</sup> Ibid..



Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegjæringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegjæringer_kan_vi_ute)

tilregnelighetssaker, derav 29 gjenåpnet og 20 ikke gjenåpnet av Gjenopptakelseskommisjonen.<sup>22</sup>

Det er – så langt jeg kan se – derfor ikke blitt foretatt noen generell kvalitativ gjennomgang av enkeltsaker behandlet av Gjenopptakelseskommisjonen som inkluderer årene etter mai 2009. Kun et svært begrenset antall av ikke gjenåpnede saker har vært gjenstand for systematisk analyse.

## **Metode – kvalitativ analyse av Gjenopptakelseskommisjonens saker**

Samtlige av Gjenopptakelseskommisjonens 307 saker behandlet fra opprettelsen i 2004 til og med august 2019 ble gjennomlest, for å identifisere saker hvor digitale bevis hadde betydning for gjenåpningen.

Et utvalg av 100 ikke gjenåpnede saker ble også gjennomgått, for å se på hvilke digitale bevis domfelte henviserte til, og hvilke begrunnelser domfelte gjorde gjeldende i relasjon til disse bevisene i gjenåpningsbegjæringen. Utvalget ble gjort ved søk på nøkkelord blant de 1400 sakene som på det tidspunkt lå på Lovdata. Nøkkelordene «internet», «datamaskin», «mobil», «pc», «chat» og «overvåkningsvideo» resulterte i 273 treff på ikke gjenåpnede saker.<sup>23</sup> Fra dette utvalget ble så 100 tilfeldige saker valgt ut via *Random Number Generator*.<sup>24</sup> Utvalget ble kontrollert for duplikater siden flere begjærer gjenåpning flere ganger. Gjennomgang av de 100 sakene viste at 35 av sakene inneholdt falske positive, som f.eks. at en mobil er brukt som slagvåpen, eller at saken gjelder tyveri av en datamaskin. I de øvrige 65 sakene var digitale bevis hele eller deler av bakgrunnen for begjæringen om gjenåpning, og dannet grunnlag for de videre analysene.

For å identifisere og kategorisere begrunnelsene som domfelte anførte, ble en kvalitativ innholdsanalyse gjennomført. Først ble begrunnelsene identifisert, og så analysert med tanke på fellestrekk. Dette er en prosess som innebærer noe fortolkning, siden både omtalen av bevisene og begrunnelsene fra de domfelte varierer.

---

<sup>22</sup> Stridbeck, U. & Grøndahl, P. (2012), «Utilregnelighet 'under radaren'? Gjenopptakelseskommisjonens vurdering av saker med tvil om tilregnelighet – en pilotstudie», *Lov og Rett* 51(05), s. 301–312.

<sup>23</sup> Søk med åpen endelse, men ikke utvidet med synonymer.

<sup>24</sup> Versjon 5.4, utviklet av Nicholas Dean, lastet ned fra Apple's App Store.

## Resultat og drøfting

### Digitale bevis i gjenåpnede saker

Siden Stridbecks arbeidsgruppe ikke gikk i dybden på *hvilke bevistyper* som har hatt betydning for gjenåpning eller avvisning, og Dullums undersøkelse kun omfattet noen få saker, fant jeg ingen svar på spørsmålet om hvorvidt digitale bevis har hatt betydning i disse sakene. Ved gjennomgangen av de 307 gjenåpnede sakene fra 2004 til og med august 2019 fant jeg kun 6 saker hvor digitale bevis så ut til å ha hatt betydning for gjenåpningen. 4 av disse sakene var gjenåpnet til gunst for siktede, og 2 til ugunst. Kun to av disse var avgjort da Dullums og Stridbecks arbeidsgruppe gjorde sine undersøkelser. En oppsummering av disse sakene og utfallet etter gjenåpningen følger nedenfor:

#### Gjenåpning til gunst, strpl. § 391

- GK-2017-147: *Mishandling i nære relasjoner*  
En mann ble dømt for å ha mishandlet og voldtatt sin kone og mishandlet to døtre. Det ble avgitt nye forklaringer fra de fornærmede til gunst for domfelte. Nye tekstmeldinger og chat, som støttet at den dømte faren ikke kontrollerte og mishandlet døtrene sine, ble overlevert kommisjonen. Saken endte med frifinnelse for de gjenåpnede postene etter ny behandling i Agder lagmannsrett.<sup>25</sup>
- GK-2017-138: *Tyveri av lommebok med bankkort og 800 kr fra en eldre dame*  
Gjerningspersonen som begikk tyveriet, ble identifisert på bakgrunn av overvåkningsfilm. Det ble ikke sikret andre bevis i saken, og politiet gjennomførte ikke sikring av informasjon som understøttet domfeltes alibi. Denne tredje gjenåpningsbegjæringen førte til gjenåpning til gunst for domfelte, og saken endte med frifinnelse etter ny behandling i Eidsivating lagmannsrett.<sup>26</sup>
- GK-2013-106: *Voldtekt av 15 år gammel gutt*  
Fornærmede våknet i domfeltes leilighet med tape på hender og føtter. Funn av bilder på domfeltes mobil indikerte seksuelt misbruk av fornærmede. Domfelte hevdet han

---

<sup>25</sup> LA-2018-181018.

<sup>26</sup> LE-2019-24145.

var uskyldig, og at misbruket var gjennomført av andre. Han hevdet også at andre hadde fotografert fornærmede med domfeltes mobil. Etter beslutning om gjenåpning til gunst for domfelte ble saken sendt til Frostating lagmannsrett for ny behandling, men etter at domfelte for andre gang ikke møtte til rettsbehandling uten lovlig forfall, ble saken avvist.<sup>27</sup>

- GK-2004-89: *Narkotika, innførsel av 9,5 kg heroin*

Det ble inngitt en ny forklaring hvor domfeltes bror erkjente at det var han som hadde begått den straffbare handlingen. Trafikkdata i saken understøttet også den nye forklaringen. Saken ble gjenåpnet til gunst for domfelte. I ny straffesak ble han dømt igjen,<sup>28</sup> og nye gjenåpningsbegjæringer (GK-2007-122, GK-2013-21) ble ikke tatt til følge.

### **Gjenåpning til ugunst, strpl. § 393**

- GK-2019-34: *Seksuelle overgrep / besittelse av bilder av seksuelle overgrep mot barn*

En mann ble dømt for seksuell handling med et barn under 16 år. To år senere forklarte to som tidligere var avhørt som vitner, at mannen også hadde begått slike handlinger mot dem. Det ble også gjort funn av overgrepbilder på mannens pc under ransaking. Saken ble gjenåpnet til gunst for domfelte, men er ikke avgjort.<sup>29</sup>

- GK-2009-90: *Narkotika, oppbevaring av 29 kg hasj*

Nye opplysninger, i form av vitneforklaring og opplysninger fra kommunikasjonskontroll, gjorde det utvilsomt at siktede var skyldig i å ha oppbevart narkotika – som han var frifunnet for. Andre bevis i saken, bl.a. trafikkdata, understøttet også de nye opplysningene.<sup>30</sup> Saken ble gjenåpnet til ugunst for domfelte.

---

<sup>27</sup> 14-011184AST-FROS.

<sup>28</sup> LE-2005-97694.

<sup>29</sup> Pr. oktober 2019.

<sup>30</sup> Utfallet etter gjenåpning framgår ikke i Lovdata.

Av de 307 gjenåpnede sakene omhandlet altså kun 6 saker databevis, hvorav 4 av disse ble gjenåpnet til gunst for domfelte. De digitale bevisene i disse sakene har blitt gransket i ulik grad av Gjenopptakelseskommisjonen.

I saken som omhandlet voldtekt av en 15 år gammel gutt (GK-2013-106), ble domfeltes mobiltelefon gjenstand for nye grundige undersøkelser. Gjenopptakelseskommisjonen engasjerte Ibas<sup>31</sup> for å undersøke hvorvidt den domfelte mannens forklaring om at noen andre hadde tatt bildene av fornærmede, kunne stemme. Gjengivelsen av Ibas' undersøkelser vitner om grundige og godt dokumenterte undersøkelser, med et resultat som ikke understøttet domfeltes påstand. Databeviset ble derfor ikke tillagt vekt for kommisjonens avgjørelse om gjenåpning. Gjenåpningen ble imidlertid begrunnet i ny dokumentasjon som ga grunnlag for tvil om domfelte framkalte bevisstløs tilstand hos fornærmede.

I tyverisaken (GK-2017-138) gikk det 10 år fra pågripelsen i 2009 til den domfelte kvinnen ble frikjent mai 2019. Det framkommer ikke av dokumentasjonen at det er innhentet noen form for ekspertise for å vurdere opptaket fra overvåkningskameraet, verken under etterforskningen, under rettsprosessen eller ved Gjenopptakelseskommisjonens behandlinger av saken. Ut fra dokumentasjonen av sakens gang kan man lese at saken først ble behandlet i Sør-Trøndelag byrett, hvorpå den ble anket til Frostating lagmannsrett.<sup>32</sup> Domfelte anket til Høyesterett, men anken ble nektet fremmet. Så begjærte den domfelte kvinnen gjenåpning, og fikk avslag i 2015 og 2017. På tredje forsøk, i 2018, besluttet Gjenopptakelseskommisjonen gjenåpning. Saken ble behandlet i Eidsivating lagmannsrett i mai 2019, og kvinnen ble frifunnet for tyveriet.<sup>33</sup>

### **Digitale bevis i ikke gjenåpnede saker**

Det var altså svært få av de gjenåpnede sakene hvor digitale bevis hadde betydning for beslutningen. De 6 sakene med digitale bevis utgjør 1,9 % av gjenåpnede sakene. Blant sakene som ikke har ført til gjenåpning, fant jeg at det i *domfeltes begrunnelse* for gjenåpning påberopes feil eller usikkerhetsmomenter ved digitale bevis i langt flere saker.

Ut fra undersøkelsesmetoden kan man imidlertid ikke gi et sikkert forholdstall på hvor mange av de ikke gjenåpnede sakene som inneholdt databevis. Det ble gjennomført søk etter

---

<sup>31</sup> Ibas Ontrack AS er et privat firma som gjennomfører datatekniske undersøkelser på oppdrag.

<sup>32</sup> TSTRO-2009-172386, LF-2010-40043.

<sup>33</sup> LE-2019-24145.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegjæringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegjæringer_kan_vi_ute)

databasevis, og disse ga treff i 273 ikke gjenåpnede saker som er tilgjengelig på Lovdata.<sup>34</sup> Av de 273 sakene ble et utvalg på 100 saker undersøkt, og etter siling av falske positive og duplikater gjensto 65 saker i utvalget. Med forbehold om at en generalisering fra dette utvalget er beheftet med usikkerhetsmomenter, kan man anta at minst 177 av de 273 sakene (65 %) vil omhandle digitale bevis. Det utgjør altså 12,6 % av de 1400 sakene som er tilgjengelig på Lovdata.

Undersøkelsene viser at domfelte svært sjelden får positivt svar på sin gjenåpningsbegjæring hvor digitale bevis inngår som hele eller deler av begrunnelsen. Det lave antallet gjenåpnede saker til gunst for domfelte, hvor databasevis har hatt betydning, får meg til å stille spørsmål om feil og usikkerhetsmomenter omkring digitale bevis og presentasjonen av disse «går under radaren» i større grad enn andre bevis.

### Typer digitale bevis

Det er et stort spenn i alvorlighetsgrad blant de 65 sakene. De spenner fra trusler og mindre vinningsforbrytelser til grove voldtekter og overlagte drap. I de 65 sakene fantes også stor variasjon i type digitale bevis som ble gjort gjeldende av domfelte. For å kunne si noe om forekomsten av de ulike bevisene ble de samlet i kategorier på bakgrunn av fellestrekk.

Antall N=65	Type bevis
27	Kommunikasjon på e-post, SMS, chat, sosiale medier
14	Innhold på datamaskin (bilder, video, dokumenter)
14	Teledata (trafikkdata og basestasjonsopplysninger)
13	Innhold på mobiltelefon (bilder, video, kontakter)
8	Lydopptak
4	Videoovervåking, bilder eller film
2	Annet (innhold på web-sider, digitale bilder)

Tabell 1: Kategorier av digitale bevis i de 65 analyserte sakene som ikke var gjenåpnet.

<sup>34</sup> 1400 saker var tilgjengelig på Lovdata på tidspunktet for undersøkelsene.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegjæringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegjæringer_kan_vi_ute)

Skiller man kommunikasjon fra annen type innhold, er dette den kategorien digitale bevis som går igjen oftest. Trafikkdata, innhold på mobil og innhold på pc opptrer så å si like ofte. Slår man imidlertid sammen innhold (bilder, video, dokumenter og kontaktopplysninger) fra både mobil og pc, opptrer denne kategorien like hyppig som kommunikasjon. Man kan derfor si at de vanligste typer digitale bevis ser ut til å være kommunikasjon, innhold på pc/mobiltelefon og teledata. Dette gir et inntrykk av hvilke typer digitale bevis domfelte oftest trekker fram, men det er imidlertid viktig å huske at utvalget er trukket ut på bakgrunn av søkeord. Andre eller flere søkeord kunne endret eller nyansert dette bildet.

Selv om det er stor variasjon i typer digitale bevis i gjenåpningsbegjæringene, vil de mest vanlige bevisene i utgangspunktet trolig ikke oppleves som vanskelige å forstå med henblikk på relevans for straffesaken. De vil være gjenkjennelige, som bilder, tekstmeldinger, og dokumenter. I mange tilfeller vil imidlertid relevansvurderingen avhenge av at man også forstår metadataene (data om data), som f.eks. hva en IP-adresse faktisk forteller, hva tidsstemplet for *last accessed* innebærer av handlinger, eller hvor nøyaktig posisjon man kan slutte ut fra en basestasjonsopplysning. Når det gjelder pålitelighetsvurderingen, kan bevisene være beheftet med både *tekniske feil*<sup>35</sup> og feil under behandlingen fra sikring til presentasjon – såkalt *ikke-tekniske feil*.<sup>36</sup> Man kan derfor si at det som kanskje heller er fellestrekket ved disse bevisene, er at de utgjør et stort mangfold med hensyn til kompleksitet som knytter seg til pålitelighetsvurderingen. Spørsmålet man kan stille seg, er om de profesjonelle aktørene i retten har tilstrekkelig kunnskap til å utfordre relevans og påliteligheten av bevisene, eller om de legger vurderingen til den som presenterer beviset, til grunn. I norske rettssaler presenteres digitale bevis av alt fra den nyutdannede politibetjenten til den erfarne og kompetente eksperten. Hvem som tillegges vekt som ekspert, kan nok derfor også variere.

## **Begrunnelser fra de domfelte**

Analysen av begrunnelsene i de domfeltes gjenåpningsbegjæringene resulterte i seks ulike kategorier. I noen tilfeller omhandlet gjenåpningsbegjæringen flere ulike bevis, eller det var

---

<sup>35</sup> Casey, E. (2002), «Error, uncertainty, and loss in digital evidence», *International Journal of Digital Evidence* 1(2), s. 1–45.

<sup>36</sup> Sunde, N. & Dror, I.E. (2019), «Cognitive and Human Factors in Digital Forensics. Problems, Challenges and the Way Forward», *Digital Investigation* 29, s. 101–108.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegjæringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegjæringer_kan_vi_ute)

flere begrunnelser knyttet til det enkelte bevis. Det totale antallet begrunnelser fordelt på disse kategoriene er derfor større enn antallet saker de er hentet fra.

Antall N=65	Begrunnelse
26	Retten har misforstått eller feilvurdert det digitale beviset.
24	Relevante digitale bevis til gunst for siktede eller som belyser fornærmedes (manglende) troverdighet, er ikke innhentet/sikret.
14	Domfelte har selv innhentet/sikret relevante digitale bevis som er overlevert til Gjenopptakelseskommissjonen.
10	Domfelte er ikke riktig person, andre har brukt den digitale enheten, eller det skjedde utenfor domfeltes kontroll (f.eks. bruk av mobil/pc, nedlasting fra internett).
2	Politiet manipulerte det digitale beviset eller løy om det i retten.
1	Feil i rettsprosessen.

Tabell 2: Kategorier av begrunnelser som omhandlet digitale bevis i de 65 ikke-analyserte sakene som ikke var gjenåpnet.

I det følgende vil kategoriene av begrunnelser diskuteres i lys av teori, tidligere forskning og eksempler fra utvalget. Eksempelene er alle hentet fra dokumentasjonen på Lovdata.

### **Retten har misforstått/feilvurdert beviset**

Ser man hen til de domfeltes begrunnelser, er det også grunn til bekymring. Analysen av domfeltes begrunnelse for gjenåpning viste at det domfelte oftest anfører er at det digitale beviset er misforstått eller feilvurdert av retten. Det faktum at det kan være lett å forstå innholdet i et digitalt bevis, utelukker ikke at det kan herske ulike oppfatninger om betydningen av innholdet. Ulike fortolkninger kan også lett oppstå dersom informasjonen tas ut av sin opprinnelige kontekst. Et eksempel på at retten ifølge domfelte har misforstått eller feilvurdert det digitale beviset, er hentet fra sak GK-2013-11:

Endelig pekes det i begjæringen på at trafikkdata fra saken viser kontakt mellom G og V2s mobiltelefoner. A har forklart at V2 satt i samme bil som domfelte og ham selv.

Ettersom G og V2 har hatt telefonkontakt i det aktuelle tidsrommet, kan de ikke ha sittet i samme bil.<sup>37</sup>

Nå er det ikke slik at man skal slutte at det er gjort feil kun fordi den domfelte hevder det. En domfelt kan ha mye å tjene på å få saken sin gjenåpnet, eller han/hun kan selv ha misforstått hvilke bevis som faktisk ble sikret under etterforskningen, eller ført som bevis i retten. Men det er likevel grunn til å gå inn i begrunnelsene, og deres fellestrekk, for å se om de kan peke i retning av mulige systematiske feil.

Dersom det er riktig, som mange av de domfelte hevder, at retten i mange tilfeller ikke har forstått hva beviset innebærer og beviset har hatt avgjørende betydning for utfallet, kan det ha medført uriktige avgjørelser av skyldspørsmålet eller straffeutmålingen. Her kan vi se hen til forskningen fra England og Wales, hvor man avdekket at justisfeil hang sammen med hvordan beviset ble presentert i retten, hvor verdien eller sannsynligheten av beviset ble overdrevet. I denne undersøkelsen ble det også påvist feil ved digitale bevis.<sup>38</sup> Dette var f.eks. bevis fra SIM-kort, overvåkingsvideo, innhold fra internettside og innhold på DVD-plate.<sup>39</sup> Den engelske saken med overvåkingsvideo har noen likhetstrekk med den saken som omtales i denne artikkelen (GK-2017-138). Under etterforskningen av et ran hadde en ekspert («senior forensic consultant») gjenkjent en person på overvåkingskamera, men uttrykt usikkerhet omkring identifiseringen i rapporten. Denne usikkerheten ble ikke formidlet i retten, hvor eksperten formidlet en sikker identifisering av siktede. I ankeforhandlingen ble konklusjonsgraden i rapporten kjent, og usikkerheten rundt identifiseringen førte til at tiltalte ble frikjent.

Vi må derfor stille oss spørsmålet om de profesjonelle aktørene i retten, herunder dommer, aktor og forsvarer, har tilstrekkelig kunnskap i form av digital og vitenskapelig kapital til å forstå de digitale bevisenes mening eller betydning. Tilstrekkelig digital og vitenskapelig kapital innebærer også kunnskap nok til å utfordre de digitale bevisene ved å stille relevante spørsmål om deres relevans og pålitelighet, om troverdigheten til den som har utført undersøkelsene, og – ikke minst – til å nyttiggjøre seg svaret.

---

<sup>37</sup> [https://lovdata.no/pro/#document/GK/avgjorelse/gk-2013-11/KAPITTEL\\_1-3](https://lovdata.no/pro/#document/GK/avgjorelse/gk-2013-11/KAPITTEL_1-3) (besøkt 10.9.2019).

<sup>38</sup> Smit, N.M., Morgan, R.M. & Lagnado, D.A. (2018), «A systematic analysis of misleading evidence in unsafe rulings in England and Wales», *Science & Justice* 58(2), s. 128–137.

<sup>39</sup> E-postkommunikasjon med N. Smit, 5. april 2018.



## **Relevante bevis til gunst for domfelte eller ugunst for fornærmede er ikke sikret**

Analysen viser at mange av de domfelte klager over en ensidig etterforskning. Den nest hyppigste kategorien er hvor domfelte anfører at relevante bevis til gunst for domfelte, eller som kan belyse fornærmedes (manglende) troverdighet, ikke er innhentet eller sikret. Det følgende fra sak GK-2009-79 er et eksempel på at relevante digitale bevis til gunst for siktede, eller som belyser fornærmedes troverdighet, ifølge forsvarerne ikke er innhentet /sikret.

Forsvarerne har søkt å finne opplysninger som kan svekke den fornærmedes troverdighet eller øke de domfelte troverdighet. Det anføres at det burde vært innhentet teledata fra fornærmedes mobiltelefon, idet dette kunne belyst hvorvidt hennes forklaring var korrekt.<sup>40</sup>

Professor Eivind Kolflaath gjorde en studie av bevisvurderingen i norsk rett og overvar mer enn 100 domskonferanser i årene 2005–2009, noe som resulterte i boken *Bevisbedømmelse i praksis*. Han la merke til det han omtaler som «presumsjoner» i bevisbedømmelsen, altså det vi gjerne bare legger til grunn. Han påpeker: «I fraværet av motindikasjoner vil presumsjonen fortrenge vurderingen.»<sup>41</sup> Fraværet av motindikasjoner er problematisk dersom de ikke er forsøkt identifisert eller undersøkt.

Digitale bevis er flyktige og endres eller slettes raskt. Dersom det er riktig som mange av de domfelte hevder, at relevante bevis ofte ikke er innhentet eller sikret, kan dette derfor være årsak til uopprettelige feil, ved at slike motindikasjoner – som kanskje en gang fantes – nå er borte. Her er det først og fremst naturlig å rette søkelyset mot etterforskningen og spørre seg om politiet har oppfylt sine forpliktelser til å etterforske med tilstrekkelig kvalitet, herunder om etterforskningen har vært tilstrekkelig objektiv, og om uskyldspresumsjonen ble ivaretatt. Slike feil kan forplante seg gjennom hele straffesakskjeden dersom det ikke finnes kompetanse til å avdekke feilen.

## **Domfelte har selv sikret bevis**

---

<sup>40</sup> <https://lovdata.no/pro/#document/GK/avgjorelse/gk-2009-79/premiss> (besøkt 10.9.2019).

<sup>41</sup> Kolflaath, E. (2013), *Bevisbedømmelse i praksis*, Bergen: Fagbokforlaget, s. 86.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegjæringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegjæringer_kan_vi_ute)

I flere av de undersøkte sakene har domfelte selv framskaffet nye bevis, og dette begrunnes i at politiet har etterforsket for ensidig og/eller at retten har feiltolket bevis. Dette sitatet er hentet fra sak GK-2015-113 hvor domfelte selv har sikret digitale bevis, som ble levert sammen med gjenåpningsbegjæringen:

På forespørsel fra domfelte 29. september 2014 ble hans mobiltelefon igjen sikret av politiet. Den ble avlest og det ble funnet slettede meldinger, men ikke fra tidsrommet 31. mars til 25. april 2013. Tre år senere ble kopier av CD-er utlevert domfeltes tidligere forsvarer. Domfelte greide i fengselet å rekonstruere flere hundre tekstmeldinger. Nærmere 500 er mellom D og domfelte. Det ble avdekket totalt 247 ulike chatter/samtaler der deltakeren i den ene het [nummer], og deltakeren i en annen het D. Med andre ord kunne politiet ha fått treff både på dette navnet, dette telefonnummeret og i dette tidsrommet.

Dette viser at D slettet mye kommunikasjon mellom seg selv og domfelte. Dette gjorde hun både på sin egen og på domfeltes telefon. Domfelte hadde forklart for politiet at D slettet meldinger på hans telefon og at hun hadde koden til hans telefon, men ingen trodde ham.<sup>42</sup>

Gjenopptakelseskommisjonen fant at det som var anført som nye bevis eller nye omstendigheter fra domfelte, ikke var egnet til frifinnelse, anvendelse av en mildere strafferegulering eller en vesentlig mildere straff, og gjenåpningsbegjæringen ble ikke tatt til følge.

### **Noen andre har utført handlingen / det skjedde utenfor domfeltes kontroll**

Felles for de aller fleste digitale bevis er at det ikke er gitt hvem som har benyttet den digitale enheten som genererte beviset, altså hvem som snakket i telefonen eller hvem som benyttet datamaskinen. Undersøkelser av den digitale enheten vil kunne gi indikasjoner på hvem som genererte beviset, men dette vil ofte være beheftet med usikkerhet. På digitale enheter kan også ting skje som følge av hvordan programmer fungerer. Dette kan være programmer som kan tjene både gode og ondsinnede formål, og de kan operere uten direkte styring fra den som utviklet programmet. Det følgende er et eksempel fra sak GK-2013-8 hvor domfelte hevder at nedlasting av ulovlige bilder fra internett skjedde utenfor hans kontroll:

---

<sup>42</sup> [https://lovdata.no/pro/#document/GK/avgjorelse/gk-2015-113/KAPITTEL\\_1-3](https://lovdata.no/pro/#document/GK/avgjorelse/gk-2015-113/KAPITTEL_1-3) (besøkt 10.9.2019).

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegieringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegieringer_kan_vi_ute)

En politietterforsker vitnet om bildene som ble funnet på pc'en. Domfelte forklarte at da han søkte på voksenporno en gang, poppet det plutselig opp mange barnepornografiske bilder. I tingretten sa politietterforskeren at det ikke var mulig at flere bilder kunne poppe opp uten at en hadde trykket på linkene. I lagmannsretten endret etterforskeren denne forklaringen og sa det var mulig. De fant 180 bilder på pc'en. Ti av disse kunne være av modeller som var over 16 år. De 170 andre bildene poppet opp ukontrollert. Det fremkommer også av saksdokumentene at disse er lastet ned innenfor et veldig kort tidsrom. Da han ikke klarte å stoppe bildene, skrudde han av pc'en og trakk ut kontakten. Dette skjedde i 2007. Han brukte aldri maskinen etter det. Det kan Telenor bekrefte.<sup>43</sup>

Gjenopptakelseskommisjonen vurderte at det ikke forelå nye omstendigheter eller nye bevis som var egnet til å føre til frifinnelse eller mildere straff. De fant heller ikke forhold som gjorde det tvilsomt at dommen var riktig. Begjæringen om gjenåpning i sak GK-2013-8 ble forkastet.

Sak GK-2013-106, hvor domfelte hevdet seg uskyldig i voldtekt av en 15 år gammel gutt, er et eksempel på at Gjenopptakelseskommisjonen satte i gang grundige undersøkelser for å få svar på om andre kunne ha benyttet domfeltes mobiltelefon. Å trekke slutninger uten å gjøre undersøkelser som tar høyde for at domfeltes plausible forklaring kan stemme, vil i mange tilfeller stride mot objektivitetsprinsippet i strpl. §§ 55 og 226.

### **Politiet har manipulert beviset eller løyet om det i retten**

Dette sitatet er hentet fra sak GK-2016-98, hvor domfelte hevder at politiet har manipulert beviset:

Det var på utestedet Goggen han traff fornærmede, og ikke Z som politiet påstår. Bildet fra overvåkningskameraet er kuttet og viser derfor ikke nedre del av domfeltes bein. Man kan derfor ikke se at domfelte står i trappen utenfor (navn på utested).

---

<sup>43</sup> [https://lovdata.no/pro/#document/GK/avgjorelse/gk-2013-8/KAPITTEL\\_1-3](https://lovdata.no/pro/#document/GK/avgjorelse/gk-2013-8/KAPITTEL_1-3) (besøkt 10.9.2019).

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegj\\_aeringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegj_aeringer_kan_vi_ute)

Domfelte stiller spørsmål ved hvorfor bildet er kuttet slik av politiet. Han mener politiet i (stedsnavn) er ute etter ham fordi han tidligere er blitt tatt for piratkjøring.<sup>44</sup>

Denne kategorien kan både handle om manglende vitenskapelig og digital kapital hos politietterforsker slik at bevisene ubevisst blir manipulert eller framstilt uriktig. Politiet nyter stor tillit, men denne tilliten skal ikke tas for gitt. Det finnes tallrike eksempler fra USA hvor politiet har løyet om eller manipulert bevis i retten.<sup>45</sup> I USA er fenomenet omtalt som «testilying».<sup>46</sup> Interne kontrollmekanismer er derfor nødvendig for å sikre at bevis ikke blir manipulert eller framstilt på en feilaktig måte, verken med viten og vilje eller som følge av ukyndig håndtering og feil. Per i dag finnes ikke et kvalitetsrammeverk som ivaretar dette i norsk politi.<sup>47</sup>

### **Feil i rettsprosessen**

Feil i tilknytning til digitale bevis kan skje gjennom hele straffesakskjeden. Den minst hyppige kategorien av begrunnelser fra de domfelte omhandlet feil under rettsprosessen. Eksemplet er hentet fra sak GK-2011-167.

Bevis ble ikke fremlagt før under rettssaken – han sikter da til tekstmeldinger fra C (født 1996) til domfelte som ble vist under saken. I all hovedsak har ikke C sendt disse til mor mens hun var hos ham; tidspunktene kan han underbygge ved reiselister for ham selv og dagbok fra C som kan vise hvor hun har vært. Reiselister var han kjent med før anke ble sendt, men dagboken først noe senere.<sup>48</sup>

Domfelte peker her på retten til kontradiksjon, og mener han ikke fikk anledning til å kommentere bevis før de ble lagt fram i retten.

Om man så løfter blikket fra den enkelte kategori, kan man si at de domfeltes anførsler om digitale bevis i gjenåpningsbegjæringene peker på hele straffesakskjeden, fra identifisering og

---

<sup>44</sup> [https://lovdata.no/pro/#document/GK/avgjorelse/gk-2016-98/KAPITTEL\\_1-3](https://lovdata.no/pro/#document/GK/avgjorelse/gk-2016-98/KAPITTEL_1-3) (besøkt 10.9.2019).

<sup>45</sup> Se f.eks. National Registry of Exonerations, under kategorien Official Misconduct (OM). <http://www.law.umich.edu/special/exoneration/Pages/about.aspx> (besøkt 10.9.2019).

<sup>46</sup> Se f.eks. <https://www.nytimes.com/2018/03/22/nyregion/police-lying-new-york.html> (besøkt 10.9.2019).

<sup>47</sup> Sunde, N. (2019), «Digitale bevis – menneskelige feil», i Sunde, I.M. & Sunde, N. (red.), *Det digitale er et hurtigtog! Vitenskapelige perspektiver på politiarbeid, digitalisering og teknologi* (s. 53–82), Bergen: Fagbokforlaget.

<sup>48</sup> [https://lovdata.no/pro/#document/GK/avgjorelse/gk-2011-167/KAPITTEL\\_1-2](https://lovdata.no/pro/#document/GK/avgjorelse/gk-2011-167/KAPITTEL_1-2) (besøkt 10.9.2019).

sikring av bevis, til behandlingen av bevisene i retten. To fellesnevnerer her er kvalitet og kompetanse, som blir diskutert i neste punkt.

## **Digitale bevis – kvalitet og kompetanse**

Det er kvalitetsmessige forhold rundt hvordan dataetterforskningen organiseres og gjennomføres i Norge, som gir grunn til å tro at det kan skje ulike feil i sikringen, analysen eller presentasjonen av digitale bevis. Det finnes en rekke internasjonale «beste praksis»-guider og standarder for håndtering av digitale spor, men ingen forpliktende kvalitetsstandard som spesifikt regulerer håndteringen av digitale spor og bevis i norsk politi. I *Kvalitetsrundskrivet* påhviler ansvaret for kvalitet den enkelte medarbeider, som har et selvstendig ansvar for å holde seg faglig oppdatert innenfor sitt ansvarsområde og utføre sitt arbeid i tråd med gjeldende rutiner og kvalitetskrav.<sup>49</sup> Den politifaglige etterforskningsleder har ansvar for at etterforskningsskritt gjennomføres i samsvar med anerkjente metoder og framgangsmåter.<sup>50</sup> Riksadvokaten understreker behovet for notoritet omkring tekniske spor, og det legges til grunn at det ved alvorlige forhold benyttes «særlig kvalifisert personell» til sporsikring.<sup>51</sup> Utover dette oppstiller ikke rundskrivet noen spesifikke krav til håndteringen av digitale spor og bevis. Straffeprosessloven er det regelverk som styrer hvordan etterforskning, og da følgelig også dataetterforskning, skal gjennomføres.

I en artikkel i tidsskriftet *Science & Justice* sammenlignes kvalitetssystemene for henholdsvis datatekniske undersøkelser, DNA og fingeravtrykk i England, og den konkluderer med at dataetterforskning har et vagt og dårlig beskrevet system for kvalitetskontroll.<sup>52</sup> Professor Eoghan Casey har i flere av sine ledere i tidsskriftet *Digital Investigation* uttrykt bekymring for manglende vitenskapelig fokus innenfor dataetterforskning, og hvordan dataetterforskere uten tilstrekkelig kompetanse og bevissthet kan påvirke hvordan dommere oppfatter bevisverdien gjennom presentasjonen i retten.<sup>53</sup>

---

<sup>49</sup> Riksadvokatens rundskriv 3/2018, *Kvalitetskrav til straffesaksbehandlingen i politiet og ved statsadvokatembetene mv. (Kvalitetsrundskrivet)*, s. 5.

<sup>50</sup> Ibid, s. 10.

<sup>51</sup> Ibid, s. 28–29.

<sup>52</sup> Page, H., Horsman, G., Sarna, A. & Foster, J. (2019), «A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn?», *Science & Justice* 59(1), s. 83–92.

<sup>53</sup> Casey, E. (2015), «The growing importance of data science in digital investigations», *Digital Investigation* 14(C), A1-A2, og Casey, E. (2018), «Clearly conveying digital forensic results», *Digital Investigation* 24, s. 1–3.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegi\\_aeringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegi_aeringer_kan_vi_ute)

Per i dag er ingen av politiets datalaboratorier i Norge akkreditert. Det er ingen krav til sertifisering, og det er ikke satt andre minimumskrav for å gjennomføre sikring og analyse av databeslag utover Politidirektoratets rundskriv *Behandling av beslag i straffesaker*.<sup>54</sup> Her framgår det at sikring av digitale spor og bevis ikke må gjennomføres av personell uten adekvat opplæring, teknisk utstyr og programvare. Hva som anses som adekvat teknisk utstyr og programvare, er ikke nærmere spesifisert. Det samme var lenge tilfellet med formuleringen «adekvat opplæring», og da jeg høsten 2016 intervjuet dataetterforskere fra Oslo politidistrikt, fortalte de med sivil bakgrunn at de kun hadde fått én dags opplæring i etterforskningsrelaterte tema som straffeprosess i forbindelse med tildeling av begrenset politimyndighet.<sup>55</sup> Nå er det lys i enden av tunnelen, for i 2019 kom Politidirektoratet med *Nasjonale rolledefinisjoner med kompetansekrav*, hvor det stilles krav til både etterforskningsfaglig og teknologisk utdanning for sivile dataetterforskere, som det er svært mange av i norsk politi.<sup>56</sup> At Politidirektoratet nå, i tillegg til krav om teknologisk kompetanse, også har satt krav til etterforskningsfaglig utdanning for sivile dataetterforskere, er derfor svært positivt.

## Avslutning

Skjer det systematiske feil ved behandling av digitale bevis i det norske straffesakssystemet? Svaret er at vi ikke vet. I denne artikkelen har jeg gjennom undersøkelsen av Gjenopptakelseskommisjonens saker vist at digitale bevis ser ut til å ha hatt betydning for gjenåpningen i kun 1,9 % av sakene. Blant de ikke gjenåpnede sakene var andelen hvor domfelte gjorde forhold omkring digitale bevis gjeldende, langt større. De domfeltes begrunnelser for gjenåpning peker i retning av feil i hele straffesakskjeden, fra mangelfull eller ensidig sikring av digitale bevis til feiltolkninger i retten. Manglende krav til kvalitet i dataetterforskningen i norsk politi, og manglende vitenskapelig og digital kapital hos de profesjonelle aktørene som skal utfordre de digitale bevisene, gir grunn til bekymring. På bakgrunn av dette stiller jeg derfor spørsmålet om det kan være slik at vurderingen av digitale

---

<sup>54</sup> Politidirektoratet (2010), *Behandling av beslag i straffesaker* (Rundskriv RPOD-2010-7). Oppdatert 19.6.2017. Oslo: Politidirektoratet.

<sup>55</sup> Sunde, N. (2017), *Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation* (masteroppgave), Gjøvik: Fakultetet for informasjonsteknologi og elektroteknikk, Norges teknisk-naturvitenskapelige universitet. <http://hdl.handle.net/11250/2450280> (besøkt 10.9.2019).

<sup>56</sup> Politidirektoratet (2019), *Nasjonale rolledefinisjoner med kompetansekrav for etterforskningsfeltet versjon 1.0*, Oslo: Politidirektoratet.

Akseptert versjon. Endelig versjon:

[https://www.idunn.no/tidsskrift\\_for\\_strafferett/2020/01/digitale\\_bevis\\_i\\_norske\\_gjenaapningsbegi\\_aeringer\\_kan\\_vi\\_ute](https://www.idunn.no/tidsskrift_for_strafferett/2020/01/digitale_bevis_i_norske_gjenaapningsbegi_aeringer_kan_vi_ute)

bevis i for stor grad blir bygget på presumsjoner om kvalitet, og ikke blir gjenstand for tilstrekkelig kritisk vurdering av forsvarere, påtaleansvarlige og dommere. Dersom dette er riktig, kan det i ytterste konsekvens lede til at uskyldige blir dømt. Men, selv om feil ikke forplanter seg helt til saken når sitt endelige utfall, kan de ramme hardt. Følgende eksempel er riktignok hentet fra dansk rett, men er godt egnet til å illustrere poenget: En kvinnelig veterinær ble i 2013 tiltalt for å ha drept sin mann med medikamenter fra sin veterinærpraksis. Kvinnen hevdet sin uskyld og at hun hadde vært et annet sted, mens basestasjonsopplysninger indikerte at hun hadde vært i nærheten av åstedet. I domsslutningen sto det følgende: «Retten må herefter konstatere, at det ikke på baggrund af masteoplysningerne i sagen er muligt med blot nogenlunde præcision at fastslå tiltaltes nøjagtige placering i de relevante masters dækningsområder.»<sup>57</sup> Det ble avsagt frifinnende dom i saken. Da hadde kvinnen sittet 11 måneder i varetekt.

For å besvare hvorvidt systematiske feil skjer ved behandlingen av digitale bevis – så vel som andre bevistyper – er det på tide med en ny gjennomgang av Gjenopptakelseskommissjonens saker. Det er 10 år siden bevistyper ble tatt i betraktning, og det skjedde på grunnlag av et nokså lite antall saker. I dag foreligger et betydelig større grunnlagsmateriale, som kanskje kan gi svar på om det finnes en sammenheng mellom systematiske feil og bevistyper også i Norge. Dette er viktig kunnskap som vil kunne bidra til å forebygge justisfeil og styrke rettssikkerheten til partene i norske straffesaker.

---

<sup>57</sup> Dom avsagt 8. november 2013 av Retten i Hillerød, Danmark. Rettens nr. 9-2348/2013.