Land	Norge
Domstol	Haugaland og Sunnhordland tingrett
Parter	Norsk Medikal AS, A Utvik AS og Haver Malermesterfirma Emberland AS mod Nordlo Haugesund AS
Dato for afgørelse	28. september 2023
Afgørelsestype	Dom
Status	Endelig
Dato for publicering i domsdatabasen	27. september 2024
Omtalt i It-kontraktret, 2. udgave	Ikke omtalt
Gengivet fra	Haugaland og Sunnhordland tingretts domsbog

HAUGALAND OG SUNNHORDLAND TINGRETT

DOM

Avsagt:	28.09.2023 i Haugaland og Sunnhordland tingrett, Haugesund
Saksnr.:	23-016539TVI-THOS/THAU
Dommer:	Tingrettsdommer Leif Egil Holstad
Saken gjelder:	Erstatning for mislighold av kontrakt

Norsk Medikal A/S	Advokat Toralf Haver
A Utvik AS	Advokat Toralf Haver
Malermesterfirma Emberland AS	Advokat Toralf Haver

mot

Nordlo Haugesund AS	Advokat Tage Brigt Andreassen Skoghøy

DOM

Saken gjelder krav om erstatning fra tre selskaper mot leverandør av IT-tjenester etter at hackerangrep hos IT-leverandør medførte økonomisk tap hos de tre nevnte selskapene.

Kort om sakens bakgrunn

Malermesterfirma Emberland AS, heretter «Emberland», A.Utvik AS – heretter «Utvik» og Norsk Medikal AS – heretter «Norsk Medikal» -, samlet også benevnt som «saksøkerne», inngikk hver for seg i hhv 2014, 2018 og 2019 tilnærmet likelydende avtaler med Nordlo Haugesund AS - heretter «Nordlo» - om kjøp av såkalte ASP-tjenester, dvs. IT-tjenester som driftes via skyløsning av en tjenesteleverandør (Application Service Provider).

Emberland ble stiftet i 1936 og er et av landets eldste malermesterfirma, som primært leverer tjenester til profesjonelle kunder i området Nord-Rogaland. Selskapet har ca. 18 malere og omsatte for ca. 17 millioner kroner i 2021 og ca. 32 millioner kroner i 2022.

Utvik er en større eiendomsaktør på Sør-Vestlandet som forvalter og utvikler boligeiendom, og er boligprodusent av 40-100 boliger i året. Selskapet har 10 ansatte og hadde i 2021 en omsetning 170 millioner kroner og 112 millioner kroner i 2022.

Norsk Medikal er grossist av medisinsk utstyr. Selskapet importerer, markedsfører og selger medisinsk utstyr og tilknyttet forbruksmateriell til små lege- og tannlegekontor, samt større sykehus. Selskapet har kontor og importlager i Haugesund. Norsk Medikal har ingen faste utsalgssteder og baserer sitt kommersielle konsept på nettsalg, hvor omsetning i 2021 og 2022 var på rundt 11 millioner kroner. Selskapet har to ansatte.

Ingen av de tre selskapene hadde intern IT-funksjon/-støtte.

Nordlo Haugesund AS ble opprettet ved at Appex Operations AS ble utfisjonert fra Appex AS. Fisjonen ble registrert gjennomført i foretaksregisteret den 7. desember 2019 og selskapet fikk sitt nåværende navn den 24. oktober 2020. Selskapet er i dag heleid av det svenske eierselskapet Nordlo Group AB og hadde i 2021 en omsetning på 35 millioner norske kroner.

Den 21. april 2021 ble Nordlo utsatt for et cyberangrep. Nordlo meldte avvik til Datatilsynet den 25.04.2021 og sendte også oppdatering til Datatilsynet på samme avvik den 02.05.2021. Gjennom Nordlos Cyber-forsikring i Tryg ble bistand fra Ateas cybersikkerhetsteam rekvirert, for kartlegging av hendelsesforløp, omfang og få reetablert driften til Nordlo og tjenesten til kundene, herunder at kundene igjen fikk tilgang til sine systemer med dokumenter, regnskap, kunde- og ordresystem mv.

Saksøkerne var som følge av cyberangrepet uten tilgang til sine systemer i en lengre periode. For Norsk Medikals og Utviks del fra nedstengning den 22.04.2021 til de gradvis fikk tilbake tilgang til data i slutten av mai-medio juni 2021, og selskapene hadde reetablert normal drift medio august-primo september 2021. Emberland fikk ultimo mai 2021 beskjed om at alle data, med få unntak, var tapt. Selskapet rekonstruerte selv informasjon og var i tilnærmet normalt drift i november 2021.

Det var korrespondanse mellom selskapene og Nordlo, hvor også advokater ble engasjert av partene, hvor tema var avklaringer om faktum fra Nordlos side, deres håndtering av sikkerheten før angrepet mv. Det ble også varslet erstatningskrav.

De tre saksøkerne tok den 30.01.2023 ut fastsettelsessøksmål mot Nordlo for Haugaland og Sunnhordland tingrett, med påstand om at Nordlo var erstatningsansvarlig for det økonomiske tap saksøkerne hadde lidt som følge av kontraktsbrudd fra Nordlos side.

I tilsvar fra Nordlo datert 24.02.2023 ble det nedlagt påstand om frifinnelse, og det ble også krevd at retten behandlet erstatningskravenes omfang.

I planmøte den 28.02.2023 var partene enige om at søksmålet ble utvidet til også å gjelde fullbyrdelsessøksmål, altså utmåling av erstatning. Nordlo ønsket ikke å gjennomføre rettsmekling i saken.

Hovedforhandling ble avholdt 04.-06.09.2023. Partene avgav partsforklaringer og det ble ført to sakkyndige vitner samt foretatt dokumentasjon slik det er markert i dokument-samlingen vedlagt rettsboken.

Saksøkernes påstandsgrunnlag

Saksøkerne anfører at Nordlo har brutt sine hovedforpliktelser etter avtalene med saksøkerne, og at Nordlo har utvist grov uaktsomhet ved avtalebruddet.

Det vises til bakgrunnsretten hva gjelder ansvaret for direkte og indirekte tap.

Nordlo er en profesjonell leverandør av IT-tjenester, og spørsmålet om kontraktens krav er oppfylt på en aktsom måte skal ta utgangspunkt i en streng profesjonell norm.

Når det gjelder subsumsjonen er risiko for cyberangrep iflg Tore Solbergs egen partsforklaring «veldig kjent i bransjen», «vanlig» - med noen reservasjoner - og «den største risikoen man har», noe som også ble bekreftet av de sakkyndige vitnene Thorsheim og Skei. Det man må «forvente» er innenfor kontrollansvaret og det er ingen fritaksgrunn. Dersom Nordlo som IT leverandør er kjent med en slik risiko kan den ikke påberopes som fritaksgrunn uten at dette er uttrykkelig omhandlet i avtalen. Den alternative handlingen for

Nordlo vil her måtte være å gi klar beskjed om at Nordlo ikke tilbyr slik sikkerhet eller at den er begrenset, og at kundene må foreta egne tilpasninger/sikkerhetsforanstaltninger for å trygge data. Når det ikke gjort i denne saken fratas kundene mulighet til å tilpasse seg. En villeder da kunden til å tro at en er trygg.

Når retten skal vurdere hva som er avtalt mellom partene skal utgangspunktet være en objektiv tolkning, jf. Rt-2002-1155 og Rt-2010-1345, og at kontraktens ordlyd må tillegges stor vekt. Avtalene med saksøkerne er inngått mellom profesjonelle parter.

Nordlos hadde flere hovedforpliktelser etter avtalen. Selskapet «påtar seg ansvaret for drift av kundens dataprogrammer», og en naturlig forståelse av ordlyden er at Nordlo alene har ansvaret for dataprogrammenes drift, funksjonalitet og virkemåte. Videre at de «garanterer 99,5% oppetid» og responstid, og en naturlig forståelse av denne ordlyden er at Nordlo har gitt en «garanti» for oppetiden. Videre fremgår det av avtalen at Nordlo «tar sikkerhetskopi av Kundens data flere ganger hver virkedag», som oppbevares i annen bygning og siste sikkerhetskopi skal tilbakeleveres kunde på forespørsel. Det er en sentral kontraktsforpliktelse å sikre integriteten til dataene gjennom sikkerhetskopiering. En naturlig forståelse av ordlyden er at Nordlo har ansvaret for at det tas adekvat sikkerhetskopi av kundenes data. I ordet «sikkerhetskopi» ligger det at en kopi av informasjon er lagret med hensikt å kunne gjenskape informasjonen dersom den opprinnelige lagringen helt eller delvis går tapt. Ordet «sikkerhet» brukes i tillegg, altså ikke bare en «kopi», men en «sikkerhetskopi». Det er en klar og tydelig ordlyd som må tillegges stor vekt. Sist er en av forpliktelsene også å ta vare på de lagrede dataene og beskytte disse, som følger motsetningsvis av avtalenes punkt 9, jf. «ved forhold som skyldes Kunden, har Leverandøren ikke ansvar for feil og mangler ved data, eller tap som skyldes at disse bortfaller.» En naturlig forståelse av bestemmelsen er at Nordlo har ansvaret for feil eller mangler ved data, eller tap som skyldes at disse bortfaller, dersom forholdene skyldes Nordlo.

Nordlo er alene ansvarlig for at sikkerheten ivaretas, noe som er erkjent av Nordlo v/Solberg selv, og bekreftet av de sakkyndige vitnene.

Det er avtalt at konsekvensen av mislighold er at saksøkerne kan *«kreve erstatning for dokumentert økonomisk tap etter alminnelige prinsipper for erstatninger i avtaleforhold.»*

Bevisbyrden snus for øvrig ved grov uaktsomhet, jf. Hagstrøm og Stenvik «Erstatningsrett» s. 433 og når det gjelder bevismulighet vises det til samme bok og side, og Rt-2009-920 avsnitt 35 og 36.

Nordlo anfører at to av avtalenes bestemmelser utelukker eller begrenser erstatningsansvar, nemlig force majeure i punkt 8 og ansvarsbegrensningen i punkt 10. Saksøkerne anfører at verken force majeure eller ansvarsbegrensningen kommer til anvendelse.

Om force majeure vises det til Hagstrøms Obligasjonsrett punkt 12.3.1 og HR-2016-1235 avsnitt 40. Et cyberangrep er verken en uventet eller ekstraordinær hendelse for en profesjonsutøver som leverer IT-tjenester. Tvert imot ligger beskyttelse mot cyberangrep innenfor kjernen av Nordlos forpliktelser. Cyberangrepet ligger heller ikke utenfor Nordlos *«kontroll»*. Det ligger klart innenfor Nordlos eget virkeområde. Det foreligger åpenbart ikke en force majeure hendelse.

I avtalens punkt 1 er ordlyden at Nordlo *«garanterer 99,5 % oppetid på tjenestene i normal arbeidstid regnet kvartalsvis»* og i punkt 10 at erstatningen *«ikke overstige et beløp som tilsvarer 3 månedsleier i henhold til denne Avtalen»*. Ordet «garanti» betyr et løfte om å svare for feil, mao at en påtar seg ansvar for egenskapen, også erstatningsansvar, uten hensyn til skyld. I Anne Cathrine Røed «Foreldelse av fordringer» fremgår at *«Foreldelsesloven § 3 nr. 4 må naturlig forstås slik at den kun får anvendelse der det foreligger en reell garanti, slik at skyldneren i en større risiko eller et større ansvar enn det som følger av det regulære mangelsansvar. Ved såkalte «tomme» garantier der det kun er gitt et tilsagn basert på de deklaratoriske regler, er garantitilsagnet uten realitet, slik at de særregler som gjelder for garantier ikke kan få anvendelse.»*

Garantien vil være en «tom» garanti uten realitet dersom ansvarsbegrensningen gjøres gjeldende, det er med andre ord klar ordlydsmotstrid. Det samlede økonomiske tapet er på 4 567 355 kroner, mens beløpet som tilsvarer 3 månedsleier på maksimalt 60 663 kroner. Dersom ansvarsbegrensningen kommer til anvendelse innebærer det at Nordlo kun dekker ca. 1,3 % av det faktiske økonomiske tapet. Det blir da ikke riktig at man «garanterer» for oppetiden. En eventuell uklarhet må tolkes i Nordlos disfavør, jf. Rt-2006-1715 avsnitt 49, Rt-2012-1267 avsnitt 67 og Giertsen «Avtaler» 4. utgave side 171 Avtalen er laget av Nordlo, er deres standardavtale og regulerer kontraktsytelse på deres eget spesialfelt, nemlig IT leveransene. Ansvarsbegrensningen kan følgelig ikke komme til anvendelse.

Det gjøres også gjeldende at avtalen må revideres for brudd på hovedforpliktelsene i kontrakten. I Viggo Hagstrøm «Obligasjonsrett» 3. utgave s. 687 gis det uttrykk for at *«For det annet synes domstolene ikke å ville tillegge en fraskrivelse rettsvirkning etter sitt umiddelbare innhold når det er skjedd et betydningsfullt kontraktsbrudd som ikke ville få virkninger om fraskrivelsen fullt ut skal opprettholdes.»* og *«Innskrenkende fortolkning av fraskrivelsesklausuler som ellers ville ha medført at et betydelig kontraktsbrudd ikke får virkninger, har lang tradisjon i rettspraksis, også innenfor kommersielle avtaleforhold, der ansvars- og risikofraskrivelser er sedvanlige og kan være kombinert med forskjellige forsikringsordninger.»* Det vises også til Rt-1911-1037 og Rt-1982-1357.

Bestemmelsene om oppetid, virkemåte og sikkerhetskopi er grunnleggende kontraktsforpliktelser. Nordlo har brutt kontraktens hovedforpliktelser og med ansvarsfraskrivelsene blir alle disse «tomme» forpliktelser. Ansvarsbegrensningene må derfor tolkes innskrenkende.

Begrensningene må også tilsidesettes basert på forutsetningsbetraktninger, jf. Viggo Hagstrøm «Obligasjonsrett» 3. utgave s. 690: *«Når ordlyden er klar, har domstolene i realiteten underkjent klausuler som ville innebære at betydelige kontraktsbrudd ikke fikk virkninger, ved å anta at forutsetninger for anvendelse av klausulene ikke var til stede, jf. eksempelvis Rt. 1935 s. 497 og Rt. 1969 s. 679.»* Det vises også til Rt-1969-679. Plikten til å sørge for sikker lagring av data, oppetid og virkemåte ligger hos Nordlo. Dette vil være i strid med partenes forutsetninger hvis saksøkerne skulle være ansvarlig for tap av data.

Subsidiært anføres at ansvarsbegrensningen må settes til side som ugyldig etter avtaleloven § 36, jf. at bestemmelsene i avtalen vil *«virke urimelig»* eller er *«i strid med god forretningsskikk»*. Det følger av forarbeidene (NOU 1979:32 s. 39) at ugyldighetsreglene i avtaleloven er: *«begrunnet i behovet for å beskytte den svake kontraktspart og er ment å skulle bøte på det misbruk som en ubegrenset kontraktsfrihet kan lede til.»* Det vises også til Hagstrøms Obligasjonsrett 3 utgave side 38 og fremlagt voldgiftsdom avsagt 18.12.2013 - som har klare likhetstrekk med vår sak – og dom avsagt av Oslo tingrett den 01.12.2012.

Selv om avtalene er inngått mellom profesjonelle, er Nordlo den profesjonelle part i denne sammenheng. Saksøkerne hadde ikke kompetanse eller nødvendige interne ressurser til å selv håndtere drift, vedlikehold og sikring av IT-systemer. Ansvarsbegrensningene vil medføre at saksøkerne ikke har noen form for vern eller effektiv beføyelse mot Nordlos mislighold av sine hovedforpliktelser. Nordlo har ingen beskyttelsesverdig interesse i å beskytte seg mot tap som skyldes at selskapet ikke har oppfylt hovedforpliktelsene sine etter avtalene. Det anføres at beløpsbegrensningen på *«3 månedsleier»* medfører at det foreligger en klar ubalanse i kontraktsforholdet, og at dette ikke står i noen sammenheng sett hen til skadepotensialet og den risikoprofil som Nordlos virksomhet naturlig er forbundet med.

Det vises også til Rt-1994-626, på side 630, hvor situasjonen i vår sak er den motsatte, nemlig at det vanskelig kan hevdes at ansvarsbegrensningene er et utslag av noen bevisst avveining av partenes motstridende interesser, at Nordlo må bære risikoen for egen forretningsvirksomhet og at Nordlo ikke kan fraskrive seg ansvaret for den mest sentrale delen av sin yteplikt. Saksøkerne har videre ikke hatt mulighet til å tegne forsikring som ville dekket erstatningsansvar som dette, idet cyberforsikring bare dekker teknisk bistand og rådgivning for å kartlegge omfang av dataangrep og gjenoppbygging av programvare og data. Cyberforsikring dekker ikke direkte eller indirekte økonomisk tap. Det er forøvrig begrensninger i hva cyberforsikringen dekker dersom visse sikkerhetstiltak ikke er gjennomført, som i vårt tilfelle.

Atter subsidiært anføres at ansvarsbegrensningen uansett må settes til side fordi Nordlo har opptrådt grovt uaktsomt. Det vises til Hagstrøms «Obligasjonsrett» side 39 og Rt-1926-712. Saksøkerne anfører at Nordlos opptreden utgjør et markert avvik fra forsvarlig handlemåte. Ansvaret i profesjonelle forhold er skjerpet og en mer betydningsfull faglig

svikt er ofte i seg selv tilstrekkelig for å kunne betegnes som grovt uaktsomt. Det vises til Rt-1989-1318 om advokatansvar. For vurderingen av Nordlo vises det til Schjølbergs «Cyberkriminalitet» side 139 og 141, hvor det på sistnevnte side gjengis hvilke forebyggende tiltak Gjensidige anbefaler. Det anføres at disse tiltakene må være oppfylt for å få dekning, noe de ikke var i vårt tilfelle. Nordlo sørget ikke for tilstrekkelig sikkerhet og forsvarlige rutiner rundt oppbevaring og lagring av data, jf. at serveren hadde «gammel usupportert, upatchet og utdatert programvare som mulig kan ha blitt utnyttet.», det ble ikke skiftet passord regelmessig, det var manglende tofaktorautentisering, det var ingen geografisk begrensning på innlogging, de hadde ikke regelmessige brannøvelser og det var manglende segmentering. Thorsheims vurdering var klar, han mente at det samlet sett utvilsomt forelå markerte avvik. Det dreier seg om brudd på de sentrale bestemmelsene i avtalene. Tap av data og nedstengte systemer som følge av cyberangrep er en svært påregnelig fare ved ASP-tjenester, og Nordlo var klar over den store skaderisikoen som forelå ved mangelfulle rutiner og infrastruktur. Nordlo tok bevisst denne risikoen.

Som følge av kontraktsbruddet har saksøkerne lidt økonomisk tap, og ved denne vurderingen må beløp knyttet til omsetning og intern tid nødvendigvis bli noe skjønnsmessig. Det alminnelige beviskravet er «sannsynlighetsovervekt». Det vises til partsforklaringene og fremlagt dokumentasjon. Norsk Medikal AS har sannsynliggjort et tap på 399 519 kroner, Malermesterfirma Emberland AS på 2 694 588 kroner og A Utvik AS på 1 473 248 kroner. Beløpene knytter seg til omsetningstap, bruk av interne ressurser og fakturaer fra eksterne.

Saksøkernes påstand

1. Nordlo Haugesund AS betaler erstatning til Norsk Medikal AS, Malermesterfirma Emberland AS og A Utvik AS som følge av kontraktsbrudd i forbindelse med cyberangrep i april 2021, utmålt etter rettens skjønn.

2. Norsk Medikal AS, Malermesterfirma Emberland AS og A Utvik AS tilkjennes sakskostnader.

Saksøktes påstandsgrunnlag

Sakens kjerne er at rettssaken står mellom fire skadelidte etter et cyber-/hackerangrep. Nordlo hadde vitterlig hatt fokus på sikkerhet, jf. forklaringene til Skei og Solberg. De hadde planer og rutiner, og da alarmene gikk hos Nordlo ble datasenteret avstengt kort tid etterpå. Da Atea kom inn et par dager senere var Nordlo veldig godt i gang og hadde kontroll. Det var kun 4 av 250 kunder som mistet data. Ingen vet hva som ville ha skjedd hvis infrastrukturen hadde sett litt annerledes ut. Sakkyndig vitne Skei gav uttrykk for at det ikke finnes en «silver bullet». Cyberforsikring må tegnes dersom man vil pulverisere skadeomfanget over tid heller enn å ta engangskostnaden selv. Ingen av saksøkerne valgte

å forsikre seg mot tap, og har nå reist søksmål med krav om erstatning etter cyberangrep, som følge av påstått manglende oppfyllelse av ASP-kontrakter

Nordlo bestrider erstatningskravene som er fremsatt. Stikkordsmessig anføres det at cyberangrepet var utenfor Nordlo sin kontroll, hvor pliktene da suspenderes i perioden som angrepet og vanskene varte. Sikkerhetskopier ble tatt og oppbevart kontraktsmessig. Saksøkerne har ikke dokumentert tapene de krever erstattet, og det vises til at kun 3-9 % av kravene gjelder kostnader som saksøkerne faktisk har pådratt seg, resten er «skjønnsmessig» angitt, uten noe underlagsdokumentasjon. Det anføres videre at det er uforklart hvordan hver enkelt tapspost står i årsak til et eventuelt kontraktsbrudd. Kontraktens ansvarsbegrensninger gjør seg fullt ut gjeldende, og Nordlo har ikke påtatt seg forretningsrisikoen til hver enkelt kunde; de var selv ansvarlige for å forsikre verdien av egne data. Det er heller ikke grunnlag for tilsidesettelse/revisjon av avtalen. Nordlo har ikke handlet grovt uaktsomt. Ansvarsbegrensningene er ikke urimelig, jf. avtaleloven § 36

Nordlo har driftet og tilgjengeliggjort programmene overfor saksøkerne i henhold til avtalen, foruten en nedetidsperiode i april-mai 2021, og kundene er også kreditert for nedetiden. Nordlo har tatt sikkerhetskopier og oppbevart dem i annen bygning enn datasentralen ihht avtalene. Norsk Medikal og Utvik har fått tilbake data fra nettopp disse sikkerhetskopiene. Emberlands data derimot gikk tapt i cyberangrepet og kunne ikke tilbakeleveres.

Nordlo hadde fokus på sikkerhet og det anføres at sikkerhetskopiene var tilstrekkelig beskyttet. Da angrepet skjedde pågikk arbeid hos Nordlo med å flytte ut backup og management til eget nett, og dette arbeidet begrenset skadene.

Når det gjelder tofaktor-autentisering var dette anbefalt fra Nordlos side, men valgfritt for kundene. Hva gjelder saksøkernes anførsler om bytte av passord på servicekontoer og geografisk avgrensning vises det til forklaringene til Solberg og Skei. Nordlo hadde videre et godt «patchet» operativsystem, og det Atea gav uttrykk for om utdatert programvare gjaldt ikke privilegerte programmer. «Brannøvelser» var utført og planer på plass. Det kan her ikke oppstilles en teoretisk terskel.

I relasjon til Emberlands datatap og nedetiden, blir det et spørsmål om hvorvidt cyberangrepet var «utenfor Nordlos kontroll». Det gjøres gjeldende at erstatningskravene er basert på feilslutninger om at cyberangrep av enhver art mot leverandører av skytjenester er påregnelige. Det anføres at nedetid og kryptering av Emberlands sikkerhetskopier skyldes hackernes profesjonalitet, jf. den beskrevne fremgangsmåte og Solbergs og Skeis forklaringer. Nordlo oppdaget angrepet veldig kort tid etter eksekvering, og begynte avstenging for skadebegrensning. Nordlo hadde også iverksatt en rekke sikkerhetstiltak for å redusere risikoen for cyberangrep. Cyberangrepet var utenfor Nordlos kontroll, og forpliktelsene ble derfor suspendert i perioden, jf. kontrakten pkt. 8 første ledd. Nordlo kan

derfor ikke holdes ansvarlig for nedetiden som oppstod under angrepet. Det samme gjelder dataene til Emberland, som ble kryptert og som ikke lot seg gjenopprette.

Avtalens ordning skiller mellom direkte og indirekte tap, hvor erstatning for direkte tap ved mislighold av kontrakten er begrenset til 3 ganger månedsleien, mens indirekte tap ikke erstattes. Det anføres at dette ikke er uvanlig avtale, jf. at også kjøpsloven skiller mellom direkte og indirekte tap, og avtalen er heller ikke vanskelig å forstå og forholde seg til.

Tapene som kreves dekket er stort sett udokumenterte og årsakssammenhengen uforklart. Det er gjentakende for alle saksøkerne at hverken Nordlo eller retten settes i stand til selv å vurdere saksøkernes skjønnsfastsettelse av sine tap, da en ikke tas med i vurderingene skjønnet baseres på. Fortjenestetapet, som utgjør det aller vesentligste av kravet, er indirekte tap og ikke erstatningsberettiget.

Det er ikke grunnlag for tilsidesettelse av avtalene. Avtalene – som er inngått mellom profesjonelle parter - er helt greie å forstå, det er avtalt en risikofordeling som er balansert opp mot vederlagene fra saksøkerne. Om gjensidighet i kontraktsforhold vises det til Rt-2014-351 avsnitt 46 og Hagstrøms m.fl. «Obligasjonsrett» 2021 side 11. Det er ingen generell regel om at ansvarsbegrensninger ikke kan gjøres gjeldende ved grov uaktsomhet. Det vises til Hagstrøm «Obligasjonsrett» 2011 side 552 og Rt-1994-626 «Kainspektør-dommen» på side 630, Lilleholt «Kontraktsrett og obligasjonsrett» 2017 side 396 og Hagstrøm «Obligasjonsrett» 2021 side 694. Når det gjelder profesjonsansvaret og grov uaktsomhet – terskelen – vises det til Rt-1995-1350, på side 1356, Rt-1989-1318, på side 1322 og Rt-2006-321 avsnitt 33. Det er heller ikke grunnlag for revisjon av avtalen i medhold av avtalelovens §36.

Saksøktes påstand

1. Nordlo Haugesund AS frifinnes.

2. Norsk Medikal AS, Malermesterfirma Emberland AS og A. Utvik AS dømmes - in solidum - til å betale sakskostnadene.

Rettens vurdering

Retten skal vurdere om Nordlo har misligholdt sine hovedforpliktelser etter avtalen med saksøkerne og er erstatningsansvarlige for det direkte og indirekte tap saksøkerne anfører å være påført ved misligholdet.

Appex AS, nå Nordlo, inngikk separat avtale med Emberland i 2014, Utvik i 2018 og Norsk Medikal i 2019 om kjøp av ASP-tjenester. ASP er forkortelsen for «Application Service Provider» og innebærer at Nordlo var leverandør av IT-tjenester over internett,

altså en sentralisert driftstjeneste hvor Nordlo driftet en datasentral som forvaltet/ tilgjengeliggjorde kundenes data og applikasjoner med en påloggingsløsning via nett.

I likelydende bestemmelser i punkt 1 i avtalene fremgår bl.a. følgende:

«*Drift*
Leverandøren påtar seg ansvaret for drift av Kundens dataprogrammer og skal gjøre disse tilgjengelige via Internett. Leverandøren skal sørge for at Kunden har tilgang til funksjonalitet og virkemåte i programmene. Leveransen skal foregå ved hjelp av Leverandørens standard maskinutrustning plassert hos Leverandøren.»

Oppetidsgaranti og responstid
Leverandøren garanterer 99,5% oppetid på tjenestene i normal arbeidstid regnet kvartalsvis. Responstid ved kritiske feil i normal arbeidstid er maksimum 30 minutter fra mottak av henvendelse. Med kritiske feil menes feil som forårsaker bortfall av funksjonalitet som fører til at brukere ikke får utført sine operasjoner og heller ikke kan utføre sine operasjoner på annen måte.

Sikkerhetskopiering og tilbakekopiering
Leverandøren tar sikkerhetskopi av Kundens data flere ganger hver virkedag. Sikkerhetskopier oppbevares i annen bygning enn datasentralen. Dersom Kunden ber om det skal Leverandøren tilbakekopiere angitte data fra siste sikkerhetskopi.»

Den 21. april 2021 ble Nordlo utsatt for et cyberangrep som medførte nedetid for bl.a. saksøkerne, og hvor dataene til Emberland gikk tapt. Det følger av punkt 10 i avtalene at «*Det foreligger mangelfulle tjenester dersom tjenestene etter Oppstartsdag ikke oppfyller de krav som fremgår av denne Avtalen.*»

Nordlo har gjort gjeldende at det forelå en «force majeure» hendelse - i det angrepet var «utenfor Nordlos kontroll», hvor det da følger av avtalene at partenes plikter overfor hverandre suspenderes i den perioden tilstanden vedvarer. Retten viser til avtalens punkt 8 første avsnitt, som – med rettens understreking – har følgende ordlyd:

«*8. FORCE MAJEURE OG VANHJEMMEL*
Dersom Avtalens gjennomføring helt eller delvis hindres, eller i vesentlig grad vanskeliggjøres av forhold som ligger utenfor partenes kontroll, suspenderes partenes plikter i den utstrekning forholdet er relevant, og for så lang tid som forholdet varer. Slike forhold inkluderer, men er ikke begrenset til, streik, lockout, og ethvert forhold som etter norsk rett vil bli bedømt som force majeure.»

Om vurderingen av «kontrollsfæren» har Høyesterett i Rt-2022-192-A, avsnitt 72, uttalt følgende: «*Oppsummeringsvis legger jeg etter dette til grunn at vilkåret om at årsaken til*

mangelen må ligge utenfor selskapets kontroll, må vurderes konkret. Det avgjørende er om årsaken ligger innenfor det selgeren – etter en objektiv vurdering – kunne kontrollere eller påvirke gjennom planlegging, styring og kontroll med virksomheten. Foreligger det handlingsalternativer for selger som ville ha forhindret årsaken til mangelen, ligger årsaken normalt innenfor selgers kontroll, med mindre årsaken skyldes ekstraordinære forhold. Det er ikke avgjørende om selgeren har opptrådt aktsomt.»

Retten viser også til Rt-2008-537, avsnitt 58, hvor det fremgår det at: *«Innenfor kontraktsretten er den alminnelige regel antatt å være at debitor ved mislighold av generisk bestemte forpliktelser hefter på objektivt grunnlag, men dersom misligholdet skyldes en hindring som ligger utenfor debitors kontroll, og som han ikke med rimelighet kan forventes å ha tatt i betraktning på avtaletiden, blir han fri for ansvar såfremt hindringen er av en slik karakter at det ikke med rimelighet kan ventes at han har kunnet unngå eller overvinne følgene av den (« kontrollansvar »). For kjøp som omfattes av kjøpsloven, følger denne regel av kjøpsloven § 40 første og andre ledd, jf. § 27, og gjelder også individuelt bestemte forpliktelser. Dersom det ikke finnes særlig lovregulering, må ordningen med kontrollansvar også gjelde utenfor kjøpslovgivningens område, men slik at den på ulovfestet grunnlag bare gjelder for generisk bestemte forpliktelser, se Hagstrøm, op.cit. side 502 ff. Innenfor området for kjøpsloven gjelder det objektive ansvar bare direkte tap, se kjøpsloven § 40, jf. § 67. Hvis det ikke finnes særlig hjemmel for annet, må dette også antas å gjelde utenfor kjøpslovens område.*

Retten vil bemerke at det har skjedd en betydelig profesjonalisering innen «ransomware», hvor godt organiserte kriminelle aktører bryter seg inn i dataservere til myndigheter, bedrifter, organisasjoner mv, krypterer data og krever store løsepengesummer i kryptovaluta – som ikke kan spores - for å gi den rammede sine data tilbake. Ryuk-viruset, som er benyttet i denne saken, knyttes til internasjonal organisert kriminalitet.

Det vil alltid oppstå sikkerhetshull som profesjonelle hackere vil kunne finne og utnytte for å komme seg inn på datasystemer, og for å være best mulig rustet mot angrep må datasystemene ha de til enhver tid siste sikkerhetsoppdateringene fra programvareleverandørene og ha de nødvendige preventive tiltak. Foruten bl.a. geo-sperre og påloggingsmetode vil dette kunne bestå i å vanskeliggjøre en angripers navigering gjennom infrastrukturen om angriper først kommer seg inn på datasystemet, hvor målet for angriperen vil være å få administratorrettigheter og gjøre mest mulig skade/kryptere data.

Når det gjelder det konkrete hendelsesforløpet i cyberangrepet Nordlo ble utsatt for viser retten til følgende – ubestridte - beskrivelse som er gitt i tilsvaret datert 24.02.2023:

«*Cyberangrepet ble gjennomført ved at trusselaktører fra Østerrike og Taiwan logget seg inn via en såkalt «RD Gateway» den 21. april 2021 kl. 23:50, med brukerkontoen til en av Nordlos kunder, som ledet til en av Nordlos terminalservere. Det er ikke kjent hvordan*

trusselaktørene fikk tak i denne kundens påloggingsdetaljer, men trolig via en «phishing mail». Veien inn til server og kundemiljø ble aksessert via denne kundens bruker-PC.

Ved hjelp av denne tilgangen ble det sluppet et såkalt «cobalt strike beacon» på serveren, trolig for å tilegne seg administrasjonsrettigheter. Trusselaktørene foretok så en rekognosering av miljøet før de logget seg av infrastrukturen kl. 03:19 den 22. april 2021. Trusselaktørene logget seg inn igjen samme dag kl. 19:03, og benyttet flere administrator-kontoer, for det IT-ekspertene kaller «lateral movement» og eksekvering av «Ryuk ransom-ware». Trusselaktørene tok i bruk en SOCKS-proxy (SystemBC) som har fungert som «staging»- og «jump»-server, slo av Windows Defender via GPO og hentet ut angrepsdata, før de detonerte «Ryuk ransomware» på en håndfull servere kl. 23:00.

En særlig egenskap ved «Ryuk ransomware» er at den sprer seg selv til øvrige systemer. Trusselaktørene igangsatte også krypteringsprosesser manuelt, og skal under angrepet ha introdusert enda en «Ryuk ransomware»-versjon, uten at en har klart å finne frem til bakgrunn og detoneringstidspunktet.

Disse aktørenes struktur og arbeidsmetodikk er et stikkord i relasjon til angrepsomfanget. Dette var ikke et enkelt virus som ble installert, men en gruppering av hackere som fikk tilgang til en kundes brukerkonto og passord. De har jobbet aktivt i miljøet for å trenge dypt inn i nettverket/infrastrukturen, og iverksatte flere omfattende angrep mot drifts-miljøet. Trusselaktørene har installert egne, «skjulte» proxy-servere for å kamuflere sitt «staging»-miljø, og har med dette fått anledning til å arbeide målrettet og effektivt slik at angrepet ble av denne karakter.

Hendelsen ble oppdaget kort tid etter angrepet ble iverksatt, av Nordlos systemer for overvåking og varsling, og Nordlos personell stoppet angrepet og startet nedstengning av det rammede miljøet.

Nordlo tok kontakt med trusselaktørene i form av å oppgi en epost-adresse i en mottatt link/skjema. Kravet som ble fremmet var på 116 bitcoin, altså kr 50-60 millioner. Kravet ble ikke akseptert av Nordlo. Det var ingen garanti for at trusselaktørene ved betaling ville ha sendt dekrypteringsnøkler/-programmer som faktisk fungerte, og det var også en risiko for at slike dekrypteringsnøkler/-programmer igjen ville ha opprettet nye sårbarheter. Gjenoppretningsarbeidet var allerede i gang, og ville i hovedsak gå ut på det samme, uavhengig av om man benyttet Nordlos backup- eller dekrypteringsnøkler kjøpt av trussel-aktørene. Mye av de berørte dataene ville uansett ikke ha latt seg dekryptere ettersom de var ødelagt under angrepet. Trusselaktørene mistet for øvrig tilgang til systemer og data kort tid etter angrepet var iverksatt, så en betaling ville ikke ha hindret ytterligere skade.

Angrepet ledet til ulik nedetid for ulike kunder, deriblant for Saksøkerne, og blant annet for Emberland var det ikke mulig å gjenopprette filer/data. Dataene gikk tapt som en følge av

et målrettet angrep hvor trusselaktørene fikk tilgang til noen backup-servere og disk-systemet for disse. Sikkerhetskopiene på de berørte serverne ble slettet og diskene ble skrevet over slik at dataene ikke kunne gjenopprettes.»

Retten skal foreta en konkret vurdering, hvor det er Nordlo som har bevisbyrden for at det forelå en «force majeure» hendelse som etter avtalen – og bakgrunnsretten – fritar Nordlo for ansvar for misligholdet. Vurderingen skal foretas ut fra hva partene på avtaletids-punktet kunne forutse, og det er da etter rettens syn ikke tvilsomt at det – hvor det er tale om en løpende ytelse – må hensyntas den teknologiske utviklingen som finner sted i etterkant av avtaleinngåelsen. Vurderingen må ta utgangspunkt i hvordan forholdene var i mars-april 2021.

Hackerne fikk ifølge sakkyndig vitne Skei inngang til datasystemets driftsmiljø ved å bruke en kundes brukernavn og passord som var på avveie.

Det er etter rettens syn ikke tvilsomt at en av Nordlos hovedforpliktelser etter avtalen var å tilby saksøkerne en dataløsning som ivaretok den nødvendige sikkerhet mot bl.a. cyber-angrep. Det må stilles strenge krav til IT-leverandørens egne sikkerhetstiltak, da et angrep vil være svært kritisk for Nordlo selv og ikke minst også for kundenes virksomheter.
I 2021 var tofaktorautentisering en bransjestandard, men mange kunder – ikke bare hos Nordlo - valgte det bort. Det må her hensyntas at det er forskjell på om en bedrift eller enkeltperson velger ikke å benytte seg av dette til eget datasystem, og hvorvidt Nordlo – som IT-leverandør – lar kundene foreta pålogging til Nordlos datasystem uten tofaktor-autentisering. Nordlo gjorde det valgfritt for kundene om de ville benytte seg av tofaktor-autentisering Tofaktorautentisering er et enkelt preventivt tiltak som i stor grad vil hindre eller vanskeliggjøre et hackerangrep. Etter rettens syn er dette et tiltak som klart påvirker sikkerheten mot angrep og som Nordlo kunne benyttet seg av. Nordlo kunne enten krevd at alle kundene brukte tofaktorautentisering, eller eksempelvis «isolert» kundene som ikke ville bruke dette fra de andre kundene i samme driftsmiljø på grunn av den økte sikkerhets-risiko den aktuelle kunde representerte.

Det å bruke geografiske begrensninger ifht fra hvilke land pålogging kan skje vil også kunne hindre eller forsinke en angriper, selv om det dog ikke kreves så gode data-kunnskaper for unngå dette eksempelvis ved å bruke proxy-server som er lokalisert i Norge. Bruk av regionsperre krever også at kunden er bevisst på de ansattes reisevirk-somhet til land som vil rammes av sperren som settes opp. Nordlo hadde ikke regionsperre, og også dette er et sikkerhetstiltak de kunne benyttet seg av og som kunne påvirket angrepets gang.

Ifølge Atea hadde Nordlo et godt «patchenivå» på operativsystemet, hvor alle opp-dateringene var tatt, men de hadde også utdatert programvare hvor det ikke var foretatt sikkerhetsoppdateringer på lang tid, bl.a. på Google Chrome 2019 og Office 2018. Dette

innebærer sårbarheter som angriperne kan ha utnyttet når de først var inne på systemet. Hvordan hackerne har navigert seg videre i infrastrukturen er ikke kjent, og det kan være mange veier de profesjonelle hackere kan ha benyttet. Sakkyndig vitne Skei gav uttrykk for at det er minst «200 veier» videre.

Når det gjelder nedetid og tap av data er det klart at sikkerhetskopier på et eget nettverk som var fysisk atskilt fra det andre datasystemet ville hindret eller redusert konsekvensene av cyberangrepet betraktelig. En slik forpliktelse følger ikke direkte av avtalens ordlyd om sikkerhetskopier, men i lys av utviklingen mtp det sikkerhetsnivå som forventes – herunder det store cyberangrepet som hadde rammet Hydro i 2019 – var dette en sikkerhetstiltak som burde iverksettes. Nordlo hadde da også påbegynt slik segmentering, og dette hindret at angrepet fikk enda større konsekvenser. Også dette var et sikkerhetstiltak Nordlo hadde kontroll over og som påvirket datasikkerheten, spesielt da ifht Emberland som tapte alle data.

Slik retten ser det benyttet Nordlo seg ikke av de tilgjengelige adekvate tiltak som kunne forhindret angrepet eller redusert følgene av dette. Hindringen var ikke utenfor Nordlos kontroll i dette tilfellet, idet Nordlo ikke hadde iverksatt sikkerhetstiltak som bl.a. krav om tofaktorautentisering, regionsperre, oppdatert programvare og dels back-up fysisk atskilt i eget nettverk. Sistnevnte som nevnt ifht Emberland. Det forelå ikke en force-majeure hendelse som omfattes av avtalenes punkt 8.

Det følger av avtalen at saksøkerne kan kreve «erstatning for dokumentert økonomisk tap etter alminnelige prinsipper for erstatninger i avtaleforhold». Slik retten forstod det er det ikke uenighet om at det er tale om en avtalt generisk ytelse hvor Nordlo er erstatnings-ansvarlig på objektivt grunnlag for misligholdet overfor saksøkerne hva gjelder deres direkte tap. For saksøkernes indirekte tap kreves i tillegg uaktsomhet fra Nordlos side.

Det neste spørsmålet er imidlertid om de avtalte begrensingene i avtalen kommer til anvendelse, eller om disse må settes til side slik saksøkerne anfører. Avtalenes ordlyd skal i utgangspunktet tolkes objektivt, og ordlyden tillegges stor vekt, jf. bl.a. Rt-2002-1155 og Rt-2010-1345 avsnitt 59.

Retten viser til de siterte avtalebestemmelsene ovenfor, og under punkt 10 fremgår – med rettens understreking - bl.a. følgende ordlyd under «*Erstatning, ansvarsbegrensning»; Ved mislighold i henhold til pkt. 10, kan den part som rammes kreve erstatning for dokumentert økonomisk tap etter alminnelige prinsipper for erstatninger i avtaleforhold. Indirekte tap dekkes imidlertid ikke. Som indirekte tap regnes, dog ikke begrenset til, Kundens tap av fortjeneste av enhver art, tap grunnet driftsavbrudd, avsavnstap, samt krav fra tredjepart. Erstatningskravet etter denne bestemmelse kan ikke overstige et beløp som tilsvarer 3 månedsleier i henhold til denne Avtalen.*

Saksøkerne har vist til, jf. siterte avtalebestemmelser ovenfor, at Nordlo påtok seg ansvaret for drift av saksøkernes dataprogrammer, altså drift og tilgang til funksjonalitet og virkemåte i programmene. Videre garanterte Nordlo for en 99,5% oppetid og responstid, og etter avtalen skulle de skulle ta sikkerhetskopi av saksøkernes data flere ganger daglig. Det er bl.a. vist til at det er benyttet begrepet «sikkerhetskopi», og at disse skulle tilbakeleveres kunde på forespørsel, jf. anførslene gjengitt på side 5-7 ovenfor, med henvisninger til litteratur og rettspraksis.

Slik retten ser det inneholder ikke avtalen om oppetid en «tom garanti» som innebærer at ansvarsbegrensningene i punkt 10 må settes til side som følge av ordlydsmotstrid. Kravet til høy oppetid innebærer en forpliktelse for Nordlo og en forventning hos saksøkerne om rask respons fra Nordlo ved eventuell nedetid/feil som oppstår. Om Nordlo ikke oppfyller sin forpliktelse om bl.a. oppetid suspenderes kundens betalingsforpliktelse for den aktuelle perioden, samtidig som kunden også vil kunne kreve dekket sitt direkte økonomiske tap, begrenset inntil tilsvarende 3 månedsleier. Det er ikke tale om en tom garanti, men en avtale med klar avgrensning ifht det økonomiske tap som kreves dekket av Nordlo. Avtalen er enkel å forstå og det foreligger etter rettens syn ingen uklarheter eller motstrid i avtalebestemmelsene som innebærer at ansvarsbegrensningen må settes til side.

Saksøkerne har videre anført at avtalen må revideres for «brudd på hovedforpliktelsene» eller forutsetningsbetraktninger med henvisning til at et vesentlig kontraktsbrudd ikke vil få virkning om begrensningen skal stå seg, og at ordlyden derfor må tolkes innskrenkende. Ved rettens vurdering er det mange av de samme momentene som gjør seg gjeldende ved vurderingene av om Nordlo har handlet grovt uaktsomt og om ansvarsbegrensningene skal settes til side som urimelige etter avtaleloven §36.

Retten vil derfor først gi en generell beskrivelse og vurdering av avtalens bestemmelser og oppbygging, en vurdering av Nordlos handlemåte, før retten deretter knytter dette opp mot saksøkernes anførsler.

Når avtalen som helhet skal vurderes må avtalens bestemmelser gjengitt ovenfor og Nordlos forpliktelser etter denne ses i sammenheng med det vederlag saksøkerne betalte for ASP-tjenesten og de krav som ble stilt til kunden.

Det er på det rene at Norsk Medikal betalte 3 693 kroner, Emberland 2 945 kroner og Utvik 13 584 kroner pr. måned til Nordlo for ASP-tjenesten ved inngåelsen av avtalen. De nevnte vederlag bestod av delbeløp for ASP-løsningen, lisens på Officepakken og Visma, for PC, Office Pro, Exchange og for MS SQL, som ble multiplisert med antall brukere. I tillegg ble det betalt for epost og for virtuell server. I vederlaget lå f.eks. ikke rådgivningstjeneste, da bistand utover avtalen ble betalt pr. time.

Retten vil bemerke at det er tale relativt beskjedne vederlag for det som er angitt ovenfor vurdert opp mot kostnadene som ville påløpt om kunden selv skulle drifte dette internt med datautstyr og egen IT-ansvarlig, enten ansatt eller konsulent på timebasis. Vederlaget gjenspeiler etter rettens syn på ingen måte den betydelige forretningsrisiko det vil innebære for Nordlo om Nordlo også skulle være erstatningsansvarlig utover de avtalte 3 månedsleiene for direkte tap. Nordlo har mellom 250-300 kunder av ulik størrelse og ulik omsetning, og det indirekte tapet, som f.eks. fortjenestetap, som etter avtalen ikke kan kreves, vil kunne bli betydelige. Ifølge Solberg kunne de beskytte kundenes data i sitt system, men de kunne ikke garantere for sikkerheten.

Ansvarsbegrensningen må ses i sammenheng med avtalens punkt 3 hvor det - med rettens understreking – fremgår som «Krav til kunden» at: «*Kunden er ansvarlig for å bruke utstyr, programmer og data som foreskrevet, samt legge forholdene til rette slik at Leverandøren kan utføre sine plikter, herunder ved å gi Leverandøren nødvendig tilgang til sine lokaler, programmer, data, adekvat informasjon etc. Kunden er ansvarlig for arbeidsstasjon og nettverk for å kommunisere med data-sentralen til Leverandøren. Kunden er selv ansvarlig for å forsikre verdien av egne data*.»

Det fremgår således uttrykkelig av avtalen at det er begrenset ansvar for Nordlo og at kunden selv må tegne forsikring – såkalt cyberforsikring – for verdien av egne data. Ingen av saksøkerne valgte å gjøre dette. Det skal bemerkes at flere av Nordlos kunder hadde tegnet cyberforsikring og fikk datateknisk bistand rekvirert av forsikringsselskapet for å begrense sine tap. Saksøkerne har anført at en cyberforsikring ikke dekker direkte og indirekte tap, noe det ikke ble ført bevis for at er tilfelle. Det fremgår bl.a. av Scjølberg «Cyberkriminalitet» kapittel 10 «Cyberkriminalitet og forsikring» side 141 at «*Ved avtale om cyberforsikring omfatter forsikringstilbudet fra Gjensidige blant annet at bedriften får IT-bistand og hjelp til å minimalisere skadevirkningene hvis bedriften skulle bli utsatt for dataangrep. Bedriften får også dekket kostnader til å reinstallere og gjenopprette data og programvare samt eventuelt driftstap*.» (rettens understreking).

Om avtalen ikke hadde inneholdt en ansvarsbegrensning legger retten uten videre til grunn at Nordlos vederlag da ville gjenspeilt den betydelige forretningsrisikoen det potensielle erstatningsansvaret medførte for Nordlo. Nordlo måtte selv forsikret seg mot dette, om det lot seg gjøre. Med 250-300 kunder av ulik størrelse og omsetning sier det seg selv at vederlaget måtte vært markert høyere enn det faktisk var. Det ville for øvrig vært vanskelig for Nordlo å vurdere hele kundeporteføljens potensielle direkte og indirekte økonomiske tap ved et hackerangrep og nedetid som i dette tilfelle. Det er slik retten ser det både hensiktsmessig og mest naturlig at det var den enkelte kunde som var nærmest til å tegne cyberforsikring tilpasset dennes behov, og det er også hos saksøkerne avtalen eksplisitt plasserer ansvaret for å gjøre dette.

Nordlo kan etter rettens syn lastes for at det ikke ble stilt krav om tofaktorautentisering overfor den enkelte kunde som hadde tilgang til Nordlos datasystemer via ASP-tjenesten. Det var som nevnt tidligere mange brukere hos Nordlo - og også generelt sett - som valgte bort en slik sikkerhetsløsning våren 2021, selv om det var anbefalt av Nordlo overfor kundene. Nordlo kunne som dataleverandør imidlertid stilt krav om slik pålogging, evt. «isolert» kunden og tatt høyere vederlag. På den måten ville sikkerheten både for Nordlo selv og de øvrige kundene vært ivaretatt på et høyere sikkerhetsnivå. Dette tiltaket ville i hvert fall gjort tilgangen til systemet betydelig vanskeligere for angriperne. Regionsperre kan brukes som sikkerhetstiltak, men dette er vurderingssak ifht kundenes reisevirksomhet og kan være vanskelig i praksis. Hertil kommer det forhold at regiosperre kan omgås ved å bruke VPN-tilbydere, og om brukerkontoen f.eks. er atea.no vet de at denne er plassert i Norge.

I følge sakkyndig vitne Thorsheim var det alvorlige mangler i forhold til de forventninger en har til denne type driftsmiljø. Han pekte bl.a. på manglende tofaktorautenisering, manglende regionsperre, ikke regelmessig passordskifte og manglende segmentering. Ifølge Thorsheim eskalerte viruset via dårlige passord og dårlig «patchet» programvare. Sakkyndig Skei var mer forsiktig. Han gav uttrykk for at programmene burde vært oppdatert, men pekte samtidig på at det ikke var tale om privilegerte programmer og at angriperne sannsynligvis bare ville blitt forsinket et par timer med å nå sine mål. Var de først innenfor var det minst 200 veier til mål. Han trodde derfor ikke at det var det som hadde vært utslagsgivende i denne saken. Ifølge Solberg hadde en ikke funnet ut av hvordan hackerne fikk administratorrettigheter.

Retten legger til grunn at hackerangrepet mot Nordlo ble utført av godt organiserte utenlandske kriminelle med svært høy teknologisk kompetanse. Selv om sikkerhetstiltak som tofaktorautentisering kunne vært iverksatt er det svært vanskelig å verne seg mot denne type datakriminalitet, og det er rettens oppfatning at det var deres profesjonalitet som var årsaken til at de klarte å ramme Nordlo i en slik grad som de gjorde. Selv om det er påpekt enkelte sårbarheter i Nordlos datasystem vurderer retten bevisene slik at Nordlo har hatt fokus på – og hatt - god datasikkerhet. Ifølge Nordlos daglige leder, Terje Solberg, hadde de daglige rutiner for sjekk av logger for bl.a. brannmurer og back-up, og hadde automatisk overvåkning og varsling ved spesielle hendelser. Sakkyndig vitne Skei forklarte at Nordlo hadde et godt «patchet» operativ-system, som var oppdatert til dags dato. Microsoft-patchene var på plass. Ifølge Solberg byttet alle brukerne regelmessig passord. I tråd med Microsofts anbefalinger må passordskifte ikke være for hyppig, da det kan ha den konsekvens at brukeren lager enklere passord. Skei opplyste at passordskifte omtalt i Ateas rapport gjaldt et engangsskifte etter angrepet. Solberg forklarte at det på servicekontoer – i tråd med anbefalinger- ikke ble byttet passord med mindre det var mistanke om passord som kunne ha kommet på avveie. Skeie mente en måtte ha veldig god kontroll på hvor dette brukes, men at det bør gjøres regelmessig og at det kan diskuteres hvor ofte.

Hackerne kom seg som nevnt inn på datasystemet via brukernavn og passord på avveie. Hackerne logget seg på og foretok en del rekognosering for å kartlegge nettverket, tok ut data og logget av. De var så borte i 15 timer før de logget på igjen på kvelden. De gikk inn via fjernstyringsverktøy via samme domenekontroller som tidligere og slo av antivirus innebygd i Windows, før de deretter detonerte «Ransomware» både manuelt og automatisk på en del servere, som spredde seg via serverne. Det var en «digital eksplosjon» som ifølge Solberg rammet vilkårlig. Serverne ble låst og filer kryptert. Solberg var på vakt og fikk opp varsler om at filer var kryptert, og forstod da med en gang at de med stor sikkerhet var angrepet. Han stengte datasenteret i løpet av minutter ved at strømforsyningen ble slått av. Intern varsling ble sendt ut og det ble satt krisestab. Datatilsynet og kunder ble varslet, og arbeidet med gjenoppretting ble startet og pågikk gjennom helgen. Solberg forklarte at de hadde planer og rutiner, og da angrepet var et faktum var det slike planer som ble fulgt. Skei forklarte at Nordlo var veldig godt i gang med gjenoppretting og hadde ifølge ham kontroll da Atea kom inn i bildet noen dager etter angrepet.

Når det gjelder en av hovedforpliktelsene til Nordlo, nemlig å sikre back-up for kundene, følger det av avtalen at Nordlo skulle ta sikkerhetskopi av kundens data flere ganger daglig og at sikkerhetskopier skulle oppbevares i annen bygning en datasentralen. Dette ble overholdt av Nordlo. Videre skulle Nordlo etter avtalen på kundens forespørsel tilbake-kopiere angitte data fra siste sikkerhetskopi. Nedetiden var lang for saksøkerne, og Emberland fikk aldri sine data tilbake. Da hackerangrepet skjedde hadde Nordlo påbegynt – og nær fullført – arbeidet med å flytte ut back-up i eget nettverk, altså fysisk server i eget nett frikoblet «produksjonsområdet», for å bedre sikkerheten ytterligere. Ifølge Solberg hadde ikke Hydro hatt dette da de ble angrepet, og det hadde vært et av problemene. Om Nordlo hadde vært ferdig med arbeidet hadde de antakelig ikke opplevd de konsekvensene som de gjorde, at de ble mer begrenset, men en kunne ifølge Solberg ikke vite det. Ifølge Skei var det dette arbeidet som reddet Nordlo. Kun 4 av 250 kunder mistet data, noe som ifølge Skei gjorde at de hadde hatt en bra rate.

Solberg forklarte at de under gjenopprettingsarbeidet hadde satt opp skift slik at det ble jobbet døgnet rundt, og hvor opptil 60 ansatte var involvert. Det var ulike team, hvor de foretok en renseprosess på serverne. Dette var ifølge Solberg omfattende og tidkrevende arbeid hvor det var lett å gjøre feil. De måtte være sikre på at virus ikke fulgte med tilbake på serverne. Proplan var inne ved gjenopprettingsarbeidet. De gikk 3 dager tilbake i tid på back-up, da de var sikre på at hackerne ikke hadde vært inne på systemet så lenge. Ifølge Solberg var alle kunder rammet, men noen i mindre grad enn andre. Noen av kundene hadde kriseplaner og håndterte dette derfor bedre enn andre.

Det er ikke tvilsomt at både Nordlo og de tre saksøkerne ble svært hardt rammet ved hackerangrepet, og at saksøkerne hadde lang nedetid som gikk ut over deres omsetning. For Emberland - som mistet alle sine data - var det mest kritisk.

Som retten imidlertid har vært inne på tidligere er den inngåtte avtale - mellom dem som næringsdrivende - klar på hvilke forpliktelser hver av partene har, hvilke ansvarsbegrensninger som gjelder for Nordlo ved mislighold fra deres side, og den er klar på at saksøkerne må tegne forsikring for å få dekket inn evt. økonomisk tap som følge av tap av data, nedetid osv. Det hefter ikke uklarheter ved forståelsen av ordlyden og det foreligger slik retten ser det heller ikke ordlydsmotstrid, jf. hva retten har bemerket om dette tidligere.

Saksøkerne har gjort gjeldende at Nordlos grove brudd på hovedforpliktelsene i kontrakten må føre til at denne revideres og tolkes innskrenkende, slik at ansvarsfraskrivelsen ikke kan gjøres gjeldende overfor saksøkerne. Etter saksøkernes syn kan Nordlo følgelig ikke høres med at ansvaret i sin helhet er fraskrevet ved kontrakt. Det er vist til Viggo Hagstrøm «Obligasjonsrett» 3. utgave s. 687, hvor det fremgår: *«For det annet synes domstolene ikke å ville tillegge en fraskrivelse rettsvirkning etter sitt umiddelbare innhold når det er skjedd et betydningsfullt kontraktsbrudd som ikke ville få virkninger om fraskrivelsen fullt ut skal opprettholdes.»* og videre at *«Innskrenkende fortolkning av fraskrivelsesklausuler som ellers ville ha medført at et betydelig kontraktsbrudd ikke får virkninger, har lang tradisjon i rettspraksis, også innenfor kommersielle avtaleforhold, der ansvars- og risikofraskrivelser er sedvanlige og kan være kombinert med forskjellige forsikringsordninger.»*

Retten vurderer disse anførslene i sammenheng med neste anførsel om at avtalen – gitt at ordlyden er klar og ikke skal revideres – må settes til side basert på forutsetningsbetraktninger. Det er her vist til samme bok av Viggo Hagstrøm s. 690, hvor det bl.a. fremgår at «*Når ordlyden er klar, har domstolene i realiteten underkjent klausuler som ville innebære at betydelige kontraktsbrudd ikke fikk virkninger, ved å anta at forutsetninger for anvendelse av klausulene ikke var til stede, jf. eksempelvis Rt. 1935 s. 497 og Rt. 1969 s. 679.*» Saksøkerne har anført at det var deres forutsetning at de slapp å tenke på sikkerheten, da dette var Nordlos ansvar. I motsatt fall vil det være slik at Nordlo har en forpliktelse, men at det ikke har noen virkning for Nordlo om de bryter avtalen.

Som retten har bemerket tidligere er det rettens oppfatning at Nordlo hadde tilstrekkelig og god sikkerhet, og at det må hensyntas at misligholdet er en følge av et målrettet hackerangrep fra utenlandske profesjonelle aktører. Det er riktig at Nordlo hadde et ansvar for å ivareta sikkerheten, men dette innebærer ikke at også saksøkerne selv har et ansvar for å vurdere hva som kan bli følgene av et hackerangrep mot datasystemet de er en del av. Ingen kan til enhver tid garantere 100% for sikkerheten på et datasystem, og avtalen er som nevnt klar på Nordlos begrensede ansvar og at det er kundens ansvar å benytte seg av muligheten til å forsikre sine data. Anførslene kan etter rettens syn ikke føre frem.

Saksøkerne har videre anført at ansvarsbegrensningene må kjennes ugyldige etter avtaleloven §36, idet det vil virke urimelig eller være i strid med god forretningsskikk å gjøre disse gjeldende. Det vises til anførslene om dette gjengitt under saksøkernes påstandsgrunnlag.

Det følger av avtalelovens §36 andre ledd at det *«Ved avgjørelsen tas hensyn ikke bare til avtalens innhold, partenes stilling og forholdene ved avtalens inngåelse, men også til senere inntrådte forhold og omstendighetene for øvrig.»*

Retten viser til Rt-2012-1537 avsnitt 46, hvor det fremgår at «*Avtaleloven § 36 gir domstolene anledning til å sette til side eller revidere en avtale blant annet når denne på grunn av endrete forhold er blitt urimelig for en part, og til å endre avtalen for å avbøte fortsatt urimelighet. Terskelen for lemping er høy – det er de helt klare urimeligheter som rammes. For avtaler mellom næringsdrivende kreves spesielt mye. Jeg viser til Rt-2003-1132 avsnitt 46, hvor førstvoterende bruker karakteristikken «kvalifisert urimelig» for å angi grensen. En eventuell revisjon skal dessuten være begrenset til det som er nødvendig for å avbøte den kvalifiserte urimeligheten – målet er altså ikke å oppnå et mest mulig balansert avtaleforhold.*»

Videre fremgår det av Hagstrøm, Obligasjonsrett (2021) på side s. 699 at «*For det annet må det sies at kontraktfestede begrensninger av ansvaret for indirekte tap i næringsvirksomhet er lettere å akseptere. Konsekvenstap i næringsvirksomhet kan bli meget omfattende, og det ligger gjerne i de verdier som er involvert, og i virksomhetenes størrelse, at dette generelt sett er påregnelig. For et slikt konsekvenstap kan sterke grunner tilsi at realdebitor må kunne fraskrive ansvaret, samtidig som skadelidte gjerne har oppfordring til å sikre sine egne interesser ved avbruddsforsikring og lignende*.»

Som Høyesterett peker på i Rt-2012-1537 er terskelen høy for å sette en avtale mellom næringsdrivende til side som urimelig, og at det er de helt klare urimeligheter som rammes. I Giertsen, Avtaler 2021, uttales det da også at «*Vi har ennå ingen dom i Høyesterett der et krav etter avtl. § 36 har ført frem mellom profesjonelle (august 2021).*»

Det er i vår sak tale om en avtalt risikofordeling mellom næringsdrivende i en gjensidig bebyrdende avtale, hvor saksøkernes vederlag må vurderes opp mot saksøktes fortjenestemargin og forretningsrisiko uten ansvarsbegrensninger. Det er – som Hagstrøm omtaler like ovenfor – tale om konsekvenstap som kan bli betydelige, og som partene har avtalt at det er saksøkerne som sikre seg mot gjennom forsikring. Selv om Nordlo er profesjonell på IT-sikkerhet er det typisk at det ved mulig hackerangrep fra en tredjepart kan oppstå slikt økonomisk tap. Etter rettens syn er ansvarsbegrensningene ikke urimelige og det vil ikke være i strid med god forretningsskikk å gjøre dem gjeldende. Anførsel om ugyldighet og revisjon etter avtl. §36 kan ikke føre frem.

Slik retten ser det har Nordlo ikke handlet grovt uaktsomt, og saksøkernes anførsel om at disse begrensningene ikke kan gjøres gjeldende som følge av grov uaktsomhet kan derfor heller ikke føre frem. For at en handlemåte skal kunne karakteriseres som grovt uaktsom må denne representere et markert avvik fra vanlig forsvarlig handlemåte, jf. bl.a. Rt-1989-1318 (advokatansvar). Ved vurderingen tillegges det vekt at det er tale om en profesjonell

aktør, hvor aktsomhetsnormen er streng på dennes fagfelt. Retten viser til bemerkningene og vurderingene ovenfor om sikkerheten på datasystemet, hva Nordlo hadde av tiltak – herunder også påbegynt og nær fullført segmentering - og hvilke svakheter og sårbarheter som forelå. Det vises også til at det som det er gitt uttrykk for om et svært profesjonelt utført hackerangrep, og hvordan Nordlo agerte på dette. Etter rettens syn representerer Nordlos handlemåte samlet sett ikke et markert avvik fra de krav og forventninger en må stille datasikkerheten til dem som IT-leverandør av ASP-tjeneste. Det er ikke grunnlag for å sette til side ansvarsbegrensningene i avtalen som følge av grov uaktsomhet.

Oppsummeringsmessig er Nordlo erstatningsansvarlig for saksøkernes direkte tap innenfor rammen av 3 månedsleier, som er i samsvar med inngått avtale. Dette innebærer at Norsk Medikal tilkjennes en erstatning fra Nordlo på 11 079 kroner, Emberland på 8 835 koner og Utvik på 40 752 kroner.

Sakskostnader

Det følger av tvisteloven §20-2 første ledd at en part som har vunnet saken har krav på full erstatning for sine sakskostnader fra motparten. Saken er vunnet hvis parten har fått medhold fullt ut eller i det vesentlige, jf. tvl. §20-2 andre ledd.

I Rettsdatas kommentarer til bestemmelsen fremgår det at:
«*Medhold «i det vesentlige» er oppnådd når resultatet for parten er så gunstig at motparten ikke har oppnådd noe av betydning sammenholdt med det som ville vært situasjonen om motparten hadde akseptert den vinnende parts standpunkt fullt ut før sak ble reist. Parten har da nådd frem på vesentlige punkter. Tilsvarende vil gjelde dersom motparten taper saken praktisk talt fullt ut, bortsett fra å ha fått medhold på et mindre vesentlig punkt. Forarbeidene nevner som eksempel en erstatningssak som omhandler en rekke større erstatningsposter samt en mindre erstatningspost, som får det utfall at motparten kun får medhold i det som gjelder erstatningsposten av bagatellmessig karakter.*

Ved vurderingen av om en part har fått medhold i det vesentlige, er det ikke bare forholdet mellom partenes påstander og domsresultatet som er relevant. Det må også ses hen til hvor hovedtyngden i de reelle tvistepunktene har ligget, jf. Rt. 2010 s. 727. Det skal således foretas en bredere vurdering enn kun den relative differansen mellom påstand og domsresultat, se bl.a. Rt. 2011 s. 699 og Rt. 2013 s. 232. Et avvik fra et angitt maksimumsbeløp kan lettere være forenlig med at saken i det vesentlige er vunnet hvis tvisten hovedsakelig har gjeldt spørsmål om grunnlag for erstatning eller oppreisning, jf. Rt. 2010 s. 508.»

Det er slik retten ser det ikke tvilsomt at Nordlo har fått medhold i det vesentlige, selv om Nordlo ikke fikk medhold i at det forelå en force-majeure hendelse. Det saksøkerne har oppnådd i resultat er av liten og ingen betydning for dem, og minnelige løsninger forut for saksanlegg ville åpenbart vært innenfor rekkevidde dersom dette hadde vært aktuelt for

saksøkerne. Hovedtyngden av saken lå klart på saksøkernes anførsler om tilsidesettelse/ revisjon av ansvarsbegrensningene, som ikke førte frem.

Retten har vurdert hvorvidt det foreligger tungtveiende grunner som tilsier at saksøkerne helt eller delvis skal fritas for erstatningsansvar, jf. tvl. §20-2 tredje ledd, men funnet at så ikke er tilfelle.

Nordlo har etter dette krav på full erstatning, som dekker alle deres nødvendige kostnader ved saken, jf. tvl. §20-5 første ledd. Ved vurderingen av om kostnadene har vært nødvendige, legges det vekt på om det ut fra betydningen av saken har vært rimelig å pådra dem.

Advokat Skoghøy har fremlagt sakskostnadsoppgave der salærkravet er på 890 139 kroner ekskl. mva, for arbeid han og adv.flm. Netland har utført. Det er krevd dekket salær basert på 266 timers arbeid med saken, inkludert reisetid. Det er foretatt tidsfordeling mellom de to prosessfullmektigene og lagt til grunn en gjennomsnittlig timepris fordelt også på de ulike stadier av saken. Gjennomsnittlig timepris på de ulike stadier ligger på hhv 3 237 kroner, 3 044 kroner og 4 300 kroner. Det er opplyst at salæret er redusert i størrelses-orden 39,5 timer, som dog fremkommer med rabatterte timesatser og ikke reduserte arbeidstimer. I tillegg er det krevd 25 559 kroner for kostnader prosessfullmektigene har hatt til reise og opphold, samt 1 500 kroner for utgifter partsrepresentant har hatt til lunsj to rettsdager.

Advokat Haver gav uttrykk for at kravet etter hans syn var høyt. Adv. Haver fremla sakskostnadsoppgave der salærkravet er på 650 000 kroner ekskl. mva, basert på 206 timers arbeid og en gjennomsnittlig timepris på 3 155 kroner. Adv. Haver representerer tre parter, som dog – med unntak av for utmåling av økonomisk tap – har hatt helt sammen-fallende påstandsgrunnlag.

Retten stilte et spørsmålstegn ved at det ble benyttet to prosessfullmektiger/advokater under saksforberedelsen og hovedforhandlingen, og tar til etterretning at begge sider har funnet det nødvendig.

Etter rettens syn er Nordlos sakskostnadskrav høyt sakens omfang og kompleksitet tatt i betraktning. Selv om saken reiste en del juridiske problemstillinger rundt force-majeure og ansvarsbegrensningene i avtalene var sakens faktiske sider begrenset. Hvordan selve hackerangrepet ble gjennomført var ikke omstridt og fokuset var i stor grad rettet mot ulike sider av Nordlos håndtering av sine avtaleforpliktelser og ivaretakelse av datasikkerheten. For denne del av saken var det en del datatekniske forhold – dels kompliserte for ikke datakyndige personer – som måtte belyses. Nordlos prosessfullmektig besvarte spørsmål om slike forhold under saksforberedelsen. Ateas ene rapport stod særlig sentralt – i en dokumentsamling på 176 sider - og det ble ført to sakkyndige vitner i tillegg til at det ble

avgitt partsforklaringer. Når det gjelder utmåling av eventuell erstatning var denne i stor grad basert på skjønnsmessige vurderinger fra saksøkernes side og lite dokumentasjon. Det var i utgangspunktet satt av 4 dager til hovedforhandlingen, noe en antok var god tid. Saken ble i tidsplanen inntatt i sluttinnlegget redusert til 2 ½ dag. Det ble på dag 1 klart at saken kunne avvikles på 2 rettsdager, men Nordlos prosessfullmektig fastholdt at en ønsket å gjennomføre prosedyrene ved oppstart av dag 3, som planlagt. Retten forholdt seg til dette. Adv. Skoghøy har som nevnt opplyst at de har redusert sitt salærkrav med rabattert timepris tilsvarende 39,5 timer. Kravet er likevel 240 000 kroner høyere enn adv. Havers krav. Med høy timesats forutsettes det også en spesialisering som gjenspeiles i hva som er nødvendig tidsforbruk i en konkret sak, og det blir uansett en samlet vurdering hva saken tåler at pådras av kostnader ut fra dens omfang, kompleksitet og betydning for parten. Det samlede erstatningskrav mot Nordlo beløp seg til nær 4 600 000 kroner, selv om den formelle påstanden var at erstatningen skulle utmåles etter rettens skjønn.

Retten har kommet til at salærkravet fra Nordlos prosessfullmektig skal reduseres til 750 000 kroner, jf. tvl. §20-5. I tillegg kommer nevnte 25 559 kroner og 1 500 kroner, slik at samlet beløp blir 777 059 kroner.

De tre saksøkerne har ført felles sak mot Nordlo med identiske påstandsgrunnlag, og retten har kommet til at sakskostnadsansvaret skal være solidarisk, jf. tvl. §20-6.

DOMSSLUTNING

1. Nordlo Haugesund AS dømmes til å betale erstatning til
   - Norsk Medikal AS med 11 079-ellevetusenogsyttini- kroner,
   - Malermesterfirma Emberland AS med 8 835-åttetusenåttehundreogtrettifem- kroner og
   - A. Utvik AS med 40 752-førtitusensjuhundreogfemtito- kroner,

   innen 14-fjorten- dager etter dommens forkynnelse.

2. Norsk Medikal AS, Malermesterfirma Emberland AS og A Utvik AS dømmes – in solidum – til innen 14-fjorten- dager fra dommens forkynnelse å betale Nordlo Haugesund AS sine sakskostnader med 777 059-sjuhundreogsyttisjutusenogfemti-ni- kroner.

Retten hevet

Leif Egil Holstad

Veiledning om anke i sivile saker vedlegges.

Veiledning om anke i sivile saker

I sivile saker er det reglene i tvisteloven kapitler 29 og 30 som gjelder for anke. Reglene for anke over dommer, anke over kjennelser og anke over beslutninger er litt ulike. Nedenfor finner du mer informasjon og veiledning om reglene.

Ankefrist og gebyr
Fristen for å anke er én måned fra den dagen avgjørelsen ble gjort kjent for deg, hvis ikke retten har fastsatt en annen frist. Disse periodene tas ikke med når fristen beregnes (rettsferie):

- fra og med siste lørdag før palmesøndag til og med annen påskedag
- fra og med 1. juli til og med 15. august
- fra og med 24. desember til og med 3. januar

Den som anker, må betale behandlingsgebyr. Du kan få mer informasjon om gebyret fra den domstolen som har behandlet saken.

Hva må ankeerklæringen inneholde?
I ankeerklæringen må du nevne

- hvilken avgjørelse du anker
- hvilken domstol du anker til
- navn og adresse på parter, stedfortredere og prosessfullmektiger
- hva du mener er feil med den avgjørelsen som er tatt
- den faktiske og rettslige begrunnelsen for at det foreligger feil
- hvilke nye fakta, bevis eller rettslige begrunnelser du vil legge fram
- om anken gjelder hele avgjørelsen eller bare deler av den
- det kravet ankesaken gjelder, og hvilket resultat du krever
- grunnlaget for at retten kan behandle anken, dersom det har vært tvil om det
- hvordan du mener at anken skal behandles videre

Hvis du vil anke en tingrettsdom til lagmannsretten
Dommer fra tingretten kan ankes til lagmannsretten. Du kan anke en dom hvis du mener det er

- feil i de faktiske forholdene som retten har beskrevet i dommen
- feil i rettsanvendelsen (at loven er tolket feil)
- feil i saksbehandlingen

Hvis du ønsker å anke, må du sende en skriftlig ankeerklæring til den tingretten som har behandlet saken. Hvis du fører saken selv uten advokat, kan du møte opp i tingretten og anke muntlig. Retten kan tillate at også prosessfullmektiger som ikke er advokater, anker muntlig.

Det er vanligvis en muntlig forhandling i lagmannsretten som avgjør en anke over en dom. I ankebehandlingen skal lagmannsretten konsentrere seg om de delene av tingrettens avgjørelse som er omtvistet, og som det er knyttet tvil til.

Lagmannsretten kan nekte å behandle en anke hvis den kommer til at det er klar sannsynlighetsovervekt for at dommen fra tingretten ikke vil bli endret. I tillegg kan retten nekte å behandle noen krav eller ankegrunner, selv om resten av anken blir behandlet.

<u>Retten til å anke er begrenset i saker som gjelder formuesverdi under 250 000 kroner</u>
Hvis anken gjelder en formuesverdi under 250 000 kroner, kreves det samtykke fra lagmannsretten for at anken skal kunne bli behandlet.

Når lagmannsretten vurderer om den skal gi samtykke, legger den vekt på

- sakens karakter
- partenes behov for å få saken prøvd på nytt
- om det ser ut til å være svakheter ved den avgjørelsen som er anket, eller ved behandlingen av saken

Hvis du vil anke en tingretts kjennelse eller beslutning til lagmannsretten
En *kjennelse* kan du som hovedregel anke på grunn av

- feil i de faktiske forholdene som retten har beskrevet i kjennelsen
- feil i rettsanvendelsen (at loven er tolket feil)
- feil i saksbehandlingen

Kjennelser som gjelder saksbehandlingen, og som er tatt på bakgrunn av skjønn, kan bare ankes dersom du mener at skjønnsutøvelsen er uforsvarlig eller klart urimelig.

En *beslutning* kan du bare anke hvis du mener

- at retten ikke hadde rett til å ta denne typen avgjørelse på det lovgrunnlaget, eller
- at avgjørelsen åpenbart er uforsvarlig eller urimelig

Hvis tingretten har avsagt dom i saken, kan tingrettens avgjørelser om saksbehandlingen ikke ankes særskilt. Da kan dommen isteden ankes på grunnlag av feil i saksbehandlingen.

Kjennelser og beslutninger anker du til den tingretten som har avsagt avgjørelsen. Anken avgjøres normalt ved kjennelse etter skriftlig behandling i lagmannsretten.

Hvis du vil anke lagmannsrettens avgjørelse til Høyesterett
Høyesterett er ankeinstans for lagmannsrettens avgjørelser.

Anke til Høyesterett over *dommer* krever alltid samtykke fra Høyesteretts ankeutvalg. Samtykke gis bare når anken gjelder spørsmål som har betydning utover den aktuelle saken, eller det av andre grunner er særlig viktig å få saken behandlet av Høyesterett. Anke over dommer avgjøres normalt etter muntlig forhandling.

Høyesteretts ankeutvalg kan nekte å ta anker over *kjennelser* og *beslutninger* til behandling dersom anken ikke reiser spørsmål av betydning utover den aktuelle saken, og heller ikke andre hensyn taler for at anken bør prøves. Anken kan også nektes fremmet dersom den reiser omfattende bevisspørsmål.

Når en anke over kjennelser og beslutninger i tingretten er avgjort ved kjennelse i lagmannsretten, kan avgjørelsen som hovedregel ikke ankes videre til Høyesterett.

Anke over lagmannsrettens kjennelser og beslutninger avgjøres normalt etter skriftlig behandling i Høyesteretts ankeutvalg.

Veiledning om anke i sivile saker

I sivile saker er det reglene i tvisteloven kapitler 29 og 30 som gjelder for anke. Reglene for anke over dommer, anke over kjennelser og anke over beslutninger er litt ulike. Nedenfor finner du mer informasjon og veiledning om reglene.

Ankefrist og gebyr
Fristen for å anke er én måned fra den dagen avgjørelsen ble gjort kjent for deg, hvis ikke retten har fastsatt en annen frist. Disse periodene tas ikke med når fristen beregnes (rettsferie):

- fra og med siste lørdag før palmesøndag til og med annen påskedag
- fra og med 1. juli til og med 15. august
- fra og med 24. desember til og med 3. januar

Den som anker, må betale behandlingsgebyr. Du kan få mer informasjon om gebyret fra den domstolen som har behandlet saken.

Hva må ankeerklæringen inneholde?
I ankeerklæringen må du nevne

- hvilken avgjørelse du anker
- hvilken domstol du anker til
- navn og adresse på parter, stedfortredere og prosessfullmektiger
- hva du mener er feil med den avgjørelsen som er tatt
- den faktiske og rettslige begrunnelsen for at det foreligger feil
- hvilke nye fakta, bevis eller rettslige begrunnelser du vil legge fram
- om anken gjelder hele avgjørelsen eller bare deler av den
- det kravet ankesaken gjelder, og hvilket resultat du krever
- grunnlaget for at retten kan behandle anken, dersom det har vært tvil om det
- hvordan du mener at anken skal behandles videre

Hvis du vil anke en tingrettsdom til lagmannsretten
Dommer fra tingretten kan ankes til lagmannsretten. Du kan anke en dom hvis du mener det er

- feil i de faktiske forholdene som retten har beskrevet i dommen
- feil i rettsanvendelsen (at loven er tolket feil)
- feil i saksbehandlingen

Hvis du ønsker å anke, må du sende en skriftlig ankeerklæring til den tingretten som har behandlet saken. Hvis du fører saken selv uten advokat, kan du møte opp i tingretten og anke muntlig. Retten kan tillate at også prosessfullmektiger som ikke er advokater, anker muntlig.

Det er vanligvis en muntlig forhandling i lagmannsretten som avgjør en anke over en dom. I ankebehandlingen skal lagmannsretten konsentrere seg om de delene av tingrettens avgjørelse som er omtvistet, og som det er knyttet tvil til.

Lagmannsretten kan nekte å behandle en anke hvis den kommer til at det er klar sannsynlighetsovervekt for at dommen fra tingretten ikke vil bli endret. I tillegg kan retten nekte å behandle noen krav eller ankegrunner, selv om resten av anken blir behandlet.

<u>Retten til å anke er begrenset i saker som gjelder formuesverdi under 250 000 kroner</u>
Hvis anken gjelder en formuesverdi under 250 000 kroner, kreves det samtykke fra lagmannsretten for at anken skal kunne bli behandlet.

Når lagmannsretten vurderer om den skal gi samtykke, legger den vekt på

- sakens karakter
- partenes behov for å få saken prøvd på nytt
- om det ser ut til å være svakheter ved den avgjørelsen som er anket, eller ved behandlingen av saken

Hvis du vil anke en tingretts kjennelse eller beslutning til lagmannsretten
En *kjennelse* kan du som hovedregel anke på grunn av

- feil i de faktiske forholdene som retten har beskrevet i kjennelsen
- feil i rettsanvendelsen (at loven er tolket feil)
- feil i saksbehandlingen

Kjennelser som gjelder saksbehandlingen, og som er tatt på bakgrunn av skjønn, kan bare ankes dersom du mener at skjønnsutøvelsen er uforsvarlig eller klart urimelig.

En *beslutning* kan du bare anke hvis du mener

- at retten ikke hadde rett til å ta denne typen avgjørelse på det lovgrunnlaget, eller
- at avgjørelsen åpenbart er uforsvarlig eller urimelig

Hvis tingretten har avsagt dom i saken, kan tingrettens avgjørelser om saksbehandlingen ikke ankes særskilt. Da kan dommen isteden ankes på grunnlag av feil i saksbehandlingen.

Kjennelser og beslutninger anker du til den tingretten som har avsagt avgjørelsen. Anken avgjøres normalt ved kjennelse etter skriftlig behandling i lagmannsretten.

Hvis du vil anke lagmannsrettens avgjørelse til Høyesterett
Høyesterett er ankeinstans for lagmannsrettens avgjørelser.

Anke til Høyesterett over *dommer* krever alltid samtykke fra Høyesteretts ankeutvalg. Samtykke gis bare når anken gjelder spørsmål som har betydning utover den aktuelle saken, eller det av andre grunner er særlig viktig å få saken behandlet av Høyesterett. Anke over dommer avgjøres normalt etter muntlig forhandling.

Høyesteretts ankeutvalg kan nekte å ta anker over *kjennelser* og *beslutninger* til behandling dersom anken ikke reiser spørsmål av betydning utover den aktuelle saken, og heller ikke andre hensyn taler for at anken bør prøves. Anken kan også nektes fremmet dersom den reiser omfattende bevisspørsmål.

Når en anke over kjennelser og beslutninger i tingretten er avgjort ved kjennelse i lagmannsretten, kan avgjørelsen som hovedregel ikke ankes videre til Høyesterett.

Anke over lagmannsrettens kjennelser og beslutninger avgjøres normalt etter skriftlig behandling i Høyesteretts ankeutvalg.