Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

Reglene om tapsfordeling ved misbruk av elektroniske signaturløsninger i finansavtaleloven 2020 kapittel 3 del III

Forfattere: Slyngstadli, Ole Martin Juul og Kjørven, Marte Eidsand

Publiseringsdato: 23. mai 2023
Publisert av: Karnov forlag
Inngår i artikkelsamling: Bruk og misbruk av elektronisk identifikasjon – ISBN 978-82-93816-31-7
Lenke til hele publikasjonen i Lovdata Pro: https://lovdata.no/pro/KARNOV/karnov-2022-03

Artikkelen ble publisert 23. mai 2023. Kilder det er lenket til, kan senere ha blitt erstattet eller fjernet.

1 Innledning[1]

Ny finansavtalelov ble vedtatt i desember 2020 og trådte i kraft 1. januar 2023.[2] Loven viderefører i stor grad reglene i finansavtaleloven 1999[3], men inneholder også enkelte nyvinninger. En slik nyvinning er reglene i lovens kapittel 3 del III om blant annet tapsfordeling når avtaler om finansielle tjenester er basert på ID-tyveri og signert med en falsk elektronisk signatur. Det er disse reglene som er tema for denne artikkelen.

La oss begynne med et eksempel: Hans Tastad misbruker Peder Ås' BankID til å inngå en låneavtale med Lillevik Forbrukslånsbank i Ås' navn og stikker deretter av med pengene. Hans Tastad vil i en slik situasjon alltid være skadevolder og erstatningsrettslig ansvarlig for banken og eventuelt Peder Ås' (skadelidtes) tap. Fordi det kan være vanskelig å få dekning for tapet direkte fra svindleren, har vi imidlertid sett i praksis at bankene ofte har

[1] Deler av artikkelen er basert på Ole Martin Juul Slyngstadli, «Ansvar ved misbruk av digital signatur», i Anders Løvlie, Axel Hodnefjeld og Kristine-Petrine Olthuis, red., *Festskrift, Jussbuss 50 år*, Oslo, 2021, s. 89–103.

[2] Lov 18. desember 2020 nr. 146 om finansavtaler (finansavtaleloven).

[3] Lov 25. juni 199 nr. 46 om finansavtaler og finansoppdrag (finansavtaleloven)

rettet krav mot BankID-innehaveren istedenfor. Påstanden vil da være at også BankID-innehaveren er skadevolder i erstatningsrettslig forstand, idet uaktsom håndtering av BankID har muliggjort svindelen, og på den måten påført banken et tap. Peder Ås har for eksempel lagt fra seg BankID-brikken på kontoret og/eller har et passord som er lett å gjette, og dette kan utgjøre ansvarsgrunnlag for et erstatningsansvar overfor Lillevik Forbrukslånsbank.

De nye reglene i finansavtaleloven §§ 3-20 og 3-21 oppstiller begrensninger i bankenes adgang til å holde BankID-innehaveren ansvarlig på erstatningsrettslig grunnlag i slike situasjoner. I tillegg oppstiller kapittel 3 del III plikter for brukerne av elektroniske signaturløsninger (i loven kalt «rettighetshaver»), i praksis BankID-innehaverne, i § 3-19. Kapittelet inneholder også plikter for henholdsvis aktørene som tilbyr elektroniske signaturløsninger (i loven kalt «tilbyderen»), se § 3-17, og finansinstitusjoner som tilbyr å inngå avtaler om finansielle tjenester med bruk av slike systemer (i loven kalt «tjenesteytere»), se § 3-18.

Bestemmelsene om tapsfordeling ved misbruk av elektronisk signatur er utformet etter modell av reglene om ansvar for tap ved misbruk av betalingsinstrumenter (ikke-godkjente betalingstransaksjoner).[4] Reglene om tapsfordeling etter ikke-godkjente betalingstransaksjoner er felleseuropeiske og følger av direktiv (EU) 2015/2366 om betalingstjenester (PSD 2).[5] Verken PSD 2 eller andre rettsakter fra EØS stiller krav til nasjonal rett når det gjelder tapsfordelingen etter misbruk av elektroniske signaturløsninger.[6] Reglene om dette i finansavtaleloven kapittel 3 del III er altså særnorske. Selv om misbruk av elektronisk signatur ikke er regulert i PSD 2, følger det av forarbeidene at reglene må ses i sammenheng med de PSD 2-baserte reglene om ikke-godkjente betalingstransaksjoner.[7] Dette gjelder særlig fordi man i Norge bruker en teknisk løsning, BankID, som fungerer både som en elektronisk ID (eID), et betalingsinstrument og en elektronisk signaturløsning. Reglene skal sikre et likt beskyttelsesnivå for BankID-innehaveren enten en svindler velger å misbruke BankID til å tømme offerets konto (ikke-godkjente betalingstransaksjoner) eller til å signere en låneavtale (eller andre avtaler om finansielle tjenester) i offerets navn.

Formålet med denne artikkelen er å gi en oversikt over de nye reglene om misbruk av elektronisk signatur i finansavtaleloven kapittel 3 del III. Reglene er på noen punkter

---

[4] Prop. 92 LS (2019–2020) s. 183.

[5] Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked.

[6] Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked har regler om elektronisk signatur, men regulerer ikke spørsmål om tapsfordeling ved misbruk.

[7] Prop. 92 LS (2019–2020) s. 173.

uklare, og det er ikke rom for å gå i dybden på alle problemstillingene reglene reiser, utover den oversikten artikkelen er ment å gi.

I punkt 2 skal vi gå nærmere inn på reglenes forhistorie og hvilke hensyn de er ment å ivareta. Deretter vil vi i punkt 3 redegjøre for reglenes anvendelsesområde, begrepsbruk og fravikelighet og i punkt 4 for hvilke plikter som pålegges ulike involverte aktører.

Den sentrale bestemmelsen om tapsfordeling følger av finansavtaleloven § 3-20, som begrenser omfanget av det ansvaret pseudounderskriveren[8] (BankID-innehaveren) pådrar seg etter «ellers gjeldende rettsregler». Dette er i hovedsak en henvisning til et mulig erstatningsansvar for pseudounderskriveren med hjemmel i alminnelige erstatningsrettslige regler. I punkt 5 skal vi gå nærmere inn i hva som skal til for at vilkårene for erstatning er oppfylt, særlig i lys av Høyesteretts avgjørelse i HR-2020-2021-A (Easybank-dommen).

Dersom vilkårene for å holde pseudounderskriveren ansvarlig etter alminnelige erstatningsrettslige regler er oppfylt, er omfanget av ansvaret begrenset til de egenandelene som følger av finansavtaleloven § 3-20 annet til femte ledd. Pseudounderskriveren er normalt ansvarlig for en egenandel på 450 kroner, jf. annet ledd. Av tredje ledd følger det at pseudounderskriveren svarer med en egenandel på 12 000 kroner der tapet skyldes at hen grovt uaktsomt har unnlatt å oppfylle pliktene som følger av finansavtaleloven § 3-19. Dersom pliktene er brutt forsettlig, må pseudounderskriveren dekke hele tapet, jf. fjerde ledd. Hva som skal til for å konstatere henholdsvis grovt uaktsomt og forsettlig pliktbrudd, blir behandlet i punktene 6 og 7.

I finansavtaleloven § 3-20 femte ledd er det et unntak fra reglene om kundens egenandeler: På visse vilkår, blant annet dersom tapet skyldes tjenesteyteren selv, eller tap har oppstått etter at pseudounderskriveren har varslet om fare for misbruk, må tjenesteyteren i alle tilfeller bære tapet selv. Det gjelder altså selv om pseudounderskriveren har opptrådt grovt uaktsomt eller forsettlig. Hva unntakene nærmere bestemt betyr, behandles i punkt 8.

Endelig har finansavtaleloven § 3-21 en bestemmelse om lemping av rettighetshaverens egenandelsansvar. Bestemmelsen vil bli behandlet i punkt 9, før vi kommer med noen avsluttende bemerkninger i punkt 10.

2 Forhistorie og hensyn

Samfunnet generelt, og finansnæringen spesielt, har vært gjennom en eventyrlig digitaliseringsreise. For bankene har utviklingen gitt store rasjonaliserings- og

[8] Begrepet «pseudounderskriver» benyttes som «benevnelse på den som tilsynelatende har skrevet den ugyldige elektroniske signaturen», jf. Prop. 92 LS (2019–2020) s. 174. I artikkelen brukes begrepet som synonym for «rettighetshaver», jf. finansavtaleloven § 3-16 bokstav b.

effektivitetsgevinster.[9] Samtidig innebærer utviklingen økt risiko for svindel og økonomiske tap, særlig i relasjon til betalingstransaksjoner og låneopptak.

I 2013 nedsatte Finans Norge en arbeidsgruppe som skulle vurdere ulike problemstillinger som oppstår ved (hel)digitalisering av prosessen med søknad og innvilgelse av lån.[10] Arbeidsgruppen pekte på at elektronisk kredittbehandling ville gi en raskere og mer effektiv saksbehandling, som ville frigjøre ressurser i bankene, og at kundene på sin side ville nyte godt av raskere utbetaling av kreditt. Arbeidsgruppen pekte imidlertid også på at digitalisering ville medføre at det «oppstår nye former for risiko». Spesifikt pekes det på at svært rask saksbehandling

«kan åpne for kjøpepress og uoverveid opptak av kreditt til spill, kjøp av rusmidler, risikofylte investeringer, risiko for kriminelle anslag, vold og press i familieforhold etc. Risiko for falsk og forfalskning vil også være annerledes ved at forfalskning blir knyttet opp mot en anonym avtalesituasjon og bruken av elektronisk legitimasjon som BankID. Bankens mulighet for å fange opp slike situasjoner vil være mindre enn ved et fysisk møte. Det samme gjelder risikoen for ugyldighet ved sinnssykdom hos kredittkunden og tilblivelsesmangler som kan oppstå fordi det ikke har foregått en tilstrekkelig utveksling av konkret og individuell informasjon ved avtaleinngåelsen» (vår kursivering).[11]

Arbeidsgruppen viste videre til at dersom BankID misbrukes til å disponere over en innskudds- eller kredittkonto i nettbanken, ville BankID-innehaveren være beskyttet mot tap gjennom reglene i daværende finansavtalelov 1999 § 35 om uautoriserte betalingstransaksjoner. Hovedregelen var den samme da som nå: Banken må bære tapet. Det gjelder selv om kunden eventuelt har vært uaktsom. Ved misbruk av BankID til inngåelse av kredittavtaler peker arbeidsgruppen på at det derimot vil være «et alminnelig uaktsomhetsansvar som gjelder», og her er det «intet øvre tak på det erstatningsansvar som vedkommende kan pådra seg». Finans Norges arbeidsgruppe antok imidlertid at

«bankene må forvente at domstolene vil se hen til regelen i fin.avtl. § 35, og legge en noe strengere uaktsomhetsnorm til grunn (enn simpelt uaktsomhetsansvar) hva gjelder kundens oppbevaring av BankID/sikkerhetsmekanisme og oppdatering av programvare

---

[9] Prop. 92 LS (2019–2020) s. 184.

[10] Finans Norge. *Elektroniske kredittavtaler. De ulike stadier for en elektronisk kredittavtale og de juridiske problemstillinger som oppstår.* Finans Norge 2013. Hentet fra https://www.finansnorge.no/aktuelt/nyheter/2013/10/rapport-om-juridiske-problemstillinger-ved-elektroniske-kredittavtaler-/ (hentet 31.03.2023). Denne artikkelen lå inntil starten av 2023 tilgjengelig på Finans Norges hjemmesider, men er nå tilsynelatende fjernet.

[11] Finans Norge. *Elektroniske kredittavtaler. De ulike stadier for en elektronisk kredittavtale og de juridiske problemstillinger som oppstår.* Finans Norge 2013. Hentet fra https://www.finansnorge.no/aktuelt/nyheter/2013/10/rapport-om-juridiske-problemstillinger-ved-elektroniske-kredittavtaler-/ (hentet 31.03.2023), s. 8. Denne artikkelen lå inntil starten av 2023 tilgjengelig på Finans Norges hjemmesider, men er nå tilsynelatende fjernet.

mv. i den nedre del av uaktsomhetsskalaen. Arbeidsgruppen anbefaler således at bankene til en viss grad påtar seg ansvar og 'pulveriserer' tap som oppstår i den nedre del av uaktsomhetsskalaen når det gjelder håndtering og bruk av BankID/ sikkerhetsmekanismene i forhold til kredittavtaler».[12]

Rapporten viser at finansnæringen i lang tid har vært klar over den økte risikoen for ID-tyveri og falsk som ville komme med en digitalisering av kredittprosessen. Nå, ti år senere, vet vi at risikoen også materialiserte seg.[13] Derimot fikk Finans Norges arbeidsgruppe ikke rett i at domstolene ville se hen til finansavtalelovens regler om uautoriserte betalingstransaksjoner, og kreve en kvalifisert form for skyld før privatpersoner ble pålagt å betale bankers tap etter svindel utført av tredjepersoner. Tvert imot er det en omfattende underrettspraksis som har lagt til grunn en svært streng aktsomhetsnorm for pseudounderskriveren.[14] Eksempler på forhold som har blitt lagt til grunn som erstatningsbetingende uaktsomhet av domstolene og Finansklagenemnda, er å bruke nettbanken i samme rom som samboer og å skrive ned passordet selv om man er 93 år og har Alzheimers sykdom.[15]

Etter at disse historiene etter hvert kom frem i offentligheten, startet diskusjonene om hvorvidt ofre for ID-tyveri hadde god nok rettslig beskyttelse. Justis- og beredskapsdepartementet sendte i 2017 ut et høringsnotat med forslag til ny finansavtalelov.[16] Forslaget inneholdt nye regler om tapsfordeling ved misbruk av digitale signaturer, utformet etter modell av reglene om tapsfordeling ved uautoriserte betalingstransaksjoner. Det innebar at finansnæringen måtte ta en større andel av tapet. Til tross for store protester fra næringen i høringsrunden, ble forslaget fra 2017, med enkelte endringer, fulgt opp med en proposisjon 29. april 2020.[17]

---

[12] Finans Norge. *Elektroniske kredittavtaler. De ulike stadier for en elektronisk kredittavtale og de juridiske problemstillinger som oppstår.* Finans Norge 2013. Hentet fra https://www.finansnorge.no/aktuelt/nyheter/2013/10/rapport-om-juridiske-problemstillinger-ved-elektroniske-kredittavtaler-/ (hentet 31.03.2023), s. 8. Denne artikkelen lå inntil starten av 2023 tilgjengelig på Finans Norges hjemmesider, men er nå tilsynelatende fjernet.

[13] En empirisk undersøkelse av saker behandlet hos de gratis rettshjelptiltakene Jussbuss, Juridisk rådgivning for kvinner (JURK) og Gatejuristen viser at disse tre tiltakene i perioden 2015–2021fikk inn minst 180 saker om misbruk av eID i forbindelse med opptak av lån, se E.B. Brataas, M.S. Stokke, A. Svensson, *Rapport om misbruk av eID*, Universitetet i Oslo, 2022.

[14] Prop. 92 LS (2019–2020) s. 175.

[15] Se Marte Eidsand Kjørven, «BankID-svindel og økonomiske justismord», *Lov og Rett*, nr. 1. 2021, s. 5–6 med videre referanser.

[16] Justis- og beredskapsdepartementet (2017) – Snr. 17/4746. Marte Eidsand Kjørven, en av forfatterne av denne artikkelen, har vært med å skrive høringsnotatet som ansatt rådgiver i Lovavdelingen.

[17] Prop. 92 LS (2019–2020)

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

I proposisjonen uttalte departementet at det ikke finnes gode grunner til å forskjellsbehandle tilfeller av svindel med betalingstransaksjoner og svindel i forbindelse med kredittavtaler.[18] Det er videre vist til at en rettstilstand

«der gevinsten først og fremst kommer næringen selv til gode, mens det først og fremst er kunden som skal ha risikoen for misbruk, … neppe [er] holdbar på sikt hvis man ønsker å opprettholde tilliten til digitale løsninger».[19]

Risiko- og pulveriseringshensyn står også sentralt. Det uttales i proposisjonen blant annet at finansinstitusjonene

«har langt flere muligheter enn den enkelte rettighetshaveren til å iverksette tiltak for å unngå at tredjepersoner misbruker de elektroniske signaturfremstillingsdataene, og til å pulverisere tap i den forbindelse. Departementet viser som eksempel til at når kredittyteren utbetaler kredittbeløp til andre enn rettighetshaveren selv, og stiller kredittbeløpene til disposisjon svært raskt, må det kunne hevdes at kredittyteren selv legger forholdene til rette for misbruk».[20]

Etter at proposisjonen ble fremlagt, fortsatte diskusjonene og debatten, og det var også uenighet blant Justiskomiteens medlemmer på Stortinget.[21] Fremskrittspartiets medlemmer stemte mot vedtakelse av de nye reglene om misbruk av elektroniske signaturløsninger. Øvrige partier var for, men ønsket seg i ulik grad ytterligere vern for privatpersoner sammenliknet med departementets forslag. Reglene ble til slutt vedtatt av Stortinget i desember 2020, men med enkelte endringer knyttet til kundens ansvar for tap ved forsettlig pliktbrudd (se nærmere om dette i punkt 7). Likevel skulle det gå over to år til før reglene omsider trådte i kraft i januar 2023.

Til tross for store diskusjoner og til dels høy temperatur i debatten som til slutt ledet frem til reglene om tapsfordeling ved misbruk av elektroniske signeringsløsninger i finansavtaleloven kapittel 3 del III, er utviklingen i tråd med en 40 års gradvis utvidelse av forbrukervernet knyttet til økonomisk svindel knyttet til digitalisering av finansielle tjenester. Allerede i 1985 ble det innført regler om tapsfordeling ved misbruk av kredittkort i kredittkjøpsloven.[22] På slutten av 1990-tallet ble reglene utvidet til også å gjelde misbruk av debetkort,[23] og i 2009 ble vernet utvidet til å gjelde alle betalingstransaksjoner, herunder overføringer fra nettbank, jf. finansavtaleloven 1999

---

[18] Prop. 92 LS (2019–2020) s. 183.

[19] Prop. 92 LS (2019–2020) s. 184.

[20] Se Prop. 92 LS (2019–2020) s. 183. Se også Ot.prp. nr. 41 (1998–99) s. 128 om egenandeler ved uautoriserte betalingstransaksjoner, som bygger på de samme hensynene.

[21] Jf. Innst. 104 L (2020–2021).

[22] Lov 21. juni 1985 nr. 82 om kredittkjøp m.m. § 13.

[23] NOU 1994: 19 s. 66.

§ 35.[24] Den siste endringen kom som en følge av gjennomføring av direktiv 2007/64/EF om betalingstjenester (PSD 1) og innebar at kunden ble beskyttet mot tap som følge av misbruk av BankID til overføringer i nettbank. En ytterligere utvidelse av vernet til å gjelde misbruk av BankID ved inngåelse av låneavtaler og andre avtaler om finansielle tjenester kan på denne måten ses som en naturlig videreutvikling av forbrukervernet i takt med den tilsvarende økte risikoen som har kommet som en følge av den teknologiske utviklingen.

3 Anvendelsesområde, begrepsbruk og fravikelighet

Finansavtaleloven kapittel 3 del III har overskriften «Elektronisk signatur og elektronisk segl» og regulerer plikter og ansvar ved bruk av systemer for elektronisk signering av avtaler om finansielle tjenester. Bestemmelsen i § 3-16 inneholder enkelte definisjoner og en angivelse av kapittelets virkeområde.

Av § 3-16 første ledd bokstav a fremgår det at «elektronisk signatur» i §§ 3-17 til 3-21 er tilsvarende det som i forordning (EU) nr. 910/2014 (eIDAS-forordningen) er definert som en «kvalifisert elektronisk signatur». En elektronisk signatur som er «kvalifisert» etter forordningen, er på høyeste sikkerhetsnivå. Deretter følger elektroniske signaturer som er «avanserte», og på laveste sikkerhetsnivå finner vi alle elektroniske signaturer som ikke oppfyller kravene til å være «kvalifiserte» eller «avanserte».

Det er uklart hvilken funksjon definisjonen i finansavtaleloven § 3-16 første ledd bokstav a er ment å ha. I første ledd vises det til at definisjonene i § 3-16 skal legges til grunn for forståelsen av §§ 3-17 til 3-21. I disse bestemmelsene er det imidlertid først og fremst begrepet «elektroniske signaturfremstillingsdata», ikke «elektronisk signatur», som brukes. For eksempel dreier den sentrale bestemmelsen i § 3-20 om tapsfordeling seg om «misbruk av elektroniske signaturfremstillingsdata». I § 3-16 første ledd bokstav d er «misbruk» definert som «tap, tyveri eller uberettiget tilegnelse av elektroniske signaturfremstillingsdata». I eIDAS-forordningen artikkel 3 nr. 13 er «elektroniske signaturfremstillingsdata» definert som «entydige data som underskriveren bruker til å framstille en elektronisk signatur». Elektroniske signaturfremstillingsdata brukes til å fremstille elektroniske signaturer på ulike sikkerhetsnivåer og er altså ikke unikt for *kvalifiserte* elektroniske signaturer. Spørsmålet er om definisjonen innebærer at anvendelsesområdet til finansavtaleloven kapittel 3 del III er avgrenset til kun å regulere misbruk av elektroniske signaturfremstillingsdata som inngår i kvalifiserte elektroniske signaturer.

Det er flere forhold som taler for at lovgiver kun har ment å regulere *kvalifiserte* elektroniske signaturer. I forarbeidene heter det således at i proposisjonen «benyttes

[24] Jf. finansavtaleloven 1999 § 35 og direktiv 2007/64/EF om betalingstjenester i det indre marked artikkel 60 og 61.

'elektronisk signatur' i kortform for kvalifiserte elektroniske signaturer som er fremstilt ved bruk av kvalifisert sertifikat i et kvalifisert elektronisk signaturfremstillingssystem».[25] Videre er definisjonen av «rettighetshaver» etter finansavtaleloven § 3-16 første ledd bokstav b «en fysisk person som har rett til å fremstille en elektronisk signatur som kan benyttes til å inngå avtale om finansiell tjeneste». Ettersom elektronisk signatur er definert som «kvalifisert» elektronisk signatur etter bokstav a, tilsier dette at ansvarsbegrensningene etter § 3-20 bare kan påberopes når det er brukt en kvalifisert signaturløsning.

Denne avgrensningen er imidlertid underlig. Det er vanskelig å se gode argumenter for at kundene skal få dårligere rettslig beskyttelse mot tap dersom banker velger å tilby finansielle tjenester basert på et system for elektronisk signering med lavere sikkerhetsnivå enn «kvalifisert». Finansinstitusjoner kan i så fall omgå finansavtalelovens utvidede ansvar ved å tilby signering med løsninger som har lavere sikkerhetsnivå. Dette har neppe vært lovgivers intensjoner. Det er mulig at lovgiver har forsøkt å rette opp i dette ved å innta en regel i finansavtaleforskriften § 3-15 som slår fast at «[s]om elektronisk signatur etter finansavtaleloven § 3-16 til § 3-18 regnes også elektronisk signatur i samsvar med [eIDAS-forordningen]». Her er tilsynelatende alle elektroniske signaturer omfattet, ikke bare de kvalifiserte. Problemet er imidlertid at bestemmelsen bare gjelder for §§ 3-16 til 3-18 og altså ikke for reglene om ansvar og egenandeler i § 3-20. Spørsmålet har imidlertid neppe stor praktisk betydning, ettersom det for alle praktiske formål er BankID som brukes ved inngåelse av avtaler om finansielle tjenester. BankIDs signaturløsning oppfyller kravene til kvalifiserte elektroniske signaturer.

Videre defineres begrepet «tilbyder» i finansavtaleloven § 3-16 første ledd bokstav b som en

«tilbyder av tillitstjenester som leverer en eller flere kvalifiserte tillitstjenester, som har fått tildelt status som kvalifisert av et tilsynsorgan, og som tilbyr en elektronisk tjeneste bestående av fremstilling, kontroll og validering av elektroniske signaturer».

Dette er en henvisning til reglene i eIDAS-forordningen om hvem som kan tilby tjenester knyttet til elektroniske signaturløsninger. I tillegg oppstiller kapittelet rettigheter og plikter for «tjenesteytere». En «tjenesteyter» er etter finansavtaleloven § 1-4 tredje ledd en «fysisk eller juridisk person som tilbyr finansielle tjenester eller finansoppdrag som ledd i næringsvirksomhet».

Begrepsbruken i kapittelet er ikke helt intuitiv, men vi kan tenke oss følgende eksempel: Peder Ås inngår en avtale om BankID med Lillevik Sparebank. Peder Ås er da «rettighetshaver», og Lillevik Sparebank er «tilbyder», jf. § 3-16. En svindler får tak i Peder Ås' BankID og inngår en forbrukslånsavtale med Lillevik Forbrukslånsbank. Lillevik

[25] Prop. 92 LS (2019–2020) s. 182.

Forbrukslånsbank er i denne sammenheng «tjenesteyter». Bestemmelsene i §§ 3-17 til 3-21 regulerer tilbyderens og rettighetshaverens plikter ved inngåelse av avtale om bruk av elektronisk signatur og tapsfordelingen mellom rettighetshaver og tjenesteyter ved misbruk av elektronisk signeringsløsning ved inngåelse av avtale om finansielle tjenester. Som synonym for «rettighetshaver» bruker vi i denne artikkelen også «pseudounderskriver».[26]

Finansavtaleloven § 3-20 regulerer ansvar for tap ved «misbruk av elektroniske signaturfremstillingsdata». Som nevnt er elektroniske signaturfremstillingsdata de dataene som underskriveren bruker for å fremstille en elektronisk signatur. Av forarbeidene fremgår det at elektroniske signaturfremstillingsdata for eksempel kan være «en BankID-brikke som gir en engangskode kunden skal benytte sammen med sitt personlig passord for å signere elektronisk», men også kan være «av en annen type teknologi – eksempelvis basere seg på biometri».[27]

Begrepet «elektroniske signaturfremstillingsdata som inngår i en kvalifisert elektronisk signatur» er presist, men omstendelig og intuitivt ikke så forståelig. I overskriften til bestemmelsen i § 3-20 heter det «misbruk av elektronisk signatur». I fortsettelsen vil vi bruke disse uttrykkene synonymt.

Regelen i § 3-20 har overskriften «Ansvar for tap ved misbruk av elektronisk signatur». Anvendelsesområdet til denne bestemmelsen er altså avgrenset gjennom definisjonen av «misbruk» i § 3-16 første ledd bokstav d: «tap, tyveri eller uberettiget tilegnelse av elektroniske signaturfremstillingsdata». Som nevnt ovenfor kan signaturfremstillingsdata for eksempel være koder generert av en BankID-brikke. Et praktisk viktig spørsmål er om det dreier seg om «misbruk» i finansavtalelovens forstand dersom pseudounderskriveren frivillig har overlatt sikkerhetsinformasjon til BankID til en tredjeperson. BankID-innehaveren overlater for eksempel sin BankID-brikke og passord til et familiemedlem som skal hjelpe vedkommende å levere skattemeldingen. Familiemedlemmet leverer skattemeldingen, men tar også opp et forbrukslån i BankID-innehaverens navn og spiller bort pengene på nett. De fleste vil nok kategorisere dette som «misbruk» av innehaverens BankID etter en naturlig språklig forståelse. Men språklig er det ikke like opplagt at forholdet faller inn under en av de tre kategoriene som loven regner som «misbruk», nemlig «tap, tyveri eller uberettiget tilegnelse av elektroniske signaturfremstillingsdata».

Forarbeidene taler for at lovgiver likevel har forutsatt at slike situasjoner skal reguleres av lovens tapsfordelingsregler. I forarbeidene nevnes som eksempel en situasjon der

---

[26] Begrepet «pseudounderskriver» benyttes som «benevnelse på den som tilsynelatende har skrevet den ugyldige elektroniske signaturen», jf. Prop. 92 LS (2019–2020) s. 174. I artikkelen brukes begrepet som synonym for «rettighetshaver», jf. finansavtaleloven § 3-16 bokstav b.

[27] Prop. 92 LS (2019–2020) s. 182.

rettighetshaveren har fått bistand fra en tredjeperson til å betale regninger, slik at «hjelperen får kjennskap til personlig sikkerhetsinformasjon».[28] Det uttales at rettighetshaveren ikke nødvendigvis har handlet med forsett i en slik situasjon, og dermed kan «påberope seg ansvarsbegrensning» etter bestemmelsen om grov uaktsomhet i tredje ledd.[29] Lovgiver må altså ha forutsatt at et slikt tilfelle utgjør «misbruk» av elektroniske signaturfremstillingsdata, fordi spørsmålet om hvor grensen mellom egenandel ved grov uaktsomhet etter tredje ledd og fullt ansvar etter fjerde ledd går, ikke vil komme på spissen hvis reglene overhodet ikke får anvendelse i en slik situasjon.

Etter vårt syn må det på bakgrunn av dette regnes som «misbruk» av elektroniske signaturfremstillingsdata dersom en person bruker en annens BankID-brikke til en disposisjon uten å ha rettighetshaverens samtykke til denne disposisjonen. Det må gjelde selv om rettighetshaveren altså har samtykket til at vedkommende kan bruke rettighetshaverens BankID i en annen sammenheng.[30]

4 Aktørenes plikter

4.1 Plikter for tilbydere og tjenesteytere

I finansavtaleloven §§ 3-17 og 3-18 oppstilles det plikter for henholdsvis tilbydere av elektroniske signaturløsninger og tjenesteytere som tilbyr å inngå avtale ved bruk av elektronisk signatur. Formålet med bestemmelsene er å legge til rette for at det er enkelt for kundene å sperre elektroniske signaturløsninger, og å sikre notoriteten knyttet til varsel fra kunden om misbruk. For å redusere det potensielle skadeomfanget dersom uvedkommende har fått urettmessig tilgang til noens elektroniske signaturfremstillingsdata, er det viktig at rettighetshaver raskt og enkelt kan få sperret videre bruk.

Tilbydere av elektroniske signaturløsninger skal etter § 3-17 opplyse om hvordan rettighetshaveren kan varsle om misbruk. Tilbyderen skal kunne motta slike varsler «til enhver tid», og skal «straks» hindre «enhver videre bruk av de elektroniske signaturfremstillingsdataene» etter at varsel er mottatt. Varsel fra kunden om misbruk skal bekreftes skriftlig, og dokumentasjon for mottatt varsel skal oppbevares i minst 18 måneder, jf. annet ledd. Bestemmelsen er utformet etter modell av § 4-23 annet og tredje ledd om plikter for den som utsteder betalingsinstrumenter.

---

[28] Innst. 104 L (2020–2021) s. 21.

[29] Innst. 104 L (2020–2021) s. 21–22.

[30] Dette har en side til avtalerettslige regler om fullmakt, og spørsmålet er nærmere drøftet i Marte Eidsand Kjørven og Line Utne Norland, «Elektroniske signaturer og avtalebinding», i Marte Eidsand Kjørven, Maria Astrup Hjort og Tone Linn Wærstad, red., *Bruk og misbruk av elektronisk identifikasjon*.

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

Det følger av § 3-18 at tjenesteytere som tilbyr kunder å inngå avtale ved bruk av elektronisk signatur, «skal ha lett tilgjengelige opplysninger om hvordan kunden skal varsle om misbruk av elektroniske signaturfremstillingsdata for de elektroniske signaturene som tjenesteyteren aksepterer». Opplysningsplikten etter § 3-18 er, i motsetning til opplysningsplikten etter § 3-22, ikke begrenset til å gjelde før avtale inngås.[31] Poenget her er at rettighetshaveren (BankID-innehaveren) ikke har et kontraktsforhold med alle mulige tjenesteytere som tilbyr avtaleinngåelse med for eksempel BankID. Når en person blir oppmerksom på mulig misbruk knyttet til en bestemt tjenesteyter, skal det være enkelt å finne ut hvordan tjenesteyteren kan varsles om dette. Det må derfor foreligge generell informasjon som er offentlig tilgjengelig, for eksempel på tjenesteyterens nettside.

4.2 Rettighetshaverens plikter

Rettighetshaverens plikter fremgår av finansavtaleloven § 3-19. Første ledd oppstiller krav om at signaturløsningen skal brukes i samsvar med «vilkårene for utstedelse og bruk», og at rettighetshaver skal ta «alle rimelige forholdsregler for å beskytte personlig sikkerhetsinformasjon». I dette ligger det en plikt til å beskytte for eksempel passord og engangskoder. Bestemmelsen er utformet etter modell av tilsvarende bestemmelse om kundens plikter ved bruk av betalingsinstrumenter i § 4-23 første ledd.

Vilkårene for utstedelse og bruk skal «være objektive, ikke innebære forskjellsbehandling og stå i forhold til formålet», jf. § 3-19 første ledd siste punktum. Vilkår som pålegger rettighetshaveren svært strenge plikter, vil ikke være bindende. Dette kan begrunnes med at slike vilkår ikke står «i forhold til formålet», eller at de er urimelige, jf. også avtaleloven § 36 og direktiv 93/13/EØF om urimelige kontraktsvilkår i forbrukerforhold. Det støttes også av HR-2020-2021-A, hvor Høyesterett uttaler om den tidligere bestemmelsen i finansavtaleloven 1999 at «[v]urderingen av hva som er *rimelige forholdsregler*, må bygge på hva som [er] praktisk mulig uten at det utgjør en urimelig stor byrde for innehaveren …».[32]

Omfanget av rettighetshaverens ansvar etter § 3-20 fastlegges med utgangspunkt i en vurdering i to ledd. Et grunnvilkår er at det foreligger brudd på rettighetshaverens plikter etter § 3-19. Deretter vil omfanget av egenandelen bero på om dette pliktbruddet skyldes grov uaktsomhet eller forsettlige forhold hos rettighetshaveren. Vi kommer derfor nærmere tilbake til kundens plikter under drøftelsene av kundens ansvar i fortsettelsen.

---

[31] Prop. 92 LS (2019–2020) s. 358.

[32] Dommens avsnitt 98 (kursivert i original). Se også Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtale § 4-30 fjerde ledd», *Lov og Rett,* nr. 6. 2021, s. 335–366, punkt 2 for en nærmere drøftelse av hva som ligger i kundens plikt til å beskytte personlig sikkerhetsinformasjon.

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

I § 3-19 annet ledd er det oppstilt en varslingsplikt for rettighetshaveren. Konsekvensene av unnlatt varsling er at «rettighetshaveren taper sin rett til ansvarsbegrensning etter § 3-20», jf. tredje ledd. Det er ikke dermed sagt at rettighetshaveren i slike tilfeller vil være ansvarlig for tapet. Hvorvidt rettighetshaveren (pseudounderskriveren) er ansvarlig overfor finansinstitusjonen, vil i tilfeller av for sen varsling bero utelukkende på alminnelige erstatningsrettslige regler.

Varslingsplikten inntrer når rettighetshaveren «blir oppmerksom på misbruk av elektroniske signaturfremstillingsdata», jf. § 3-19 annet ledd. Det er ikke nok at rettighetshaveren *burde* blitt oppmerksom på misbruk. Etter lovens ordlyd er det klart at plikten først inntreffer når rettighetshaveren faktisk har oppdaget misbruk, jf. også tredje ledd.

Selv om varslingsplikten i utgangspunktet først inntrer ved faktisk kunnskap om misbruk, følger det av tredje ledd annet punktum at rettighetshaveren også taper retten til å påberope reglene om ansvarsbegrensning i § 3-20 dersom det har gått mer enn 13 måneder etter at rettighetshaveren «måtte forstå at et misbruk har funnet sted». Hva som ligger i «måtte forstå», er ikke helt klart, men det innebærer i hvert fall noe mer enn «burde forstå». Kriteriet kan forstås som grovt uaktsom uvitenhet eller som et krav om forsett, men med et lempet beviskrav når det gjelder forsettet.[33]

Når forholdet først er oppdaget, må imidlertid rettighetshaveren handle raskt («uten ugrunnet opphold»). Det er noe uklart om rettighetshaveren må varsle overfor både tilbyderen og tjenesteyteren. I annet ledd er det vist til at det skal varsles i samsvar med rutiner oppgitt av «tjenesteyteren *eller* tilbyderen som har utstedt den aktuelle elektroniske signaturen» (vår kursivering). I tredje ledd er det ikke presisert til hvem varsel må gis for at de beskrevne konsekvensene skal inntreffe. Det kan for eksempel tenkes at Peder Ås i vårt eksempel uten ugrunnet opphold varsler til Lillevik Sparebank for å få sperret BankID-en sin. Han bruker deretter noe tid på å få oversikt over konsekvensene av misbruket, og varsler Lillevik Forbrukslånsbank først en stund etter at han har oppdaget at det trolig er tatt opp et lån i hans navn der. I en slik situasjon har han varslet innen fristen overfor tilbyder (Lillevik Sparebank), men ikke overfor tjenesteyter (Lillevik Forbrukslånsbank). Spørsmålet er om Peder Ås i en slik situasjon taper retten til å påberope seg reglene om ansvarsbegrensning i denne situasjonen.

Etter vårt syn bør § 3-19 annet og tredje ledd forstås slik at det bare er manglende varsel uten ugrunnet opphold overfor *tilbyder* som fører til bortfall av rett til å gjøre gjeldende ansvarsbegrensning. Det har avgjørende betydning for å begrense videre tap overfor flere og andre tjenesteytere at rettighetshaver får sperret sin eID så raskt som mulig når misbruk oppdages. Det må være dette hensynet som ligger bak den svært korte varslingsfristen. For den enkelte tjenesteyter har det derimot i de fleste tilfeller liten eller

[33] Viggo Hagstrøm mfl., *Obligasjonsrett,* 3. utg., Universitetsforlaget, 2021, s. 164–165.

ingen betydning om pseudounderskriveren varsler raskt eller lar det gå noe mer tid. I det klassiske tilfellet av lånebedrageri vil tapet være pådratt idet lånet er utbetalt. Hvis pseudounderskriveren først oppdager misbruket etter dette tidspunktet, har det derfor ingen betydning for tapets størrelse hvor raskt hen varsler tjenesteyter. Her må man også ta i betraktning at misbruk av noens eID kan involvere svært mange tjenesteytere. Det kan derfor være krevende for rettighetshaver å varsle alle disse raskt. Dette må i hvert fall tas i betraktning ved vurderingen av hvor rask respons som kan kreves for å være «uten ugrunnet opphold».

Ordlyden i unntaket fra varslingsplikten i § 3-19 tredje ledd tredje punktum indikerer at bestemmelsen ikke bare regulerer varsel til tilbyder, men også varsel til den enkelte tjenesteyter. Her fremgår det at dersom «tjenesteyteren har unnlatt å gi rettighetshaveren transaksjonsopplysninger eller annen relevant informasjon hvor transaksjon eller avtale som misbruket har ledet til, fremgår, og som etter loven her skal gis til tjenesteyterens kunder», tapes retten til ansvarsbegrensning «først 13 måneder etter at rettighetshaveren ble kjent med misbruket». I vårt eksempel betyr dette at dersom Lillevik Forbrukslånsbank ikke har gitt lovpålagte opplysninger *til Peder Ås* om den svindelbaserte transaksjonen eller avtalen, er det tilstrekkelig at Peder Ås varsler innen 13 måneder etter at han oppdaget misbruket. Det er altså ikke tilstrekkelig at svindleren – Hans Tastad i vårt eksempel – har fått opplysningene. Lovpålagte opplysninger er for eksempel opplysninger om «hvordan kunden skal varsle om misbruk av elektroniske signaturfremstillingsdata for de elektroniske signaturene som tjenesteyteren aksepterer», jf. § 3-18.[34]

5 Kundens ansvar etter «ellers gjeldende rettsregler»

Regelen om begrensning av rettighetshavers ansvar etter finansavtaleloven § 3-20 forutsetter at kunden i utgangspunktet er ansvarlig overfor tjenesteyter «i samsvar med ellers gjeldende rettsregler».[35] Henvisningen til «ellers gjeldende rettsregler» viser ifølge forarbeidene til «erstatningsansvar utenfor kontrakt, eller i kontrakt om det forut for misbruket eksisterer en avtale mellom rettighetshaveren og tjenesteyteren som regulerer kundens plikter for oppbevaring og håndtering av signaturløsningen».[36] Det må altså først foretas en vurdering av om vilkårene for erstatning etter alminnelige erstatningsrettslige regler er oppfylt. Dersom disse vilkårene ikke er oppfylt, blir det i alle tilfeller ikke tale om noe økonomisk ansvar for den som er utsatt for ID-tyveri.

---

[34] Se punkt 4.1.

[35] Se Marte Eidsand Kjørven og Line Utne Norland, «Elektroniske signaturer og avtalebinding», i Marte Eidsand Kjørven, Maria Astrup Hjort og Tone Linn Wærstad, red., *Bruk og misbruk av elektronisk identifikasjon*, om forholdet mellom finansavtaleloven § 3-20 og spørsmål om deling av eID kan utgjøre en avtalerettslig fullmakt slik at innehaveren blir bundet.

[36] Prop. 92 LS (2019–2020) s. 358.

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

Uttalelsene i forarbeidene viser til at vurderingen av om det foreligger ansvarsgrunnlag for erstatning, vil kunne variere avhengig av om det forut for misbruket foreligger en avtale som fastsetter bestemte plikter og rettigheter mellom rettighetshaveren og tjenesteyteren, altså finansinstitusjonen som er utsatt for svindel. Hvis en slik avtale foreligger, vil den kunne få betydning for spørsmålet om erstatningsansvar. Det vanlige er imidlertid at spørsmål om erstatning typisk oppstår i relasjon til en annen bank enn den banken som har utstedt BankID til kunden, jf. eksempelet vårt, der Peder Ås har en BankID-avtale med Lillevik Sparebank, mens en forbrukslånavtale inngås i Lillevik Forbrukslånsbank av en svindler som misbruker Peder Ås' BankID. Det er da Lillevik Forbrukslånsbank som fremmer et erstatningskrav mot Peder Ås.

Når en signatur – elektronisk eller fysisk – er påført et kontraktsdokument av en tredjeperson, er den avtalerettslige hovedregelen at avtalen ikke blir bindende for pseudounderskriveren.[37] Avtalen rammes da av den ulovfestede ugyldighetsgrunnen «falsk», som er en sterk ugyldighetsgrunn fordi «løftegiveren aldri har avgitt et løfte».[38] Tjenesteyteren kan følgelig ikke holde vedkommende ansvarlig etter avtalen. Kunden kan imidlertid bli erstatningsansvarlig dersom de alminnelige vilkårene for erstatning er oppfylt: ansvarsgrunnlag, økonomisk tap og adekvat årsakssammenheng.

Det vil sjelden være problematisk å konstatere at det har oppstått et tap; tjenesteyteren har utbetalt en sum penger til uvedkommende som ikke blir tilbakebetalt eller ellers dekket. Dette kan skyldes at svindleren for eksempel er ukjent eller ikke betalingsdyktig. Det er derfor spørsmålet om ansvarsgrunnlag for pseudounderskriveren og om tapet er adekvat, som gjerne vil komme på spissen.

I HR-2020-2021-A (Easybank-dommen) har Høyesterett tatt stilling til hvordan alminnelige erstatningsregler skal forstås i et tilfelle av digitalt ID-tyveri. Saken gjaldt en person (A) som hadde fått sin BankID misbrukt av et ektepar. As BankID-brikke ble oppbevart på et gatekjøkken, liggende på en kontorplass i en veske plassert i en skuff med andre kodebrikker. Kontorplassen var ikke adskilt fra de øvrige lokalene. Skuffen var ikke sikret med lås og var følgelig tilgjengelig for andre ansatte som hadde tilgang til dette området. Spørsmålet Høyesterett tok stilling til, var om A hadde opptrådt erstatningsbetingende uaktsomt, slik at Easybank, som hadde utbetalt et forbrukslån etter misbruket av BankID-brikken, kunne kreve tapet erstattet av A. Høyesterett kom enstemmig til at det ikke forelå ansvarsgrunnlag etter alminnelige erstatningsrettslige regler, og at A følgelig ikke kunne holdes ansvarlig for Easybanks tap.

På tidspunktet da dommen ble avsagt, var ny finansavtalelov ikke vedtatt. Høyesterett viste imidlertid til lovforslaget og uttalte blant annet at de hensyn lovforslaget bygger på,

---

[37] Jo Hov, *Avtaleslutning og ugyldighet. Kontraktsrett I*, 3. utg., Papinian, 2002, s. 237.

[38] Johan Giertsen, *Avtaler,* 3. utg., Universitetsforlaget, 2014, s. 170.

er relevante også ved fastleggelsen av innholdet i de ulovfestede erstatningsreglene, særlig aktsomhetsnormen.[39]

Høyesterett formulerte vurderingstemaet som et spørsmål om hvorvidt A hadde tatt «alle rimelige forholdsregler» for å verne seg mot misbruk av BankID-brikken.[40] Vurderingen må «bygge på hva som [er] praktisk mulig uten at det utgjør en urimelig stor byrde for innehaveren eller vil gjøre selve bruken av BankID upraktisk».[41] Det kreves altså ikke tiltak for å beskytte seg mot misbruk som gjør at brikken ikke lar seg benytte uten anstrengelser av et visst omfang. BankID er for de fleste blitt en nødvendighet i hverdagen, og en rekke både offentlige og private tjenester krever innlogging ved bruk av BankID som identifikasjon, noe som altså spiller inn på uaktsomhetsterskelen.

Det legges til grunn at culpanormen som utgangspunkt er objektiv, og at erstatningsansvar kan pålegges overfor den som «kunne og burde handlet annerledes», men at det «likevel [er] rom for en viss relativisering».[42] Det vil si at én og samme handling kan vurderes som uaktsom i relasjon til en gruppe skadelidte og som aktsom i relasjon til en annen gruppe skadelidte. Det avgjørende er rolleforventningen til skadelidte, og det pekes på at det i enkelte tilfeller vil være åpning for at ansvaret faller bort dersom skadelidte står nærmest til å foreta tiltak som kan eliminere risikoen.[43] Det mest prinsipielt interessante med dommen er vurderingene av forhold på finansinstitusjonens side. Når uaktsomhetsterskelen settes, uttales det i avsnitt 61 at

«[d]er avtaleparten, tjenesteyteren, tilhører en gruppe som kan forventes selv å iverksette tiltak for å unngå tap, må dette etter mitt syn få betydning når man skal stilling til om innehaveren i det enkelte tilfellet har opptrådt uaktsomt og ut fra det blir erstatningsansvarlig.»

Risikobetraktningen det pekes på her, er noe annet enn en reduksjon av erstatningsansvaret som følge av skadelidtes medvirkning etter skadeserstatningsloven § 5-1. En vurdering av medvirkning er først aktuelt etter at ansvar er konstatert hos skadelidte. Det sentrale i et tilfelle som dette er hvem som har «skapt risikoen», og hvem som er «nærmest til å iverksette tiltak for å unngå tap».[44] Det må dermed ved fastsettelse av uaktsomhetsterskelen gjøres en vurdering av hvor fremtredende skadevolders rolle (i våre saker er det altså BankID-innehaveren som er skadevolder) er i at skaden oppstår, sett opp mot hvilke tiltak skadelidte kan iverksette for å minimere skaderisikoen. Jo

---

[39] HR-2020-2021-A avsnitt 61. Se også avsnitt 49.

[40] HR-2020-2021-A avsnitt 54.

[41] HR-2020-2021-A avsnitt 98.

[42] HR-2020-2021-A avsnitt 56.

[43] HR-2020-2021-A avsnitt 57.

[44] Marte Eidsand Kjørven, «BankID-svindel – HR-2020-2021-A», *Nytt i privatretten*, nr. 4. 2020, s. 14–17.

enklere tiltak skadelidte kan iverksette, desto mer fremtredende blir skadelidtes rolle, noe som påvirker om skadevolder har opptrådt uaktsomt, og hvor terskelen settes.

A kunne i saken «bebreides» for oppbevaringen, men forholdene på Easybanks side ble avgjørende for at det likevel ikke forelå ansvarsgrunnlag for A. At Easybank er en «profesjonell aktør» som hadde valgt å inngå avtale om et lånebeløp som for en enkeltperson er «betydelig», og at innvilgelsen hadde skjedd «utelukkende basert på identifikasjon og elektronisk signatur gjennom BankID», ble tillagt avgjørende vekt.[45] Det pekes på at det var mulig for banken å «foreta ytterligere kontrolltiltak» før utbetalingen fant sted. Dersom banken hadde foretatt enkle kontrolltiltak, var det «stor sannsynlighet for at misbruket ville vært unngått». Banken hadde da «bevisst valgt en handlemåte som innebar en klar risiko for tap».[46]

Når terskelen for ansvar skal settes, er det dermed sentralt å vurdere hvilke tiltak skadelidte har i sin verktøykasse, og hvor enkelt det er å iverksette dem. For banker er det relativt enkle tiltak som kan gjennomføres for å sikre at den som signerer lånet digitalt, rent faktisk er personen som har søkt om det. Høyesterett nevner tiltak som å sjekke at kontoen lånet utbetales til, står i låntakers navn. Det kan også tenkes andre tiltak, og Høyesterett er åpen for dette, jf. uttalelsen «ett av tiltakene som en utlånsbank bør benytte».[47] Andre tiltak kan være en SMS til vedkommendes registrerte telefonnummer, et brev til vedkommendes folkeregistrerte adresse eller elektroniske postkasse, eller en videosamtale med kunden før større summer utbetales. At banken «bør» benytte slike tiltak, peker mot hva som kan forventes, og hva som kan gjøre det urimelig å ilegge rettighetshaveren ansvar. Dette momentet harmonerer godt med pulveriseringshensynet.

I tillegg til ansvarsgrunnlag må det foreligge økonomisk tap og adekvat årsakssammenheng for at vilkårene for erstatningsansvar skal være oppfylt. Kravet til adekvans innebærer for det første at tapet må være påregnelig, det vil si at skaden ikke må være en usannsynlig, fjern eller atypisk følge av den skadevoldende handling.[48] For det andre innebærer adekvansvilkåret at det må skje en avgrensning av erstatningsansvaret mot skader som ikke har en tilstrekkelig nærhet til den skadevoldende handlingen. Den sentrale dommen i denne sammenheng er Rt-1973-1268 (Flymanøverdommen). Ser man nærmere på begrunnelsen i denne dommen, er det mange likheter med HR-2020-2021-A.

Flymanøverdommen gjaldt et militærfly som under uaktsom flyvning kuttet en kraftledning slik at et stort antall abonnenter ble uten strøm i ca. 36 timer. En av

---

[45] HR-2020-2021-A avsnitt 104.

[46] HR-2020-2021-A avsnitt 104.

[47] HR-2020-2021-A avsnitt 107.

[48] Viggo Hagstrøm, *Obligasjonsrett*, 2. utg., Universitetsforlaget, 2011, s. 466.

abonnentene, en eier av et oppdrettsanlegg på Hitra, fremmet krav om erstatning for tap som følge av strømbruddet. Høyesterett kom til at det ikke forelå tilstrekkelig nærhet mellom den skadevoldende handlingen og tapet, og at staten derfor ikke kunne holdes erstatningsansvarlig.

Høyesteretts begrunnelse bygger særlig på en risikobetraktning:

«Spørres det om hvem som i alminnelighet er nærmest til å bære risikoen for skader av den omhandlede art, kan svaret neppe være særlig tvilsomt. De enkeltpersoner og bedrifter som er utsatt for å lide skade, vil som regel ha en større eller mindre kontroll over sin situasjon. De må ta foreliggende skademuligheter med i sine beregninger og treffe de for hver især hensiktsmessige tryggingstiltak, faktisk eller rettslig.»

Høyesterett peker videre på at

«[s]kadens uberegnelighet og under ugunstige omstendigheter ruinerende omfang er et annet og reelt moment av betydning som gjør det betenkelig å trekke grensene for erstatningsplikten for vidt».

Disse betraktningene ligger svært tett på den argumentasjonen Høyesterett har brukt i Easybank-dommen, selv om argumentasjonen i Easybank-dommen er knyttet til vilkåret om ansvarsgrunnlag. I begge dommene vises det til risikobetraktninger og skadelidtes egne muligheter for å begrense skaden, i kombinasjon med potensielt ruinerende konsekvenser som ikke kan begrenses på en hensiktsmessig måte for skadevolderne.

Skadepotensialet dersom en svindler får hånd om noens BankID, er nærmest ubegrenset: Svindleren kan endre opplysninger i offentlige registre slik at det ser ut som BankID-innehaveren har stor formue og høy inntekt. Deretter kan svindleren ta opp store lån i BankID-innehaverens navn. I tillegg kan svindleren kjøpe dyre biler, klokker osv., eller til og med opprette et aksjeselskap i offerets navn med vedkommende registrert som daglig leder og/eller styreleder. Deretter kan svindleren ta opp lån, kjøpe varer og tjenester, også i aksjeselskapets navn. Det er da også mulig å svindle offentlige myndigheter, for eksempel ved å kreve mva.-refusjon på fiktive handler. De skadelidte kan altså være både privatpersoner, selskaper, finansinstitusjoner og offentlige aktører, og totalbeløpet kan bli ruinerende for BankID-innehaveren.

På samme måte som i Flymanøverdommen har de potensielle skadelidte mulighet for å sette i verk ulike tiltak for å avverge tap. Offentlige myndigheter *kan* og *bør* ha gode kontrolltiltak. Det samme gjelder finansinstitusjoner; de bør sikre seg at de betaler ut lån til rette vedkommende. Næringsdrivende som selger varer og tjenester, for eksempel biler, har også mulighet for å sette i verk kontrolltiltak.

Når Høyesterett i Easybank-dommen valgte å avgjøre saken på vilkåret om ansvarsgrunnlag, har det sammenheng med hvordan partene hadde lagt opp saken. Partene var enige om at øvrige vilkår for erstatning var oppfylt, og at det springende

punktet derfor var spørsmålet om hvorvidt det forelå ansvarsgrunnlag. Etter vårt syn, og ikke minst basert på den faktiske argumentasjonen til Høyesterett, kunne spørsmålet kanskje like gjerne blitt reist som et spørsmål om hvorvidt tapet hadde den nødvendige nærhet til den skadevoldende handlingen. En dom fra Gjøvik tingrett er et eksempel på en slik argumentasjonsmåte.[49] Saken dreide seg om et tilfelle av misbruk i nære relasjoner. Svindelofferet hadde oppgitt passordet til sin BankID til sin daværende samboer, og tingretten fant at dette utgjorde ansvarsgrunnlag for erstatning. Tingretten fant imidlertid at det ikke forelå adekvat årsakssammenheng, fordi svindelofferets rolle var så lite fremtredende.

Forarbeidene til finansavtaleloven har også enkelte uttalelser som kan gi veiledning til aktsomhetsvurderingen etter alminnelig erstatningsrett.[50] Uttalelsene om hva som følger av ulovfestede regler om erstatning, har imidlertid ikke vekt som forarbeider i denne sammenhengen, selv om de faktisk står i forarbeidene til finansavtaleloven. For eksempel vil Easybank-dommen, som falt etter at forarbeidene ble skrevet, være vesentlig mer tungtveiende enn lovgivers antakelser om hva som fulgte av ulovfestede erstatningsrettslige regler på tidspunktet for lovforslaget.

Forarbeidene peker på visse typetilfeller som anses uaktsomme, for eksempel å «skrive ned passord eller koder på en slik måte at de enkelt vil kunne misbrukes av en tredjepart».[51] Uttalelsen tilsier at det ikke anses uaktsomt i seg selv å skrive ned passord eller koder. Det kan imidlertid være uaktsomt dersom nedtegningen gjør det «enkelt» for en tredjepart å misbruke opplysningene. Her må man imidlertid ta i betraktning den brede risikovurderingen Høyesterett har slått fast i Easybank-dommen. Dessuten er det å skrive ned passordene faktisk anbefalt av mange sikkerhetseksperter, inkludert det offentlige organet Nasjonal sikkerhetsmyndighet (NSM). NSM er et direktorat som er underlagt Justis- og beredskapsdepartementet, og som har ansvar for IKT-sikkerhet og forebyggende arbeid. NSM skriver under overskriften «Noen råd om passord til folk flest»: «Lag deg gjerne en skriftlig liste over dine brukernavn og passord på de tjenestene du bruker.»[52] Samtidig oppfordres det til å behandle denne listen med forsiktighet og til å skrive den med penn og papir og ikke digitalt.

Forarbeidene gir også noen eksempler på tilfeller som *ikke* vil føre til ansvar. Det gjelder hvor tredjeparten benytter seg av «avanserte metoder» for å fremskaffe passord og koder, herunder skjult filming, overvåking av mobiltelefon og datamaskiner og liknende.

---

[49] TGJOV-2017-170313.

[50] Prop. 92 LS (2019–2020) s. 358.

[51] Prop. 92 LS (2019–2020) s. 358.

[52] Roar Thon, «Noen råd om passord til folk flest», 2020. https://nsm.no/hold-deg-oppdatert/meninger/noen-rad-om-passord-til-folk-flest (hentet 31.03.2023).

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

For en uvitende person vil det være «nærmest umulig» å beskytte seg mot dette, og i slike tilfeller skal det derfor «mye til» for å konstatere uaktsomhet på slikt grunnlag.[53]

Et siste typetilfelle som trekkes frem i forarbeidene, er at det ikke skal anses uaktsomt om familiemedlemmer deler postkasse, selv om det kan gi andre i familien uberettiget tilgang til rettighetshaverens post. Dersom den uvedkommende tredjeparten skaffer seg tilgang gjennom urettmessig å åpne posten, skal det altså ikke kunne konstateres ansvar basert på dette alene.[54]

Dersom de alminnelige vilkårene for erstatning er til stede, foreligger det i utgangspunktet et ansvar for rettighetshaveren. Merk likevel at ansvaret etter «ellers gjeldende rettsregler» «kan lempes eller settes ned som følge av alminnelige regler om lemping eller skadelidtes medvirkning».[55] Denne summen utgjør, i tråd med alminnelig erstatningsrettslige regler, maksgrensen for rettighetshaverens/skadevolderens ansvar. I tillegg til at det må tas stilling til om det foreligger ansvarsgrunnlag, økonomisk tap og adekvat årsakssammenheng, må det derfor vurderes om rettighetsansvaret skal settes ned etter regelen om skadelidtes medvirkning i skadeserstatningsloven § 5-1 og/eller lempes etter regelen i skadeserstatningsloven § 5-2.[56] Det er det beløpet man dermed kommer frem til, ferdig nedsatt og lempet, som deretter begrenses av regelen i finansavtaleloven § 3-20.

Hovedregelen er at pseudounderskriverens ansvar settes ned til en egenandel på 450 kroner etter finansavtaleloven § 3-20 annet ledd. Etter lovens ordlyd skal egenandelen likevel ikke få anvendelse i tilfeller der «rettighetshaveren ikke kunne ha oppdaget misbruket på forhånd og heller ikke har opptrådt svikaktig». Formuleringen er hentet fra reglene om ikke-godkjente betalingstransaksjoner i finansavtaleloven § 4-30, men passer ikke like godt ved misbruk av elektroniske signaturer, ettersom ansvar for rettighetshaveren her forutsetter at de alminnelige vilkårene for erstatning er oppfylt. Det er ikke et grunnvilkår for reglene om ikke-godkjente betalingstransaksjoner. Det er vanskelig å se for seg at det foreligger ansvarsgrunnlag for BankID-innehaveren i en situasjon der hen «ikke kunne ha oppdaget misbruket på forhånd».

6 Egenandel på 12 000 kroner ved grovt uaktsomme pliktbrudd

Etter finansavtaleloven § 3-20 tredje ledd svarer rettighetshaveren med en egenandel på inntil 12 000 kroner dersom tapet skyldes at vedkommende «grovt uaktsomt» har unnlatt å oppfylle sine plikter etter § 3-19 første og annet ledd.

---

[53] Prop. 92 LS (2019–2020) s. 358.

[54] Prop. 92 LS (2019–2020) s. 358.

[55] Innst. 104 L (2020–2021) s. 21.

[56] Se nærmere i punkt 9 om lemping.

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

I Rt-2004-499 var spørsmålet om en bankkunde hadde opptrådt grovt uaktsomt etter reglene om uautoriserte betalingstransaksjoner i tidligere finansavtalelov 1999 § 35. Konkret var spørsmålet om kunden hadde opptrådt grovt uaktsomt ved å oppbevare bankkortene sine sammen med en syvende sans hvor han hadde notert kodene i kamuflert form. Kortene ble stjålet, og et av dem ble benyttet til å ta ut 10 000 kroner. Flertallet på tre dommere konkluderte med at kunden ikke hadde opptrådt grovt uaktsomt.

Høyesterett legger til grunn at grov uaktsomhet fordrer en «kvalifisert form for uaktsomhet». Oppførselen må representere et «markert avvik fra vanlig forsvarlig handlemåte», og det må dreie seg om «en opptreden som er sterkt klanderverdig», hvor vedkommende er «vesentlig mer å klandre enn hvor det er tale om alminnelig uaktsomhet».[57] Man må altså først ta stilling til den alminnelige terskelen for uaktsomhet og deretter vurdere om skadevolderen er vesentlig mer å bebreide. Det er HR-2020-2021-A (Easybank-dommen) som er den sentrale avgjørelsen for fastleggelse av terskelen for simpel uaktsomhet. Dommen er nærmere omtalt i forrige punkt.

I forarbeidene er det ikke gitt særskilte anvisninger om av hva som skal anses grovt uaktsomt.[58] Som nevnt ovenfor gir imidlertid forarbeidene noen eksempler på hva som etter lovgivers syn anses *simpelt* uaktsomt, herunder å skrive ned passord og koder slik at de «enkelt» vil kunne misbrukes av en tredjepart.[59] Når det å skrive ned passordet slik at det «enkelt» kan misbrukes av en tredjepart, karakteriseres som uaktsomt, peker det mot at det skal nokså mye til før det foreligger grov uaktsomhet.[60]

7 Fullt ansvar for kunden ved forsettlig pliktbrudd

Det følger av § 3-20 fjerde ledd at

«[r]ettighetshaveren svarer med en egenandel tilsvarende det tapet tjenesteyteren kan gjøre gjeldende i samsvar med ellers gjeldende rettsregler, dersom rettighetshaveren har misligholdt en eller flere av sine plikter etter § 3-19 første og annet ledd forsettlig slik at rettighetshaveren måtte forstå at misligholdet kunne innebære en nærliggende fare for at de elektroniske signaturfremstillingsdataene kunne bli misbrukt».

Språklig er det pussig å tale om en «egenandel» som svarer til «det tapet tjenesteyteren kan gjøre gjeldende i samsvar med ellers gjeldende rettsregler». Poenget er at dersom

---

[57] Rt-2004-499 avsnitt 32 med henvisning til Rt-1989-1318. Se også Rt-1995-486 og Rt-2006-321.

[58] Prop. 92 LS (2019–2020) s. 358.

[59] Prop. 92 LS (2019–2020) s. 358.

[60] Det vises for øvrig til Admir Habibija, «Tapsfordeling mellom bank og kunde ved misbruk av elektroniske betalingsinstrumenter – når har kunden opptrådt grovt uaktsomt?», i Marte Eidsand Kjørven, Maria Astrup Hjort og Tone Linn Wærstad, red., *Bruk og misbruk av elektronisk identifikasjon*, for en nærmere analyse av hva som utgjør et grovt uaktsomt pliktbrudd etter de tilsvarende reglene om uautoriserte betalingstransaksjoner.

det foreligger forsettlig pliktbrudd, blir kunden fullt ut ansvarlig som om særreguleringen i finansavtaleloven tenkes borte. Merk likevel, som nevnt ovenfor, at ansvaret etter «ellers gjeldende rettsregler» «kan lempes eller settes ned som følge av alminnelige regler om lemping eller skadelidtes medvirkning».[61] Denne summen utgjør, i tråd med alminnelige erstatningsrettslige regler, maksgrensen for rettighetshaverens/skadevolderens ansvar. Det virker imidlertid anstrengt å kalle dette en «egenandel».

Grensen mellom grov uaktsomhet og forsett har stor praktisk betydning. Dersom noen har fått hånd om en annens BankID, kan tapet potensielt bli stort. Dersom det for eksempel er tatt opp et (eller flere) forbrukslån på flere hundre tusen kroner, har det stor betydning for BankID-innehaveren om hen må dekke 12 000 kroner eller hele beløpet.

Etter ordlyden er pliktbruddet «forsettlig» når rettighetshaveren «måtte forstå at misligholdet kunne innebære en nærliggende fare for at de elektroniske signaturfremstillingsdataene kunne bli misbrukt». Bestemmelsen reiser for det første spørsmål om hvorvidt rettighetshaveren må ha vært bevisst plikten og pliktbruddet for at det kan foreligge forsett. Dernest blir det spørsmål om hva som ligger i kravet om at rettighetshaveren «måtte forstå» at pliktbruddet kunne medføre fare for misbruk.

I proposisjonen uttaler departementet at det «kan være noe uklart hva som nærmere ligger i skyldkravet forsett på privatrettens område».[62] I fortsettelsen drøftes begge problemstillingene som nevnt ovenfor. Departementet legger til grunn at ved forsettsvurderingen er det «uten betydning om rettighetshaveren eventuelt ikke er kjent med eller misforstår sine forpliktelser etter loven eller avtalen ('rettsvillfarelse')».[63] For den andre problemstillingen konkluderer departementet med at det ikke er «behov for å gå så langt som å kreve at forsettet må omfatte tapet».[64] Departementet bygger derfor tilsynelatende på en forståelse av forsett som innebærer at det er tilstrekkelig at kunden har gjort en bevisst handling som objektivt sett utgjør et pliktbrudd. Denne forståelsen av forsett ble imidlertid uttrykkelig fraveket ved behandlingen av lovforslaget på Stortinget, og ordlyden i § 3-20 fjerde ledd om rettighetshavers ansvar ved forsett ble endret.[65]

Det er klart ut fra lovens ordlyd slik den til slutt ble vedtatt, at det kreves en grad av skyld i relasjon til tapet, selv om det kan være noe uklart hva som nærmere bestemt ligger i at rettighetshaveren «måtte forstå at misligholdet kunne innebære en nærliggende fare for

---

61 Innst. 104 L (2020–2021) s. 21.

62 Prop. 92 LS (2019–2020) s. 186.

63 Prop. 92 LS (2019–2020) s. 186.

64 Prop. 92 LS (2019–2020) s. 186.

65 Ordlyden i den tilsvarende bestemmelsen om ansvar ved uautoriserte betalingstransaksjoner i § 4-30 fjerde ledd ble også endret.

at de elektroniske signaturfremstillingsdataene kunne bli misbrukt».[66] Derimot kan det være noe mer uklart om Stortinget med det også tok avstand fra departementets uttalelse om betydningen av pliktvillfarelse.

Høyesterett har i HR-2022-1752-A (Olga-svindel) slått fast at det tilsvarende forsettsbegrepet i finansavtaleloven 1999 § 35 om uautoriserte betalingstransaksjoner skal forstås slik at «kunden må ha vore medviten om pliktbrotet» (avsnitt 50). Bevissthet om «pliktbruddet» forutsetter at kunden er kjent med innholdet av den normen som brytes, og de faktiske handlingene som eventuelt innebærer brudd på denne normen. Faktisk og/eller rettslig villfarelse utelukker dermed forsett.

Til tross for at det ut fra forarbeidene er noe uklart hva lovgiver har ment om betydningen av villfarelse, taler de beste grunner etter vårt syn for at ny finansavtalelov tolkes på samme måte som det Høyesterett har slått fast er gjeldende rett for finansavtaleloven 1999 på dette punktet. Både departementet og justiskomiteen uttaler seg om hva de mener vil være en regel som samsvarer med forståelsen av forsett i formueretten for øvrig. Departementets uttalelser om rettsvillfarelse er del av en drøftelse av «hva som nærmere ligger i skyldkravet forsett på privatrettens område»[67], og justiskomiteen viste i innstillingen til at den reviderte ordlyden vil være i samsvar med «ellers gjeldende rettsregler».[68] Det er med andre ord ingenting i forarbeidene som skulle tilsi at lovgiver har ønsket en rettsstilling som sett fra kundens side er strengere enn det som følger av en forståelse av forsettsbegrepet ellers i formueretten generelt eller en innstramming av det som var rettstilstanden hva gjelder forsettsbegrepet etter finansavtaleloven 1999.[69]

Det vises for øvrig til Kjørven, Høgberg og Woxholth (2021) for en grundigere drøftelse av hva som ligger i finansavtalelovens forsettbegrep når det gjelder de tilsvarende reglene om ikke-godkjente betalingstransaksjoner.[70] Tilsvarende må gjelde for forståelsen av forsettsbegrepet i § 3-20 om misbruk av elektronisk signatur.

8 Tjenesteyters ansvar for tap som skyldes pliktbrudd mv.

I finansavtaleloven § 3-20 første ledd oppstilles den praktiske hovedregelen om at tjenesteyteren må bære tapet ved misbruk av elektroniske signaturløsninger. Annet til

---

[66] Se Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtale § 4-30 fjerde ledd», *Lov og Rett,* nr. 6. 2021, s. 335–366 for en grundigere drøftelse av hva som ligger i finansavtalelovens forsettsbegrep.

[67] Prop. 92 LS (2019–2020) s. 186.

[68] Innst. 104 L (2020–2021) s. 22.

[69] Se også Marte Eidsand Kjørven, «Misbruk av BankID. Olgasvindel-saken – HR-2022-1752-A», *Nytt i Privatretten*, nr. 3. 2022, s. 21–24.

[70] Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtale § 4-30 fjerde ledd», *Lov og Rett,* nr. 6 2021, s. 335–366.

fjerde ledd innebærer unntak fra dette utgangspunktet, idet kunden kan bli ansvarlig for hele eller deler av tapet avhengig av graden av klanderverdighet på kundens hånd. Femte ledd utgjør et unntak fra disse unntakene, som dermed bringer oss tilbake til hovedregelen om at tjenesteyteren må bære tapet.

Dersom vilkårene i femte ledd er oppfylt, skal rettighetshaver ikke bære noen del av tapet. Dette gjelder selv om vilkårene for egenandelsansvar etter andre til fjerde ledd er oppfylt. Det betyr at dersom kunden for eksempel forsettlig har brutt pliktene etter § 3-19, er det likevel tjenesteyteren som må bære tapet dersom et av alternativene i § 3-20 femte ledd bokstav a til e er oppfylt. Bestemmelsen tilsvarer § 4-30 femte ledd, og ordlyden stammer fra PSD 2 artikkel 74 nr. 2 og 3.

Det følger av første punktum at rettighetshaveren ikke svarer «for tap som skyldes tjenesteyteren selv, noen som opptrer på tjenesteyterens vegne, eller noen som tjenesteyteren selv representerer». Et spørsmål er om bestemmelsen skal forstås slik at tapet *utelukkende* må skyldes tjenesteyteren selv eller dennes representant. En slik tolkning gir imidlertid liten mening, fordi i en slik situasjon vil det uansett ikke være ansvarsgrunnlag for rettighetshaveren etter «ellers gjeldende rettsregler». Tjenesteyteren kan derfor i alle tilfeller ikke velte noe av tapet over på rettighetshaveren når tapet (utelukkende) skyldes tjenesteyteren selv. Med en slik tolkning vil bestemmelsen i § 3-20 femte ledd første punktum derfor ikke få noen praktisk betydning.

En alternativ tolkning er at bestemmelsen får anvendelse i tilfellene der tapet skyldes forhold på *både* tjenesteyterens og rettighetshaverens side. Det kan for eksempel hende at tapet skyldes at rettighetshaveren har overlatt sin BankID til en tredjeperson, som fikk tatt opp lån i en bank fordi banken hadde sviktende sikkerhetsrutiner. Dersom dette utgjør ansvarsgrunnlag hos både BankID-innehaveren og banken, følger det av skadeserstatningsloven § 5-1 at «erstatningen [kan] settes ned eller falle bort for så vidt det er rimelig når en tar hensyn til atferden, og dens betydning for at skaden skjedde, omfanget av skaden og forholdene ellers». Bestemmelsen slår eksplisitt fast at «[s]om medvirkning reknes det også når den direkte skadelidte eller erstatningssøkeren har latt være i rimelig utstrekning å fjerne eller minske risikoen for skade eller etter evne å begrense skaden», som er særlig relevant for skadetilfeller som skyldes misbruk av elektroniske signaturløsninger.

Finansavtaleloven § 3-20 femte ledd første punktum kan forstås som en særregulering av konsekvensene av skadelidtes medvirkning, slik at erstatningen alltid vil falle bort når tjenesteyteren har medvirket til tapet ved egen skyld. Dersom bestemmelsen tolkes på denne måten, får den praktisk betydning som en særregulering av den skjønnsbaserte bestemmelsen i skadeserstatningsloven om betydningen av skadelidtes medvirkning. I tillegg kan formålet bak reglene i finansavtaleloven kapittel 3 del III tale for en slik forståelse. Når tjenesteyteren selv har utvist skyld, og dette har medvirket til tapet, synes det mest rimelig at den profesjonelle tjenesteyteren også må bære tapet selv. På

den annen side er rettighetshaverens ansvar allerede begrenset etter § 3-20 tredje og fjerde ledd, og det kan anføres at behovet for å begrense ansvaret ytterligere ikke er påtrengende.

Bestemmelsen er ikke nærmere kommentert i forarbeidene. Det er heller ikke den tilsvarende bestemmelsen for betalingstransaksjoner i § 4-30. Løsningen må anses usikker.

I § 3-20 femte ledd annet punktum bokstav a til e er det videre listet opp en rekke spesifikke forhold som leder til at tjenesteyteren må bære tapet, «med mindre rettighetshaveren har opptrådt svikaktig»: Tjenesteyteren må for det første bære tapet dersom tapet har oppstått «etter at rettighetshaveren har varslet tilbyderen eller tjenesteyteren om misbruk eller fare for misbruk i samsvar med § 3-19 annet ledd», jf. bokstav a. Etter bokstav b gjelder det samme «når plikten til å tilrettelegge for varsling etter § 3-17 eller § 3-18 er misligholdt». Etter ordlyden er det ikke noe krav om årsakssammenheng mellom tapet og pliktbruddet. Tjenesteyteren må tilsynelatende bære tapet selv om tapet ikke *skyldes* at rettighetshaver ikke har varslet fordi det ikke er tilrettelagt.

Videre følger det av bokstav c at rettighetshaveren ikke svarer for noe tap «når den elektroniske signeringen ikke er tilstrekkelig sikker». Det er uklart hva dette skal bety, særlig i lys av at «elektronisk signatur» i § 3-16 første ledd bokstav a er definert som en «kvalifisert elektronisk signatur», som per definisjon har et høyt sikkerhetsnivå. Som nevnt i punkt 3 er det uklart om anvendelsesområdet til reglene i finansavtaleloven kapittel 3 del III er ment å være avgrenset til misbruk av kvalifiserte elektroniske signaturer. I så fall gir det liten mening å ha en regel om at rettighetshaveren ikke svarer for tap som følge av at den elektroniske signeringen ikke er tilstrekkelig sikker.

Det neste alternativet etter § 3-20 femte ledd er at «tjenesteyteren ikke har krevd sterk kundeautentisering eller tilsvarende sikkerhet i den utstrekning det for øvrig er relevant i forbindelse med avtaleinngåelse», jf. bokstav d. Det følger av forarbeidene at man med bestemmelsen har tenkt på tilfeller der svindel skjer for eksempel ved at svindleren først logger seg inn i nettbanken og deretter misbruker signaturfremstillingsdata ved opptak av kreditt. Ifølge forarbeidene «bør det få betydning dersom tjenesteyteren ikke har krevd sterk kundeautentisering i forbindelse med innloggingen».[71]

Det siste alternativet etter § 3-20 femte ledd er at det foreligger «forhold som gjør at tjenesteyteren er nærmest til selv å bære risikoen for misbruk», jf. bokstav e. Dersom tjenesteyteren har medvirket til tapet, er det et forhold som kan tilsi at tjenesteyteren er nærmest til å bære tapet. Dette dekkes imidlertid av femte ledd første punktum. Dersom bestemmelsen i bokstav e skal ha selvstendig betydning, må den dermed dekke noe

[71] Prop. 92 LS (2019–2020) s. 358.

annet enn tilfeller der tjenesteyteren selv har bidratt til tapet. Det er ikke helt enkelt å se hva slags typetilfeller som vil dekkes av alternativet, men det åpner i hvert fall for en rimelighetsvurdering.

9 Lemping av rettighetshavers ansvar

Det følger av § 3-21 første ledd at

«[r]ettighetshaverens ansvar etter § 3-20 annet og tredje ledd kan lempes når det er rimelig tatt i betraktning arten av den personlige sikkerhetsinformasjonen som var knyttet til de misbrukte elektroniske signaturfremstillingsdataene, omstendighetene som forelå da misbruket ble utført, og eventuell manglende aktsomhet eller andre forhold på tjenesteyterens side som har medvirket til at tapet oppsto».

I departementets lovforslag var det inntatt i tredje ledd at «lemping kan ikke skje hvis tapet skyldes at rettighetshaveren har opptrådt svikaktig eller forsettlig har unnlatt å oppfylle sine plikter etter § 3-19».[72] Den alminnelige erstatningsrettslige lempningsregelen i skadeserstatningsloven § 5-2 utelukker ikke lemping ved forsettlige forhold hos skadevolder, selv om det skal mer til for å lempe i slike tilfeller.[73] Den foreslåtte ordlyden kunne forstås slik at finansavtaleloven innskrenket muligheten for lemping i tråd med reglene i skadeserstatningsloven. På denne bakgrunn ble den nevnte ordlyden tatt ut i forbindelse med behandlingen i Stortinget og erstattet av en presisering om at regelen i finansavtaleloven § 3-21 «ikke [begrenser] rettighetshaverens adgang til lemping eller til å gjøre gjeldende andre innsigelser på annet grunnlag». I innstillingen er endringen begrunnet på følgende måte:

«Disse medlemmer oppfatter det slik at departementet gir uttrykk for det samme gjennom et utgangspunkt om erstatningsansvar etter ellers gjeldende rett, herunder blant annet regler om lemping, foreldelse mv. Det vil i praksis trolig være slik at flere av de momenter som allerede er vurdert i forbindelse med skadeserstatningsloven § 5-2, også inngår i en vurdering etter § 3-21. Når et eventuelt egenandelsansvar kan lempes ytterligere etter finansavtaleloven, skyldes dette etter disse medlemmers syn et behov for tilstrekkelig fleksible regler som også kan gi rettighetshaveren et rimeligere resultat enn det man i praksis har sett eksempler på etter gjeldende rett.»[74]

Regelen i finansavtaleloven § 3-21 er altså et supplement til den alminnelige lempningsregelen i skadeserstatningsloven § 5-2 som er ment å gi en *videre* lempingsadgang enn det som allerede følger av de erstatningsrettslige reglene.

---

[72] Prop. 92 LS (2019–2020) s. 413.

[73] Se Rt-2004-165.

[74] Innst. 104 L (2020–2021) s. 23.

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

Etter skadeserstatningsloven § 5-2 kan skadevolders ansvar lempes for det første der det vil være urimelig tyngende (første punktum), og for det andre i tilfeller hvor det er «rimelig at den skadelidte helt eller delvis bærer skaden» (annet punktum). Om det siste alternativet påpekes det i forarbeidene at lemping er særlig aktuelt «i tilfelle hvor det er rimelig at skaden dekkes av forsikring på skadelidtes hånd. Dette kan særlig være aktuelt dersom skaden har rammet store verdier som generelt er sterkt utsatt for skade».[75]

I Easybank-dommen uttaler Høyesterett, under henvisning til nevnte uttalelse i forarbeidene, at de «samme hensynene gjør seg … gjeldende der skadelidte på annen måte har mulighet til å forebygge og pulverisere tapet».[76] Som nevnt kom Høyesterett til at det ikke forelå ansvarsgrunnlag for BankID-innehaveren, og spørsmål om lemping kom derfor ikke på spissen. I et *obiter dictum* uttaler imidlertid Høyesterett at

«der en privatperson etter alminnelige erstatningsregler blir erstatningsansvarlig overfor en finansinstitusjon for et stort økonomisk tap som er oppstått som følge av misbruk av BankID, vil det, avhengig av de nærmere omstendighetene, kunne være grunnlag for å sette erstatningsbeløpet vesentlig ned etter lempingsregelen i skadeserstatningsloven § 5-2».[77]

I denne sammenhengen er det verdt å merke seg at beløpet i den aktuelle saken var drøyt 100 000 kroner, og at Høyesterett omtaler dette som et beløp «som for en enkeltperson er betydelig».[78]

10 Avsluttende bemerkninger

I denne artikkelen har vi gjennomgått de nye reglene i finansavtaleloven kapittel 3 del III om tapsfordeling ved misbruk av digital signatur. Reguleringen må sies å være en naturlig utvikling og utvidelse av forbrukervernet i finansavtaleloven, som har skjedd parallelt med en økning i risiko som følge av digitaliseringen. Utviklingen har gått via å regulere tapsfordelingen ved misbruk av kredittkort i 1985, til også å omfatte debetkort på slutten av 1990-tallet og nettbankoverføringer i 2009, til nå også å gjelde misbruk av digital signatur ved inngåelse av avtaler om finansielle tjenester.

Finansnæringens hovedinnvending mot reglene var at de ikke var tilstrekkelig utredet. Det er lett å være enig i at man optimalt skulle hatt en grundigere, og ikke minst en litt mindre kronglete, lovgivningsprosess. At det ble slik, må forstås i sammenheng med at antallet lånesvindelsaker eksploderte på kort tid rundt 2017. Det utviklet seg en omfattende og svært streng rettspraksis fra tingrettene, som sto sterkt i strid med

---

[75] Ot.prp. nr. 60 (1980–81) s. 45.
[76] HR-2020-2021-A avsnitt 67.
[77] HR-2020-2021-A avsnitt 109.
[78] HR-2020-2021-A avsnitt 104.

politikere og allmenhetens rettsfølelse. Mens folk fikk lagt livet sitt i ruiner i raskt tempo, var det ikke tid til ytterligere utredninger. Finansnæringen kunne selv ha unngått dette dersom den hadde fulgt opp egne anbefalinger om i større grad å bære tapet selv, slik Finans Norges rapport fra 2013 la opp til.

Nye regler av så vidt stor praktisk betydning, som ikke er utredet bredt i en NOU, og hvor ordlyden på et vesentlig punkt er endret fra proposisjonen til endelig vedtakelse på Stortinget, vil måtte inneholde en rekke uklarheter som må finne sin løsning i praksis etter at loven har trådt i kraft. Vi har i denne artikkelen pekt på flere slike uklarheter, uten at det har vært rom for å gå i dybden på hvordan alle disse uklarhetene bør løses. Særlig grensen mellom grov uaktsomhet og forsett vil ha stor praktisk betydning, og selv etter avklaringene i HR-2022-1752-A er det flere uløste spørsmål her. Formuleringen om at pseudounderskriveren «måtte forstå at det var nærliggende fare for tap», ble inntatt av Stortinget i lovarbeidets aller siste fase, og det gjenstår å se hvordan bestemmelsen vil bli praktisert.

Det som i alle tilfeller synes klart, er at den teknologiske utviklingen – og med den utviklingen av nye svindelmetoder – går svært raskt, og at lovgiver har vanskelig for å holde tritt. Forhåpentligvis vil de nye reglene, i kombinasjon med de to dommene fra Høyesterett fra 2020 og 2022, gi et mer effektivt vern for forbrukere, samtidig som det gir finansinstitusjonene et incentiv til å iverksette enda bedre tiltak for å unngå svindel. Når finansnæringen skal vurdere enkeltsaker fremover, bør den ta innover seg de sentrale formålene bak den nye reguleringen. Gjør den det, kan vi kanskje likevel slippe en lang rekke belastende, kostbare og tidkrevende rettsprosesser. For de mange som ble utsatt for økonomisk justismord på veien hit, er det dessverre for sent.[79]

[79] Marte Eidsand Kjørven. «BankID-svindel og økonomiske justismord». *Lov og Rett*, nr. 1. 2021, s. 5–6.