Bruk og misbruk av elektronisk identifikasjon

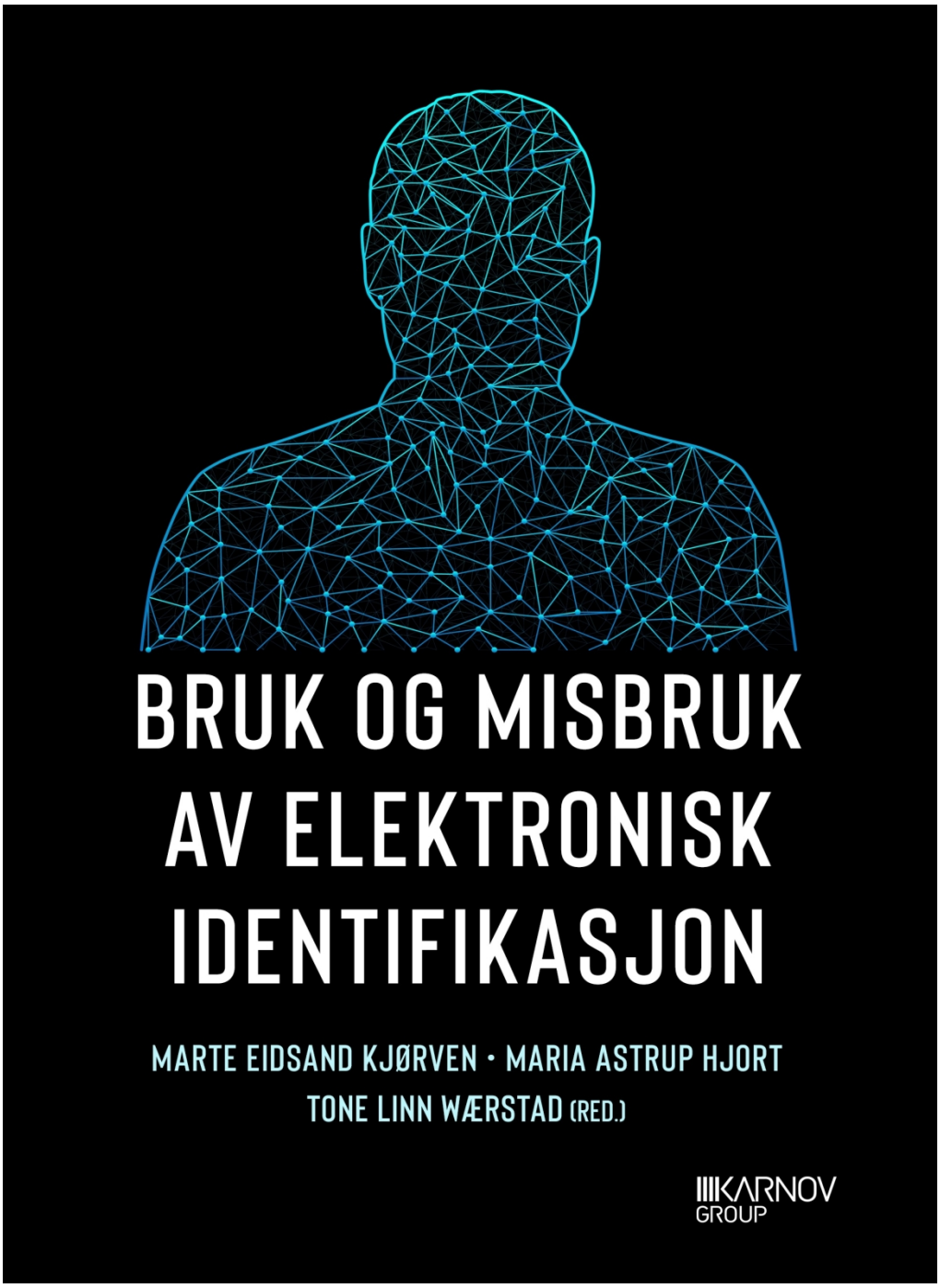
Forfatter	Kjørven, Marte Eidsand, Astrup Hjort, Maria og Wærstad, Tone Linn (red.) (ekstern lenke)

Dato	2022-11-08
Publisert	Karnov forlag (KARNOV-2022-3)

Sammendrag	Systemer for elektronisk identifikasjon (eID) spiller en nøkkelrolle i dagens samfunn. Ved bruk av eID kan vi blant annet få tilgang til private og offentlige tjenester, rapportere til skattemyndighetene, få innsikt i helseopplysninger, gjennomføre betalingstransaksjoner, overføre eiendomsretten til fast eiendom, signere lånekontrakter og registrere skilsmisse. Fordi systemer for eID også kan misbrukes til å gjennomføre en lang rekke kriminelle handlinger, inkludert ulike typer svindel, hvitvasking, korrupsjon og terrorisme, innebærer de imidlertid også en risiko både for den enkelte og for samfunnet. I tillegg er det et problem at ikke alle borgere har tilgang til en eID. Dermed stenges de også ute fra sentrale offentlige og private tjenester. Denne antologien løfter frem ulike spørsmål knyttet til bruk og misbruk av eID. Har alle rett til å få tilgang til en eID? Hvordan skjer digitale ID-tyverier, og hvem utsettes for det? Kan en avtale være bindende selv om den bygger på misbruk av noens eID? Hvem har rett til en eiendom som er overført basert på ID-misbruk? Når eID misbrukes i nære relasjoner, hvordan blir den rettslige tapsfordelingen? Og hvilken rolle spiller menneskerettighetene i dette problemkomplekset? Et grunnspørsmål for antologien er hvordan alminnelige regler innenfor blant annet avtale- og kontraktsrett og prosessrett skal forstås i møte med ny teknologi. Særskilt regulering av eID, blant annet i den nye finansavtaleloven, behandles også. I tillegg reises spørsmål om menneskerettigheter.

Utgiver	Karnov Group Norway
Versjon	1. utgave, 5. versjon
ISBN	978-82-93816-31-7
Sist oppdatert	2023-10-06

Innholdsfortegnelse



Innledning til hele antologien

Artiklene i denne antologien publiseres fortløpende.

Elektroniske signaturer og avtalebinding

Line Utne Norland og Marte Eidsand Kjørven

Fagfellevurdert artikkel

1 Innledning

Måten vi inngår avtaler på, har endret seg i takt med digitaliseringen av samfunnet, og mange avtaler inngås i dag ved bruk av elektronisk signering. I denne artikkelen[1] skal vi undersøke hvilken betydning disse endringene har for regler om avtaleinngåelse og ugyldighet, og se nærmere på spørsmålet om i hvilken utstrekning en avtale som er signert elektronisk av en tredjeperson, er bindende for den såkalte pseudounderskriveren (innehaveren av den elektroniske signaturen).

Digitalisering medfører store effektivitetsgevinster, men innebærer også potensial for misbruk.[2] Norsk senter for informasjonssikring (NorSIS) har i samarbeid med skatteetaten de siste elleve årene gjennomført årlige undersøkelser av hvor mange som utsettes for ID-tyveri. Undersøkelsen fra 2022 viste at ca. 150 000 nordmenn hadde blitt utsatt for ID-tyveri de to siste årene.[3]

Én slik form for identitetskrenkelse er inngåelse av avtaler i en annens navn. Denne typen kriminalitet kan påføre både pseudounderskriveren og medkontrahentene store tap. De avtalerettslige reglene har i denne sammenheng avgjørende betydning for hvordan dette tapet fordeles mellom pseudounderskriveren og medkontrahenten.

Hovedregelen etter alminnelig avtalerett er at man ikke blir bundet av rettslige disposisjoner som er foretatt av andre.[4] Slike disposisjoner vil rammes av den ulovfestede sterke ugyldighetsgrunnen *falsk*.[5] Dette er imidlertid ikke mer enn et utgangspunkt, og i denne artikkelen skal vi undersøke hvor langt ugyldighetsgrunnen *falsk* rekker. Dette reiser særlig spørsmål om forholdet mellom ugyldighetsgrunnen *falsk* og ulovfestede regler om *representasjon* (fullmakt). I hvilke tilfeller kan den som signerer elektronisk i en annens navn, sies å representere pseudounderskriveren på en slik måte at pseudounderskriveren blir bundet?

Drøftelsene tar utgangspunkt i norsk rett. Norsk avtalerett bygger imidlertid på et fellesnordisk samarbeid, og det kan også være relevant å se hen til nordiske kilder.[6] Högsta domstolen i Sverige har i en avgjørelse fra desember 2021 konkludert med at en mann ble bundet av en låneavtale som var signert elektronisk av samboeren.[7] Mannen hadde frivillig overgitt sin eID til samboeren for at hun skulle håndtere parets økonomi, og dette gav henne rettslig legitimasjon til å inngå den aktuelle låneavtalen på mannens vegne.[8] Dansk Højesteret har de siste tre årene avsagt fem kjennelser med spørsmål om avtalebinding på grunnlag av uaktsomhet ved håndtering av eID.[9] Resultatet ble avtalebinding i to av sakene. Dommene nevnt i dette avsnittet, og deres forhold til norsk rett, vil også bli drøftet.

Dersom avtalen *ikke* er bindende, vil tapsfordelingen mellom pseudounderskriveren og medkontrahenten måtte løses med utgangspunkt i deliktserstatningsrettslige regler. Pseudounderskriveren blir erstatningsansvarlig overfor medkontrahenten for tap som skyldes at pseudounderskriveren har opptrådt uaktsomt med sin eID.[10] Det har vært reist en rekke tvister for norske domstoler med spørsmål om rekkevidden av pseudounderskriverens erstatningsansvar overfor banker når låneavtaler er inngått basert på misbruk av BankID.[11] I mange saker har ofrene for ID-tyveri blitt holdt ansvarlig på grunnlag av svært strenge krav til aktsomhet ved håndtering av BankID. Dette er bakgrunnen for at lovgiver i 2020 vedtok særlige regler om tapsfordelingen ved misbruk av elektronisk signatur i avtaler om finansielle tjenester.[12] Etter ordlyden er det klart at de nye reglene begrenser pseudounderskrivers erstatningsansvar etter den alminnelige culparegelen. Et særlig spørsmål er om de nye reglene i finansavtaleloven om erstatningsansvar også får betydning for hvorvidt en avtale om finansielle tjenester er bindende etter alminnelige avtalerettslige regler.

Artikkelen er bygget opp på følgende måte: I punkt 2 vil vi redegjøre for hva en elektronisk signatur er, og hvilken betydning selve signaturen har for spørsmålet om hvorvidt det er inngått bindende avtale. I punkt 3 drøftes spørsmålet om pseudounderskriveren på grunnlag av samtykke, etterfølgende passivitet eller andre forhold kan bli bundet til en avtale som er signert i vedkommendes navn av en tredjeperson. Forholdet til de nye reglene i finansavtaleloven 2020 drøftes særskilt i punkt 4, før vi kommer med noen avsluttende bemerkninger i punkt 5.

2 Generelt om elektroniske signaturer og signaturens betydning for spørsmålet om hvorvidt det er inngått bindende avtale

Lov om elektroniske tillitstjenester har regler om rettslige virkninger av elektroniske signaturer.[13] Loven gjennomfører forordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS-forordningen).[14] Forordningen har til formål å «sikre at det indre

marked fungerer på en tilfredsstillende måte, og ... å oppnå et egnet sikkerhetsnivå for elektroniske identifikasjonsmidler og tillitstjeneste».[15]

eIDAS-forordningen skiller mellom elektroniske signaturer på tre sikkerhetsnivåer: «lavt», «betydelig» og «høyt». Definisjonen av en elektronisk signatur er inntatt i artikkel 25. Signaturer på høyeste sikkerhetsnivå omtales som «kvalifiserte elektroniske signaturer».[16] En kvalifisert elektronisk signatur må blant annet være entydig knyttet til underskriveren, kunne identifisere vedkommende og genereres ved bruk av elektroniske signaturfremstillingsdata med høy grad av tillit, og det må være mulig å se hvilke endringer som er gjort etter signeringen. Vi går i denne artikkelen ikke nærmere inn på de spesifikke sikkerhetskravene for de ulike typene av elektroniske signaturer.

I Norge finnes det flere systemer for kvalifisert elektronisk signatur, men den største aktøren er BankID. BankID kan benyttes til over 700 ulike formål, herunder signering av en rekke ulike typer avtaler.[17]

Etter eIDAS-forordningen skal en kvalifisert elektronisk signatur ha samme rettsvirkning som en fysisk signatur.[18] Det vil si at de alminnelige avtalerettslige reglene gjelder tilsvarende for kvalifiserte elektroniske signaturer som for fysiske signaturer. For signaturer som ikke oppfyller kravene til å være en «kvalifisert elektronisk signatur», følger det av eIDAS-forordningen artikkel 25 nr. 1 at en slik signatur ikke må «nektes rettsvirkning og gyldighet som bevis i forbindelse med rettergang alene av den grunn at den er elektronisk, eller at den ikke oppfyller kravene til kvalifiserte elektroniske signaturer». I det følgende skal det knyttes noen kommentarer til hvilken betydning selve signaturen, elektronisk eller fysisk, har for spørsmålet om hvorvidt en avtale er bindende.

Reglene om når en avtale er bindende, følger dels av avtaleloven[19], dels av ulovfestet rett.[20] Et sentralt utgangspunkt i avtaleretten er prinsippet om privat autonomi, altså selvbestemmelsesrett: Alle står fritt til å avtale det de ønsker, med den de ønsker.[21] Et annet prinsipp er formfrihetsprinsippet.[22] Alle typer disposisjoner vil altså i utgangspunktet kunne være grunnlag for en avtale – muntlig, skriftlig eller gjennom atferd. For eksempel kan disposisjonen komme til uttrykk ved en fysisk bevegelse eller ved å sende en emoji, så vel som ved å møte opp i medkontrahentens forretningslokaler og signere fysisk på et dokument.[23] Avtaleretten er teknologinøytral, og den anvendes på en rekke nye måter som ikke nødvendigvis passer så godt med det opprinnelige rammeverket.

Avtalelovens system legger opp til en modell der avtaler inngås gjennom utveksling av partsutsagnene *tilbud* og *aksept*.[24] Utenfor de rene tilfellene av tilbud og aksept, som direkte reguleres av avtaleloven, oppstiller litteraturen ulike disposisjonskriterier utledet av rettspraksis for når en avtale skal anses inngått. Det sentrale i en slik rettslig vurdering blir å avgjøre om løftegivers vilje kommer til uttrykk på en slik måte at medkontrahenten får en berettiget forventning om at løftegiver ønsker å binde seg.[25]

På denne bakgrunn kan vi slå fast at en signatur (elektronisk eller fysisk) på et kontraktsdokument ikke *i seg selv* gjør avtalen bindende etter norsk rett. For å ha innvirkning på bindingsspørsmålet må signaturen anses som et uttrykk for løftegivers vilje til å binde seg.[26]

En underskrift er imidlertid, sammenliknet med mange andre disposisjoner, en relativt sikker indikasjon på at løftegiver har ment å binde seg. Udsen beskriver underskriftens egenskaper med begrepene *autentisitet*, *integritet* og *uavviselighet*.[27] Med «autentisitet» menes at medkontrahenten kan være sikker på at løftegiver står inne for innholdet av avtalen.[28] «Integritet» betegner det forhold at innholdet ikke er blitt endret siden underskriften fant sted.[29] «Uavviselighet» vil si at den som står inne for innholdet av avtalen, altså løftegiver, ikke senere kan gå fra disposisjonen.[30] Samlet sett vil en disposisjon med disse egenskapene være egnet til å gi medkontrahenten berettigede forventninger om at løftegiver har ment å binde seg, slik at avtale som regel vil anses inngått dersom det foreligger en signatur fra løftegiver. Dette gjelder i enda større grad ved elektroniske signaturer, der tilfellet ofte vil være at medkontrahenten ikke har andre holdepunkter enn signaturen å forholde seg til.

En annen sak er at det kan oppstå *bevismessige spørsmål* om hvorvidt signaturen faktisk er avgitt av innehaveren. I finansavtaleloven 2020 § 3-6 tredje ledd er det angitt at bruken av elektronisk signatur ikke i seg selv er tilstrekkelig til å bevise at det er pseudounderskriver som har inngått avtalen.[31] Merk likevel at dette gjelder tilfeller der pseudounderskriver nekter for å ha inngått avtalen; det gjelder altså ikke spørsmålet om hvorvidt en elektronisk signert avtale i utgangspunktet er bindende. Vi går ikke her nærmere inn på de bevismessige spørsmålene, som må løses med utgangspunkt i alminnelige bevisregler.

Dersom det må legges til grunn at signaturen, fysisk eller elektronisk, er påført av en annen, er hovedregelen, som nevnt innledningsvis, at avtalen rammes av den sterke ugyldighetsgrunnen *falsk*.[32] Sterke ugyldighetsgrunner kan gjøres gjeldende selv om medkontrahenten er i god tro.[33] Som Hov poengterer: «Det er sikkert nok at den som tilsynelatende har avgitt utsagnet (pseudoavgiveren), ikke er bundet i disse tilfellene. Han vil jo ikke ha noen som helst sjanse til å beskytte seg mot misbruk av denne typen.»[34]

Det finnes lite rettspraksis og teori om hva som nærmere bestemt må til for å konstatere at ugyldighetsgrunnen *falsk* foreligger.[35] Dette har nok sammenheng med at avtaler før digitaliseringens tidsalder typisk ble inngått mens partene befant seg fysisk i samme rom. Man gikk for eksempel i banken, viste legitimasjon og signerte på låneavtalen. Da hadde man større mulighet til å kontrollere at det ble handlet med rette vedkommende, og man kunne lettere fange opp om noe virket mistenkelig. I dag er det langt flere avtaler som inngås ved at partene sitter hver for seg, og i mange tilfeller er den elektroniske signaturen det eneste holdepunktet man har for at medkontrahenten ønsker å forplikte seg. Som påpekt av Woxholth har dette også ført til en reaktualisering av falsk som ugyldighetsgrunn.[36] Den nærmere grensedragningen mellom ugyldighetsgrunnen *falsk* og tilfeller som fører til avtalerettslig binding, er tema i fortsettelsen.

3 Kan pseudounderskriver bli bundet av avtalen selv om den elektroniske signaturen er påført av en annen?

3.1 Innledende bemerkninger

Spørsmålet under dette punktet er hvor langt ugyldighetsgrunnen *falsk* rekker, og om en avtale signert av en tredjeperson likevel kan bli bindende for pseudounderskriveren i noen tilfeller. Dersom det faktisk foreligger en viljeserklæring i form av et *gyldig samtykke* fra pseudounderskriveren, blir avtalen bindende for pseudounderskriveren, se punkt 3.2. Videre kan det spørres om tredjeperson som har tilgang til en annens eID, kan ha *rettslig legitimasjon* basert på ulovfestede regler om representasjon til å binde innehaveren, se punkt 3.3. Til slutt, i punkt 3.4, skal vi undersøke i hvilken grad etterfølgende *passivitet* fra pseudounderskriveren kan føre til at han eller hun blir bundet av avtalen.

3.2 Avtalebinding på grunnlag av samtykke

Dersom pseudounderskriveren har samtykket til at tredjeperson skal signere på hans eller hennes vegne, og samtykket er gyldig, vil avtalen klart nok bli bindende for pseudounderskriveren. Som Högsta domstolen i Sverige har uttalt:

> «Det är ... inte fråga om obehörig användning när e-legitimationen används av annan än innehavaren i enlighet med innehavarens samtycke eller med stöd av en fullmakt som innehavaren har lämnat. Om innehavaren ger någon annan i uppdrag att ingå ett visst låneavtal i hans eller hennes namn och därvid ger uppdragstagaren möjlighet att använda e-legitimationen, blir låneavtalet alltså bindande för innehavaren.»[37]

Tilsvarende må gjelde også for norsk retts vedkommende. Riktignok vil en slik opptreden være et brudd på BankID-avtalen, som slår fast at «BankID er personlig og skal ikke overdras eller på annen måte overlates til eller brukes av andre enn Kunden eller Brukeren».[38] Dette kan likevel ikke ha betydning for spørsmålet om avtalebinding når BankID faktisk er overlatt til tredjeperson, som anvender den på oppdrag fra innehaveren.

Begrunnelsen for at en avtale rammes av ugyldighetsgrunnen *falsk,* er at disposisjonen ikke inneholder en viljeserklæring fra pseudounderskriver. Denne begrunnelsen slår ikke til når pseudounderskriver har villet binde seg.[39] At avtalen blir bindende i disse situasjonene, kan forankres i prinsippet om formfrihet ved avtaleinngåelse,[40] som tilsier at det er opp til partene hvordan en bindende disposisjon fremsettes.

Dersom pseudounderskriver ikke er i stand til å håndtere BankID på egen hånd, og sitter sammen med en hjelper som bistår ved helt eller delvis å taste inn nødvendig sikkerhetsinformasjon, kan situasjonen sammenliknes med en fysisk underskrift som er gjennomført ved såkalt påholden penn. Lovavdelingen har i en tolkningsuttalelse om arvelovens krav til signatur på testamenter uttalt at «det er sedvanerett i Norge at der en person undertegner et dokument, regnes i alminnelighet undertegning med påholden penn likt med vanlig

undertegning, dersom den som undertegner ikke er i stand til å føre pennen alene».[41] Det er neppe grunn til å vurdere en elektronisk signatur som er påført en avtale med bistand fra en hjelper, på en annen måte.

Det er også mulig å se situasjonen der samtykke foreligger, som en fullmakt. Dersom en person A overlater sin BankID til B for at B skal signere en avtale på As vegne, kan B sies å ha blitt utstyrt med en fullmakt.[42] Hvorvidt binding også kan skje dersom B foretar andre disposisjoner enn de A har bedt ham eller henne om, er tema under neste punkt. Her er forutsetningen at B holder seg innenfor den rett han eller hun utleder fra A gjennom samtykke eller fullmakt.

I tråd med alminnelige avtalerettslige regler må en viljeserklæring være *gyldig* for at den skal lede til en bindende avtale. Dette gjelder også der viljeserklæringen kommer til uttrykk ved at A samtykker til at B signerer elektronisk på As vegne. Hvorvidt viljeserklæringen er gyldig, må vurderes etter de alminnelige reglene om dette i avtaleloven kapittel 3 samt ulovfestede regler om ugyldighet.[43]

Dersom viljeserklæringen/samtykket rammes av en sterk ugyldighetsgrunn, som umyndighet eller grov tvang, kan ugyldighet gjøres gjeldende selv om medkontrahenten er i god tro.[44] Er det derimot tale om en svak ugyldighetsgrunn, for eksempel svik, lett tvang eller villfarelse, må medkontrahenten være uaktsom eller i ond tro for at ugyldigheten skal kunne gjøres gjeldende.[45] Det studentdrevne rettshjelpstiltaket Juridisk rådgivning for kvinner (JURK) har blant annet satt søkelyset på kvinner som utsettes for økonomisk vold i forholdet.[46]

Med mindre samtykket gis under forhold som kategoriseres under avtaleloven § 28 om vold eller trusler som fremkaller frykt for noens liv eller helbred, vil denne typen omstendigheter i beste fall utgjøre en svak ugyldighetsgrunn etter avtaleloven §§ 29, 30 eller 31. Spørsmålet blir da hvordan man skal vurdere om medkontrahenten er i aktsom god tro.

Det er en forutsetning her at pseudounderskriveren har gitt et – potensielt ugyldig – samtykke til en konkret disposisjon. Et slikt samtykke forutsetter naturligvis kunnskap om disposisjonen. Dersom pseudounderskriveren blir presset til å oppgi BankID-opplysninger uten kunnskap om hva utpresseren bruker denne informasjonen til, foreligger det overhodet ingen «viljeserklæring». I hvilken grad utpresseren kan ha rettslig legitimasjon til å opptre på vegne av pseudounderskriveren i slike situasjoner, er tema i neste punkt.

For avtaler som inngås ved bruk av elektronisk signatur, vil medkontrahenten typisk ikke ha andre holdepunkter enn signaturen å forholde seg til. Rent faktisk vil medkontrahenten derfor gjennomgående være uvitende om at det eventuelt er en tredjeperson som har påført signaturen. Et sentralt spørsmål er derfor om aktører som belager seg på elektronisk avtaleinngåelse, må foreta noen kontrolltiltak, utover bruk av en kvalifisert elektronisk signatur, for å kunne påberope seg å være i *aktsom* god tro.

Høyesterett har i HR-2020-2021-A fremhevet at en bank som velger «å inngå en avtale om lån med et beløp som for en enkeltperson er betydelig, utelukkende basert på identifikasjon og elektronisk signatur gjennom BankID», «bevisst [har] valgt en handlemåte som innebar en klar risiko for tap». Videre uttales det at det ville «vært mulig for banken å foreta ytterligere kontrolltiltak før man ubetalte [sic] lånebeløpet. Dersom man hadde gjort dette, er det stor sannsynlighet for at misbruket ville vært unngått».[47] Saken gjaldt spørsmål om pseudounderskrivers erstatningsansvar, ikke avtalebinding. Argumentet har likevel overføringsverdi som et generelt syn på hvordan risikoen forbundet med elektronisk avtaleinngåelse bør fordeles, og hvilke momenter som er relevante i den forbindelse.[48] Dersom kontrolltiltak også kunne avdekket at viljeserklæringen var ugyldig, kan det tilsi at banken ikke er i aktsom god tro.

Et liknende synspunkt er fremmet av en arbeidsgruppe nedsatt av Finans Norge i en rapport fra 2013 om digitalisering av låneavtaler. Her heter det:

> «Ved mindre alvorlige tilfeller av tilblivelsesmangler kan avtalen bli ugyldig dersom banken kjente eller burde kjenne til omstendighetene. ...
>
> ... Med en elektronisk saksbehandling vil det være vanskeligere å oppdage eller unngå denne type forhold i avtalesituasjonen. Det kan reises spørsmål ved om den omstendighet at avtalen inngås elektronisk, uten noe personlig møte mellom banken og kunden, endrer vurderingen av når det foreligger aktsom god tro hos banken. Dersom det kan legges til grunn at banken ville ha oppdaget ugyldighetsgrunnen ved et fysisk møte, antar arbeidsgruppen at bankene må være forberedt på å bære denne tilleggsrisikoen ved elektroniske avtaler.»[49]

Her ser det ut til at arbeidsgruppen mener at en god tro-vurdering må ta utgangspunkt i hva banken kunne oppdaget dersom avtalen ble inngått fysisk. Synspunktet synes å være at banken som den profesjonelle parten

er nærmest til å dekke tap som oppstår som følge av at overgangen fra fysisk til elektronisk avtaleinngåelse vil gjøre det vanskeligere å oppdage svake ugyldighetsgrunner. Banken har mulighet til å pulverisere tapet og sette inn ytterligere kontrolltiltak. Dersom det ikke stilles krav til medkontrahenten utover å konstatere at avtalen er signert elektronisk, vil beskyttelsen som er ment å ligge i reglene om svak ugyldighet, for alle praktiske formål være lite verdt i en digitalisert verden.

Oppsummert vil en avtale med en elektronisk signatur påført av tredjeperson bli bindende for pseudounderskriveren dersom det foreligger et samtykke som etter alminnelige avtalerettslige regler utgjør en gyldig viljeserklæring. Der viljeserklæringen rammes av en svak ugyldighetsgrunn, er det noe uklart hvordan man skal vurdere spørsmålet om god tro hos medkontrahenten. Det er i denne sammenheng etter vårt syn grunn til å legge vekt på hvilke tiltak som kan forventes iverksatt av medkontrahenten med tanke på å forsikre seg om at viljesærklæringen ikke rammes av en ugyldighetsgrunn (herunder både falsk og andre ugyldighetsgrunner).

3.3 Avtalebinding på grunnlag av ulovfestet representasjon?

3.3.1 Innledende bemerkninger

Spørsmålet i dette punktet er hvorvidt utlevering av BankID-opplysninger til tredjeperson kan skape en rettslig legitimasjon slik at innehaveren blir bundet av disposisjoner foretatt i hans eller hennes navn av tredjeperson. En eldre person utleverer for eksempel sine BankID-opplysninger til en nabo for bistand til å betale en regning på nett. Naboen betaler regningen, men inngår også en mobilabonnementsavtale og en kredittavtale i BankID-innehaverens navn. Spørsmålet er da om BankID-innehaveren blir bundet av naboens disposisjoner. Det kan også spørres om potensielt uaktsomme forhold som ikke inkluderer frivillig overgivelse av BankID-opplysninger, for eksempel nedtegning av passord eller å falle for et phishing-angrep, slik at tredjeperson får tilgang til nødvendig sikkerhetsinformasjon, kan skape en rettslig legitimasjon.

Dersom denne typen handlinger kan skape rettslig legitimasjon, vil pseudounderskriver i noen tilfeller kunne bli bundet av tredjepersons disposisjon på hans eller hennes vegne selv om disposisjonen ligger utenfor instruksene som ble gitt til tredjeperson.[50]

At en person får tilgang til en annens eID, og signerer i dennes navn, utgjør ikke en type fullmakt som reguleres av avtaleloven kapittel 2. Det kan imidlertid etableres fullmakt også på ulovfestet grunnlag, gjerne omtalt som «kombinasjons- eller tillitsfullmakt» eller bare «ulovfestet representasjon». Den sentrale dommen er Rt-2011-410 (Optimogården). Saken gjaldt spørsmål om hvorvidt daglig leder av en avdeling av et selskap var legitimert til å inngå leieavtale om forretningslokaler på vegne av selskapet. Vurderingstemaet ble formulert som et spørsmål om hvorvidt «medkontrahenten har fått berettigede forventninger om at vedkommende har fullmakt» (avsnitt 35).

Det typiske for slike fullmakter er at fullmaktsgiver har opptrådt på en slik måte at han eller hun ut fra rimelighetshensyn bør anses bundet.[51] En slik vurdering kan i utgangspunktet synes å passe godt på tilfellet der pseudounderskriver utstyrer den andre med det nødvendige for å inngå en avtale i hans eller hennes navn, enten tredjeperson da inngår den avtalen det er bedt om, eller en annen avtale. På den annen side er det en vesentlig forskjell fra situasjonen der en tredjeperson får tilgang til sikkerhetsinformasjon som setter vedkommende i stand til å signere elektronisk på en annens vegne, og tradisjonelle fullmaktssituasjoner, der trepartsforholdet er synlig utad. I tradisjonelle fullmaktssituasjoner vil medkontrahenten være klar over at den han eller hun handler med, handler på vegne av en annen (fullmaktsgiver).[52] I en situasjon der en tredjeperson handler på vegne av en annen ved bruk av dennes eID, vil det ikke være synlig at det er en annen enn innehaveren som påfører signaturen.

Spørsmålet om hvorvidt det kan etableres rettslig legitimasjon som binder pseudounderskriveren i slike situasjoner, har ikke blitt reist for Høyesterett i Norge. I norsk juridisk teori synes flertallet av forfattere å slutte opp om et utgangspunkt om at avtalerettslig binding er utelukket ved falsk som er muliggjort på grunn av uaktsomhet fra pseudounderskriveren, og at medkontrahenten er henvist til å kreve erstatning.[53] Både i Sverige og Danmark har det imidlertid vært en utvikling i retning av at pseudounderskriveren på visse vilkår kan bli avtalerettslig bundet i situasjoner der en elektronisk signatur er påført av en tredjeperson.

Den norske avtaleloven er et resultat av et fellesnordisk lovsamarbeid som foregikk på slutten av 1800-tallet og begynnelsen av 1900-tallet.[54] Selv om avtalelovene i Danmark, Norge og Sverige er avvikende på noen punkter, gir de i hovedsak en lik regulering av sentrale avtalerettslige spørsmål.[55] For de *ulovfestede* tilfellene kan det imidlertid tenkes at det vil være større variasjon landene imellom. Likevel vil nok mange av de samme hensynene ligge til grunn for de ulovfestede som for de lovfestede spørsmålene, slik at løsningen i mange tilfeller vil bygge på de samme avveiningene og dermed gi et noenlunde likt resultat. Det gjør at man ofte kan se hen til dansk og svensk rettspraksis i avgjørelsen av avtalerettslige spørsmål der den norske retten er uklar.[56] I det følgende vil vi derfor gjøre rede for nyere praksis fra svensk og dansk høyesterett, før vi vurderer i hvilken utstrekning tilsvarende synspunkter kan gjøres gjeldende i norsk rett.

3.3.2 Svensk rett

Högsta domstolen i Sverige (HD) tok i desember 2021 stilling til om en mann som hadde overlatt sin BankID til samboeren for at samboeren skulle betale husholdningens løpende regninger, ble bundet av avtale om lån på 18 273 svenske kroner som samboeren tok opp i hans navn, og som han ikke hadde samtykket til.[57] HD kom til at overlatelsen av BankID utgjorde en fullmakt som i den konkrete saken måtte lede til binding for BankID-innehaveren.

HD peker på at det har vært et uavklart spørsmål om fullmaktsreglene kan anvendes i en situasjon der det er skjult for medkontrahenten at det ikke er hovedmannen selv som agerer, og viser til at verken forarbeidene til den svenske *avtalslagen* eller rettspraksis gir noe svar, og at oppfatningene i teorien har vært delte. Når HD kommer til at fullmaktsreglene kan få anvendelse, er det særlig begrunnet i at det synes å ha liten betydning for fullmaktsgiver og fullmektigen om det er synlig for medkontrahenten at fullmektigen opptrer via en mellommann. Når HD kommer til at fullmaktsreglene kan få anvendelse, er det særlig begrunnet i hensynet til omsetningslivet. Det synes å ha liten betydning for fullmaktsgiver og fullmektigen om det er synlig for medkontrahenten at fullmektigen opptrer via en mellommann: «tredje man bör i båda situationerna kunna förlita sig på att råatthandlingen binder huvudmannen».[58]

Ikke enhver situasjon der noen har fått tilgang til en annens eID, vil imidlertid gi grunnlag for rettslig legitimasjon som binder innehaveren. HD slår for det første fast at et grunnvilkår er at tredjepersonen utleder en rett fra innehaveren til å bruke dennes eID.[59] Dersom en slik rett ikke kan utledes fra innehaveren, vil det dreie seg om en «obehörig användning» av en annens eID, og disposisjonen vil ikke være bindende for innehaveren. Det presiseres at i tilfeller der sikkerhetskoder mv. er tilegnet «genom tillgrepp, vilseledande eller liknande förfarande», kan binding ikke oppstå, fordi «innehavaren aldrig har avsett att e-legitimationen skulle nyttjas av annan för någon typ av rättshandlingar».[60] Binding er bare mulig dersom eID-en er overlatt til tredjeperson «i syfte att mottagaren ska få använda den för visst eller vissa ändamål».[61]

Uttalelsene kan forstås slik at det er et absolutt vilkår at det foreligger et *gyldigsamtykke* om at tredjeperson skal bruke innehavers eID til én eller flere bestemte rettshandlinger. Rammes samtykket av en ugyldighetsgrunn, kategoriseres forholdet som en «obehörig användning», og binding på grunnlag av fullmakt er utelukket. Henvisningen til «vilseledande» tyder på at dette også gjelder for omstendigheter som ellers vil kategoriseres som en svak ugyldighetsgrunn. HDs uttalelser tyder også på at rent uaktsomme forhold faller utenfor; disse kan ikke danne grunnlag for et gyldig samtykke fordi det er et vilkår at innehaveren har «avsett att e-legitimationen skulle nyttjas av annan för någon typ av rättshandlingar».[62]

Dersom grunnvilkåret om gyldig samtykke til å bruke eID-en i innehaverens navn til en eller annen rettshandling er oppfylt, må det foretas en konkret vurdering av om medkontrahenten har «befogad tillit till att rättshandlingen vidtogs av en behörig person».[63] Ved vurderingen av om medkontrahenten kan ha slike berettigede forventninger, tar HD utgangspunkt i at tredjeperson normalt må kunne ha tillit til at en eID på høyt sikkerhetsinvå kun brukes av innehaveren selv, eller i det minste brukes med innehaverens samtykke. Vurderingen må imidlertid ta hensyn til «vilket slag av avtal som det rör sig om, vilken verksamhet som avtalet gäller, hur vanlig avtalstypen är och vilka åtaganden som avtalet innebär». Konkret peker HD på at overlatelse av eID til tredjeperson vil innebære en fullmakt som binder innehaveren for «ordinära transaktioner, däribland upptagandet av mindre lån». Videre uttaler HD at dersom

> «e-legitimationen däremot används för rättshandlingar av mera speciellt slag, såsom upptagandet av större lån, har tredje man mindre anledning att hysa befogad tillit. Det gäller i synnerhet när

> innehavaren är en konsument. I sådana fall kan det krävas att tredje man gör ytterligare kontroller för att få bekräftat att rättshandlingen härrör från innehavaren».[64]

Synspunktet kan forstås som et utslag av det alminnelige fullmaktsrettslige utgangspunktet om at disposisjoner foretatt av en fullmektig som går utenfor de interne instruksene, ikke binder hovedmannen dersom medkontrahenten ikke er i aktsom god tro. Hvorvidt medkontrahenten er i aktsom god tro, må ses i sammenheng med hvilke kontrolltiltak det kan forventes at medkontrahenten iverksetter. På grunn av den generelle faren for misbruk av eID bør det i forbindelse med større transaksjoner, som inngåelse av lån av betydelig beløp, kunne forventes at en tredjeperson forsikrer seg om at han eller hun handler med rette vedkommende. Dette er de samme hensyn Høyesterett bygger på i HR-2020-2021-A, selv om denne saken som nevnt gjaldt spørsmål om erstatningsansvar og ikke om avtalebinding.

I subsumsjonen la HD blant annet vekt på at formålet med å overlate BankID til samboeren nettopp var at hun skulle foreta økonomiske disposisjoner i innehaverens navn. Lånebeløpet var beskjedent, og det var ikke omstendigheter ved låneopptaket som gav banken oppfordring til å gjennomføre særskilte kontroller. Konklusjonen ble derfor at det forelå en fullmakt, og at pseudounderskriveren ble bundet av låneavtalen.

3.3.3 Dansk rett

I dansk rett har offentlige myndigheter lenge vært oppmerksom på de særlige problemstillinger som oppstår som følge av overgangen fra fysiske til digitale transaksjoner og avtaleinngåelser. Allerede i 1998 ble det nedsatt et offentlig utvalg som fikk i oppdrag å utrede ulike sider av digital handel og digital kommunikasjon. Som en del av dette arbeidet ble det utarbeidet en egen betenkning om elektroniske signaturer.[65] Utvalget avgav sin endelige rapport i 2004.[66]

I betenkningen om elektroniske signaturer gjennomgikk utvalget de avtale- og erstatningsrettslige implikasjonene av uberettiget bruk av systemer for elektroniske signaturer. Drøftelsene bygger blant annet på Henrik Udsens doktoravhandling *Den digitale signatur -ansvarsspørgsmål*.[67]

Når det gjelder spørsmål om avtalebinding, fremgår det at utgangspunktet etter dansk rett er at en avtale med en digital signatur som er påført av en annen enn innehaveren, som utgangspunkt rammes av ugyldighetsgrunnen *falsk*. Det pekes videre på at dette utgangspunktet forlates dersom tredjeperson må sies å ha en fullmakt. Utvalget peker i den forbindelse på at

> «[d]en blotte overgivelse af den private nøgle med tilhørende adgangskode til en anden antages næppe i sig selv at indebære, at den pågældende herved får fuldmagt eller i øvrigt kan anses som legitimeret til at indgå aftaler på certifikatindehaverens vegne».[68]

Vurderingen av om det foreligger en fullmakt i slike situasjoner, må avgjøres ut fra en

> «samlet vurdering af det samlede hændelsesforløb, herunder kendskab til, hvilke oplysninger den enkelte løftemodtager måtte have været i besiddelse af om forholdet mellem certifikatindehaveren og den, der (uberettiget) har afgivet løftet ved brug af den digitale signatur.
>
> Hvis den private nøgle er kompromitteret som følge af certifikatindehaverens egen uagtsomhed, og certifikatindehaveren ikke efterfølgende sørger for at få spærret sin signatur, vil dette efter omstændighederne kunne indgå i den samlede vurdering af, om certifikatindehaveren bliver aftaleretligt forpligtet. Manglende spærring vil således efter omstændighederne kunne medføre, at certifikatindehaveren anses for at have givet besidderen af den private nøgle, der uhindret får mulighed for fortsat at anvende denne, fuldmagt hertil. Der skal dog formentlig temmelig meget til, og navnlig må det formentlig kræves, at certifikatindehaveren har viden om, at den private nøgle er kompromitteret».[69]

Det legges altså opp til en konkret vurdering, der også uaktsomhet kan danne grunnlag for en fullmakt som innebærer at pseudounderskriveren blir bundet. Det skal likevel mye til før fullmakt kan konstateres på et slikt grunnlag. Antakelig må det kreves en kvalifisert form for uaktsomhet.[70] Et minstekrav synes å være at pseudounderskriver kjenner til at NemID er havnet på andres hender, og at pseudounderskriver har unnlatt å foreta nødvendige eller anbefalte skritt for å unngå videre tap, slik som å sperre brikken.

Utvalget fant ikke grunn til å foreslå særskilte regler om rettsvirkningene av elektroniske signaturer. Etter utvalgets oppfatning er det mest hensiktsmessig om spørsmål om avtalebinding blir avgjort av domstolene basert på en konkret vurdering av omstendighetene i den enkelte sak.[71]

I de siste tre årene har dansk Højesteret i fem saker tatt stilling til hvordan denne konkrete vurderingen skal foretas i praksis.

Den første saken gjaldt en ung mann med rusproblemer som angivelig ble presset til å gi fra seg kopi av pass, kredittkort med kode samt kodekort og personlig passord til NemID som nedbetaling av en narkotikagjeld på 15 000 danske kroner.[72] Gjennom misbruk av kredittkort og NemID ble mannen pådratt ca. 400 000 danske kroner i gjeld. Den konkrete saken som ble prøvd for domstolen, gjaldt tvangsfullbyrdelse av et gjeldsbrev på grunnlag av et forbrukslån på 50 000 danske kroner.

Højesteret kom til at låneavtalen og tilhørende gjeldsbrev var gyldig og bindende. Under henvisning til uttalelsene i betenkningen om e-signaturer vises det til at det må gjøres en konkret vurdering, der sentrale momenter er

> «under hvilke omstændigheder tredjemand er kommet i besiddelse af indehaverens nøgle (brugernavn, adgangskode og nøglekort til NemID), om indehaveren har haft kendskab til, at tredjemand er kommet i besiddelse af de pågældende oplysninger, og om indehaveren har gjort, hvad der var muligt for at forhindre misbrug, f.eks. ved at spærre sit NemID så hurtigt som mulig».[73]

Subsumsjonen er svært kort; det vises kun til at

> «af de grunde, der er anført af landsretten, [har] A udvist en sådan grad af uaktsomhed, at han i forhold til Basisbank hæfter for låneoptagelsen på aftaleretligt grundlag, selv om underskriften ikke er tilføjet digitalt af ham selv».[74]

Heller ikke landsretten gir imidlertid en begrunnelse for avtalebinding ut over å vise til at A har utlevert personlig sikkerhetsinformasjon, og at «en samlet vurdering af hændelsesforløbet» innebærer at A har utvist en slik grad av uaktsomhet at han blir bundet av avtalen.

Mannen som ble utsatt for svindelen, hadde blant annet anført at sikkerhetsopplysningene ble utlevert under trussel om vold, og at avtalen derfor var ugyldig etter avtaleloven § 28. Han hadde videre anført at han som følge av psykiske diagnoser ikke forstod at opplysningene kunne misbrukes til å ta opp lån. Han anførte også at han ikke burde fått lån, og at banken i alle tilfeller kunne oppdaget svindelen dersom de hadde hatt bedre sikkerhetsrutiner. Mannen bodde hjemme hos moren sin og levde av sosiale stønader. Ingen av disse anførslene kommenteres av Højesteret.

Den andre saken gjaldt en mann som ble kontaktet av to venner på Facebook.[75] De bad om hans hjelp til å skaffe 40 000 danske kroner for å bistå en annen felles venn som hadde behov for penger. Pseudounderskriver ble bedt om å overlevere NemID og passord. Han fikk forklart at disse opplysningene skulle brukes til å få penger ut fra en konto. Det ble søkt om og innvilget et lån på 43 000 danske kroner, som ble satt inn på mannens konto. Han tok deretter ut 40 000 danske kroner i kontanter, som han leverte til vennen. De resterende 3000 danske kronene var vederlag for at han bistod med å hjelpe vennene. Samme kveld ble han mistenksom og lurte på hvor pengene hadde kommet fra. Han anmeldte forholdet til politiet neste dag.

Højesteret gjentok her begrunnelsen fra den første dommen og viste til at mannen etter en konkret helhetsvurdering hadde opptrådt så uaktsomt at han ble avtalerettslig bundet.

Den tredje saken gjaldt et tilfelle av svindel mellom nærstående: En mann brukte samboerens NemID til å ta opp tre lån på til sammen 44 000 danske kroner.[76] Mannen hadde fått tilgang til samboerens NemID ved å fotografere kodekortet hun hadde liggende i lommeboka. Brukernavn og passord var lagret på parets felles nettbrett. Kvinnen visste ikke om låneopptakene. Højesteret konkluderte med at kvinnen ikke hadde utvist en grad av uaktsomhet som kunne tilsi verken avtalebinding eller erstatningsansvar overfor kreditorene.

I den fjerde saken hadde en psykisk utviklingshemmet mann overgitt NemID-opplysninger til en ukjent mann han hadde skrevet meldinger med på Facebook Messenger.[77] Svindleren hadde utgitt seg for å være en jente og hadde bedt om mannens NemID-opplysninger for å kunne betale en regning. Mannens motivasjon for å gi fra seg NemID-opplysningene var et ønske om å innlede et kjæresteforhold med «jenta». Mannen hadde ikke økonomisk vergemål, men ble bistått av en kommunal hjemmeveileder i økonomiske spørsmål. Svindleren tok opp et lån på 13 400 danske kroner i mannens navn.

Højesteret konkluderte med at mannen i utgangspunktet hadde opptrådt på en slik måte at han ble bundet av låneavtalen og gjeldsbrevet. Avtalen ble likevel ikke funnet bindende, idet den ble rammet av ugyldighet etter værgemålsloven § 46 om avtaler som er «indgået af en person, der på grund af sindssygdom, herunder svær demens, hæmmet psykisk udvikling, forbigående sindsforvirring eller en lignende tilstand manglede evnen til at handle fornuftmæssigt».

Den siste saken gjaldt et par, A og B, som ble lurt til å gi fra seg NemID-opplysninger. Svindleren hadde ringt både A og B og utgitt seg å være fra politiet. Han ba om å få NemID-opplysninger under dekke av å skulle etterforske et hackerangrep på Bs Instagram-konto.[78] A og B sendte sine NemID-opplysninger på sms slik de ble bedt om, og det ble tatt opp en rekke lån. I tillegg ble kontoen tappet for penger. «Politimannen» hadde opplyst at etterforskningen var taushetsbelagt i seks dager. Da A fortalte om hendelsen til en venn etter seks dager, ble han gjort oppmerksom på at han kunne ha blitt utsatt for svindel, og forholdet ble politianmeldt. Den konkrete saken gjaldt et lån på 62 000 danske kroner.

Højesteret gjentok først standardformuleringen som er brukt i de fire første sakene, om at spørsmålet om avtalebinding må avgjøres ut fra en konkret helhetsvurdering. Deretter presiseres det imidlertid at *hovedregelen* er at man ikke blir bundet i tilfeller av falsk, og at overlevering av NemID-opplysninger i seg selv ikke er tilstrekkelig til å konstatere avtalebinding. Denne hovedregelen er ikke fremhevet i tidligere avgjørelser. Højesteret konkluderte med at A og B ikke er avtalerettslig bundet av låneavtalen. Banken hadde i tillegg anført at A og B var ansvarlig for bankens tap på grunnlag av erstatningsrettslige regler. Denne anførselen kommenterer ikke Højesteret.

Selv om dansk rett bygger på at spørsmålet om binding må bero på en konkret vurdering av hvorvidt NemID-innehaveren har opptrådt uaktsomt, gir de fem dommene et samlet bilde som ikke er så ulikt det svensk HD har trukket opp i dommen beskrevet ovenfor. Også i dansk rett synes man å bygge på en grensedragning mellom tilfeller der tredjeperson utleder en rett fra innehaveren av NemID til å legitimere seg som denne, og tilfeller der en slik rett ikke kan utledes fra innehaveren. Dette er særlig tydelig i den siste dommen. «Politimannen» legitimerte seg ikke, og A og B var klar over at man ikke bruker NemID for å autentisere seg på Instagram. Dekkhistorien som ble gitt, var derfor ikke særlig troverdig. En alminnelig uaktsomhetsvurdering kunne lett lede til konklusjonen om at A og B hadde opptrådt uaktsomt. Likevel synes særlig den første dommen å være streng sett fra NemID-innehaverens side. En konkret og skjønnsmessig vurdering av den enkelte sak, med tilhørende svært knappe begrunnelser fra Højesteret, skaper dessuten lav forutsigbarhet.

3.3.4 Forholdet til norsk rett

Oppsummert synes rettstilstanden i Sverige, etter dommen fra Högsta domstolen, å være at frivillig overlevering av BankID til en tredjeperson i den hensikt at tredjepersonen skal foreta rettslige disposisjoner på pseudounderskriverens vegne, kan medføre en fullmakt som fører til binding for pseudounderskriveren. Forutsetningen er at tredjepersonen utleder en rett fra pseudounderskriveren til å anvende dennes eID til en eller annen disposisjon. Rent uaktsomme forhold kan derimot ikke lede til binding. I dansk rett kan avtalebinding konstateres på grunnlag av uaktsomhet, men det kreves en kvalifisert uaktsomhet, og Højesteret har understreket at hovedregelen er at avtalen ikke binder når den er basert på digitalt id-tyveri.

For norsk retts vedkommende har spørsmålet ikke blitt prøvet av Høyesterett. I teorien har det som nevnt vært enighet om at medkontrahenten er henvist til å kreve erstatning fra pseudounderskriveren, og at avtalen ikke blir bindende. Spørsmålet er om rettsutviklingen i Danmark og Sverige påvirker norsk rett, slik at det også her er en utvidet adgang til å bygge på ulovfestet representasjon. Dette er et uavklart spørsmål, men etter vårt syn bør man for norsk retts vedkommende holde fast ved at avtalen rammes av falsk når den er signert av en tredjeperson uten pseudounderskriverens samtykke.

For svensk retts vedkommende må Högsta domstolens konklusjon forstås i lys av at adgangen etter svensk rett til å kreve erstatning for rene formuestap («ren förmögenhetsskada») etter skadesståndslagen er svært begrenset.[79] Medkontrahenten kan derfor, i motsetning til etter norsk rett, ikke kreve erstatning for formuestap som oppstår på grunn av uaktsom håndtering av en eID. Dermed oppstår det et behov for å legge fullmaktsinstituttet på strekk for å kunne etablere rettslig grunnlag for økonomisk ansvar for BankID-innehaveren i enkelte situasjoner der dette virker rimelig.

I norsk rett er dette behovet for å legge avtaleretten på strekk ikke til stede, da det er mulig for medkontrahenten å påberope seg alminnelige erstatningsrettslige regler der BankID-innehaveren har utvist skyld. Generelt synes

erstatningsretten å være bedre egnet til å håndtere den interesseavveiningen som må foretas i situasjoner av misbruk av BankID.

Misbruk av en annens BankID for egen økonomisk vinning innebærer en straffbar identitetskrenkelse etter straffeloven § 202. I saker der spørsmål om tillitsfullmakt har blitt behandlet i norsk Høyesterett, har ikke fullmektigen foretatt disposisjoner i egen vinnings hensikt. I Rt-2011-410 (Optimogården), for eksempel, inngikk ikke daglig leder leieavtalen med siktemål å utnytte eiendommen privat eller på annen måte skaffe seg egen vinning. Daglig leder inngikk avtalen i selskapets, ikke egen, interesse.

Et tilfelle der en person misbruker en annens BankID til å inngå for eksempel en låneavtale, hvor formålet er at pengene skal tilflyte vedkommende selv, har lite til felles med klassiske fullmaktssituasjoner. Derimot kan det være mer nærliggende å bygge på fullmaktssynspunkter der disposisjonen reelt sett er foretatt i BankID-innehaverens interesse. En ektefelle bruker for eksempel den andre ektefellens BankID til å binde renten på ektefellens studielån eller for å inngå en mobilabonnementsavtale som er tiltenkt ektefellen – selv om samtykke ikke er innhentet på forhånd. Disse situasjonene vil heller ikke rammes av straffelovens forbud mot identitetskrenkelse, idet de ikke er foretatt med forsett om å oppnå «uberettiget vinning» eller «påføre en annen tap eller ulempe».

Etter vårt syn bør man som et minimum ikke kunne etablere en fullmakt i tilfeller der disposisjonen rammes av straffelovens forbud mot identitetskrenkelse. Det finnes imidlertid noen eksempler på underrettspraksis som bygger på at overlevering av BankID til en tredjeperson, som deretter misbruker denne i egen vinnings hensikt, etablerer en fullmakt, slik at tredjepersonens disposisjoner blir bindende for pseudoinnehaveren.[80] Disse dommene har naturligvis begrenset rettskildemessig verdi, og i fravær av andre autoritative kilder hva gjelder norsk rett, bør de heller ikke tas til inntekt for at frivillig overlevering av signaturfremstillingsdata skal anses som et fullmaktsforhold.[81]

Etter vårt syn taler de beste grunner etter dette for å legge til grunn en forståelse av de ulovfestede fullmaktsreglene som utelukker tillitsfullmakt, i tilfeller der «representasjonen» er usynlig for medkontrahenten. Som et minimum bør fullmakt være utelukket dersom «fullmektigens» handlinger rammes av straffelovens forbud mot identitetskrenkelse. Konklusjonen må imidlertid anses usikker.

For det tilfellet at norsk rett skulle åpne for en forståelse av de ulovfestede fullmaktsreglene som innebærer at pseudounderskriver kan bli avtalerettslig bundet av en elektronisk signatur som er påført av tredjeperson, er det grunn til å understreke at man må ha ugyldighetsreglene for fullmakter i mente. Det er for eksempel ikke upraktisk at BankID-opplysninger blir fratvunget eller fralurt pseudounderskriver under omstendigheter som ellers vil føre til at viljeserklæringen blir ugyldig, jf. punkt 3.2.

Det alminnelige avtalerettslige utgangspunktet er at en fullmakts gyldighet må avgjøres i to ledd: (1) overfor fullmektig og (2) overfor medkontrahent.[82] I utgangspunktet må disposisjonene i begge ledd være gyldige for at gyldig bindende avtale skal oppstå. Dersom noen blir frarøvet personopplysninger og sikkerhetsinformasjon under omstendigheter som ellers vil rammes av en sterk ugyldighetsgrunn, kan det i alle tilfelle ikke bli tale om en fullmakt som leder til binding. Lassen fremholder at det må gjelde som alminnelig regel at

> «hvis fullmaktsgivelsen rammes av en *sterk ugyldighetsgrunn* ... så blir det ingen fullmakt av [sic]; alle fullmektigens disposisjoner blir følgelig uforpliktende for fullmaktsgiveren. Er for eksempel fullmaktsgivelsen sinnssykt motivert – influert av fullmaktsgiverens sinnssykdom – så er den alltid ugyldig. De disposisjoner fullmektigen foretar i henhold til en slik fullmakt faller sammen, uansett hvor fornuftige de måtte være».[83]

Dette må gjelde også her: Tilegnelse av en annens BankID ved grov tvang, ved å utnytte personens sinnslidelse etc. kan under ingen omstendigheter lede til en rettslig legitimasjon som kan føre til binding for BankID-innehaveren. Noe mer tvilsomt kan spørsmålet være der noen har tilegnet seg en annens BankID ved omstendigheter som ellers faller inn under en svak ugyldighetsgrunn, for eksempel «ordinær» tvang etter avtaleloven § 29.

Problemet er at det i realiteten ikke foreligger en fullmaktserklæring som reglene om ugyldighet kan anvendes på. Her bør man trolig legge seg på den linje Högsta domstolen tilsynelatende har lagt seg på, og oppstille det som et grunnvilkår for en eventuell tillitsfullmakt at det foreligger et gyldig samtykke til bruk av eID-en til én eller flere bestemte disposisjoner. Følgelig vil fullmakt være utelukket der samtykket er rammet av en eller annen ugyldighetsgrunn – uavhengig av om denne er sterk eller svak.

3.4 Avtalebinding på grunnlag av etterfølgende passivitet fra pseudoavgiver

I litteraturen er det diskutert hvorvidt pseudounderskriver har plikt til å varsle godtroende medkontrahent når avtalen er inngått ved falsk.[84] I forlengelsen av dette er det også et spørsmål hva som er virkningen av utelatt varsling for pseudounderskriver, dersom pseudounderskriver har slik plikt: Blir pseudounderskriver avtalerettslig bundet eller kun erstatningsansvarlig?[85] Dette er spørsmålene som skal drøftes i det videre.

Hauge problematiserer hva som er grunnlaget for varslingsplikten. Som hun påpeker, vil plikten i noen tilfeller være kontraktsfestet.[86] Dette gjelder for avtaler inngått ved bruk av BankID, hvor avtalens punkt 4.2 gir kunden en plikt til å underrette utsteder «snarest mulig» etter at hun får mistanke om eller blir kjent med «at BankID og/eller tilhørende passord og personlig kode er kommet bort eller at uvedkommende har fått kjennskap til passord/personlig kode».[87] Etter avtalen har pseudounderskriver altså plikt til å melde fra til utstederen av BankID dersom hun blir kjent med eller mistenker at noen har signert med hennes elektroniske signatur.

Et spørsmål som oppstår, er om pseudounderskriver også har plikt til å melde fra til *medkontrahenten* (som typisk er en annen enn den som har utstedt BankID). Hov tar til orde for at det må finnes en slik plikt.[88] Begrunnelsen for dette er at hensynet til pseudounderskrivers eventuelle motvilje mot å angi en falskner, når dette for eksempel er et familiemedlem, ikke kan få så stor vekt at det går utover godtroende tredjepersons berettigede forventninger.[89] Her ser man at hensynet til omsetningslivet og det å kunne stole på ektheten av en avtale blir vektlagt. Dette må også være et sterkt argument når det gjelder elektronisk signatur, som i enda større grad enn en fysisk signatur kan brukes til å validere en persons identitet. Også Woxholth synes å legge til grunn at man har en plikt til å varsle medkontrahenten.[90]

Både Hov og Woxholth viser til avgjørelsen i Rt-1918-689. Saken gjaldt en forretningsmann som i over to år forholdt seg passiv, selv om han mottok varsler fra banken som viste at det var utstedt en rekke veksler i hans navn. Førstvoterende bemerker at pseudounderskriver ikke varsler banken, men «fortsætter forholdet, som om alt var i orden».[91] Det legges vekt på at pseudounderskriver var en forretningsmann, og at falskneriet hadde pågått over lengre tid. Dette kan tilsi at varslingsplikten ikke vil inntre i tilfeller der det kun er inngått én avtale, og at det har betydning om falskneriet skjer i pseudounderskrivers private eller profesjonelle sfære.

Det synes altså som om rettstilstanden i Norge er slik at pseudounderskriver har en plikt til å varsle medkontrahent. Det kan likevel hende at plikten først blir aktuell dersom det er falskneri som foregår over noe lengre tid, eller der pseudounderskrivers forhold tilsier at han eller hun har en særlig oppfordring til å være oppmerksom på at slikt kan skje. På den annen side er dette standpunktet hentet fra en svært gammel avgjørelse. Det kan hevdes at samfunnet og retten har endret seg i såpass stor grad at synspunktet ikke lenger kan legges til grunn. Som Hauge påpeker, kan det til og med i noen tilfeller inntre en varslingsplikt overfor potensielle medkontrahenter hvis pseudounderskriver er kjent med at det er sannsynlighet for at misbruk kan ha skjedd – typisk ved tap av kort og kode.[92] Dette må være et uttrykk for at varslingsplikten lettere vil inntre på områder hvor man er kjent med at falskneri kan skje.

Det vil imidlertid i mange tilfeller være problematisk å vite hvem man eventuelt skal varsle. BankID kan benyttes som både elektronisk signatur og autentisering på svært mange forskjellige tjenester og måter, og det kan neppe forventes at en pseudounderskriver skal helgardere seg og kontakte alle potensielle medkontrahenter. Det bør nok legges til grunn at pseudounderskrivers varslingsplikt først inntrer når han har en konkret mistanke, eventuelt når han har faktisk kunnskap om forholdet.

Både Woxholth og Hov mener at manglende varsling kun kan medføre et erstatningsansvar, og at det ikke vil føre til at pseudounderskriver blir bundet av avtalen.[93] Også Giertsen og Hauge mener at erstatning er utgangspunktet.[94] Hauge setter imidlertid spørsmålstegn ved riktigheten av at falsk behandles annerledes enn ugyldighetsgrunnene *grov tvang* og *mekanisktvang*, hvor manglende varsling fører til at pseudounderskriver blir bundet av avtalen.[95] Selv om dette synspunktet nok kunne diskuteres videre, må dagens rettstilstand anses fastslått, fordi løsningen for grov og mekanisk tvang er hjemlet i lov og forarbeider, hvilket ikke er tilfellet for falsk.[96]

I de tilfeller hvor pseudounderskriver har en plikt til å varsle, vil manglende varsling kun føre til erstatningsansvar der det foreligger årsakssammenheng mellom den manglende varslingen og medkontrahentens økonomiske tap.[97] Det vil si at dersom en falsk elektronisk signatur brukes til å inngå én

avtale, og pseudounderskriver ikke oppdager dette før etter at medkontrahenten har ytt sin del og dermed fått sitt økonomiske tap, vil varslingsplikten være uten reell betydning.

Oppsummert synes det altså å kunne oppstilles en plikt for pseudounderskriver til å varsle medkontrahenten når pseudounderskriver blir klar over eller får en mistanke om misbruket. Manglende reklamasjon kan likevel ikke føre til at pseudounderskriver blir bundet til avtalen. Pseudounderskriver blir kun erstatningsansvarlig, og kun dersom det er adekvat årsakssammenheng mellom den manglende varslingen og det økonomiske tapet.

En annen sak er at pseudounderskriveren har anledning til å godkjenne disposisjonen i ettertid, slik at en avtale som i utgangspunktet ble rammet av falsk, likevel blir bindende.[98]

4 Om forholdet mellom avtalebinding og nye regler om ansvarsbegrensning ved misbruk av elektroniske signaturfremstillingsdata i finansavtaleloven

4.1 Overordnet om forholdet mellom avtalebinding og nye regler i finansavtaleloven om ansvarsbegrensning ved misbruk

Problemet med digitalt ID-tyveri og falske digitale signaturer kan tenkes å oppstå i alle typer avtaler som kan inngås elektronisk. I praksis ser vi imidlertid at problemet er særlig utbredt for låneavtaler. Årsaken er opplagt: Ved å utgi seg for å være en annen kan en svindler få utbetalt store lånebeløp og oppnå økonomisk vinning.

Gjeldende finansavtalelov (heretter «finansavtaleloven 1999»)[99] regulerer kun ansvar etter uautoriserte betalingstransaksjoner, slik som kortbelastninger og kontooverføringer.[100] *Inngåelse av* avtaler om finansielle tjenester, for eksempel avtaler om betalingstjenester eller kreditt, utgjør ikke «uautoriserte betalingstransaksjoner» og faller derfor utenfor gjeldende regulering om dette i finansavtaleloven. Pseudounderskrivers ansvar for avtaler som er signert digitalt av en tredjeperson, avgjøres etter alminnelige kontrakts- og erstatningsrettslige regler.[101] Det betyr at rettighetshaver blir bundet til kontrakten så langt dette følger av alminnelige regler om avtalebinding, som vi har gjort rede for i foregående punkter. I tillegg gjelder den alminnelige culpanormen, slik at pseudounderskriver blir ansvarlig for hele det økonomiske tapet dersom han eller hun har opptrådt uaktsomt.[102]

I 2020 ble det vedtatt en ny finansavtalelov (heretter «finansavtaleloven 2020»). Det er ventet at loven vil tre i kraft i januar 2023. Med den nye loven innføres en spesialregulering av ansvarsspørsmålet for misbruk av elektronisk signatur til inngåelse av avtaler om finansielle tjenester, se §§ 3-16 til 3-21. Det følger av § 3-20 første ledd at

> «[e]rstatningsansvar som tjenesteyteren kan gjøre gjeldende mot rettighetshaveren i samsvar med ellers gjeldende rettsregler for misbruk av elektroniske signaturfremstillingsdata, kan ikke overstige de egenandeler som følger av annet til femte ledd».

Pseudounderskriver svarer som hovedregel med en egenandel på inntil 450 kroner.[103] Har pseudounderskriver handlet grovt uaktsomt, svarer han eller hun med inntil 12 000 kroner.[104] Dersom pseudounderskriver forsettlig har misligholdt sine plikter etter finansavtaleloven § 3-19, kan vedkommende holdes ansvarlig for det fulle beløpet han eller hun er ansvarlig for etter «ellers gjeldende rettsregler».[105] Pliktene innebærer å bruke signaturfremstillingsdataene i samsvar med vilkårene for utstedelse og bruk og å ta alle rimelige forholdsregler for å beskytte signaturfremstillingsdataene. De nye reglene er utformet etter modell av reglene som gjelder for uautoriserte betalingstransaksjoner.

Etter ordlyden er det klart at de nye reglene begrenser pseudounderskrivers *erstatningsansvar* etter den alminnelige culparegelen. Spørsmålet er imidlertid om reglene også får betydning for hvorvidt en avtale om finansielle tjenester er bindende etter alminnelige avtalerettslige regler.

I punkt 3 har vi vurdert tre mulige grunnlag for avtalebinding når signaturen er påført av en annen. Som det fremgår der, kan pseudounderskriver bli bundet dersom han eller hun har (gyldig) samtykket til signeringen. Det må gjelde også etter ikrafttredelsen av finansavtaleloven 2020. I en slik situasjon foreligger det ikke «misbruk» av elektroniske signaturfremstillingsdata, jf. § 3-16 første ledd bokstav d.

Som vi har vist, er det stor grad av usikkerhet knyttet til om avtalebinding kan skje på grunnlag av ulovfestet representasjon (fullmakt) eller etterfølgende passivitet. Det gjør at det er aktuelt å vurdere forholdet mellom

alminnelig avtalerett og finansavtalelovens regler for disse tilfellene. Spørsmålet er om finansavtalelovens regulering av *erstatningsansvar* påvirker vurderingen av *avtalerettslig binding*.

4.2 Ansvar ved frivillig eller uaktsom overgivelse av BankID-opplysninger

Ovenfor, i punkt 3.3, har vi konkludert med at de beste grunner taler for at frivillig overlevering av BankID til en tredjeperson ikke bør føre til avtalebinding for BankID-innehaveren, men at konklusjonen er usikker. Etter vårt syn må det imidlertid være klart at for *finansielle tjenester* vil særreguleringen i finansavtaleloven 2020 i alle tilfeller måtte bli avgjørende for omfanget av det økonomiske ansvaret for BankID-innehaveren.

Reglene om ansvarsbegrensning for BankID-innehaveren skal etter finansavtaleloven 2020 § 3-16 få anvendelse når det foreligger «misbruk av elektroniske signaturfremstillingsdata», jf.finansavtaleloven 2020 § 3-20 første ledd. «Misbruk» er definert som «tap, tyveri eller uberettiget tilegnelse av elektroniske signaturfremstillingsdata», se finansavtaleloven 2020 § 3-16 første ledd bokstav d. En situasjon der en tredjeperson bruker en annens BankID (uten dennes samtykke) for å berike seg selv, utgjør etter en naturlig språklig forståelse «misbruk» av elektroniske signaturfremstillingsdata.

Det må være på det rene at simpel uaktsomhet ikke kan føre til avtalebinding for avtaler om finansielle tjenester, med det resultat at pseudounderskriveren blir ansvarlig i henhold til avtalen. Det er klart forutsatt i forarbeidene at en elektronisk signatur som er påført av en tredjeperson, innebærer falsk, og at avtalen ikke blir avtalerettslig bindende for pseudounderskriveren.[106] Reguleringen i finansavtaleloven 2020 bygger på en klar forutsetning om at en pseudounderskriver som har opptrådt simpelt uaktsomt, ikke skal være ansvarlig for mer enn en egenandel på 450 kroner. Ved grov uaktsomhet er egenandelen 12 000 kroner.[107] Denne klare lovgiverviljen kan ikke omgås ved å holde pseudounderskriver ansvarlig på et avtalerettslig grunnlag, fordi det i så fall ville medføre en uthuling av det forbrukervernet loven er ment å gi.[108]

Basert på de eksemplene som er omtalt i finansavtalelovens forarbeider, synes det også klart at tilfeller der noen frivillig har gitt fra seg BankID til en tredjeperson, også skal være omfattes av lovens ansvarsbegrensninger. Justiskomiteen peker på at

> «eldre personer og personer som ikke kan språket godt, og som har behov for hjelp av andre til å betale regninger, også [vil] være dekket av egenandelen på 12.000 kroner istedenfor å måtte være ansvarlig for hele tapet som en eventuell svindel forårsaker».[109]

Uttalelsen gjelder forståelsen av når det foreligger forsettlig pliktbrudd, hvor Stortinget gikk inn for en ordlyd som avvek fra den som var foreslått av Justis- og beredskapsdepartementet.[110] Den bygger imidlertid på en klar forutsetning om at situasjonen som sådan skal vurderes med utgangspunkt i grensen mellom grov uaktsomhet og forsett, og at kunden skal kunne påberope seg egenandelen på 12 000 kroner i en slik situasjon. Dermed vil det også her være en omgåelse av lovgiverviljen å bygge på fullmaktsbetraktninger, med det resultat at kunden blir bundet av avtalen og dermed ansvarlig for det fulle tapet (i tillegg til avtalte renter).

Vi kan også se hen til reglene om ikke-godkjente betalingstransaksjoner i finansavtaleloven 2020 § 4-30. I forarbeidene er det lagt til grunn at bestemmelsen i § 3-20 bygger på denne, slik at det er relevant å undersøke hva som gjelder her.[111] Begrepet «ikke-godkjent betalingstransaksjon» er definert i finansavtaleloven 2020 § 4-2 første ledd: «En betalingstransaksjon anses som godkjent bare dersom betaleren har gitt sitt samtykke til at betalingstransaksjonen gjennomføres».[112] Her gis det anvisning på at det kun er de transaksjonene rettighetshaver positivt har samtykket til, som anses som godkjente. Det tilsier at det samme bør gjelde for vurderingen av når en elektronisk signatur er misbrukt, slik at begrepet «misbruk» i § 3-16 omfatter alle tilfeller der pseudounderskriver ikke har påført signaturen selv eller samtykket til at noen andre påfører signaturen på hans vegne. I slike situasjoner har lovgiver forutsatt at ansvarsbegrensningene i § 3-20 skal få anvendelse, og at avtalen derfor ikke er bindende for pseudounderskriveren.

Dette stemmer også godt overens med konklusjonene under punkt 3, hvor vi har argumentert for at et samtykke til den konkrete disposisjonen medfører binding for pseudounderskriveren, men at øvrige forhold ikke vil lede til avtalebinding, kun eventuelt erstatningsansvar. En annen sak er at frivillig overlevering av BankID-opplysninger under visse omstendigheter kan utgjøre et forsettlig pliktbrudd etter § 3-20, slik at pseudoinnehaveren blir ansvarlig for hele tapet.

4.3 Ansvar på grunnlag av etterfølgende passivitet

Som nevnt i punkt 3 er det noe uenighet om hvorvidt manglende varsling etter falsk kan medføre avtalebinding, eller om pseudounderskriver kun blir erstatningsansvarlig. Det er også et spørsmål om det i det hele tatt kan oppstilles en plikt til å varsle, og i så fall overfor hvem en slik plikt gjelder. I finansavtaleloven 2020 § 3-19 er det gitt regler om pseudounderskrivers varslingsplikt. Bestemmelsen lyder:

> «Rettighetshaveren taper sin rett til ansvarsbegrensning etter § 3-20 dersom rettighetshaveren ikke varsler om misbruk av elektroniske signaturfremstillingsdata uten ugrunnet opphold etter å ha fått kjennskap til misbruket. Det samme gjelder dersom rettighetshaveren ikke har varslet om misbruk senest 13 måneder etter at rettighetshaveren måtte forstå at et misbruk har funnet sted. Retten til ansvarsbegrensning tapes likevel først 13 måneder etter at rettighetshaveren ble kjent med misbruket, 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.»[113]

En alminnelig språklig forståelse av bestemmelsen tilsier at pseudounderskriver har to varslingsfrister å forholde seg til: én relativ frist, «uten ugrunnet opphold» etter at pseudounderskriver har fått faktisk kunnskap om at signaturfremstillingsdataene er misbrukt, og én absolutt frist på 13 måneder etter at pseudounderskriver «måtte forstå» at det hadde skjedd misbruk. Den siste fristen kan gis et senere utgangspunkt, fra det tidspunktet pseudounderskriver får faktisk kunnskap om misbruket, dersom tjenesteyter har misligholdt sine opplysningsplikter etter loven.

Her er det altså innført en spesiell regulering av plikten, slik at det ikke er et tvilsomt spørsmål om pseudounderskriver har plikt til å varsle. Det er også innført en regulering av konsekvensen av unnlatt varsling. Etter lovens ordlyd blir ikke pseudounderskriver bundet til avtalen og taper ikke muligheten til å fremme innsigelser mot avtalen, men mister retten til ansvarsbegrensning. Det vil si at pseudounderskriver kan holdes erstatningsansvarlig ved unnlatt varsling. Til forskjell fra den alminnelige avtaleretten er det ikke et vilkår at det foreligger adekvat årsakssammenheng mellom finansinstitusjonens tap og den manglende varslingen. Det gjør at reguleringen – sett fra pseudounderskriverens side – kan sies å være strengere for avtaler om finansielle tjenester enn for andre typer avtaler.

5 Avsluttende bemerkninger

Formålet med denne artikkelen har vært å undersøke i hvilke tilfeller en innehaver av elektronisk signatur kan bli bundet til en avtale når signaturen er påført av en annen enn pseudounderskriver selv. Det var også et formål å undersøke hva som vil være forholdet mellom den alminnelige avtaleretten og avtaler som reguleres av finansavtaleloven 2020.

Vi har vist at spørsmålet om avtalebinding løses på samme måte uavhengig av om signaturen er fysisk eller elektronisk, og at digitalisering av avtaleinngåelser har ført til ny aktualitet for den tidligere lite brukte ugyldighetsgrunnen *falsk*. Den klare hovedregelen er fortsatt at en avtale ikke er bindende når signaturen er påført av en annen enn pseudounderskriver selv, men det kan tenkes unntak. Pseudounderskriveren blir bundet dersom han eller hun har gitt et gyldig samtykke til disposisjonen. Vi har argumentert for at frivillig eller uaktsom overgivelse av elektroniske signaturfremstillingsdata ikke fører til en ulovfestet representasjonsrett for den som har fått tilgang til disse dataene. Særlig i lys av rettsutviklingen i Sverige og Danmark er imidlertid dette en usikker konklusjon.

For avtaler om finansielle tjenester vil likevel særreguleringen i finansavtaleloven 2020 i alle tilfeller stenge for avtalebinding i andre situasjoner enn der pseudounderskriveren har samtykket til disposisjonen.

6 Litteraturliste

Andersen (2013) Andersen, Mads Bryde. *Grundlæggende aftaleret*. 4. utg., København: Gjellerup, 2013

Arnholm (1964) Arnholm, Carl Jacob. *Privatrett, II: Avtaler*. Oslo: Johan Grundt Tanum, 1964

Askeland (2019) Askeland, Bjarte. «Rettsoppfatninger som rettskilde», i Alf Petter Høgberg og Jørn Øyrehagen Sunde, red., *Juridisk metode og tenkemåte,* Oslo: Universitetsforlaget, 2019, s. 452-475.

Finans Norge (2013) Finans Norge. *Elektroniske kredittavtaler. De ulike stadier for en elektronisk kredittavtale og de juridiske problemstillinger som oppstår underveis.* Finans Norge, 2013. https://www.finansnorge.no/contentassets/0bcdecfea95948fab9525848189d1548/last-ned-rapporten/rapport-fra-arbeidsgruppe-om-juridiske-problemstillinger-ved-elektroniske-kredittavtaler.pdf [lest 08.11.21]

Giertsen (2021) Giertsen, Johan. *Avtaler*. 4. utg., Oslo: Universitetsforlaget, 2021

Hagstrøm (2011) Hagstrøm, Viggo. *Obligasjonsrett*. 2. utg., Oslo: Universitetsforlaget, 2011

Hauge (2009) Hauge, Hilde. *Ugyldighet ved formuerettslige disposisjoner.* Oslo: Universitetsforlaget, 2009

Hov (2007) Hov, Jo. *Avtaleslutning og ugyldighet. Kontraktsrett I.* 4. utg., Oslo: Papinian, 2007

Hultmark (1997) Hultmark, Christina. *Elektronisk handel och avtalsrätt.* Stockholm: Nordstedts Juridik, 1997

Karstoft (2019) Karstoft, Susanne. «Misbrug af NemID til optagelse af lån». *Ugeskrift for Retsvæsen*, U.2019B, s. 339-348

Kjørven (2020) Kjørven, Marte Eidsand. «Who pays when things go wrong? Online financial fraud and consumer protection in Europe and Scandinavia», *European Business Law Review,* 2020, *31*(1), s. 77-110.

Kjørven mfl. (2021) Kjørven, Marte Eidsand, Alf Petter Høgberg og Geir Woxholth. «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)». *Lov og Rett*, 2021, *60*(6), s. 335-366

Lassen (1992) Lassen, Birger Stuevold. *Kontraktsrettslig representasjon.* 2. utg., Oslo: Universitetsforlaget, 1992

Norland (2021) Norland, Line Utne. *Avtalebinding ved misbruk av elektroniske signaturer*. Masteroppgave, Universitetet i Oslo, 2021. Jussbuss stensilserie nr. 152. https://foreninger.uio.no/jussbuss/publikasjoner/masteroppgaver/avtalebinding-ved-misbruk-av-elektronisk-signatur.pdf

Udsen (2002) Udsen, Henrik. *Den digitale signatur – ansvarsspørgsmål.* København: Forlaget Thomson, 2002

Udsen (2006) Udsen, Henrik. «Uagtsomhed som aftalestiftende retsfaktum – et bidrag til den aftaleretlige forpligtelseslære». *Tidsskrift for Rettsvitenskap,* 2006, *119*(1), s. 104-152

Werenskjold (2020) Werenskjold, Kari Kiperberg. *BankID-svindel i nære relasjonar. Spørsmålet om avtalebinding i lys av det menneskerettslege vernet mot økonomisk vald.* Masteroppgave, Universitetet i Oslo, 2020

Woxholth (2017) Woxholth, Geir. *Avtalerett*. 10. utg., Oslo: Gyldendal, 2017

Woxholth (2021) Woxholth, Geir. *Avtalerett*. 11. utg., Oslo: Gyldendal, 2021

Noter

1 Artikkelen bygger på Line Utne Norlands masteroppgave *Avtalebinding ved misbruk av elektroniske signaturer* (2021). Avhandlingen er publisert i Jussbuss' stensilserie nr. 152. Artikkelen inneholder en omskrevet og bearbeidet drøftelse av utvalgte problemstillinger fra avhandlingen. Blant annet er nyere praksis fra Högsta domstolen i Sverige og Højesteret i Danmark, som har kommet til etter at avhandlingen ble levert, inkludert. Andre problemstillinger fra avhandlingen er utelatt fra eller forkortet i artikkelen. Dette gjelder blant annet en analyse av juridisk teori for å undersøke spørsmålet om hvorvidt uaktsomhet kan føre til avtalerettslig binding, og spørsmålet om binding kan oppstå ved etterfølgende godkjennelse av en ugyldig disposisjon. For en drøftelse av disse vises det til avhandlingen.

2 Jf. Giertsen (2021) s. 207.

3 Jf. Norsk senter for informasjonssikring (2022), «Nye tall: 150 000 nordmenn har opplevd ID-tyveri de siste årene» [pressemelding] [lest 1. september 2022].

4 Jf. Hov (2007) s. 237.

5 Jf. Woxholth (2021) s. 309.

6 Jf. Hagstrøm (2011) s. 88, Giertsen (2021) s. 24.

7 Högsta domstolen, dom 9. desember 2021, mål nr. T 930-21.

8 *eID* er en forkortelse for «elektronisk identifikasjon» og brukes for identitetskontroll i elektroniske tjenester. En eID kan i tillegg inkludere en elektronisk signeringsløsning. I Norge er MinID og BankID eksempler på eID-løsninger som også støtter elektronisk

signering. I Sverige heter den mest brukte eID-løsningen også BankID, men det er ikke det samme systemet som i Norge. I Danmark har man brukt et system som heter NemID, som er i ferd med å erstattes av MitID.

9 U.2019.1192,U.2019.1197,U.2021.2320, U 2022.411 og U.2022.414. Sakene gjelder misbruk av NemID, som er den danske ekvivalenten til BankID. Det er en betalings- og identifiseringsløsning der brukeren må oppgi et personlig passord samt en kode fra et kodekort. På samme måte som BankID i Norge kan NemID brukes til å avgi en kvalifisert elektronisk signatur. NemID er i ferd med å bli erstattet av MitID. Se NemID, «Digital signatur» [lest 2.9.2022].

10 Jf. HR-2020-2021-A.

11 Se Kjørven (2020) med videre henvisninger.

12 Lov 18. desember 2020 nr. 146 om finansavtaler (finansavtaleloven 2020).

13 Lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester).

14 Jf. lov om elektroniske tillitstjenester § 1.

15 Jf. forordning (EU) nr. 910/2014 artikkel 1.

16 Jf. forordning (EU) nr. 910/2014 artikkel 3 nr. 11 og 12, jf. artikkel 26 og 28.

17 Se BankIDs nettside, https://www.bankid.no/privat/bruksomrader/ [lest 2.9.2022].

18 Jf. forordning (EU) nr. 910/2014 artikkel 25 nr. 2.

19 Lov 31. mai 1918 nr. 4 om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer.

20 Jf. Giertsen (2021) s. 14.

21 Jf. Woxholth (2021) s. 27.

22 Jf. Woxholth (2021) s. 31.

23 Jf. Giertsen (2021) s. 123

24 Jf. Woxholth (2017) s. 63.

25 Jf. Rt-2001-1288. Se også Woxholth (2021) s. 71.

26 Jf. Hultmark (1997) s. 23.

27 Jf. Udsen (2002) s. 16.

28 Jf. Udsen (2002) s. 17.

29 Jf. Udsen (2002) s. 18.

30 Jf. Udsen (2002) s. 18.

31 Jf. finansavtaleloven 2020 § 3-6.

32 Jf. Giertsen (2021) s. 223.

33 Jf. Woxholth (2017) s. 268.

34 Jf. Hov (2007) s. 237.

35 Jf. Woxholth (2017) s. 281.

36 Jf. Woxholth (2021) s. 309.

37 Jf. Högsta domstolens dom 9. desember 2021, mål nr. T 930-21 avsnitt 15.

38 Se «Avtalevilkår for PersonBankID og AnsattBankID – PDS» (punkt 4.1), tilgjengelig på https://www.bankid.no/globalassets/dokumenter/apne-sider/bankid/dnb_pds_personal-v1.1.pdf [lest 2.9.2021].

39 Sml. Rt-1936-459. Se også Eidsivating lagmannsretts dom 14. april 2021, LE-2020-150864 – LE-2020-150885.

40 Jf. HR-2017-971-Aavsnitt 36.

41 Lovavdelingens uttalelse 18. oktober 1995, JDLOV-1995-7090.

42 Illustrerende i så måte er Bankklagenemndas uttalelse i BKN-2001-18, hvor en mann (NN) hadde signert dels fysisk, dels elektronisk i forbindelse med flere uttak fra ektefellens konto da ektefellen var syk. Bankklagenemnda uttalte at signeringene «har karakter av å være foretatt 'med påholden penn', selv om signeringen ikke nødvendigvis skjedde på denne måten». Videre ble det uttalt at «uttakene har vært i samsvar med kontohavers vilje, slik at det må sies at NN fullt ut handlet på oppdrag fra kontohaver». Nemnda konkluderte med at «det foreligger et fullmaktsforhold i saken, og at NN derfor var berettiget til å foreta uttakene».

43 Det er ikke rom for en fullstendig redegjørelse for alle vilkår knyttet til de ulike ugyldighetsgrunnene her. Se Werenskjold (2020) for en nærmere analyse av ugyldighetsgrunner knyttet til misbruk av BankID i nære relasjoner.

44 Jf. Woxholth (2017) s. 268.

45 Jf. Woxholth (2017) s. 269.

46 Ingeborg Skov Høye, «BankID kan åpne for identitetstyveri, bedrageri og økonomisk vold» [debattinnlegg], *Aftenposten*, 16. september 2021. Se Werenskjold (2020) for en grundig fremstilling av økonomisk vold i relasjon til misbruk av BankID. Bufdir definerer økonomisk vold som tilfeller der «noen tar eller bruker en annen persons penger, eiendeler eller ressurser uten å ha rett eller lov til det», se Bufdir, *TryggEst – veileder TryggEst-kommuner*på bufdir.no.

47 Se avsnitt 104.

48 Se også Giertsen (2021) s. 223, som fremholder at medkontrahentens aktsomhetsplikt innebærer en plikt til å ha gode nok rutiner til

å fange opp misbruk av elektroniske signaturer.

49 Se Finans Norge (2013) s. 63.

50 Se eksempelvis Lassen (1992) for en fremstilling av reglene om dette.

51 Jf. Woxholth (2017) s. 220.

52 Jf. Woxholth (2021) s. 230.

53 Woxholth (2021) s. 309, Hauge (2009) s. 110, Giertsen (2021) s. 223 og Hov (2007) s. 238. Arnholm (1964) s. 275 åpner imidlertid for at en person som har håndtert et sjekkhefte uaktsomt, kan komme til å bli bundet som om sjekken var ekte. Se Norland (2021) s. 22-25 for en analyse av rettsoppfatningen i norsk juridisk teori.

54 Jf. Andersen (2013) s. 53.

55 Jf. Arnholm (1964) s. 2.

56 Jf. Woxholth (2017) s. 47. I HR-2020-2401-A (flypassasjerdommen) uttalte Høyesterett at «hensynet til nordisk rettsenhet kan ha en viss vekt», se avsnitt 61.

57 Högsta domstolen dom 9. desember 2021, mål nr. T 930-21.

58 Avsnitt 32.

59 Avsnitt 11.

60 Avsnitt 13.

61 Avsnitt 16.

62 Avsnitt 13.

63 Avsnitt 33.

64 Avsnitt 36.

65 Betænkning nr. 1456, *e-signaturs retsvirkninger* (2004).

66 Beretning nr. 1517, *Beretning om elektronisk aftaleindgåelse og handel* (2004).

67 Udsen (2002). Se også Udsen (2006).

68 Betænkning nr. 1456, *e-signaturs retsvirkninger* (2004) s. 106-107.

69 Betænkning nr. 1456, *e-signaturs retsvirkninger* (2004) s. 107.

70 Jf. Karstoft (2019) s. 340.

71 Betænkning nr. 1456, e-signaturs retsvirkninger (2004) s. 109-110.

72 U.2019.1192.

73 Jf. U.2019.1192 på s. 1197.

74 Jf. U.2019.1192 på s. 1197.

75 U.2019.1197.

76 U.2021.2320.

77 U.2022.411.

78 U.2022.414H.

79 Se skadeståndslag (1972:207) 2 kap. § 2 jf. 1 kap. § 2.

80 Se TGLOM-2020-36796 og TGJOV-2020-72142-2.

81 Jf. Askeland (2019) s. 462.

82 Jf. Hov (2007) s. 349, Lassen (1992) s. 62, Woxholth (2017) s. 235.

83 Lassen (1992) s. 63.

84 Jf. Hov (2007) s. 238.

85 Jf. Hov (2007) s. 238.

86 Jf. Hauge (2009) s. 303.

87 Se «Avtalevilkår for PersonBankID og AnsattBankID – PDS», tilgjengelig på https://www.bankid.no/globalassets/dokumenter/apne-sider/bankid/dnb_pds_personal-v1.1.pdf [lest 2. september 2022].

88 Jf. Hov (2007) s. 238.

89 Jf. Hov (2007) s. 238.

90 Jf. Woxholth (2021) s. 309.

91 Jf. Rt-1918-689s. 690.

92 Hauge (2009) s. 303.

93 Jf. Hov (2007) s. 238, Woxholth (2021) s. 309.

94 Jf. Giertsen (2021) s. 222, Hauge (2009) s. 303.

95 Jf. Hauge (2009) s. 303.

96 Jf. Hauge (2009) s. 303.

97 Jf. Woxholth (2021) s. 310.

98 Woxholth (2021) s. 309 og Hauge (2009) s. 323. Se Norland (2021) s. 30-31 for en fremstilling av dette.

99 Lov 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag (finansavtaleloven).

100 Jf. finansavtaleloven 1999 § 35. Se også HR-2020-2021-Aavsnitt 36, hvor det uttales at det ikke finnes lovregulering av spørsmålet. Spørsmålet om hvorvidt en betaling er «uautorisert» (eller «ikke godkjent», som er terminologien i finansavtaleloven 2020), må imidlertid også løses på grunnlag av alminnelige avtalerettslige regler om viljeserklæringer og representasjon. Se Kjørven mfl. (2021), som drøfter spørsmål om representasjon i relasjon til reglene om uautoriserte / ikke godkjente betalingstransaksjoner.

101 Jf. HR-2020-2021-Aavsnitt 36.

102 Jf. HR-2020-2021-Aavsnitt 51.

103 Jf. finansavtaleloven 2020 § 3-20 andre ledd.

104 Jf. finansavtaleloven 2020 § 3-20 tredje ledd.

105 Jf. finansavtaleloven 2020 § 3-20 fjerde ledd.

106 Jf. Prop.92 LS (2019–2020)s. 83.

107 Jf. finansavtaleloven 2020 § 3-20 andre og tredje ledd.

108 Jf. finansavtaleloven 2020 § 1-9.

109 Jf. Innst.104 L (2020–2021)s. 22.

110 Uttalelsen er gitt av justiskomiteens mindretall, som fikk flertall på Stortinget.

111 Jf. Prop.92 LS (2019–2020)s. 183.

112 Jf. finansavtaleloven 2020 § 4-30 første ledd jf. § 4-2 første ledd.

113 Jf. finansavtaleloven 2020 § 3-19 tredje ledd.

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

Ole Martin Juul Slyngstadli og Marte Eidsand Kjørven

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 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] Hverken 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 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 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 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]

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 sammenlignet 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 § 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 '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 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 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.

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.

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 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.

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, 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 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 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 lignende. 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.

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.

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 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».[60] 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».[61] 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')».[62] 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».[63] 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.[64]

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 at de elektroniske signaturfremstillingsdataene kunne bli misbrukt».[65] 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»[66], og justiskomiteen viste i innstillingen til at den reviderte ordlyden vil være i samsvar med «ellers gjeldende rettsregler».[67] 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.[68]

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.[69] 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 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».[70]

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 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».[71] 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.[72] 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.»[73]

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.

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».[74]

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».[75] 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».[76]

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».[77]

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 stod sterkt i strid med 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.[78]

Litteratur og juridisk teori

Brataas, Ellen Bennin, Mira Stokke og Amelia Ella Svensson. *Rapport om misbruk av eID. Empirisk studie av kjennetegn ved svindelsaker behandlet hos rettshjelpstiltakene Jussbuss, JURK og Gatejuristen, for å avdekke digitale sårbarheter ved bruk av eID.* SODI-rapport 1/2022. Universitetet i Oslo, 2022. https://www.jus.uio.no/ifp/forskning/prosjekter/sodi/publikasjoner/rapporter-mv/sodi-rapport-1-2022.pdf (hentet 31.03.2023).

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).

Giertsen, Johan. *Avtaler,* 3. utg. Universitetsforlaget, 2014.

Hagstrøm, Viggo. *Obligasjonsrett,* 2. utg. Universitetsforlaget, 2011.

Hagstrøm, Viggo mfl. *Obligasjonsrett*, 3. utg. Universitetsforlaget, 2021.

Hov, Jo. *Avtaleslutning og ugyldighet. Kontraktsrett I,* 3. utg. Papinian, 2002.

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

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

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

Kjørven, Marte Eidsand, 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.

Kjørven, Marte Eidsand 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.* Karnov, 2022.

Slyngstadli, Ole Martin Juul. «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.

Thon, Roar. «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)

Noter

1 Deler av artikkelen er basert på Slyngstadli (2021).

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

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

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, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om oppheving av direktiv 2007/64/EF.

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

7 Prop.92 LS (2019–2020) s. 173.

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.

9 Prop.92 LS (2019–2020) s. 184.

10 Finans Norge (2013). Denne artikkelen lå inntil starten av 2023 tilgjengelig på Finans Norges hjemmesider, men er nå tilsynelatende fjernet.

11 Finans Norge (2013) s. 8.

12 Finans Norge (2013) s. 8.

13 En empirisk undersøkelse av saker behandlet hos de gratis rettshjelpstiltakene 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 Brataas, Svensson og Mira Stokke (2022).

14 Prop.92 LS (2019–2020) s. 175.

15 Se Kjørven (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)*Lov om finansavtaler (finansavtaleloven) og samtykke til godkjennelse av EØS-komiteens beslutninger nr. 125/2019 og 130/2019 av 8. mai 2019 om innlemmelse i EØS-avtalen av direktiv 2014/17/EU om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål (boliglånsdirektivet) og delegert kommisjonsforordning (EU) nr. 1125/2014*.

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 (1998–1999) 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.

24 Jf. finansavtaleloven 1999 § 35 og direktiv 2007/64/EF artikkel 60 og 61.

25 Prop.92 LS (2019–2020) s. 182.

26 Se fotnote 8.

27 Prop.92 LS (2019–2020) s. 182.

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 Kjørven og Norland (2022).

31 Prop.92 LS (2019–2020) s. 358.

32 Dommens avsnitt 98 (kursivert i original). Se også Kjørven mfl. (2021) punkt 2 for en nærmere drøftelse av hva som ligger i kundens plikt til å beskytte personlig sikkerhetsinformasjon.

33 Hagstrøm mfl. (2021) s. 164-165.

34 Se punkt 4.1.

35 Se Kjørven og Norland (2022) 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.

37 Hov (2002) s. 237.

38 Giertsen (2014) s. 170.

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 Kjørven (2020).
45 HR-2020-2021-A avsnitt 104.
46 HR-2020-2021-A avsnitt 104.
47 HR-2020-2021-A avsnitt 107.
48 Hagstrøm (2011) s. 466.
49 TGJOV-2017-170313.
50 Prop.92 LS (2019–2020) s. 358.
51 Prop.92 LS (2019–2020) s. 358.
52 Thon (2020).
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.
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 Innst.104 L (2020–2021) s. 21.
61 Prop.92 LS (2019–2020) s. 186.
62 Prop.92 LS (2019–2020) s. 186.
63 Prop.92 LS (2019–2020) s. 186.
64 Ordlyden i den tilsvarende bestemmelsen om ansvar ved uautoriserte betalingstransaksjoner i § 4-30 fjerde ledd ble også endret.
65 Se Kjørven mfl. (2021) for en grundigere drøftelse av hva som ligger i finansavtalelovens forsettsbegrep.
66 Prop.92 LS (2019–2020) s. 186.
67 Innst.104 L (2020–2021) s. 22.
68 Se også Kjørven (2022) s. 21-24.
69 Kjørven mfl. (2021).
70 Prop.92 LS (2019–2020) s. 358.
71 Prop.92 LS (2019–2020) s. 413.
72 Se Rt-2004-165.
73 Innst.104 L (2020–2021) s. 23.
74 Ot.prp.nr.60 (1980–1981) s. 45.
75 HR-2020-2021-A avsnitt 67.
76 HR-2020-2021-A avsnitt 109.
77 HR-2020-2021-A avsnitt 104.
78 Kjørven (2021) s. 5-6.

Tapsfordeling mellom bank og kunde ved misbruk av elektroniske betalingsinstrumenter - når har kunden opptrådt grovt uaktsomt?

Admir Habibija

Fagfellevurdert artikkel

1 Innledning[1]

De siste tiårene har betalingssystemet i Norge blitt nærmest heldigitalisert. Betalingskort har erstattet kontanter, og digitaliseringen har bidratt til en gradvis utfasing av den fysiske banken. Overgangen til elektroniske betalingsløsninger innebærer store effektivitetsgevinster, men fører samtidig med seg økt risiko for svindel. I 2021 ble det i Norge rapportert om tap knyttet til misbruk av betalingskort tilsvarende 159,3 millioner kroner og tap knyttet til nettbanksvindel tilsvarende 346 millioner kroner.[2]

Tredjepersons misbruk av betalingsinstrument og tilhørende kode eller passord, og særlig såkalt *phishing*, er blant de vanligste tilfellene av misbruk av betalingsinstrumenter i Norge[3] og i Europa.[4] «Phishing» er en form for sosial manipulering, hvor svindleren spiller på fristelser, frykt, tillit og/eller en opplevelse av tidspress for å «fiske» etter informasjon om et betalingsinstrument og personlig sikkerhetsinformasjon. Vanligvis skjer dette gjennom en e-post eller tekstmelding som er lik eller identisk med en reell melding fra en institusjon man har tillit til, eksempelvis egen bank eller offentlige institusjoner.[5] E-posten eller sms-en inneholder en lenke til en falsk nettside som ser ut som eksempelvis innloggingssiden til svindelofferets nettbank eller Skatteetatens nettsider. Dersom offeret legger inn sikkerhetsinformasjon på nettsiden i et forsøk på å logge seg inn, vil svindleren kunne bruke denne informasjonen til å logge seg på den reelle nettbanken og tømme offerets konto.

En særlig form for phishing er «voice phishing» eller «vishing», hvor svindleren tar telefonisk kontakt med offeret. De mye omtalte «Olga-sakene», hvor eldre personer blir oppringt av svindlere og fralurt BankID-informasjon, er eksempler på «vishing».[6]

Det kan også utgjøre en risiko for svindel dersom kunden skriver ned passord og PIN-koder og oppbevarer disse lett tilgjengelig for nærstående eller andre tredjepersoner. Kunden kan også oppgi sikkerhetsinformasjon frivillig til tredjepersoner, for eksempel for å få hjelp til betale regninger.

Svindleren vil naturligvis alltid være økonomisk ansvarlig for tapet. Fordi det ofte er vanskelig å finne svindleren og holde ham eller henne ansvarlig, blir spørsmålet i praksis ofte om det er kunden (kontohaveren) eller betalingstjenesteyteren (banken) som skal bære tapet. Ansvarsfordelingen mellom bank og kunde ved ikke godkjente betalingstransaksjoner var i hovedsak ulovfestet frem til vedtakelsen av finansavtaleloven (1999).[7] Unntaket var kredittkort, som var regulert av kredittkjøpsloven av 1985.[8] Etter kredittkjøpsloven § 13 var kunden som hovedregel ansvarlig for hele tapet ved utvist ved forsett eller grov uaktsomhet og for en egenandel på 500 kroner ved uaktsomhet. Utenom disse tilfellene fulgte risikoplasseringen av finansinstitusjonenes standardkontrakter. Den manglende lovreguleringen innebar at tapet ble plassert hos kunden allerede ved simpel uaktsomhet.[9] Før kredittkjøpsloven var ansvarsfordelingen i sin helhet overlatt til kontraktsrettslig regulering. I forarbeidene til kredittkjøpsloven fremhever Kredittkjøpsutvalget at finansinstitusjonene, som den sterke avtalepart, i sine standardkontrakter i praksis la all risiko for misbruk av kredittkort og betalingskort over på kundene.[10]

I dag reguleres ansvarsfordelingen av finansavtaleloven (2020) § 4-30.[11] Bestemmelsen gjennomfører reglene i direktiv (EU) 2015/2366 (PSD 2) om tapsfordeling ved ikke godkjente betalingstransaksjoner.[12] Reglene er i hovedsak en videreføring av tilsvarende regler i finansavtaleloven (1999) § 35.

Hovedregelen etter finansavtaleloven (2020) § 4-30 er at betalingstjenesteyteren er ansvarlig for tap som skyldes en ikke godkjent betalingstransaksjon. Dette objektive ansvaret modereres i de påfølgende leddene. Etter annet ledd svarer kunden på visse vilkår for en egenandel på inntil 450 kroner. Ved misbruk av elektronisk betalingsinstrument svarer kunden for en egenandel på inntil 12 000 kroner dersom tapet skyldes at kunden har opptrådt grovt uaktsomt. Kunden svarer for hele tapet ved forsettlig pliktbrudd og ved grovt uaktsomt pliktbrudd i andre tilfeller enn ved misbruk av elektronisk betalingsinstrument. Grensen mellom de tre tersklene for egenandel har dermed avgjørende betydning for hvor stor del av tapet henholdsvis kunden og banken må bære. Spørsmålet som skal besvares i denne artikkelen, er når kunden har opptrådt «grovt uaktsomt» i finansavtalelovens forstand. Jeg skal i den sammenheng særlig undersøke i hvilken grad typiske forhold som fører til tap – å falle for *phishing*- og *vishing*-angrep samt skrive ned passord eller PIN-kode – innebærer at kunden har opptrådt grovt uaktsomt.[13] Praksis fra Finansklagenemnda viser at dette er typiske tilfeller hvor tvist om tapsfordelingen etter misbruk av elektroniske betalingsinstrumenter finner sted.

I det følgende vil jeg i punkt 2 først gi en oversikt over reguleringen av ikke godkjente betalingstransaksjoner, herunder når en transaksjon er «ikke godkjent». Kundens plikter med hensyn til håndtering av betalingsinstrumentet og kundens varslingsplikt gjennomgås i punkt 3. Deretter behandles det som er artikkelens hovedtema, grensen for grov uaktsomhet, i punktene 4 til 7. Jeg skal først redegjøre for hva som er

vurderingstemaet for grovt uaktsomme pliktbrudd i punkt 4. Deretter drøftes særskilt betydningen av kundens individuelle forhold i punkt 5 og betydningen av manglende sikkerhetsrutiner hos betalingstjenesteyteren i punkt 6. I punkt 7 vil jeg nærmere undersøke den nedre grensen for hva som utgjør grovt uaktsomme pliktbrudd på kundens hånd, i utvalgte typetilfeller.

Ved fastleggelse av reglene i finansavtaleloven vil de EØS-rettslige rammene som følger av PSD 2, danne et utgangspunkt. Som jeg skal komme tilbake til, åpner imidlertid PSD 2 eksplisitt for at graden av kundens uaktsomhet vurderes i tråd med nasjonal rett.

Høyesterett har i to nylige saker, HR-2020-2021-A og HR-2022-1752-A, behandlet spørsmålet om kundens ansvar for tap etter BankID-svindel. HR-2020-2021-A gjaldt misbruk av elektronisk signatur (BankID) til lånopptak og omhandlet følgelig ikke betalingstransaksjoner. HR-2022-1752-A gjaldt spørsmålet om hvorvidt kunden hadde handlet forsettlig etter finansavtaleloven (1999) § 35 tredje ledd. Ingen av dommene gjelder direkte de spørsmål som skal drøftes i denne artikkelen. De er likevel relevante i denne artikkelen, ettersom Høyesterett i begge sakene går inn på reglene om ikke godkjente betalingstransaksjoner og systemet for ansvarsfordelingen mellom kunde og finansinstitusjon etter finansavtaleloven (1999). I tillegg til disse avgjørelsene har Høyesterett kun ved ett tilfelle, i Rt-2004-499, behandlet spørsmålet om grov uaktsomhet ved ikke godkjente betalingstransaksjoner. Samtlige av disse dommene vil derfor være relevante å behandle nærmere i denne artikkelen.

Videre vil praksis fra Finansklagenemnda brukes til å eksemplifisere de aktuelle svindeltilfellene.[14] Svært få svindelsaker behandles i domstolene, og ofte begynner og slutter saken i Finansklagenemnda. Bakgrunnen for dette er at disse tilfellene i hovedsak har en begrenset tvistesum på opp til 12 000 kroner, og kostnadene ved å føre en sak for domstolene vil i de fleste tilfeller overgå tvistesummen. I praksis innebærer dette at Finansklagenemnda er organet som vil anvende regelverket overfor forbrukere i de aller fleste tilfellene. Gjennomgangen vil vise at den terskelen Finansklagenemnda har anvendt, neppe er i samsvar med gjeldende rett. Nyere praksis tyder imidlertid på at flertallet i nemnda er i ferd med å justere seg. Særlig interessant er en helt fersk avgjørelse fra mars 2023, FinKN-2023-188, som synes å innebære et taktskifte. Dette vil kommenteres nærmere under punkt 7.3. På grunn av tvistesummen i disse sakene vil spørsmålet neppe komme opp for domstolene. Noen rettspolitiske betraktninger rundt dette vil bli drøftet avslutningsvis i punkt 8.

2 Innledende om reguleringen av ikke godkjente betalingstransaksjoner

Helt siden vedtakelsen av finansavtaleloven (1999) har hovedregelen vært at betalingstjenestetilbydere må bære tapet etter ikke godkjente (tidligere kalt «uautoriserte») betalingstransaksjoner. Det er samfunnsøkonomiske hensyn som er den bærende begrunnelsen for en slik regel:[15] Det er gunstig for samfunnet å legge til rette for bruk av elektroniske betalingsinstrumenter uten at kundene må påta seg en betydelig økonomisk risiko. Betalingstjenestetilbyderne kan pulverisere tapet og oppfordres samtidig til å utvikle sikre betalingsløsninger. Prevensjonshensyn tilsier på den annen side at kunden bør ha et insentiv til å håndtere betalingsinstrumenter med tilhørende sikkerhetsinformasjon med forsiktighet.

Systemet med økende egenandeler for kunden basert på graden av klander skal balansere disse hensynene. I HR-2022-1752-A avsnitt 35 trekkes disse hensynene frem ved gjennomgangen av systemet i finansavtaleloven (1999) § 35, hvor det ved fravær av et forsettlig pliktbrudd blir understreket at «[g]runnen til at ansvaret for kunden ikkje er uavgrensa i slike høve, er at det er tenleg for bankane og samfunnet å leggje til rette for at kundane nyttar elektroniske betalingsinstrument». Høyesterett fremhever i denne sammenheng at finansinstitusjonene kan pulverisere tapet ved å spre kostnadene på kundemassen.

Det følger av § 4-30 første ledd at banken bare er ansvarlig for tap som skyldes en «ikke godkjent betalingstransaksjon, jf. § 4-2».[16] Det følger videre av § 4-2 første ledd at en betalingstransaksjon er godkjent «bare dersom betaleren har gitt sitt samtykke til at betalingstransaksjonen gjennomføres».[17] Motsetningsvis vil betalingstransaksjonen være «ikke godkjent» dersom betaleren *ikke* har gitt samtykke til den. Definisjonen stiller ingen nærmere krav til innholdet i samtykket, utover at samtykket «skal gis i den formen og på den måten som er avtalt mellom betaleren og betalingstjenesteyteren», jf. § 4-2 annet ledd. Betalingstjenesteyternes standardavtaler for bruk av betalingskort detaljregulerer ikke hvordan samtykke skal gis, men nøyer seg med å henvise til at en betalingstransaksjon er godkjent «bare dersom betaleren har gitt sitt samtykke til betalingstransaksjonen ...».[18] Avtaleverket for BankID henviser til reglene i finansavtaleloven.[19] Det følger

imidlertid av sammenhengen at samtykke forutsetter at det er *kunden* som må ha bekreftet betalingen med personlig kode eller annen personlig sikkerhetsanordning.[20]

Forarbeidene til finansavtaleloven (2020) slår fast at § 4-2 viderefører det som da var gjeldende rett, og viser til avtalerettslige utgangspunkter når det uttales at et «samtykke kan være generelt utformet og gjelde et bredt spekter av tjenester, eller det kan være mer avgrenset og konkretisert. Det er mot denne bakgrunnen regler om samtykkekrav i finansavtaleloven må forstås».[21] Hva som utgjør et rettslig bindende samtykke etter § 4-2, må forstås på bakgrunn av avtalerettslige regler om hva som utgjør en rettslig bindende disposisjon. Dersom kunden skulle bestride at et samtykke er gyldig, må spørsmålet løses etter bestemmelsene om ugyldige viljeserklæringer i avtaleloven,[22] supplert av ulovfestede ugyldighetsregler, inkludert falsk.[23]

Et særlig spørsmål oppstår i de tilfellene der kunden blir lurt til selv å gjennomføre betalingstransaksjonen, eksempelvis ved såkalt kjærlighetssvindel, hvor kunden overfører penger til en annen person i den tro at vedkommende har funnet kjærligheten. Et annet eksempel er fakturasvindel, hvor kunden gjennomfører en betaling basert på en forfalsket faktura.

Fellesnevneren for de ovennevnte tilfellene er at det er kunden selv som utsteder betalingsordren. Betalingstjenesteyteren er etter § 4-28 første ledd ansvarlig overfor betaleren for «korrekt gjennomføring» av en betalingstransaksjon som iverksettes av betaleren.[24] Betalingstransaksjonen er korrekt gjennomført når betalingsoppdraget gjelder en betalingsmottaker som det angitte kontonummeret eller annen entydig identifikasjon utpeker, jf. § 4-26 første ledd.[25] Betalingstjenesteyteren trenger følgelig kun å sørge for at det er samsvar mellom det angitte kontonummeret og den *faktiske* betalingsmottakeren.[26] Når kunden selv angir slik betalingsinformasjon, plikter betalingstjenesteyteren å gjennomføre betalingstransaksjonen i tråd med den oppgitte betalingsinformasjonen. Kunden har da selv godkjent betalingstransaksjonen, til tross for å ha blitt lurt av en tredjeperson.[27] Ansvarsbegrensningene i § 4-30 kommer da ikke anvendelse.[28] Hvorvidt det i et konkret tilfelle foreligger et slik samtykke, kan imidlertid være uklart, og det kan oppstå flere grensetilfeller. I lys av artikkelens tema behandles imidlertid ikke dette nærmere her.

Hovedregelen om bankens ansvar for tap som skyldes ikke godkjente betalingstransaksjoner, innebærer en gjennomføring av PSD 2 artikkel 73. Det følger videre av artikkel 74 nr. 1 at kunden på sin side skal bære tap som skyldes «manglende opfyldelse af en eller flere af de forpligtelser, der er fastsat i artikel 69, begået med forsæt eller ved grov forsømmelse». I fjerde avsnitt fremgår det imidlertid at medlemsstatene kan velge å begrense kundens ansvar dersom kunden ikke har opptrådt svikaktig eller begått et forsettlig pliktbrudd. Lovgiver har for norsk retts vedkommende valgt å benytte seg av denne muligheten, idet ansvaret ved grov uaktsomhet er begrenset til 12 000 kroner når tapet er skjedd ved bruk av et «elektronisk betalingsinstrument», jf. finansavtaleloven (2020) § 4-30 tredje ledd.

Bruk av «betalingsinstrument» har funnet sted når et «betalingsoppdrag» er iverksatt ved bruk av en «personlig innretning» eller «et sett av fremgangsmåter som er avtalt mellom kunden og betalingstjenesteyteren», jf. finansavtaleloven (2020) § 1-5 annet ledd.[29] Med «betalingsoppdrag» menes «en anmodning fra en betaler eller betalingsmottaker til en betalingstjenesteyter om å foreta en betalingstransaksjon», jf. § 1-5 femte ledd. At betalingsinstrumentet er «elektronisk», innebærer at det er brukt et betalingsinstrument for gjennomføring av et betalingsoppdrag hvor dataene innsamles elektronisk – uten manuell kontroll av betalingen.[30]

Både forarbeidene til finansavtaleloven (2020) og finansavtaleloven (1999) forutsetter at bruk av betalingskort med tilhørende kode er omfattet av definisjonene, og det er på det rene at bruk av betalingskort til å gjennomføre en betalingstransaksjon utgjør bruk av et «elektronisk betalingsinstrument», jf. § 1-5 annet ledd.[31] Når BankID brukes som elektronisk autentisering til å iverksette betalingssansaksjoner i nettbanken, vil de prosedyrene som må følges, samlet utgjøre bruk av et betalingsinstrument.[32] Dette legges til grunn av Høyesterett i både HR-2020-2021-A avsnitt 38 og HR-2022-1752-A avsnitt 29.

Virkningen av at ansvarsbegrensningene påberopes, er at betalingstjenesteyteren «straks, og senest innen utgangen av den påfølgende virkedagen» plikter å tilbakebetale beløpet og rentetapet fratrukket egenandelen i finansavtaleloven (2020) § 4-30 jf. § 4-32 første ledd.

Reglene om ikke godkjente betalingstransaksjoner i § 4-30 gjelder i utgangspunktet både for kunder som er forbrukere, og kunder som er næringsdrivende, men er ufravikelige for forbrukere, jf. finansavtaleloven (2020) § 1-9. Artikkelen konsentrerer seg først og fremst om kunder som er forbrukere.

3 Kundens plikter

3.1 Innledende om kundens plikter og kundens varslingsplikt

Det følger av finansavtaleloven (2020) § 4-30 tredje ledd at ved misbruk av elektroniske betalingsinstrumenter er kunden ansvarlig for en egenandel på 12 000 kroner dersom «tapet skyldes at kunden ved grov uaktsomhet har unnlatt å oppfylle en eller flere av sine plikter etter § 4-23 første ledd eller § 4-24 første ledd». Vurderingen av kundens ansvar ved misbruk av elektroniske betalingsinstrumenter skjer altså i to steg: Det må først konstateres at det foreligger et pliktbrudd. Dernest må graden av skyld vurderes, ettersom dette er den avgjørende rettsvirkningen av pliktbruddet.[33]

Varslingsplikten i finansavtaleloven (2020) § 4-24 er en delvis videreføring av finansavtaleloven (1999) § 37 første ledd og § 40 fjerde ledd og gjennomfører PSD 2 artikkel 71. Bestemmelsen slår fast at kunden uten ugrunnet opphold skal varsle betalingstjenesteyteren, i tråd med opplysningene betalingstjenesteyteren har gitt i henhold til § 4-23 annet ledd, dersom kunden blir «oppmerksom på» tap, tyveri eller uberettiget bruk eller tilegnelse av et betalingsinstrument eller en konto. Med dette forstås at kunden må ha faktisk kunnskap om den ikke godkjente betalingstransaksjonen.[34] Dette innebærer at det ikke er tilstrekkelig at kunden burde ha blitt kjent med forholdet – slik det følger av ordlyden i finansavtaleloven (1999) § 37.

I tillegg til varslingsplikten i § 4-24 er kunden pålagt plikter ved utstedelse og bruk av betalingsinstrumentet etter § 4-23. Før jeg går nærmere inn på grensen for grov uaktsomhet, vil jeg i punkt 3.2 knytte noen kommentarer til innholdet av kundens forpliktelser etter § 4-23.

3.2 Kundens plikter ved utstedelse og bruk av betalingsinstrument

Bestemmelsen i finansavtaleloven (2020) § 4-23 tilsvarer finansavtaleloven (1999) § 34 og gjennomfører PSD 2 artikkel 69 og deler av artikkel 70. Kunden pålegges etter denne bestemmelsen å bruke betalingsinstrumentet i samsvar med «vilkårene for utstedelse og bruk». Det er særskilt presisert at kunden må «ta alle rimelige forholdsregler» for å beskytte «personlig sikkerhetsinformasjon». Med «personlig sikkerhetsinformasjon» siktes det til «personaliserte innretninger som en tjenesteyter stiller til rådighet for kunde eller annen bruker for autentiseringsformål», jf. § 1-8 tiende ledd.[35] Dette omfatter eksempelvis PIN-kode eller annet passord for å bekrefte iverksettelsen av en betalingstransaksjon, herunder kodebrikke og passord knyttet til en BankID.[36]

Hva som nærmere ligger i direktivets henvisning til at sikkerhetsinformasjonen skal være «personlig», er ikke definert verken i loven eller i direktivet. I forarbeidene til finansavtaleloven (1999) antas det at «personlig sikkerhetsinformasjon» henviser til at sikkerhetsinformasjonen etter avtalen med betalingstjenesteyter ikke skal oppgis til uvedkommende.[37] Dette betyr imidlertid ikke at informasjonen er personavhengig, slik som egen underskrift eller fødselsnummer, ettersom slik informasjon ikke er noe tjenesteyter har stilt til rådighet for kunden.

Som forklart ovenfor i punkt 2 følger kundens plikter nærmere av utstedelsesavtalene for betalingskort eller for BankID. Av disse avtalene følger det, med noe varierende ordlyd, at kunden skal ta alle rimelige forholdsregler for å beskytte kode og passord og ikke bruke betalingsinstrumentet slik at andre kan se koden eller passordet. Samtidig slås det fast at kode og passord ikke skal gjøres tilgjengelig for noen, heller ikke politiet eller banken.[38] Det er imidlertid høyst tvilsomt om en slik regulering i utstedelsesavtalen står seg, ettersom det blant annet ikke er mulig å kontraktsregulere hvilke opplysninger man plikter å gi til politiet.[39]

Betalingstjenesteyteren står ikke helt fritt til å styre kundens forpliktelser gjennom en streng avtaleregulering, ettersom loven er ufravikelig til ugunst for forbrukeren, jf. § 1-9. I § 4-23 første ledd siste punktum presiseres det at «[v]ilkårene for utstedelse og bruk skal være objektive, ikke innebære forskjellsbehandling og stå i forhold til formålet». Dette begrenser betalingstjenesteyters mulighet til å avtale seg ut av et eventuelt ansvar, uten at PSD 2 eller forarbeidene til finansavtaleloven (2020) konkretiserer dette nærmere.[40]

I tillegg stiller forbrukeravtaledirektivet, rådsdirektiv 93/13/EØF om urimelige vilkår i forbrukeravtale, krav til avtalens utforming og balanse i forbrukerforhold. Artikkel 5 første punktum slår fast at avtalevilkårene skal formuleres på en «klar og forståelig måte». EU-domstolen har slått fast at det i dette ligger mer enn at avtalens innhold skal være grammatisk riktig utformet.[41] Det er for det første tale om en objektiv klarhetsstandard, hvor det sentrale er hva en alminnelig opplyst og rimelig oppmerksom forbruker ville ha forstått.[42] For det andre

pålegges næringsdrivende en forklaringsplikt, hvor forbrukeren må opplyses om avtalevilkårene og konsekvensene av disse før avtalen inngås.[43] Dette supplerer betalingstjenesteyters opplysningsplikt etter finansavtaleloven (2020) § 3-31 og vil være en sentral tolkningsfaktor ved tolkningen av utstedelsesavtalen.

Loven pålegger kunden å ta «alle rimelige forholdsregler» for å beskytte «personlig sikkerhetsinformasjon», jf. § 4-23. At forholdsreglene skal være «rimelige», innebærer en øvre grense for hvor inngripende forholdsregler det kan forventes at kunden iverksetter. I HR-2020-2021-A, som gjaldt misbruk av BankID til opptak av forbrukslån, uttalte Høyesterett seg i avsnitt 98 om hva som ligger i «rimelige forholdsregler» etter finansavtaleloven (1999) § 34:

> «Vurderingen av hva som er rimelige forholdsregler, må bygge på hva som praktisk mulig uten at det utgjør en urimelig stor byrde for innehaveren eller vil gjøre selve bruken av BankID upraktisk.»

Det forventes følgelig ikke at kunden treffer tiltak som går utover den praktiske nytten av å inneha betalingsinstrumentet.[44]

Hva som utgjør rimelige forholdsregler, må vurderes med utgangspunkt i hvordan betalingsinstrumentet brukes og oppbevares. Det er av den grunn nærliggende å lese kravet om at kunden skal ta alle «rimelige forholdsregler» for å beskytte sin personlige sikkerhetsinformasjon, i sammenheng med kravet om at betalingsinstrumentet skal brukes «i samsvar med vilkårene for utstedelse og bruk». Eksempelvis har ikke kunden tatt alle rimelige forholdsregler dersom et betalingsinstrument oppbevares nedlåst i en koffert sammen med tilhørende kode eller passord nedskrevet på et ark.[45] Kunden holdes imidlertid ikke ansvarlig for ethvert avvik fra disse pliktene. Det kreves at kunden har utvist grov uaktsomhet eller forsett for at kunden skal holdes ansvarlig utover egenandelen på 450 kroner, jf. § 4-30 annet ledd.

4 Vurderingstemaet for grovt uaktsomt pliktbrudd

Som forklart i innledningen er systemet i finansavtaleloven at betalingstjenesteyterens ansvar blir redusert i tråd med graden av klander fra kunden.[46] Verken finansavtaleloven (1999) eller finansavtaleloven (2020) definerer uttrykket «grov uaktsomhet». Ordlyden tilsier at det er tale om en høy terskel, slik at bestemmelsen er reservert for de mer alvorlige tilfellene av pliktforsømmelser, begrenset oppad mot forsett.

Heller ikke i PSD 2 er begrepet definert, men fortalen gir enkelte anvisninger om terskelen. I punkt 72 i fortalen fremgår det at

> «[s]elv om begrebet forsømmelse indebærer tilsidesættelse af diligenspligten, bør grov forsømmelse imidlertid indebære mere end blot forsømmelse og vedrøre adfærd, der involverer en betydelig grad af skødesløshed ...».

Som eksempel trekkes frem

> «opbevaring af de sikkerhedsoplysninger, der anvendes til at give tilladelse til en betalingstransaktion, ved siden af betalingsinstrumentet i et format, der på en åben og let måde kan opdages af tredjeparter».

Typisk vil dette omfatte oppbevaring av nedskrevet kode sammen med bankkortet i en lommebok.

Videre følger det av fortalen punkt 72 at «[b]eviset for og graden af den påståede forsømmelse bør generelt vurderes i henhold til national ret». Denne henvisningen til nasjonal rett er noe underlig, ettersom PSD 2 i utgangspunktet er et fullharmoniseringsdirektiv, se artikkel 107. Fullharmonisering kan nødvendigvis ikke oppnås dersom man skal bygge på ulike nasjonale konsepter av grov uaktsomhet.[47] I alle tilfelle må fortalens henvisning til nasjonal rett på dette punktet, sammenholdt med fraværet av nærmere retningslinjer i PSD 2 selv eller andre EØS-rettslige kilder, innebære at det er adgang til å trekke inn nasjonale kilder i rettsanvendelsen.

I forarbeidene til finansavtaleloven (1999) uttales det i denne forbindelse at «[f]or at kunden skal anses å ha vært grovt uaktsom, kreves det ... et markert avvik fra vanlig forsvarlig handlemåte».[48] Denne formuleringen av vurderingstema tilsvarer det som fremgår av fortalen til PSD 2, og samsvarer med utgangspunktet i norsk kontraktsrett.[49] Høyesterett bygger videre på dette utgangspunktet i Rt-2004-499, som til nå er den eneste saken hvor Høyesterett har vurdert terskelen for grovt uaktsomme pliktbrudd ved ikke godkjente betalingstransaksjoner.

Høyesterett slår i avsnitt 32 fast at kunden må ha utvist en kvalifisert form for uaktsomhet. Kundens handlinger 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». Dette tilfører imidlertid ikke noe mer enn det som allerede følger av PSD 2 og uttalelsen i forarbeidene til finansavtaleloven (1999). Dommen kommenteres nærmere under punkt 7.2. Med disse generelle utgangspunktene som grunnlag skal jeg nå gå nærmere inn på hvorvidt (a) kundens individuelle forhold og (b) manglende sikkerhetsrutiner hos betalingstjenesteyteren er relevant å vektlegge i vurderingen av om kunden har opptrådt grovt uaktsomt. Dette behandles videre i henholdsvis punkt 5 og punkt 6.

5 Betydningen av kundens individuelle forhold

Aktsomhetsvurderingen etter finansavtaleloven (2020) § 4-30 er knyttet til hvorvidt «kunden» har handlet grovt uaktsomt. Spørsmålet i dette punktet er hvorvidt kundens individuelle forhold kan ha innvirkning på aktsomhetsvurderingen, eller om kunden måles etter en rent objektiv målestokk, basert på gjennomsnittsforbrukeren. Om kunden lar seg lure av ulike svindelmetoder, vil i mange tilfeller bero på personlige forutsetninger, og det er derfor relevant å vurdere hvorvidt dette skal vektlegges i aktsomhetsvurderingen etter § 4-30.

Ordlyden i § 4-30 berører ikke kundens individuelle forhold eller personlige forutsetninger for å kunne avdekke svindel. Heller ikke PSD 2 går nærmere inn på temaet. I forarbeidene til finansavtaleloven (2020) forutsettes det imidlertid i tilknytning til vurderingen av forsettlige pliktbrudd at «eldre personer ... som har behov for hjelp av andre til å betale regninger» ikke skal være ansvarlige for hele det økonomiske tapet.[50]

Videre samme sted følger det at kunder som har behov for hjelp på grunn av mangelfulle språkkunnskaper, ikke uten videre kan holdes ansvarlige for forsettlige pliktbrudd. Med dette legger forarbeidene til grunn at også manglende språkkunnskaper er et relevant individuelt forhold i skyldvurderingen. Et slikt standpunkt er også inntatt i forarbeidene til finansavtaleloven (1999), som fremhever at krav til forsiktighet og egenkontroll varierer fra kunde til kunde, slik at det er «viktig å vurdere kundens kunnskap og innsikt i den enkelte betalingstjeneste».[51]

Forarbeidene trekker med dette frem at kundens høye alder eller mangelfulle språkkunnskap etter omstendighetene kan være relevante momenter i skyldvurderingen. Med dette åpner lovgiver for at skyldvurderingen etter § 4-30 kan påvirkes av individuelle forhold hos kunden. Selv om kun disse forholdene er nevnt, kan forarbeidene neppe forstås slik at det ikke er aktuelt å legge vekt på andre individuelle forhold hos kunden.

Individuelle forhold trekkes frem som relevante momenter i både erstatningsretten og kontraktsretten.[52] I erstatningsretten kan subjektive forhold være avgjørende for aktsomhetsvurderingen, der det eksempelvis stilles lempeligere krav til barn enn til voksne.[53] Innenfor erstatningsrettslig teori hevdes det også at høy alder i kombinasjon med alderdomssvekkelser kan føre til en mildere aktsomhetsbedømmelse.[54]

Samtidig taler reelle hensyn for at slike individuelle forhold er relevant å vektlegge, ettersom det er liten tvil om at slike forhold påvirker kundens mulighet til å avdekke svindel. Særlig fremheves det at det har oppstått et kunnskapsgap mellom yngre og eldre generasjoner med hensyn til teknologi og bruk av digitale løsninger som følge av den digitale utviklingen. Dette medfører at en avgrenset gruppe mennesker er særlig utsatt for svindel. Analoge bankkunder har i stadig mindre grad mulighet til å benytte seg av tradisjonelle betalingstjenester, og mange finner det krevende å bruke elektroniske betalingsløsninger på egen hånd. Disse kundene søker gjerne hjelp hos familie og venner, som innebærer at risikoen for svindel øker.[55] Svindlere utnytter denne mangelen på digital kunnskap, som særlig vises gjennom sakene om såkalt Olga-svindel, hvor svindlere målrettet kontakter eldre mennesker. Individuelle forhold hos kunden kan – og bør – følgelig være et viktig moment i aktsomhetsvurderingen ved misbruk av elektroniske betalingsinstrumenter.

Når det gjelder språkkunnskap, har problemstillingen tidligere blitt behandlet av lagmannsretten i LB-2016-43622 etter finansavtaleloven (1999). Saken gjaldt en kvinne som på grunn av begrensede norskkunnskaper overlot BankID og passord til sin ektefelle, som senere misbrukte dette til å ta opp lån uten at kunden var klar over hva hun signerte på. Saken gjaldt altså misbruk av elektronisk signatur, slik at finansavtaleloven (1999)s bestemmelser om tapsbegrensning ved uautoriserte betalingstransaksjoner i § 35 ikke kom til anvendelse. Alminnelig erstatningsrett var altså det rettslige grunnlaget for kundens ansvar. Det uttales på generelt grunnlag at «[m]anglende kunnskap i norsk og om det norske banksystemet burde føre til at hun var mer forsiktig med å undertegne på dokumenter som hun ikke forsto innholdet i». Kundens manglende språkkunnskaper ble ikke

tillagt vekt, og lagmannsretten anså det som uaktsomt av kunden å undertegne en avtale uten å sette seg inn i hva hun forpliktet seg til.

Dette vil imidlertid harmonere dårlig med betalingstjenesteyterens opplysnings- og forklaringsplikt, som ble berørt ovenfor i punkt 3.2. Utgangspunktet er at det er betalingstjenesteyteren som skal sørge for at kunden har fått tilstrekkelig kunnskap om bruk og risiko av betalingsinstrumentet. Dette vil i enda større grad gjelde der kunden ikke har tilstrekkelige språkkunnskaper til selv å sette seg inn i dette.

Til sammenligning har Högsta domstolen i Sverige i en avgjørelse fra 21. juni 2022 uttrykkelig fremhevet individuelle forhold hos kunden ved aktsomhetsvurderingen.[56] Saken er relevant å fremheve, ettersom reglene om tapsfordeling ved misbruk av elektroniske betalingsinstrumenter i svensk rett, i likhet med i norsk rett, bygger på PSD 2. Den aktuelle saken gjaldt et tilfelle der en kunde ble fralurt personlig sikkerhetsinformasjon tilknyttet sin BankID som gjorde det mulig for svindlerne å overføre 397 000 svenske kroner fra kundens konto. Spørsmålet for retten var om kunden hadde handlet særskilt klanderverdig («särskilt klandervärt»). Domstolen kom til at dette ikke var tilfellet, og konkluderte med at kunden hadde handlet grovt uaktsomt («grovt vårdslöst»). [57] Kundens ansvar ble begrenset til 12 000 kroner. Ved skyldvurderingen uttales det i avsnitt 28:

> «Vid bedömningen av ett eventuellt ansvar när konsumenten i samband med ett bedrägeri inte har skyddat sina personliga behörighetsfunktioner knutna till betalnings instrumentet finns det anledning att fästa särskilt avseende vid vissa faktorer. Bland dessa *ingår den miljö och situation som konsumenten befann sig i samt hans eller hennes möjlighet att skydda sig* mot en obehörig transaktion. *Konsumentens ålder och erfarenhet kan här vara av betydelse* ....» (Min utheving.)

Selv om utgangspunktet for aktsomhetsvurderingen er objektivt, peker Högsta domstolen uttrykkelig på at individuelle faktorer er sentrale ved aktsomhetsvurderingen, herunder miljøet og situasjonen kunden befinner seg i, kundens handlingsalternativer og kundens erfaring og alder. Gode grunner taler derfor for at aktsomhetsvurderingen må tilpasses kundens individuelle forutsetninger, tilsvarende slik Högsta domstolen gjør. Forarbeidene til finansavtaleloven (2020) åpner for at subjektive forhold etter omstendighetene kan være relevant ved skyldvurderingen, og trekker frem alder og språkkunnskap som eksempler på subjektive forhold. Det vil bære galt av sted dersom alle kunder vurderes etter samme objektive norm – det er med andre ord rom for individuelle tilpasninger basert på de konkrete omstendighetene. Samtidig må det understrekes at kunden ikke bevisst kan holde seg selv i villfarelse om hvilke forpliktelser vedkommende har, og på den måten omgå ansvarsreglene i finansavtaleloven.[58]

6 Betydningen av manglende sikkerhetsrutiner hos betalingstjenesteyteren

I forlengelsen av punktet ovenfor er det også relevant å spørre om forhold hos betalingstjenesteyteren kan påvirke vurderingen av hvorvidt kunden har handlet grovt uaktsomt. Særlig relevant er dette i de tilfellene der betalingstjenesteyteren, eksempelvis en bank, ikke har overholdt de sikkerhets- og kontrollrutiner den er pålagt.

Denne problematikken ble i korthet belyst av Høyesterett i HR-2020-2021-A. Saken gjaldt misbruk av elektronisk signatur før ikrafttredelsen av finansavtaleloven (2020), hvor slike tilfeller falt utenfor ansvarsbegrensningene i finansavtaleloven (1999). I avsnitt 50 flg. redegjør Høyesterett for ansvarsgrunnlaget for erstatning etter alminnelige erstatningsrettslige regler. Retten fremhever at rolleforventningen hos skadelidte og skadelidtes forhold i enkelte situasjoner kan medføre at skadelidte selv har den objektive egenrisikoen for skaden.[59]

Når BankID brukes utenfor det Høyesterett betegner som det opprinnelige bruksområdet – betalingstransaksjoner -, kan situasjonen være slik at det forventes at banken treffer sikkerhets- og kontrolltiltak utover å konstatere at BankID er riktig brukt.[60] I et *obiter dictum* legger imidlertid Høyesterett til grunn motsatt standpunkt ved ikke godkjente betalingstransaksjoner:[61]

> «Når BankID benyttes innenfor det som må betegnes som det opprinnelige bruksområdet, betalingstransaksjoner, må den klare hovedregelen være at det ikke kan kreves at institusjonen skal foreta ytterligere sikkerhets- eller kontrolltiltak utover å konstatere at BankID er brukt på riktig måte. Dette må da danne utgangspunktet for vurderingen av om innehaveren har opptrådt grovt uaktsomt etter finansavtaleloven § 35 tredje ledd.»

Høyesterett legger altså til grunn at det er tilstrekkelig for betalingstjenesteyteren å godtgjøre at BankID er brukt riktig ved gjennomføring av betalingstransaksjoner. Hvis det er tilfellet, vil skyldvurderingen i så fall bero på en isolert vurdering av hva *kunden selv* kunne og burde ha gjort.

Ettersom uttalelsen er knyttet til skyldreglene i finansavtaleloven (1999), behandlet ikke Høyesterett PSD 2, som i fortalen punkt 72 uttrykkelig slår fast at «[f]or at vurdere eventuel forsømmelse eller grov forsømmelse fra betalingstjenestebrugerens side bør der *tages hensyn til alle omstændigheder*» (min utheving). I denne sammenheng følger det av delegert kommisjonsforordning (EU) 2018/389 artikkel 2 nr. 1, som utfyller PSD 2, at betalingstjenesteytere plikter å ha «transaktionsovervågningsmekanismer, som sætter dem i stand til at afsløre uautoriserede eller svigagtige betalingstransaktioner».[62] Med andre ord plikter betalingstjenesteytere å ha sikkerhets- og kontrollrutiner på plass når BankID, eller for den saks skyld ethvert annet elektronisk betalingsinstrument, benyttes for gjennomføring av betalingstransaksjoner. At dette ikke løftes frem av Høyesterett, skyldes nok at saken ikke gjaldt betalingstransaksjoner, og at det av denne grunn ikke var behov for å behandle dette i dybden.

Betalingstjenesteyteren skal altså ha rutiner på plass for å overvåke betalingstransaksjoner med det formål å avdekke svindel og misbruk av betalingsinstrumenter. Den samme delegerte kommisjonsforordningen definerer i artikkel 18 nr. 2 bokstav c en rekke risikokriterier som betalingstjenesteyter skal vurdere ved transaksjonsovervåkningen, nemlig (i) «unormale udgifts- eller adfærdsmønstre hos betaleren», (ii) «usædvanlige oplysninger om betalerens adgang til anordninger og software», (iii) «malware-infektion i autentifikationsprocedurens sessioner», (iv) «kendte scenarier for svig i forbindelse med udbud af betalingstjenester», (v) «unormalt opholdssted for betaleren» og (vi) «højrisikoopholdssted for betalingsmodtageren».

På denne bakgrunn kan det spørres om mangel på sikkerhets- og kontrolltiltak hos betalingstjenesteyter som kunne avdekket og helt eller delvis hindret gjennomføringen av ikke-godkjente betalingstransaksjoner, må vektlegges ved vurderingen av om kunden har handlet grovt uaktsomt.

Bestemmelsene om tapsfordeling i PSD 2 artikkel 74 og finansavtaleloven (2020) § 4-30 er utelukkende knyttet til de handlinger kunden selv foretar seg, og tar ikke opp de plikter betalingstjenesteyteren har og må følge. Direktivet går ikke nærmere inn på dette, og problematikken er heller ikke behandlet i forarbeidene til finansavtaleloven (2020) for betalingstransaksjoners vedkommende. Dette innebærer at det er uklart hvilken betydning forhold hos betalingstjenesteyteren har for vurderingen av kundens skyld i disse tilfellene.

I HR-2020-2021-A ble skadelidtes forhold uttrykkelig fremhevet. Saken gjaldt riktignok misbruk av elektronisk signatur, hvor Høyesterett langt på vei begrunnet at kunden ikke hadde handlet uaktsomt, med henvisning til skadelidtes (bankens) forhold.[63] Merk at Høyesterett her la til grunn at det ikke kreves ytterligere kontroll- og sikkerhetstiltak der BankID er riktig brukt ved gjennomføring av betalingstransaksjoner, men som vist ovenfor er nok ikke dette helt treffende.

I fravær av nærmere begrunnelse er ikke Høyesteretts standpunkt særlig overbevisende. I lys av det ovennevnte, og at det er tale om et *obiter dictum*, er det derfor tvilsomt om fremtidige avgjørelser bør legge til grunn det samme standpunktet. Hvis betalingstjenesteyter ikke overholder sin plikt til å overvåke mistenkelige betalingstransaksjoner, som kunne satt dem i stand til å hindre eller begrense tap som følge av en ikke-godkjent betalingstransaksjon, taler gode grunner for at dette kan spille inn i vurderingen av kundens skyld, enten BankID er brukt til å gjennomføre betalingstransaksjoner eller til lånopptak. Dette vil være i tråd med erstatnings- og kontraktsrettslige synspunkter om at skadelidtes forhold kan ha betydning for den normative avveiningen av hvem som er nærmest til å bære risikoen.[64] Manglende etterfølgelse av pålagte kontroll- og sikkerhetstiltak innebærer at betalingstjenesteyteren bevisst eksponerer seg selv for en risiko.

Tilsvarende synspunkter har blitt reist under andre jurisdiksjoner i EU. Særlig er det verdt å fremheve at Portugals høyesterett ved flere anledninger har konkludert at betalingstjenesteyter burde ha oppdaget at det var tale om ikke godkjente betalingstransaksjoner på bakgrunn av at transaksjonene som ble gjennomført, avvek fra kundens normale handlemønstre.[65] Tilsvarende som ovenfor argumenteres det for at betalingstjenesteyters forpliktelser etter delegert kommisjonsforordning (EU) 2018/389, og manglende etterfølgelse av de kontroll- og sikkerhetstiltak som pålegges betalingstjenesteyteren, må ha betydning for vurderingen av kundens skyld.[66]

Basert på dette kan det med god grunn argumenteres for at betalingstjenesteyter plikter å ha kontroll- og sikkerhetstiltak som gjør det mulig å identifisere ikke godkjente betalingstransaksjoner. Det er ikke nødvendigvis slik at det er tilstrekkelig at betalingstjenesteyter godtgjør at det enkelte elektroniske

betalingsinstrument, det være seg BankID eller betalingskort, er brukt på riktig måte; manglende kontroll- og sikkerhetstiltak bør ha betydning i vurderingen av kundens skyld. Under enhver omstendighet er dette forhold som er relevant å vektlegge ved en eventuell vurdering av om kundens ansvar skal lempes etter finansavtaleloven (2020) § 4-31. Det faller imidlertid utenfor temaet for denne artikkelen å gå nærmere inn på spørsmål om lemping.

7 Grov uaktsomhet i utvalgte typetilfeller av ikke godkjente betalingstransaksjoner

7.1 Innledende om typetilfellene

Praksis fra Finansklagenemnda viser at spørsmål om hvorvidt kunden har opptrådt grovt uaktsomt, typisk oppstår enten (1) fordi en tredjeperson har fått tilgang til sikkerhetsinformasjon fordi denne var nedtegnet, (2) fordi kunden er utsatt for skriftlig *phishing* via e-post eller sms, eller (3) fordi kunden er utsatt for *vishing* (telefonsvindel). Det er derfor av særlig interesse å vurdere disse tre typetilfellene opp mot terskelen for grov uaktsomhet, som vil bli behandlet i de neste punktene.

7.2 Kan det være grovt uaktsomt å skrive ned personlig sikkerhetsinformasjon som PIN-kode og passord?

I dette punktet er spørsmålet om det kan være grovt uaktsomt å skrive ned personlig sikkerhetsinformasjon. Med andre ord er vurderingen om det er en «rimelig forholdsregel» for å beskytte denne sikkerhetsinformasjonen at PIN-kode og passord ikke skrives ned. Utstedelsesavtalene for BankID og betalingskort forbyr ikke å skrive ned personlig sikkerhetsinformasjon, slik som PIN-kode tilknyttet betalingskort eller passord knyttet til BankID. På grunn av mengden koder og passord man må ha kontroll på, er det mange som tyr til å skrive ned disse for å få bedre kontroll og oversikt. Nedtegningen kan skje enten fysisk på papir eller digitalt på eksempelvis telefonen.

At nedtegning av PIN-kode og passord medfører økt risiko for misbruk, er åpenbart, og det anbefales at man heller har gode og unike passord som skrives ned og oppbevares trygt, enn å ha enkle passord eller samme passord som brukes over flere tjenester.[67] Samtidig følger det av fortalen til PSD 2 punkt 72 at «opbevaring af de sikkerhedsoplysninger, der anvendes til at give tilladelse til en betalingstransaktion, ved siden af betalingsinstrumentet i et format, der på en åben og let måde kan opdages af tredjeparter» utgjør et grovt uaktsom pliktbrudd. Hvordan den nedskrevne koden eller passordet og betalingsinstrumentet oppbevares, er altså sentralt for vurderingen av grov uaktsomhet.

Høyesterett har bare ved ett tilfelle behandlet spørsmålet om grovt uaktsomme pliktbrudd ved misbruk av elektroniske betalingsinstrumenter, nemlig i Rt-2004-499. Ettersom dette er den eneste avgjørelsen fra Høyesterett som tar stilling til kundens aktsomhet ved ikke godkjente betalingstransaksjoner, vil de generelle merknadene rundt terskelen for grov uaktsomhet fortsatt være retningsgivende til tross for dommens alder. Utgangspunktene har også blitt gjentatt i nyere underrettspraksis.[68]

Saken gjaldt en kunde som hadde tre bankkort låst i en koffert i en låst leilighet i Spania. Kodene var skrevet ned i kamuflert form i en almanakk, som ble oppbevart i samme koffert som kortene. Høyesterett delte seg tre mot to, hvor flertallet konkluderte med at kunden ikke hadde opptrådt grovt uaktsomt.

Ved tolkningen av uttrykket «grov uaktsomhet» slo flertallet fast at kunden må ha utvist en kvalifisert form for uaktsomhet.[69] Som nevnt under punkt 4 må en grovt uaktsom oppførsel 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». Dette innebærer at det for det første må foreligge et objektivt avvik fra en vanlig forsvarlig handlenorm.

Det følger av flertallets videre drøftelse at utgangspunktet for vurderingen er den «alminnelige kortholder». Standarden er med andre ord ikke hvordan idealkunden ville handlet. Dette objektive avviket må være «markert», som innebærer at ikke ethvert avvik fra den alminnelige handlenormen vil omfattes. For det andre vurderes det om det foreligger en subjektiv unnskyldningsgrunn. Kundens opptreden må være «sterkt klanderverdig», slik at det må foreligge et element av bebreidelse, hvor kunden må være «vesentlig mer å

klandre» enn ved alminnelig uaktsomhet. Her er det rom for å tillegge individuelle forhold ved kunden vekt, se nærmere under punkt 5.

I den konkrete vurderingen var det sentralt om koden var notert slik at det muliggjorde en tredjepersons misbruk av kortet. Flertallet slo fast at «folk flest» antakelig ville hatt vanskeligheter med å finne riktig kode. Høyesterett trakk frem to sentrale forhold i vurderingen av om uaktsomheten kunne kategoriseres som grov, nemlig at koden kunne vært kamuflert bedre, og at kunden kunne redusert risikoen for svindel betydelig ved å ta med seg notatboken. Det sentrale i skyldvurderingen er altså kundens handlingsalternativer, hvor det var «ubetenksomt» å la kort og kode ligge sammen, til tross for at de var nedlåst i en koffert i en forsvarlig låst leilighet som ikke var spesielt utsatt for innbrudd. Uttalelsene tilsier at kort og kode ikke bør oppbevares sammen i det hele tatt, og terskelen for grov uaktsomhet kan tenkes å være nokså lav i disse tilfellene.

Høyesteretts flertall anså imidlertid ikke kundens handlinger som «sterkt klanderverdige», og kunden hadde følgelig ikke opptrådt grovt uaktsomt. Dette ble begrunnet med at oppbevaringen hadde et «klart midlertidig preg». Flertallet påpekte samtidig at vurderingen ville blitt en annen om kunden oppbevarte kort og kode i nærheten av hverandre i sitt eget hjem. Oppbevaringens midlertidige karakter og det forhold at kunden var på ferie, var altså utslagsgivende momenter.

Avslutningsvis påpekte flertallet at håndteringen av kort og kode må gis en «streng aktsomhetsvurdering». Dette forklares ikke nærmere, men ut fra sammenhengen er det mest nærliggende at aktsomhetskravet skjerpes ved håndteringen av betalingsinstrumenter og tilhørende koder og passord. Det er imidlertid uklart hvordan dette skal forstås i lys av vurderingstemaet som Høyesterett oppstiller, nemlig at det må være et «markert avvik» fra vanlig forsvarlig handlemåte, hvor kunden er «vesentlig å bebreide».

En viss veiledning følger av de videre uttalelsene om at det «spiller likevel inn at det økonomiske tap ... var begrenset til kr 10.000» (avsnitt 41). Høyesterett kommenterer altså skadeevnen, hvor kombinasjonen av oppbevaringens midlertidige karakter, og at det økonomiske tapet var begrenset, medførte at skadeevnen var relativt liten. Lest i sammenheng med at det ifølge Høyesterett forelå flere handlingsalternativer som betydelig kunne redusert tapsrisikoen, forstås uttalelsene slik at kombinasjonen av skaderisikoen og kundens mulighet til å redusere denne gjennom ulike handlingsalternativer vil utgjøre kjernen i vurderingen av grov uaktsomhet. Hvor «streng» aktsomhetsnorm som skal legges til grunn, er med andre ord relativ til skadeevnen i det enkelte tilfellet.

En slik forståelse innebærer at en kunde med betydelige midler må utvise større grad av aktsomhet enn en kunde med lite midler. Videre vil BankID måtte stå i en særstilling, ettersom det potensielle økonomiske tapet i teorien er ubegrenset. Dette har sine åpenbare begrensninger, ettersom det skaper en høyst uforutsigbar stilling i avtaleforholdet med betalingstjenesteyteren. Kunden påtar seg ikke en større tapsrisiko kun fordi vedkommende har mer midler, og aktsomhetsvurderingen må i det vesentlige bero på om det er utvist «et markert avvik fra vanlig forsvarlig handlemåte», hvor det må dreie seg om «en opptreden som er sterkt klanderverdig». Skadeevnen vil til en viss grad kunne være veiledende i denne vurderingen, men etablerer ikke i seg selv handlenormen.

Høyesteretts avgjørelse har i hovedsak blitt fulgt opp i lignende saker som har kommet opp for Finansklagenemnda. Praksisen viser at det gjennomgående slås fast at kunden har opptrådt grovt uaktsomt dersom koden har blitt oppbevart sammen med kortet i åpen eller dårlig kamuflert form.[70] Oppbevares koden *adskilt* fra betalingsinstrumentet, vil vurderingen bero på et samspill mellom hvor godt koden er kamuflert, og oppbevaringen. Samtidig innebærer situasjonen i seg selv at risikoen for misbruk blir betraktelig mindre, da svindleren må finne ut av oppbevaringsstedet for både betalingsinstrumentet og den tilhørende koden. Dette tillater at oppbevaringen kan være av mer varig karakter. Følgelig skal det mer til for at kunden har opptrådt grovt uaktsomt. Dersom det er truffet gode sikkerhetstiltak ved oppbevaringen av selve koden, vil det også måtte stilles lempeligere krav til kvaliteten på kamufleringen.[71]

7.3 Kan det være grovt uaktsomt å falle for phishing-angrep?

I dette punktet er spørsmålet om det er grovt uaktsomt av kunden å falle for phishing-svindel. Med dette menes, som forklart innledningsvis, tilfeller der kunden blir lurt til å følge en digital lenke vedkommende har mottatt på e-post, sms eller lignende. Lenken dirigerer kunden til en side som i større eller mindre grad ligner på nettsiden til kundens bank eller en annen aktør. Svindlerne har kontroll over narresiden og kan se innloggingsinformasjonen som blir tastet inn. Ved å illudere en mislykket innlogging på narresiden kan

svindlerne gjentatte ganger få nødvendig informasjon for å gjennomføre flere betalingstransaksjoner. Situasjonen er en ganske annen enn ved «tradisjonell» svindel, hvor svindleren fysisk fratar kunden betalingsinstrumentet og den tilhørende koden. Ved phishing har kunden fortsatt alt i sin besittelse, men det foreligger et objektivt pliktbrudd ved at kunden har delt personlig sikkerhetsinformasjon med uvedkommende i strid med utstedelsesavtalen.

Høyesteretts avgjørelse i Rt-2004-499 gir lite veiledning utover at kundens handlemåte må representere et markert avvik fra vanlig forsvarlig handlemåte, og kundens opptreden må være sterkt klanderverdig, slik at vedkommende må være vesentlig mer å klandre enn hvor det er tale om alminnelig uaktsomhet. Aktsomhetsvurderingen må for det første knyttes til måten kontakten finner sted på, og for det andre til innholdet i selve meldingen. Sistnevnte har igjen flere sider, herunder utformingen av meldingen, hvordan språket er, og hva selve henvendelsen gjelder.

Kontakten skjer gjerne gjennom e-post eller tekstmelding. Dette er kommunikasjonsmåter som finansinstitusjoner selv bruker for å komme i kontakt med sine kunder, og det er derfor ingenting ved selve måten kontakten finner sted på, som vil innebære at kunden har grunn til å reagere. Informasjon om hvem som er avsender, kan avsløre om det er tale om en reell henvendelse eller ikke. I mange tilfeller er imidlertid avsenderadressen tilnærmet lik, eller manipulert til å være identisk med, den banken selv vanligvis benytter. Dette medfører at vurderingen i de fleste tilfeller vil måtte bero på innholdet i meldingen.

Flere elementer ved innholdet i meldingen kan avsløre at det ikke er tale om en reell henvendelse. Det første er den grafiske utformingen og selve oppsettet. Amatørmessig utformede e-poster vil gi kunden grunn til å reagere på henvendelsen og til å tvile på om den er reell. Dernest kan språket være avslørende; dårlig språk vil være et tegn på at det ikke er kundens faktiske bank som tar kontakt. Kombinasjonen av disse elementene kan innebære at kunden har handlet grovt uaktsomt. Denne vurderingen vil påvirkes av kundens personlige forutsetninger, slik som språkkunnskap, jf. ovenfor i punkt 5. Skrivefeil er ikke i seg selv påfallende; det er det samlede inntrykket som må være avgjørende. Også innholdet i selve henvendelsen er sentralt. Kjernen er at kunden settes under et falskt tidspress for å følge en digital lenke som sender kunden til narresiden. Eksempelvis kan kunden bes om å følge en lenke til «nettbanken» for å oppdatere utløpt informasjon.

I forlengelse av dette står kundens handlingsalternativer sentralt. På den ene side kan kunden fullstendig avstå fra å trykke på slike lenker. Dette innebærer en risiko for å gå glipp av viktig informasjon som blir tilsendt kunden, og kan derfor ikke anses som et reelt alternativ. På den annen side kan kunden forsøke å ta kontakt med aktøren for å bekrefte meldingens autentisitet. Det er imidlertid ikke nødvendigvis enkelt for kunden å vite hvor man skal henvende seg. Et praktisk eksempel er at Oslo kommune i februar 2021 sendte e-poster til eldre innbyggere med en lenke til en nettside hvor de ble bedt om å registrere seg med BankID dersom de ønsket vaksine mot covid-19.[72] Dersom noen av disse innbyggerne hadde fått en fiktiv e-post fra en svindler, men tok kontakt med Oslo kommune for å verifisere henvendelsen, ville vedkommende fått beskjed om at e-posten var reell.

Det foregår omfattende informasjonskampanjer rettet mot forbrukere, og Høyesterett har uttrykkelig slått fast at kunden «må ta hensyn til» at det finnes profesjonelle svindelmetoder.[73] Prinsippet som Høyesterett uttrykker, er relevant også ved phishing. Det vil si at når visse svindelmetoder er et kjent fenomen, vil det etter omstendighetene kunne stilles strengere krav til kundens aktsomhet. Det kan imidlertid være vanskelig å skille de reelle henvendelsene fra svindelforsøkene, all den tid både offentlige og private aktører, herunder banker og diverse abonnementstjenester, faktisk sender slike meldinger til forbrukere.[74] Mens forbrukere på den ene side gjennom informasjonskampanjer frarådes å trykke på digitale lenker og oppgi BankID-passord, driver seriøse aktører på den annen side nettopp med å sende slike henvendelser til kunder og innbyggere. Så lenge dette er tilfellet, kan det faktum at kunden har blitt lurt til å falle for en slik henvendelse, ikke alene være tilstrekkelig for å konstatere grov uaktsomhet.

Vurderingen av kundens aktsomhet beror altså på en samlet vurdering av en rekke elementer ved den enkelte henvendelse. Det er i dag ingen publiserte rettsavgjørelser som omhandler spørsmålet om skyld ved phishing ved ikke godkjente betalingstransaksjoner. Finansklagenemnda har imidlertid hatt en rekke slike saker til behandling, og i motsetning til betraktningene ovenfor har nemnda hovedsakelig ansett det som grovt uaktsomt å falle for phishing. Som jeg vil vise i fortsettelsen, har Finansklagenemnda frem til nylig lagt seg på en strengere linje enn betraktningene ovenfor om hva som utgjør grov uaktsomhet, uten at det kan sies at det foreligger rettslig grunnlag for dette.

En av de første sakene Finansklagenemnda behandlet som gjaldt spørsmålet om ansvarsfordeling etter phishing, gjaldt en forbruker som hadde mottatt en e-post som tilsynelatende så ut som den kom fra Apple:[75]

> «Sakens dokumenter viser at både eposten og den nettsiden klageren ble ledet inn på, var troverdige. Adressen i lenken var, slik den kunne leses av kortholderen på skjermen, identisk med Apples korrekte internettadresse. Lenken førte likevel ikke dit, men til en falsk side. Nemnda forstår det slik at det var vanskelig eller umulig for kortholderen å se at siden ikke var ekte. Grov uaktsomhet må derfor i tilfelle begrunnes med at hun fulgte en lenke i en epost i stedet for selv aktivt å taste inn adressen. Nemnda mener at med den publisitet som finnes om svindel og med de advarsler som gis mot å la seg svindle på denne måten, må det regnes som grovt uaktsomt å gi kortopplysninger på denne måten, selv om både eposten og nettsiden var svært troverdig.»

Nemnda legger seg altså på en linje der det å falle for et phishing-angrep i seg selv regnes som grovt uaktsomt, selv i et tilfelle der det var «vanskelig eller umulig» for kunden å avsløre at det dreide seg om svindel. Denne linjen ble fulgt opp i senere praksis.

Finansklagenemnda konkluderte i FinKN-2021-107 med at kunden hadde opptrådt grovt uaktsomt da vedkommende fulgte en lenke som ble tilsendt på e-post, og som tilsynelatende kom fra Netflix. Kundens betalingskort var én måned fra å utløpe, og kunden forsto e-posten slik at hun måtte oppdatere betalingsinformasjon på nettsiden. Nemnda la vekt på at kunden burde oppdaget at avsenderadressen og nettadressen på narresiden ikke tilhørte Netflix, og at språket i e-posten var dårlig. Kunden ringte det oppgitte telefonnummeret for å verifisere henvendelsen og kom til en automatisk svarer hos (reelle) Netflix. Kunden fattet dermed ikke mistanke om svindel, sammenlignbart med eksemplet med Oslo kommune ovenfor. Nemnda la imidlertid ikke noe vekt på at kunden forsøkte å verifisere e-posten. Ved vurderingen av om pliktbruddet var grovt, uttalte nemnda at med «den publisitet som finnes om svindel og med de advarsler som gis mot å la seg svindle, mener nemnda det må regnes som grovt uaktsomt å la seg svindle på denne måten». Nemndas begrunnelse for at pliktbruddet var grovt uaktsomt, er altså hovedsakelig forankret i at phishing er en kjent svindelmetode, samtidig som nemnda i vurderingen velger å se bort fra åpenbare momenter som taler i kundens favør.

I FinKN-2020-455 fikk kunden en e-post som tilsynelatende var fra kundens bank, hvor det fremgikk at kundens bankkort var sperret. For å oppheve «sperringen» måtte kunden følge en lenke. Kunden trodde «sperringen» hadde mulig sammenheng med at han hadde vært på handelsmesser tidligere samme dag, og at kontoen i denne forbindelse kunne ha blitt «hacket». Flertallet mente avsenderadressen ikke var troverdig, og at det heller ikke ga mening at sperringen kunne oppheves ved å følge en lenke, uten at kunden forsikret seg om at det var foretatt uautoriserte transaksjoner først. Nemnda uttalte at

> «[n]år budskapet i en e-post om mottakerens bankkonto ikke har en god forklaring og et fornuftig innhold, må mottakeren kontrollere hvem som er avsender før han følger en lenke og gir fra seg kort- og sikkerhetsopplysninger».

I kombinasjon med at slik svindel etter flertallets oppfatning er «allment kjent», noe som er en høyst usikker påstand fra Finansklagenemnda, ble dette ansett som grovt uaktsomt. Mindretallet påpekte imidlertid at e-posten var profesjonelt utformet, og at avsenderadressen var troverdig. Dette, sett i sammenheng med at kunden hadde vært på handelsmesser, medførte etter mindretallets syn at kunden hadde mindre grunn til å reagere på e-posten, og mente at dette ikke kunne utgjøre grov uaktsomhet.[76]

Sakene viser at Finansklagenemnda i mindre grad er villig til å legge vekt på konkrete forhold ved den enkelte henvendelsen som kan medføre at kunden ikke har grunn til å reagere, hvor den vektlegger at phishing er en kjent svindelmetode, og selve budskapet i henvendelsen. Dette var også tilfellet i FinKN-2019-681, hvor kunden ifølge flertallet handlet grovt uaktsomt da han fulgte en lenke hvor det fremgikk at vedkommende hadde bestilt ekstra lagringsplass til sin mobiltelefon, en tjeneste kunden hadde brukt før. I denne saken er mindretallets bemerkninger av særlig interesse, ettersom de uttrykkelig fremhevet at til tross for generelle advarsler fremsto slik svindel som et utbredt og omfattende problem, og at «denne type kriminalitet ikke enkel å komme til livs». Med henvisning til rapporter fra Økokrim fremhevet mindretallet at det ligger i dagen at begrunnelsen er manglende kunnskap hos næringsdrivende og særlig privatpersoner. Dette er et sentralt poeng, som må ha stor betydning for aktsomhetsvurderingen ved denne typen svindel. Det er en grense for hvor mange slike saker Finansklagenemnda kan behandle samtidig som den opprettholder det standpunkt at kunden i det store flertallet av sakene har handlet grovt uaktsomt. Mindretallet vektla i denne saken at kundens

oppmerksomhet naturlig vil senkes når avsender tilsynelatende er kjent, og henvendelsen for øvrig fremsto autentisk.[77]

Nemndas begrunnelse i lignende saker bygger hovedsakelig på en kombinasjon av at den anser det som allment kjent at slik svindel skjer, og at det foreligger elementer ved den enkelte melding som er egnet til å skape tvil om den er reell.[78] Som jeg vil komme tilbake til lenger ned, er disse avgjørelsene neppe uttrykk for gjeldende rett.

At phishing er en svindelmetode som mange personer faller for, ble tatt opp i FinKN-2018-46, men nemnda valgte å avvise saken fra nærmere behandling. Nemnda påpeker at den har erfart at BankID som innloggingsverktøy brukes av flere aktører enn forutsatt i tidligere saker, som etter nemndas syn gjør det mindre påfallende og mindre mistenkelig å bli anmodet om å logge inn med BankID. Videre påpekes det at dette kan skape inntrykk av at det er trygt å følge lenker for så å taste innloggingsinformasjon, som igjen har innvirkning på skyldvurderingen. Tilsvarende synspunkter er fremhevet av Finanstilsynet, hvor kombinasjonen av den utstrakte bruken av BankID og variasjoner i innloggingskontekst medfører en «slitasje» på BankID og kundens kritiske sans.[79]

I de tilfellene nemnda har konkludert med at det ikke foreligger grov uaktsomhet, har dette vært begrunnet i sakenes spesielle omstendigheter. Eksempelvis ble kunden i FinKN-2018-311 gjennom e-post angivelig kontaktet av kortutsteder og ble bedt om å oppgi opplysninger for å fjerne sperren fra et bankkort. Kunden ble deretter utsatt for svindel. I dette tilfellet hadde imidlertid kunden i forkant selv forsøkt å sperre kortet, men fikk ikke kontakt med betalingstjenesteyteren. Nemnda mente at dette utgjorde såpass spesielle omstendigheter at kunden ikke kunne anses å ha handlet grovt uaktsomt.[80]

Disse sakene utgjør imidlertid unntaket fra Finansklagenemndas nokså strenge praksis. Nyere uttalelser fra 2021 og 2022 kan imidlertid tas til inntekt for at Finansklagenemnda er i ferd med å endre kurs og i større grad konkluderer med at kunden ikke har handlet grovt uaktsomt, noe FinKN-2021-788 er et eksempel på. Her hadde klageren mottatt en e-post som angivelig kom fra portalen *Jobbnorge*, med invitasjon til jobbintervju. For å bekrefte intervjuet måtte klageren følge en lenke og logge inn med BankID. Klageren fulgte lenken, med den følge at det ble gjennomført en transaksjon på 27 000 kroner. Nemnda vurderte at klageren ikke hadde handlet grovt uaktsomt, ettersom «saken skiller seg fra det som tidligere har vært vanlig i saker om phishing ved at svindleren har lyktes i å komme inn i en pågående prosess mellom klageren og den aktøren som den falske e-posten angivelig kommer fra».[81]

I FinKN-2021-1110 var tilfellet det at kunden ventet en pakke fra utlandet, men ble svindlet etter å ha fulgt en e-postlenke som angivelig var fra Posten. Nemndas flertall kom til at kunden ikke hadde handlet grovt uaktsomt. Selv om det var sider ved e-postens innhold og språkføring som var egnet til å vekke mistanke, var ikke dette nok for flertallet til å konkludere med at kunden hadde handlet grovt uaktsomt. Tilsvarende konkluderte nemndas flertall i en lignende sak i FinKN-2022-240, begrunnet med at det ikke er grovt uaktsomt «å unnlate å holde musepekeren over avsenderfeltet for å få frem den virkelige avsenderen». Denne linjen ble imidlertid ikke fulgt i FinKN-2022-242, der klager mottok en e-post som informerte om at det lå en pakke og ventet på henne, og at hun måtte betale 27 kroner for å få den tilsendt. Kunden ble deretter svindlet for i overkant av 10 000 kroner. Nemnda konkluderte med at kunden hadde handlet grovt uaktsomt, ettersom avsenderadressen tilsynelatende var fra Digipost og ikke Posten, e-posten bar preg av dårlig språkføring, og betalingsfristen på 13 dager var lengre enn leveringstiden for pakken, som skulle leveres innen 24 timer. Dette viser at konkrete forhold ved den enkelte e-posten fortsatt tillegges avgjørende vekt, selv om kunden skulle vente en tjeneste av nettopp den karakter e-posten omtaler.

I en sak fra mars 2023, FinKN-2023-188, kan det imidlertid se ut til at nemnda har senket terskelen for hva som anses som grovt uaktsomt, ytterligere. Saken gjaldt en e-post som utga seg for å være fra Skatteetaten. E-posten hadde synlig avsenderadresse: «yognuhiste@vusra.com». Nemndas flertall kom til at kunden ikke hadde opptrådt grovt uaktsomt, og uttalte i den forbindelse:

> «Flertallet er enig med foretaket i at teksten i e-posten er formulert lite profesjonelt. Flertallet mener likevel at teksten ikke er så uprofesjonell at den uten videre måtte vekke mistanke. Avsenderadressen for e-posten er lite troverdig for en e-post fra Skatteetaten. Flertallet ser det slik at en mottaker av e-post ikke nødvendigvis henger seg opp i avsenderadressen når e-posten i seg selv ikke fremstår som utroverdig.»

Nemnda har med dette beveget seg langt fra utgangspunktet som ble slått fast i de første sakene i 2017 og 2018 om at det selv i tilfeller der det er vanskelig eller umulig å se at e-posten ikke er ekte, likevel er grovt uaktsomt å «la seg svindle».

Til sammenligning kan praksis fra andre EU-land belyse hvordan de tilsvarende reglene er tolket i disse landenes respektive nasjonale lovgivning.[82] Vi kan eksempelvis se hen til Danmark og Storbritannia, som begge har implementert PSD 2 i nasjonal rett.[83] Sammenlignet med praksis fra disse landene virker tidligere praksis i Norge å følge en strengere aktsomhetsnorm i lignende saker. Nyere praksis er derimot mer på linje med slik reglene er anvendt i Storbritannia og Danmark.

Det finansielle ankenævn i Danmark konkluderte i sak 290/2018 at kunden ikke hadde handlet grovt uaktsomt. Kunden hadde fått en e-post hvor det fremgikk at vedkommendes konto ville bli belastet hvis ikke en betalingstransaksjon ble avbrutt. Kunden trykket på lenken og oppga informasjon som gjorde det mulig for svindlerne å belaste kundens konto. Ankenævnet konkluderte med at kunden ikke hadde handlet grovt uaktsomt, ettersom henvendelsen samlet sett fremsto som troverdig. Dette var tilstrekkelig for ikke å anse handlingen som grovt uaktsom.

Heller ikke i Storbritannia konkluderer The Financial Ombudsman Service med grov uaktsomhet i lignende saker. I sak DRN-4082740 (22. desember 2020) hadde kunden fått en e-post hvor det fremgikk at kundens konto hadde blitt sperret. Kunden hadde nylig gjennomført en betalingstransaksjon og trodde sperringen hadde sammenheng med dette. Kunden ble svindlet etter at han oppga sikkerhetsinformasjon på en narreside. The Financial Ombudsman la vekt på at e-posten fremsto som troverdig, og at kunden av den grunn ikke hadde grunn til å reagere. Ettersom e-posten og nettsiden kunden ble dirigert til, var overbevisende, kunne ikke kunden anses å ha handlet grovt uaktsomt.

Det samme ble resultatet i sak DRN-4139348 (2. juli 2020). Kunden hadde fått en e-post som ba ham verifisere e-posten sin ved opprettelsen av en betalingskonto og var identisk med e-posten som kunden tidligere hadde fått fra betalingstjenesteyteren. Ved å følge lenken i e-posten ga kunden svindleren tilgang til kontoen. Utgangspunktet for vurderingen var om kundens handlinger «fell so far below the standard of a reasonable person» at det utgjorde grov uaktsomhet. Det slås uttrykkelig fast at det å dele sikkerhetsinformasjon ved slik svindel ikke alene kan utgjøre grov uaktsomhet. Ettersom både e-posten og narresiden fremsto troverdig, kunne ikke kundens handlinger anses å utgjøre et markert avvik fra vanlig forsvarlig handlemåte. Det er avsagt en rekke avgjørelser hvor The Financial Ombudsman Service har kommet til samme resultat.[84] Praksisen viser at de ikke anser det som grovt uaktsomt å falle for velgjennomført og profesjonell phishing.

Gjennomgangen viser at nemndspraksis i Norge har gått nokså langt i å definere aktsomhetsnormen etter hvordan en idealkunde ville handlet, og dermed ikke har forholdt seg til utgangspunktet i Rt-2004-499 om at det er de kvalifisert klanderverdige tilfellene som faller under betegnelsen «grovt uaktsomme» pliktbrudd. Finansklagenemnda har ansett det tilstrekkelig for grov uaktsomhet at kunden har latt seg lure til å trykke på en lenke og oppgi innloggingsinformasjon, uten nærmere drøftelse av kundens forutsetninger for å avdekke om det er tale om reell henvendelse eller konkrete omstendigheter i saken.

Kun unntaksvis og under helt spesielle omstendigheter har nemnda konkludert med at kunden ikke har handlet grovt uaktsomt. I lys av hvordan terskelen for grov uaktsomhet er tolket og anvendt av Høyesterett, kan nemndas praksis hva angår phishing, etter min oppfatning ikke anses som uttrykk for en riktig vurdering av aktsomhetsterskelen. Særlig i tilfeller der henvendelsen fremstår som ekte, har det i liten grad funnet sted en vurdering av kundens bebreidelse. At kunden ikke oppfatter en slik henvendelse som et svindelforsøk, er desto mer unnskyldelig, ettersom offentlige og private aktører sender lignende henvendelser til sine kunder.

Nyere praksis, og særlig saken fra mars 2023, tyder imidlertid på et ytterligere taktskifte fra flertallet i nemnda. Etter min mening er denne saken i bedre samsvar med gjeldende rett. I skrivende stund er det ikke avklart om banken vil følge uttalelsen.[85]

7.4 Kan det være grovt uaktsomt å bli lurt til å oppgi sikkerhetsinformasjon muntlig til tredjepersoner?

I forlengelse av punktet ovenfor om phishing-svindel er det også relevant å spørre om det å falle for såkalt *vishing*-svindel er grovt uaktsomt. Som forklart innledningsvis er dette en særlig form for *phishing* der

svindleren tar telefonisk kontakt med offeret. I Norge omtales dette gjerne som «Olga-svindel», ettersom ofrene for slik svindel ofte er eldre personer.

Disse sakene har som regel omhandlet grensen mellom grov uaktsomhet og forsett. Det vil si at kunden har akseptert å ha handlet grovt uaktsomt, men bestrider at pliktbruddet var forsettlig.[86] Finansklagenemnda har i slike saker hovedsakelig konkludert med at kunden ikke har handlet forsettlig, ettersom kunden har vært i unnskyldelig rettsvillfarelse.[87]

Høyesterett har ved ett tilfelle avgjort en sak som omhandler Olga-svindel. I HR-2022-1752-A ble en kunde i en telefonsamtale, som angivelig var med kundens bank, lurt til å oppgi personlig sikkerhetsinformasjon knyttet til kundens BankID. Kundens konto ble deretter belastet for 240 336. Partene var enige om at kunden hadde handlet grovt uaktsomt; spørsmålet var om kunden hadde handlet *forsettlig*, jf. finansavtaleloven (1999) § 35 tredje ledd. Ettersom finansavtaleloven (1999) § 35 tredje ledd måtte forstås slik at «kunden må ha vore medviten om pliktbrotet for å kunne bli ramma» av bestemmelsen, og dette ikke var tilfellet i denne saken, konkluderte Høyesterett med at kunden ikke hadde handlet forsettlig.[88]

Hvorvidt kunden har handlet grovt uaktsomt i slike tilfeller, må underlegges de samme vurderinger som ved phishing-svindel som skjer ved bruk av e-post, sms eller lignende, se nærmere om dette i punkt 7.3. Som for phishing-svindel påvirkes skyldvurderingen av de faktiske omstendighetene i det konkrete tilfellet. Det er først og fremst nærliggende å trekke frem om svindleren utgir seg for å være en aktør som det er vanlig å oppgi personlig sikkerhetsinformasjon til. Eksempelvis vil det være mindre betenkelig å oppgi personlig sikkerhetsinformasjon til sin egen bank, ettersom det for den alminnelige bankkunde vil fremstå som usannsynlig at ens egen bank vil svindle dem.[89] På den annen side kan det være mer betenkelig å oppgi slik informasjon til andre aktører hvor det ikke er vanlig å gi slik informasjon – eksempelvis aktører som utgir seg for å være «tech-support».

Det kan være svært vanskelig å avsløre at en henvendelse ikke er reell. Et nummersøk vil ikke nødvendigvis hjelpe kunden, ettersom svindlere ved såkalt *spoofing* kan manipulere nummeret som ringer, slik at det fremstår som et annet. Dette kan tvert imot styrke kundens tro om at henvendelsen er reell. Henvendelsens innhold vil da være sentralt ved skyldvurderingen. Dersom svindleren utgir seg for å være kundens bank, er dette ofte for å lure kunden til å tro at et lån blir utbetalt. Under det tidspresset kunden opplever, kan det fremstå rasjonelt at passord til BankID og engangskode oppgis for å få stanset utbetalingen av lånet. Slik som ved alminnelig innlogging i nettbanken, har dette karakter av å være en måte å identifisere seg overfor banken på.

Dersom kunden imidlertid oppgir informasjonen flere ganger, vil det gi en sterkere indikasjon på at det er tale om svindel. Etter omstendighetene vil antallet ganger det bes om at passord og engangskode oppgis, kunne være avgjørende for om pliktbruddet kategoriseres som grovt uaktsomt. Samtidig kan det i seg selv være en indikasjon på at det er tale om potensiell svindel, at kunden må oppgi betalingsinformasjon over telefon, ettersom det å oppgi denne informasjonen til en tredjeperson over telefon, ikke ligger innenfor det alminnelige bruksområdet til verken BankID eller betalingskort.

Dersom kontakten fremstår som om den er fra en reell aktør, og det ikke foreligger grunn til å reagere på innholdet i henvendelsen utover det faktum at svindleren har tatt kontakt over telefon, kan kunder utsatt for vishing-svindel ut fra omstendighetene ikke nødvendigvis sies å ha handlet grovt uaktsomt. Bærende for skyldvurderingen er den faktiske villfarelsen kunden er i under kontakten med svindleren.[90]

Det å uten videre akseptere at man har handlet grovt uaktsomt, er ikke heldig for kunden – selv om en reduksjon av ansvaret fra eksempelvis 240 336 til 12 000 kroner isolert sett er å regne som en «seier». Man skal imidlertid ikke undervurdere viktigheten av å rubrisere det enkelte svindeltilfellet under «riktig» skyldform. For det første kan dette danne presedens for hva som utgjør grov uaktsomhet, uten at det i realiteten skjer en skyldvurdering, også for andre former for svindel eller nye former for svindel. På denne måten legges mer av ansvaret på kunden, uten at pliktbruddet nødvendigvis faktisk utgjør grov uaktsomhet. For det andre kan dette medføre at tvistetemaet ofte vil være hvorvidt kunden har handlet forsettlig, ettersom kunden uansett har akseptert å ha handlet grovt uaktsomt. Slik kan grensen mellom grov uaktsomhet og forsett bli mer uklar ved nye og uprøvde former for svindel, selv om dette i prinsippet ikke skal ha betydning for vurderingen av hva som utgjør et forsettlig pliktbrudd.

8 Oppsummering og noen rettspolitiske betraktninger

Sikre og trygge betalingstjenester er en forutsetning for et velfungerende betalingstjenestemarked, og et av de sentrale formålene med PSD 2 er å sørge for at forbrukere er tilstrekkelig beskyttet mot den økende risikoen elektroniske betalingsløsninger medfører.[91] Av den grunn må også ansvarsfordelingen mellom betalingstjenesteyteren og kunden innebære at tilliten til slike betalingsløsninger styrkes. EU-kommisjonen har understreket at det digitale indre markedet skal sikre EU-borgere samme sikkerhetsnivå og de samme forventninger som i hverdagen utenfor den digitale verden.[92] Praktiseringen av skyldreglene, i kombinasjon med de sofistikerte svindelmetodene som utnytter svakheter ved digitale betalingstjenester, er egnet til å skape tvil om at det oppleves like trygt å ferdes digitalt som analogt.

Svindel er ikke et nytt fenomen. Kundens betalingsinstrument og kode kan stjeles, og signaturer kan forfalskes. I de sistnevnte tilfellene er imidlertid kunden beskyttet av de ulovfestede avtalerettslige reglene om falsk, som utgjør en sterk ugyldighetsgrunn. Kunden kan da som utgangspunkt ikke holdes ansvarlig for det økonomiske tapet. Av den grunn kan det også hevdes at digitaliseringen av betalingstjenester har medført et skifte i hvordan risikoen fordeles mellom kunden og betalingstjenesteyteren når svindel har funnet sted.[93] Finansavtaleloven (2020) endrer ikke risikofordelingen som sådan, utover at kunden holdes ansvarlig for en objektiv egenandel som er mindre enn etter finansavtaleloven (1999). Ved tredjepersons misbruk av betalingskort og tilhørende kode tyder etterfølgende nemndspraksis på at terskelen for grov uaktsomhet stort sett har blitt praktisert på linje med Høyesteretts forutsetninger i Rt-2004-499. Enkeltavgjørelser viser at nemnda har lagt terskelen for grovt uaktsomme pliktbrudd høyere enn det tilsynelatende er grunnlag for, hvor begrunnelsen for at det foreligger grov uaktsomhet, både er utilstrekkelig og mangelfull. Enkeltavgjørelser fra Finansklagenemnda har imidlertid svært begrenset rettskildeverdi.

Særlig når det gjelder phishing, etablerte Finansklagenemnda over flere år en linje hvor terskelen for grov uaktsomhet ble satt såpass lavt at kunden nærmest ble holdt objektivt ansvarlig for en egenandel på 12 000 kroner dersom kunden hadde falt for slik svindel. Dette kan neppe anses å være i overensstemmelse med den terskelen for grov uaktsomhet som Høyesterett har trukket opp, selv om det i nyere praksis er en viss antydning til oppmykning av praksisen. Etter min oppfatning har kunden i nemndspraksis blitt målt etter hvordan en idealkunde hadde handlet, noe Høyesterett nettopp avfeier skal være målestokken for grov uaktsomhet. Omfanget av praksisen viser at den alminnelige bankkunde i mange tilfeller lar seg lure av disse målrettede og profesjonelle svindelforsøkene. Sett i sammenheng med at nemnda selv innrømmer at både offentlige og private aktører sender e-poster der privatpersoner bes om å oppgi BankID-passord, er det svært strengt når kunden har blitt holdt ansvarlig for grovt uaktsomme pliktbrudd når meldingen ellers med ganske høy grad av presisjon illuderer en reell henvendelse. En helt fersk avgjørelse fra mars 2023 synes å innebære et taktskifte.

Om Finansklagenemnda hittil har ansett egenandelen etter finansavtaleloven (1999) på 1200 kroner som for lav og av den grunn konkludert med grov uaktsomhet i mange av phishing-sakene, vil dette medføre en tilsidesettelse av lovgivers intensjon der nemnda egenhendig og ubegrunnet har utvidet kundens egenandel til 12 000 kroner.

Ettersom tvistesummen i disse sakene er begrenset til 12 000 kroner, er domstolene lite tilgjengelige. Å føre en sak for domstolene er en kostbar prosess, og omkostningene vil nesten uten unntak overgå tvistesummen, idet kunden risikerer å sitte igjen med regningen for både sin egen og motpartens advokat i tillegg til egenandelen. Dette gjør det problematisk å få disse sakene inn til behandling i domstolene. Finansklagenemnda blir av den grunn det eneste reelle tvisteløsningsorganet i det store flertallet av disse sakene. Det er derfor gledelig at nemnda nå kan se ut til å ha realitetsorientert seg både med tanke på de rettslige utgangspunktene for fastleggelse av terskelen for grov uaktsomhet og hva man faktisk kan forvente av enkeltpersoner med tanke på å avdekke svindelforsøk.

Litteraturliste

Andenæs (2009) Andenæs, Mads Henry. *Rettskildelære*, 2. utg. Oslo: M.H. Andenæs, 2009.

DNB (2023) «Avtalevilkår for BankAxept/Visa/Mastercard betalingskort og andre kortbaserte betalingsinstrumenter (debet) – forbruker». Hentet 31. mars 2023 fra https://www.dnb.no/portalfront/nedlast/no/privat/avtaler-vilkaar/avtale-om_betalingskort.pdf.

DNB (u.å) «Avtale om BankID». Hentet 31. mars 2023 fra https://www.dnb.no/portalfront/nedlast/no/privat/avtaler-vilkaar/terms_and_conditions_for_bankid-dnb_no.pdf.

EU-kommisjonen (2015) EU-kommisjonen, «A digital single Market Strategy for Europe», SWD (2015) 100, s. 51.

European Payments Council (2021) European Payments Council. *2021 payment threats and fraud trends report.* Brussel, 2021. https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2021-12/EPC193-21%20v1.0%202021%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf [hentet 1. november 2022].

Finanstilsynet (2022) Finanstilsynet. *Risiko- og sårbarhetsanalyse (ROS) 2022*. Oslo: Finanstilsynet, 2022. https://www.finanstilsynet.no/contentassets/d6c5910b41044d1b89f7a50a7b7315db/ros-2022.pdf [hentet 25. juli 2022].

Finanstilsynet (2020) Finanstilsynet. *Risiko- og sårbarhetsanalyse (ROS) 2020*. Oslo: Finanstilsynet, 2020. https://www.finanstilsynet.no/contentassets/816cd5c4576a484ab41749a3ff985a69/risiko--og-sarbarhetsanalyse-2020.pdf [hentet 25. juli 2022].

Grøttjord og Rosén (2014) Grøttjord, Børge og Karl Rosén. *Finansavtaleloven: med kommentarer.* Oslo: Gyldendal, 2014.

Guimarães og Steennot (2022) Guimarães, Maria Raquel og Reinhard Steennot. «Allocation of liability in case of payment fraud: Who bears the risk of innovation: A comparison of Belgian and Portuguese law in the context of PSD2», *European Review of Private Law,* årg. 30, nr. 1 (2022), s. 29-72.

Hagstrøm og Stenvik (2019) Hagstrøm, Viggo og Are Stenvik. *Erstatningsrett*, 2. utg. Oslo: Universitetsforlaget, 2019.

Hagstrøm mfl. (2021) Viggo Hagstrøm. *Obligasjonsrett*, 3. utg. ved Herman Bruserud mfl. Oslo: Universitetsforlaget, 2021.

Kjelland (2019) Kjelland, Morten. *Erstatningsrett. En lærebok*, 2. utg. Oslo: Universitetsforlaget, 2019.

Kjørven (2020) Kjørven, Marte Eidsand. «Who pays when things go wrong? Online financial fraud and consumer protection in Scandinavia and Europe». *European Business Law Review,* årg. 31, nr. 1 (2020), s. 77-109.

Kjørven mfl. (2021) Kjørven, Marte Eidsand, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)», *Lov og Rett*, årg. 60, nr. 6 (2021), s. 335-366.

Nissen (2021) Nissen, Sofie Grønntun mfl., «Oslo kommune vil at de som ønsker vaksine, skal registrere seg digitalt. For mange kan det være en komplisert prosess». *Aftenposten*, 19. februar 2021, https://www.aftenposten.no/norge/i/dlkagw/oslo-kommune-vil-at-de-som-oensker-vaksine-skal-registrere-seg-digital [hentet 28. februar 2022].

NorSIS (2021) NorSIS. *Trusler og trender 2021.* Gjøvik: NorSIS, 2021, https://norsis.no/publikasjoner/ [hentet 4. november 2022].

Norland og Kjørven (2022) Norland, Line Utne og Marte Eidsand Kjørven, «Elektoniske signaturer og avtalebidning» i *Bruk og misbruk av elektronisk identifikasjon*. Marte Eidsand Kjørven, Maria Astrup Hjort og Tone Linn Wærstad red., Karnov forlag, 1. utg. 1. versjon (2022).

Torvund (1986) Torvund, Olav, «Betalingskort (‘Kredittkort’) – betalingsinstrumenter på uryddig grunn», *Lov og Rett*, årg. 25, nr. 6 (1986), s. 336-352.

Noter

1 Artikkelen er en omarbeidet versjon av min masteroppgave, som ble ferdigstilt våren 2021, og som ble til under verdifull veiledning fra professor Marte Eidsand Kjørven. Artikkelen er skrevet etter råd og innspill fra redaktørene, dyktige kollegaer i advokatfirma DLA Piper, fagfelle og venner. En stor takk til alle.

2 Finanstilsynet (2022) s. 35-39.

3 Finanstilsynet (2022) s. 35 flg.

4 European Payments Council (2021) s. 14 flg.

5 NorSIS (2021) s. 19.

6 Se for eksempel saksforholdet i HR-2022-1752-A og nærmere under punkt 7.4.

7 Lov 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag. Reglene i finansavtaleloven (1999) § 35 gjennomførte regler i PSD 2s forløper, direktiv 2007/64/EF (PSD 1).

8 Lov 21. juni 1985 nr. 82 om kredittkjøp m.m.

9 Torvund (1986) s. 350.

10 Ot.prp.nr.34 (1980–1981) s. 81.

11 Lov 18. desember 2020 nr. 146 om finansavtaler. Loven ble vedtatt i desember 2020 og trådte i kraft 1. januar 2023.

12 Direktivet er med virkning fra 1. mai 2022 inkorporert i EØS-avtalen, se EØS-komiteens beslutning nr. 165/2019 av 14. juni 2019 om endring av EØS-avtalens vedlegg IX (Finansielle tjenester).

13 Hva som utgjør et forsettlig pliktbrudd på kundens hånd, er grundig analysert av Kjørven, Woxholth og Høgberg og behandles ikke nærmere her. Se Kjørven mfl. (2021) s. 335-366.

14 Finansklagenemndas praksis har imidlertid svært begrenset rettskildeverdi. Selv om det er en relevant rettskilde, kan ikke avgjørelsene tillegges noe særlig vekt – selv der praksisen er konsekvent. Se Andenæs (2009) s. 98 og Hagstrøm mfl. (2021) s. 62.

15 Ot.prp.nr.94 (2008–2009) s. 128.

16 Uttrykket «betalingstransaksjon» er i § 1-5 sjette ledd definert som «en handling som iverksettes av betaleren eller på dennes vegne eller av betalingsmottakeren for å innbetale, overføre eller ta ut betalingsmidler ...», jf. også PSD 2 artikkel 4 nr. 5.

17 Tilsvarende PSD 2 artikkel 64.

18 DNB (2023). Avtalevilkårene kan variere fra bank til bank, men følger i stor grad samme standard.

19 DNB (u.å), etter standard fra BITS.

20 Se eksempelvis «Avtalevilkår for BankAxept/Visa/Mastercard betalingskort og andre kortbaserte betalingsinstrumenter (debet) – forbruker» fra DNB punkt 6 om bruk av betalingskort.

21 Prop.92 LS (2019–2020) s. 276, jf. s. 279.

22 Lov av 31. mai 1918 nr. 4 om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer.

23 En nærmere gjennomgang av dette faller utenfor artikkelens tema. Se nærmere i Norland og Kjørven (2022).

24 Tilsvarende PSD 2 artikkel 89.

25 Tilsvarende PSD 2 artikkel 88.

26 Kjørven (2020) s. 91.

27 Kjørven (2020) s. 90.

28 Se eksempelvis BKN-2010-151, som gjaldt fakturasvindel, hvor en betalingstransaksjon ble ansett som godkjent til tross for at en faktura fra en håndverker var blitt forfalsket. Banken kunne etter nemndas syn ikke klandres for ikke å ha kontrollert at angitt betalingsmottaker på fakturaen samsvarte med det oppgitte kontonummeret.

29 Tilsvarende PSD 2 artikkel 4 nr. 14.

30 Ot.prp.nr.94 (2008–2009) s. 118 og Ot.prp.nr.41 (1998–1999) s. 43.

31 Prop.92 LS (2019–2020) s. 117 og Ot.prp.nr.94 (2008–2009) s. 171.

32 Prop.92 LS (2019–2020) s. 175.

33 Se HR-2022-1752-A avsnitt 37, hvor Høyesterett beskriver tilsvarende fremgangsmåte for finansavtaleloven (1999) § 35 tredje ledd.

34 Prop.92 LS (2019–2020) s. 380.

35 Tilsvarende PSD 2 artikkel 4 nr. 31.

36 Prop.92 LS (2019–2020) s. 167 og HR-2022-1752-A avsnitt 30.

37 Ot.prp.nr.94 (2008–2009) s. 121 med videre henvisning til svenske forarbeider.

38 Se DNB (2023) punkt 5 og DNB (u.å) punkt 4.1.

39 Se Kjørven mfl. (2021) s. 338.

40 Se nærmere om kundens plikt til å beskytte sikkerhetsinformasjon i Kjørven mfl. (2021) s. 337 flg.

41 C-26/13*Kásler og Rábai mot OTP Jelzálogbank Zrt.* avsnitt 71.

42 C-26/13*Kásler og Rábai mot OTP Jelzálogbank Zrt.* avsnitt 74.

43 C-186/16*Andriciuc mfl. mot Banca Românească SA* avsnitt 47.

44 Grøttjord og Rosén (2014) s. 205.

45 Slik som i Rt-2004-499, se nærmere i punkt 7.2.

46 Se HR-2022-1752-A avsnitt 35-37.

47 Se nærmere om dette i Kjørven (2020) med videre henvisninger. Se også Kjørven mfl. (2021) s. 341 flg. om skyldvurderingen etter PSD 2.

48 Se Ot.prp.nr.94 (2008–2009) s. 117.

49 Se Hagstrøm mfl. (2021) s. 507, hvor det fremheves at grov uaktsomhet først foreligger når kontraktspartens opptreden er kvalifisert klanderverdig og foranlediger sterke bebreidelser for mangel på aktsomhet.

50 Innst.104 L (2020–2021) s. 22. Uttalelsene gjelder reglene om misbruk av elektronisk signatur, jf. § 3-20, men lovgiver har forutsatt lik forståelse av reglene om henholdsvis misbruk av elektronisk signatur og ikke godkjente betalingstransaksjoner. Merk ellers at det som er mindretallets uttalelser i komiteen, er det som senere ble vedtatt med flertall på Stortinget.

51 NOU 2008:21 s. 105.

52 Hagstrøm mfl. (2021) s. 491 og Hagstrøm og Stenvik (2019) s. 169.

53 Hagstrøm og Stenvik (2019) s. 171.

54 Hagstrøm og Stenvik (2019) s. 172.

55 Finanstilsynet (2020) s. 42.

56 Högsta domstolen, dom av 21. juni 2022, mål T 4623-21.

57 I Sverige graderes kundens skyld ut fra om vedkommende har handlet grovt uaktsomt («grovt vårdslöst»), der kundens ansvar er begrenset til 12 000 kroner, eller særskilt klanderverdig («särskilt klandervärt»), der kundens ansvar er ubegrenset. Har ikke kunden handlet grovt uaktsomt eller særskilt klanderverdig, er ansvaret begrenset til en egenandel på 400 kroner.

58 Et sentralt poeng her er at villfarelse om rettslige eller faktiske omstendigheter ikke alene kan begrunne at kunden har opptrådt grovt uaktsomt, ettersom dette er selvstendige ansvarsgrunnlag og ikke utmålingsregler. Spørsmålet aktualiseres særlig i de tilfellene der banken påstår at det foreligger et forsettlig pliktbrudd. Se nærmere om dette i Kjørven mfl. (2021) s. 351 flg.

59 HR-2020-2021-A avsnitt 57.

60 HR-2020-2021-A avsnitt 59.

61 HR-2020-2021-A avsnitt 58.

62 Kommisjonsforordningen er med virkning fra 1. mai 2022 inkorporert i EØS-avtalen, se EØS-komiteens beslutning nr. 159/2020 av 23. oktober 2020 om endring av EØS-avtalens vedlegg IX (Finansielle tjenester).

63 HR-2020-2012-A avsnitt 104.

64 Kjelland (2019) s. 97-98 og Hagstrøm mfl. (2021) s. 617.

65 Guimarães og Steennot (2022) s. 69-70.

66 Guimarães og Steennot (2022) s. 71-72.

67 NorSIS (2021) s. 12-13.

68 Se eksempelvis TOSLO-2018-180834, TFRED-2019-63291 og TSOFT-2017-175325 (hvorav de to sistnevnte gjaldt misbruk av elektronisk signatur).

69 Rt-2004-499 avsnitt 32.

70 Eksempelvis FinKN-2022-324, FinKN-2020-230, FinKN-2020-52 og FinKN 2017-580.

71 Eksempelvis FinKN-2013-276, hvor nemnda konkluderte med at det ikke var grovt uaktsomt å oppbevare kort og kode i eget hjem, selv om koden var notert i klartekst.

72 Nissen (2021).

73 Rt-2004-499 avsnitt 36.

74 Kjørven (2020) s. 93 og Finanstilsynet (2022) s. 32.

75 FinKN-2017-506.

76 Tilsvarende i FinKN-2022-54, som gjaldt et lignende forhold.

77 Tilsvarende i FinKN-2019-683.

78 Se eksempelvis FinKN-2019-565, FinKN-2019-40, FinKN-2018-530 og FinKN-2017-649.

79 Finanstilsynet (2022) s. 31.

80 Tilsvarende i FinKN-2019-336 og FinKN-2019-338.

81 Tilsvarende i FinKN-2021-1086.

82 Se Kjørven (2020) s. 13 flg. for en mer inngående komparativ analyse av praksis fra de skandinaviske landene.

83 Storbritannia er fra 1. januar 2021 ikke lenger medlem av EU, men avgjørelsene som brukes, er avsagt før dette.

84 Se eksempelvis DRN-2174713 (15. september 2020), DRN-5688949 (26. april 2019) og DRN-4773354 (21. desember 2018).

85 Uttalelser fra Finansklagenemnda er kun veiledende og har ikke bindende virkning.

86 Se eksempelvis HR-2022-1752-A avsnitt 33.

87 Se nærmere i Kjørven mfl. (2021) s. 348. flg, Også nyere praksis fra Finansklagenemnda har fulgt samme argumentasjonslinje, se eksempelvis FinKN-2022-233, FinKN-2022-198 og FinKN-2022-197. Alle avgjørelsene er fra før HR-2022-1752-A, men avgjørelsene viser til lagmannsrettens dom i samme sak som på tidspunktet ikke var rettskraftig.

88 HR-2022-1751-A avsnitt 50.

89 Se Kjørven mfl. (2021) s. 339 flg., hvor det gjøres nærmere rede for tolkningen av kundens avtalefestede plikt til ikke å oppgi personlig sikkerhetsinformasjon til uvedkommende, herunder banken eller politiet, og hvordan dette bør forstås ved skyldvurderingen.

90 Se Kjørven mfl. (2021) s. 351 flg. for en nærmere gjennomgang av betydningen av faktisk og rettslig villfarelse.

91 Fortalen punkt 7.

92 EU-kommisjonen (2015) s. 51.

93 Kjørven (2020) s. 104.

Kontraheringsplikt for tilbydere av eID – særlig om forholdet mellom kontraheringsplikt og diskrimineringsvernet

Erle Katrine Sivertsen

Fagfellevurdert artikkel

1 Innledning

Elektronisk identifikasjonsbevis (eID) brukes til å identifisere personer elektronisk. I Norge er den mest brukte eID-ordningen BankID.[1] Per i dag finnes det totalt fire eID-ordninger i Norge: den statlige eID-ordningen MinID, som er klarert til sikkerhetsnivå «betydelig», og de tre private eID-ordningene BankID, Buypass og Commfides, som er klarert til sikkerhetsnivå «høyt».[2] Å ha en eID er en nødvendig forutsetning for å kunne bruke digitale tjenester som krever bekreftelse av brukerens identitet. Derfor er det et uttalt mål fra norske myndigheters side at alle som deltar i det norske samfunnet, skal ha mulighet til å anskaffe eID på det sikkerhetsnivået de har behov for.[3] Samtidig viser en områdegjennomgang av ID-forvaltningen at det er flere brukergrupper som ikke har mulighet til å få eID på øverste sikkerhetsnivå i dagens system.[4] Dette er problematisk når en rekke sentrale offentlige og private tjenester krever innlogging med eID på øverste sikkerhetsnivå.[5]

Tall fra Digitaliseringsdirektoratet viser at i 2021 hadde totalt 21 prosent av de offentlige tjenestene som hadde krav om innlogging med eID, krav om eID på øverste sikkerhetsnivå.[6] Å ha eID på øverste sikkerhetsnivå er med andre ord helt nødvendig for å kunne være en fullverdig digital borger i Norge. Likevel er det som nevnt bare private aktører som tilbyr eID på øverste sikkerhetsnivå i Norge i dag. Det oppstår derfor spørsmål om i hvilken grad de private aktørene er forpliktet til å utstede eID til alle som måtte ønske det.

Enkelte private aktører som tilbyr et nødvendig gode til allmennheten, kan pålegges en plikt til å slutte avtale med en annen – en *kontraheringsplikt*.[7] I denne artikkelen skal jeg derfor undersøke om tilbydere av eID har en kontraheringsplikt, og i så fall i hvilken utstrekning en slik privatrettslig kontraheringsplikt vil kunne avhjelpe problemene borgerne har knyttet til anskaffelse av eID på øverste sikkerhetsnivå.

En kontraheringsplikt kan være total eller partiell. En total kontraheringsplikt er en ubetinget ytelsesplikt.[8] Ved partiell kontraheringsplikt vil det derimot være adgang til å nekte å slutte avtale så fremt det foreligger «saklig grunn» til kontraheringsnektelse.[9] En absolutt ytelsesplikt er inngripende for tilbyderen og pålegges derfor kun i særskilte tilfeller. Et eksempel er apotekenes plikt til å levere medisiner som behøves straks, til tross for manglende betaling og sikkerhet.[10] I vårt tilfelle er det imidlertid tale om en tjeneste som tilbys av private aktører, uten at aktørene er pålagt noen krav fra offentlige myndigheter knyttet til utstedelse. Det er dermed andre, motstående hensyn som gjør seg gjeldende, blant annet forretningsmessige hensyn. For tilbydere av eID er det derfor et spørsmål om partiell kontraheringsplikt.

En eventuell kontraheringsplikt for tilbydere av eID vil altså ikke ha en ubegrenset rekkevidde; tilbyderne vil ha adgang til å nekte utstedelse dersom det foreligger «saklig grunn». Hvorvidt det foreligger «saklig grunn» til kontraheringsnektelse, vil kunne påvirkes av tilbydernes øvrige forpliktelser.[11] Derfor vil jeg undersøke forholdet mellom kontraheringsplikten og lovbestemte krav for tilbydere av eID, herunder vurdere om de lovbestemte kravene påvirker tilbydernes adgang til å nekte å inngå avtale om utstedelse av eID. I tillegg kan kravet om «saklig grunn» medføre at kontraheringsplikten får en side mot diskrimineringsforbudet, som er et forbud mot usaklig forskjellsbehandling.[12] En annen underproblemstilling som skal undersøkes, er derfor

forholdet mellom kontraheringsplikten og diskrimineringsforbudet. Det skal følgelig vurderes hvorvidt tilbydernes forpliktelser etter diskrimineringsforbudet fører til begrensninger i adgangen til kontraheringsnektelse.[13]

Rettskildebildet knyttet til eID-tilbyderes kontraheringsplikt og rekkevidden av denne er sammensatt. De avtalerettslige rettskildene gir lite veiledning for rekkevidden av en partiell kontraheringsplikt utover at kontraheringsnektelse er tillatt når det foreligger «saklig grunn». Ved å undersøke kontraheringsplikten opp mot noen av tilbydernes øvrige forpliktelser som kan påvirke utstedelse av eID, vil det imidlertid være mulig å etablere retningslinjer for den konkrete vurderingen av kontraheringspliktens rekkevidde. Ettersom «saklig grunn» er en rettslig standard, er det videre ikke mulig å gi en uttømmende fremstilling av innholdet i en artikkel. Som metodisk grep har jeg derfor valgt ut noen av grunnlagene tilbyderne påberoper seg ved avvisning av de ulike brukergruppene, som typetilfeller.

I punkt 2 vil jeg presentere generelle utgangspunkter for eID-tilbyderes kontraheringsplikt. Jeg vil først vurdere hvorvidt det er rettslig grunnlag for en slik kontraheringsplikt (punkt 2.1). Deretter vil jeg vurdere forholdet mellom kontraheringsplikten og tilbydernes lovbestemte forpliktelser (punkt 2.2). Jeg vil så vurdere forholdet mellom kontraheringsplikten og diskrimineringsforbudet (punkt 2.3). Deretter vil jeg foreta konkrete vurderinger av om tilbyderne har «saklig grunn» til kontraheringsnektelse i seks utvalgte typetilfeller (punkt 3). Til slutt vil jeg oppsummere og vurdere funnene i et rettspolitisk perspektiv (punkt 4).

2 Generelt om kontraheringsplikt for tilbydere av eID

2.1 Rettslig grunnlag for kontraheringsplikt

Det første spørsmålet som skal vurderes, er hvorvidt det er rettslig grunnlag for å pålegge tilbyderne kontraheringsplikt for utstedelse av eID. Kontraheringsplikt pålegges ofte den som tilbyr et nødvendig gode til allmennheten. Det gjelder derfor en *lovfestet* kontraheringsplikt for blant annet apoteker, tilbydere av forsikring og tilbydere av grunnleggende banktjenester.[14] Å ha eID på øverste sikkerhetsnivå er en forutsetning for å få digital tilgang til viktige offentlige og private tjenester i Norge. Selv om det i stor grad finnes alternative analoge løsninger, er disse ofte langt mer tungvinte. For eksempel måtte personer uten eID på øverste sikkerhetsnivå under koronapandemien bestille koronasertifikat i papirformat fordi de ikke hadde tilgang til Helsenorge.no. Dette koronasertifikatet var bare gyldig i 90 dager, mens det digitale koronasertifikatet ble oppdatert automatisk.[15] Dette er bare ett av mange eksempler som illustrerer at manglende eID på øverste sikkerhetsnivå fører til digital ekskludering. Det er klart at eID på øverste sikkerhetsnivå er et nødvendig gode. Det er derfor nødvendig å vurdere hvorvidt det gjelder en *ulovfestet* kontraheringsplikt for tilbydere av eID på øverste sikkerhetsnivå.

At det kan eksistere en ulovfestet kontraheringsplikt i konkrete tilfeller, er lagt til grunn av Høyesterett i Rt-2014-36. Dommen gjaldt rett til ferdsel i alpinanlegg for kommersielle skiskoler og rett til bruk av heisanlegget for skiskolens medarbeidere. Det første spørsmålet var hvorvidt man kan drive skiskole i et alpinsenters anlegg på grunnlag av allmennhetens ferdselsrett etter friluftsloven. I dommen kom Høyesterett til at et alpinsenter måtte la en person drive sin skiskolevirksomhet på alpinanleggets utmarksområder og innmarksområder undergitt vinterferdselsrett, men at bruk av heisanlegget falt utenfor allemannsretten. Det neste spørsmålet var derfor om alpinsenteret kunne nekte skiskolen adgang til å bruke heisanlegget på samme vilkår som det øvrige publikum. Skiskolen anførte i den forbindelse at alpinsenteret hadde plikt til å la skiskolen bruke heisanlegget til vanlig forbrukerpris i kraft av alminnelige obligasjonsrettslige prinsipper om kontraheringsplikt. I tilknytning til denne anførselen uttaler førstvoterende i avsnitt 81:

> «*Når man tilbyr en standardisert tjeneste til allmennheten, slik skiheiser er, må det riktignok gjelde et saklighetskrav ved differensiering mellom kundegrupper*. På samme måte som man kan variere prisen for heiskort på grunnlag av alder eller for hvor lang tid heisene skal brukes, må det imidlertid også være mulig å kreve at den som benytter heisene til egen næringsvirksomhet, skal betale mer enn forbrukerkundene.» (Min kursivering.)

Høyesterett kommenterte ikke eksplisitt skiskolens anførsel om at det gjelder et alminnelig obligasjonsrettslig prinsipp om kontraheringsplikt. At det gjelder en kontraheringsplikt for standardiserte tjenester som tilbys allmenheten, synes imidlertid å være forutsatt. Uttalelsen understreker at kontraheringsplikten ikke er til hinder

for at det stilles vilkår for kontrahering, og heller ikke for at disse vilkårene er forskjellige for ulike grupper, så fremt differensieringen har en saklig grunn. Alpinsenteret hadde dermed i utgangspunktet en plikt til å kontrahere, men kunne kreve ulik pris for de ulike kundegruppene. Skiskolens anførsel førte likevel ikke frem, ettersom skiskolen krevde tilgang til anlegget til forbrukerpris.

Grunnlaget for kontraheringsplikten i Rt-2014-36 var at alpinsenteret tilbød en «standardisert tjeneste til allmennheten». De ulike eID-ordningene som eksisterer i dag, er standardiserte tjenester som tilbys allmennheten. Det er generiske ytelser, og utgangspunktet i lovverket er at alle med et norsk fødselsnummer eller d-nummer kan be om å få utstedt eID.[16] Dette taler for at tilbydere av eID har en kontraheringsplikt på ulovfestet grunnlag.

Utover den ovennevnte høyesterettsdommen er det få autoritative rettskilder som berører spørsmålet om ulovfestet kontraheringsplikt. Tidligere gjaldt det klare regler om næringsdrivendes kontraheringsplikt. Etter den tidligere prisloven § 23 kunne forvaltningsorganet Prisrådet forby næringsdrivende å nekte forretningsforbindelse med en annen næringsdrivende eller forbruker hvis Prisrådet fant at «nektelsen vil skade almene interesser eller virke urimelig overfor den annen part».[17] Denne opphevede regelen har i ettertid blitt brukt som et argument i juridisk teori for at det nå gjelder en ulovfestet kontraheringsplikt.[18] Loven ble opphevet av konkurranseloven i 1993, uten at bestemmelsen om kontraheringsplikt ble videreført. I forarbeidene til konkurranseloven av 1993 drøftes spørsmålene rundt ordningen med Prisrådet. Den materielle regelen blir ikke uttrykkelig fraveket i forarbeidene, noe som kan tale for at lovgiver ikke har ment å oppheve den.[19] Dette taler igjen for at regelen om kontraheringsplikt fortsatt gjelder på ulovfestet grunnlag når nektelse vil skade allmenne interesser eller virke urimelig overfor forbrukeren.[20]

Videre ble det i juridisk teori på forsikringsrettens område tidligere hevdet at det gjaldt en kontraheringsplikt for forsikringsselskaper på ulovfestet grunnlag.[21] Denne kontraheringsplikten er i dag lovfestet, jf. forsikringsavtaleloven § 1B-3 første ledd. En av dem som argumenterte for at det gjaldt en ulovfestet kontraheringsplikt, var Trine-Lise Wilhelmsen. Wilhelmsen argumenterte for at særlig hensynet til likebehandling og at nektelse ville kunne medføre store økonomiske konsekvenser for den enkelte, talte for en kontraheringsplikt. Slik reglene var utformet, var det ikke grunnlag for å forby en individuell nektelse på grunn av tilfeldig forskjellsbehandling eller uforsvarlig risikovurdering. Videre argumenterte Wilhelmsen for at det var behov for sivilrettslige regler om urimelige kontraheringsvilkår, slik at avslag kunne bringes inn for domstolene eller Forsikringsskadenemnda.[22] I tillegg tilsa forholdet mellom kontraheringsnektelse, urimelige kontraheringsvilkår og urimelige avtalevilkår at det skulle oppstilles en regel om kontraheringsplikt, ettersom det kun var de urimelige avtalevilkårene som kunne angripes sivilrettslig ved avtaleloven § 36. På grunnlag av disse betraktningene argumenterte Wilhelmsen for at det måtte oppstilles et krav om at selskapenes kontraheringsnektelse og kontraheringsvilkår var saklig begrunnet og konsekvent.[23]

Mange av de samme argumentene som Wilhelmsen la vekt på da hun argumenterte for en ulovfestet kontraheringsplikt på forsikringsrettens område, gjør seg også gjeldende i vårt tilfelle. En kontraheringsplikt med krav om saklig begrunnelse for kontraheringsnektelse vil motvirke tilfeldige resultater og forhindre avvisning basert på usaklige forhold. Videre vil en kontraheringsplikt gjøre det mulig å bringe inn et avslag for domstolene og dermed få overprøvd grunnlaget for nektelsen. Urimelige avtalevilkår kan settes til side etter avtaleloven § 36, men denne bestemmelsen kommer først til anvendelse etter at avtale er inngått. I dette tilfellet står vi overfor en kontraheringsnektelse, slik at avtale nektes inngått. Det er dermed ikke grunnlag for en sivilrettslig kontroll av sakligheten av tilbydernes kontraheringsvilkår med mindre det eksisterer en ulovfestet kontraheringsplikt. Dette taler med styrke for at det gjelder en ulovfestet kontraheringsplikt for tilbydere av eID.

Et annet tilfelle hvor det ofte gjelder en kontraheringsplikt, er når tilbyder har konsesjon eller bevilling fra staten til å tilby en vare eller tjeneste.[24] Det er derfor nødvendig å vurdere hvorvidt systembetraktninger kan tale for at det gjelder en ulovfestet kontraheringsplikt for tilbydere av eID. Ved konsesjon er kontraheringsplikt ofte en forutsetning for konsesjonen, og kontraheringsplikten følger da av avtale eller lov. Som eksempel kan energiloven nevnes. Etter energiloven kreves det konsesjon for å bygge, eie eller drive elektriske anlegg.[25] Det følger av energiloven § 3-3 første ledd første punktum at den som er gitt områdekonsesjon etter § 3-2, «skal levere elektrisk energi til alle kunder innenfor det geografiske området konsesjonen gjelder for». Nettselskapene har en kontraheringsplikt fordi de har en konsesjon som gir dem en monopolstilling innenfor det geografiske området konsesjonen dekker.[26]

Gjennom dagens system – hvor staten krever eID på øverste sikkerhetsnivå for om lag 20 prosent av de digitale tjenestene som krever autentisering med eID, samtidig som staten ikke selv tilbyr eID på øverste sikkerhetsnivå – har staten overlatt en nødvendig samfunnsfunksjon til private tilbydere. Dette har likhetstrekk med tilfellene hvor staten krever konsesjon. Tilbyderne av eID tilbyr en tjeneste som er nødvendig for alle som deltar digitalt i det norske samfunnet. Videre eksisterer det ikke en tilsvarende tjeneste på samme sikkerhetsnivå fra det offentlige. Det er kun tre tilbydere av eID på øverste sikkerhetsnivå, og til sammen danner de et oligopol. Ved ordinære konsesjonstilfeller gjelder det en kontraheringsplikt fastsatt i lov eller avtale. Systembetraktninger, herunder at like tilfeller bør behandles likt, taler for at det også gjelder en kontraheringsplikt for tilbydere av eID.

Videre taler rimelighetshensyn for at det gjelder en ulovfestet kontraheringsplikt. En kontraheringsnektelse vil medføre at personen ikke har mulighet til å anskaffe eID på sikkerhetsnivå «høyt». Følgelig vil personen ikke ha tilgang til en rekke digitale tjenester tilbudt av både offentlige og private aktører. Kontraheringsnektelse medfører dermed stor ulempe for den enkelte. Videre er det fare for at de private tilbyderne legger seg på en strengere linje for i hvilke tilfeller de utsteder eID, enn hva som følger av lovverket. Risikoen for usaklig forskjellsbehandling minker dersom det gjelder en partiell kontraheringsplikt.

At det i visse tilfeller eksisterer en ulovfestet kontraheringsplikt, er det også bred enighet om i teorien.[27] Fredrik Stang argumenterte for at det gjaldt en kontraheringsplikt ved rettslig eller faktisk monopol. Stang uttrykker at kontraheringsplikten i disse tilfellene vil være selvsagt. Skaden som kontraheringsnektelse vil kunne påføre den enkelte, vil kunne være meget stor, mens interessen til den som nekter, som regel vil være mindre tungtveiende.[28] Videre argumenterte Carl Jacob Arnholm for at kontraheringsplikt også kan foreligge for den som tilbyr tjenester til allmennheten, med mindre det foreligger saklig grunn til å nekte.[29] Dette er fulgt opp i teorien i ettertid.[30] At det gjelder en kontraheringsplikt i slike tilfeller, ble som nevnt ovenfor også lagt til grunn av Høyesterett i Rt-2014-36.

Etter dette legges det avgjørende vekt på at utstedelse og etterfølgende bruk av eID er en standardisert tjeneste som tilbys allmennheten. Tilbyderne har oligopolmakt når det gjelder utstedelse av eID på sikkerhetsnivå «høyt». Videre er tilbyderne i en stilling som minner om konsesjonstilfellene, hvor det ofte pålegges en kontraheringsplikt for grunnleggende tjenester. Dette taler klart for at tilbyderne har kontraheringsplikt. At det ikke er noen mulighet for å prøve sakligheten av en kontraheringsnektelse gjennom dagens regelverk, taler også med styrke for en kontraheringsplikt. En kontraheringsplikt på ulovfestet grunnlag vil forhindre usaklig nektelse og gjøre nektelsen etterprøvbar for domstolene. Det er derfor grunnlag for å konkludere med at det gjelder en ulovfestet kontraheringsplikt for tilbydere av eID. Denne kontraheringsplikten er imidlertid ikke absolutt; kontraheringsnektelse tillates dersom det foreligger «saklig grunn». På den måten vil de beskyttelsesverdige interessene tilbyderne har som kan begrunne avvisning, bli ivaretatt.

2.2 Forholdet mellom kontraheringsplikt og lovbestemte krav for utstedelse av eID

Ettersom tilbyderne fortsatt vil ha en viss adgang til å nekte å inngå avtale om utstedelse av eID, er det nødvendig å vurdere rekkevidden av denne adgangen. I dette punktet skal det derfor undersøkes hvordan lovbestemte krav for utstedelse av eID påvirker tilbydernes kontraheringsplikt. Forholdet mellom tilbyder og personer som ønsker å få utstedt eID, er ikke lovregulert. Det er imidlertid enkelte av de lovbestemte kravene, herunder krav til legitimasjonsdokumenter, legitimasjonskontroll og utforming, som likevel får indirekte virkning for enkeltpersoner. Det er disse reglene som skal undersøkes nærmere i det følgende.

Reglene for eID er regulert i lov om elektroniske tillitstjenester og tilhørende forskrifter. Loven inkorporerer forordning (EU) nr. 910/2014 (eIDAS-forordningen) som norsk lov, jf. § 1 første ledd. Tilhørende forordning (EU) 2015/1502 (identifikasjonsnivåforordningen) er gjennomført ved forskrift.[31] Bestemmelsene har forrang etter EØS-loven § 2. Disse to forordningene inneholder sikkerhetskrav og krav til utforming av eID-ordninger og elektroniske signaturer.

Etter eIDAS-forordningen stilles det ulike krav til sikkerhetsnivåene «lavt», «betydelig» og «høyt».[32] De ulike sikkerhetsnivåene uttrykker grader av tillit til at den påståtte identiteten er korrekt. Hvilke minimumskrav som må være oppfylt for at en eID skal tilfredsstille et av disse sikkerhetsnivåene, er nærmere angitt i identifikasjonsnivåforordningen. For sikkerhetsnivå «høyt» kreves det at det har blitt kontrollert at personen er i besittelse av et fotografisk eller biometrisk identitetsbevis som er anerkjent av medlemsstaten, og at beviset

bekrefter den påståtte identiteten.[33] I Norge regnes pass og nasjonalt identitetskort som gyldig identitetsbevis, jf. selvdeklarasjonsforskriften § 19. I tillegg gjelder det et krav om entydig kobling til folkeregistrert person, jf. § 18.

BankID og Buypass er, i tillegg til å være eID-ordninger, avanserte elektroniske signaturer.[34] Avanserte elektroniske signaturer er elektroniske signaturer som oppfyller kravene i eIDAS-forordningen artikkel 26, jf. eIDAS-forordningen artikkel 2 nr. 11. Etter eIDAS-forordningen artikkel 26 gjelder det et krav om «fuld kontrol» (*solecontrol* I artikkel 26 bokstav c heter det at signaturen må «genereres ved hjælp af elektroniske signaturgenereringsdata, som underskriveren med en høj grad af tillid kan anvende og har fuld kontrol med». Hva «fuld kontrol» (heretter «enekontroll») innebærer, er ikke nærmere definert i bestemmelsen, men i avsnitt 51 i fortalen til eIDAS-forordningen heter det:

> «Det bør være muligt for underskriveren at overdrage et kvalificeret elektronisk signaturgenereringssystem til tredjemands varetægt, forudsat at der anvendes passende mekanismer og procedurer til at sikre, at underskriveren bevarer fuld kontrol over brugen af sine elektroniske signaturgenereringsdata, og at brugen af systemet opfylder kravene til kvalificerede elektroniske signaturer.»

Ordlyden i avsnitt 51 i fortalen knytter seg i stor grad til tekniske krav til eID-løsningen. Dette kan tale for at kravet om enekontroll kun er et krav knyttet til tilbydernes tekniske løsninger. På den annen side følger det av ordlyden i artikkel 26 at det gjelder et krav om at brukeren har enekontroll over informasjonen («data») som blir brukt til å generere signaturen. Ordlyden i artikkel 26 isolert sett kan kanskje tolkes i retning av at prinsippet om enekontroll innebærer et krav om at den elektroniske signaturen er strengt personlig og ikke kan brukes av andre.

Ordlyden er, som det fremgår av det ovennevnte, ikke helt klar. Tilbyderne tolker kravet om enekontroll som et krav om at brukeren må bevare selvstendig kontroll over bruken av sin elektroniske signatur.[35] Hensynet til elektroniske signaturers troverdighet taler for at det bør gjelde et krav om selvstendig bruk. For at en elektronisk signatur skal være like troverdig som en fysisk signatur, bør de samme prinsippene gjelde. Dersom noen signerer fysisk i en annens navn, vil dette være en falsk signatur. For å sikre troverdigheten til elektroniske signaturer bør det gjelde et krav om selvstendig bruk, slik at en elektronisk signatur som er generert av en annen enn den signaturen tilhører, anses som falsk. Det er imidlertid uklart hvorvidt et slikt krav kan hjemles i eIDAS-forordningen artikkel 26, eller om kravet kun gjelder etter alminnelige avtalerettslige regler. Hvorvidt kravet om enekontroll utgjør en saklig grunn til nektelse, vil bli nærmere behandlet i punkt 3.7.

Som gjennomgangen av regelverket ovenfor har vist, er det enkelte av kravene som påvirker tilbydernes adgang til utstedelse av eID. Det må derfor vurderes hvorvidt en kontraheringsnektelse begrunnet i lovbestemte krav utgjør «saklig grunn». Utstedelse av eID til en person som ikke oppfyller kravene i eIDAS-forordningen og tilhørende regelverk, vil stride mot lovbestemte krav. En kontraheringsplikt som pålegger tilbyderne å utstede eID i et slikt tilfelle, vil gi dårlig sammenheng i regelverket. Tilbyderne bør ikke ha en offentligrettslig plikt til å nekte utstedelse av eID og samtidig ha en privatrettslig plikt til kontrahering.[36] At kontraheringsnektelse i et slikt tilfelle kan utgjøre «saklig grunn» til nektelse, er også lagt til grunn av lovgiver i blant annet forarbeidene til finansavtaleloven § 4-1 første ledd.[37] Tilsvarende gjelder for forsikringsselskapers kontraheringsplikt.[38] At lovbestemte krav som pålegger avvisning, utgjør «saklig grunn» for kontraheringsplikt på andre rettsområder, taler for at tilsvarende må gjelde for tilbydernes ulovfestede kontraheringsplikt. En kontraheringsnektelse begrunnet i de lovbestemte kravene i eIDAS-forordningen og tilhørende regelverk utgjør dermed «saklig grunn» til kontraheringsnektelse.

2.3 Forholdet mellom kontraheringsplikt og diskrimineringsforbudet

I tillegg til å være forpliktet etter eIDAS-forordningen og tilhørende regelverk er tilbyderne forpliktet av diskrimineringsforbudet.[39] Diskrimineringsforbudet utgjør et forbud mot usaklig forskjellsbehandling.[40] En rent språklig forståelse tilsier at «saklig grunn» for kontraheringsnektelse og «usaklig forskjellbehandling» henger tett sammen. En slik kobling er imidlertid ikke gitt. Kontraheringsplikten er en privatrettslig regel på kontraktsrettens område. Diskrimineringsforbudet er på sin side en offentligrettslig regel som kommer til anvendelse på alle samfunnsområder.[41] I det følgende skal det derfor vurderes hvorvidt en systemrettet tolkning medfører at en handling som er usaklig etter offentligrettslige regler om diskriminering, samtidig er usaklig i

privatrettslig sammenheng. Dersom det er tilfellet, vil ikke vilkåret «saklig grunn» være oppfylt når en kontraheringsnektelse innebærer brudd på diskrimineringsforbudet.

For å kunne foreta en slik vurdering er det først nødvendig med en kort redegjørelse av innholdet i diskrimineringsforbudet. Diskriminering er forskjellsbehandling av mennesker som ikke følger et saklig formål, eller som er uforholdsmessig.[42] Diskrimineringsforbudet har sitt opphav i tanken om at alle mennesker er født frie og med samme menneskeverd og rettigheter.[43] Diskrimineringsforbudet innebærer både en rett til ikke å bli diskriminert, og en plikt til å motvirke og å avstå fra diskriminering. Diskrimineringsforbudet er regulert i Grunnloven § 98, en rekke internasjonale menneskerettskonvensjoner og i formell lov. For tilbydere av eID er det særlig diskrimineringsforbudet i likestillings- og diskrimineringsloven som er relevant. Dette forbudet må tolkes i tråd med Grunnloven og de internasjonale menneskerettskonvensjonene.[44]

Etter likestillings- og diskrimineringsloven § 6 er det forbudt å diskriminere «på grunn av kjønn, graviditet, permisjon ved fødsel eller adopsjon, omsorgsoppgaver, etnisitet, religion, livssyn, funksjonsnedsettelse, seksuell orientering, kjønnsidentitet, kjønnsuttrykk, alder eller kombinasjoner av disse grunnlagene». Det følger av ordlyden at listen over diskrimineringsgrunnlag er uttømmende.[45] Ordlyden «på grunn av» utgjør et krav om tilknytning mellom forskjellsbehandlingen og ett eller flere av de opplistede diskrimineringsgrunnlagene. Både direkte og indirekte forskjellsbehandling er forbudt.[46] Etter likestillings- og diskrimineringsloven § 9 første ledd er forskjellsbehandling likevel lovlig når den følger et saklig formål, er nødvendig for å oppnå formålet og ikke er uforholdsmessig inngripende. Det gjelder ikke et krav om diskriminerende hensikt.[47]

Det kan på grunnlag av dette identifiseres tre grunnvilkår for diskriminering: (1) Det må foreligge direkte eller indirekte forskjellsbehandling (2) som har tilknytning til ett eller flere diskrimineringsgrunnlag, (3) og som ikke har en begrunnelse som gjør at den likevel er tillatt.[48]

Den neste problemstillingen som skal vurderes, er om en kontraheringsnektelse som strider mot diskrimineringsforbudet i likestillings- og diskrimineringsloven § 6, medfører en plikt til kontrahering. Ordlyden i likestillings- og diskrimineringsloven § 6 gir ikke direkte uttrykk for en kontraheringsplikt, men for et generelt forbud mot å diskriminere. Forbudet innebærer imidlertid at dersom kontraheringsnektelsen er begrunnet i et av de opplistede diskrimineringsgrunnlagene, og ikke er lovlig etter likestillings- og diskrimineringsloven § 9, vil kontraheringsnektelsen være diskriminerende.

Den primære rettsvirkningen av brudd på diskrimineringsforbudet i likestillings- og diskrimineringsloven er økonomisk oppreisning og erstatning, jf. likestillings- og diskrimineringsloven § 38. Bestemmelsen står i kapittel 6 i likestillings- og diskrimineringsloven om håndheving, bevisbyrde og reaksjoner. Det er ingen andre bestemmelser i dette kapittelet som medfører en plikt til å kontrahere. Et mulig tolkningsalternativ er at likestillings- og diskrimineringsloven gir en uttømmende behandling av rettsvirkningene ved brudd på diskrimineringsforbudet. Dersom dette er tilfellet, kan det argumenteres for at et brudd på diskrimineringsforbudet ikke medfører en privatrettslig plikt til å kontrahere.

På den annen side taler hensynet til regelverkets effektivitet mot en slik tolkning. Dersom økonomisk oppreisning og erstatning er de eneste mulige rettsvirkningene av brudd på diskrimineringsforbudet i likestillings- og diskrimineringsloven, vil en part kunne fortsette den diskriminerende praksisen, med krav om betaling av oppreisning og erstatning hver gang det blir konstatert at praksisen er i strid med diskrimineringsforbudet, som eneste følge. Dersom regelverket skal tolkes slik, vil likestillings- og diskrimineringsloven trolig ikke være en tilstrekkelig gjennomføring av statens forpliktelse til å beskytte individer mot å bli diskriminert.[49]

Videre vil en slik tolkning medføre at det er dårlig sammenheng i regelverket. Etter diskrimineringsombudsloven § 11 kan Diskrimineringsnemnda treffe vedtak om pålegg om «stansing, retting og andre tiltak som er nødvendige for å sikre at diskriminering ... opphører, og for å hindre gjentakelse» dersom det foreligger brudd på likestillings- og diskrimineringsloven.[50] I forarbeidene heter det at et slikt pålegg kan være aktuelt ved brudd på diskrimineringsforbudene i diskrimineringslovgivningen.[51] Dersom en kontraheringsnektelse er i strid med likestillings- og diskrimineringsloven, vil Diskrimineringsnemnda kunne gi den aktuelle tilbyderen et pålegg om retting. Med mindre tilbyderen av andre grunner har saklig grunn til nektelse, vil et slikt pålegg om retting i praksis innebærer en plikt for tilbyderen til å kontrahere.

At kontraheringsplikt kan pålegges for å forhindre diskriminering, følger også av straffeloven § 186. Etter straffeloven § 186 er det straffbart for den som i ervervsmessig eller liknende virksomhet nekter en person varer eller tjenester når nektelsen skjer på grunnlag av personens nasjonalitet, religion eller livssyn, seksuelle

orientering, kjønnsidentitet eller kjønnsuttrykk eller nedsatt funksjonsevne.[52] Bestemmelsen vil trolig ikke komme på spissen for tilbydere av eID. Likevel danner den eksempel på at kontraheringsplikt indirekte kan følge av diskrimineringsforbudet, og eksempel på hva som ikke er «saklig grunn» til kontraheringsnektelse. Forbudet i straffeloven § 186 innebærer at en ervervsdrivende ikke har rett til å bruke de opplistede forholdene som grunn for å nekte personen varer eller tjenester på samme vilkår som andre.[53] Systembetraktninger taler dermed også imot at likestillings- og diskrimineringsloven uttømmende behandler rettsvirkningene av brudd på diskrimineringsforbudet i likestillings- og diskrimineringsloven § 6.

Etter dette er det ikke grunnlag for å tolke likestillings- og diskrimineringsloven slik at den gir en uttømmende behandling av rettsvirkningene ved brudd på diskrimineringsforbudet i likestillings- og diskrimineringsloven § 6. En kontraheringsnektelse som utgjør diskriminering, har følgelig ikke «saklig grunn». Det neste spørsmålet som må vurderes, er om den privatrettslige ulovfestede kontraheringsplikten for tilbydere av eID er begrenset til rekkevidden av diskrimineringsforbudet i likestillings- og diskrimineringsloven § 6. En slik forståelse vil innebære at enhver kontraheringsnektelse som ikke utgjør diskriminering, har «saklig grunn».

En kontraheringsplikt begrenset til diskrimineringsforbudets rekkevidde vil være begrenset til å gjelde forskjellsbehandling knyttet til et av de opplistede diskrimineringsgrunnlagene i likestillings- og diskrimineringsloven § 6. Dersom det ikke er sammenheng mellom kontraheringsnektelsen og et diskrimineringsgrunnlag, vil ikke nektelsen være diskriminerende etter likestillings- og diskrimineringsloven § 6. Tilknytningskravet medfører at diskrimineringsforbudet har begrenset rekkevidde. Som eksempel kan avvisning av personer med kriminelt rulleblad nevnes. Denne gruppen faller utenfor de opplistede diskrimineringsgrunnlagene, og en kontraheringsnektelse begrunnet i at en person har kriminelt rulleblad, vil følgelig ikke kunne utgjøre diskriminering etter likestillings- og diskrimineringsloven § 6. Dersom kontraheringspliktens rekkevidde er begrenset til rekkevidden av diskrimineringsforbudet, vil ikke tilbyderne ha kontraheringsplikt overfor denne gruppen.

Kravet om tilknytning til et diskrimineringsgrunnlag følger av at diskrimineringsforbudet skal beskytte enkeltindivider mot usaklig forskjellsbehandling knyttet til grunnleggende forhold ved en person.[54] Dette skiller seg fra den ulovfestede kontraheringsplikten, som er en privatrettslig regel begrunnet i tilbydernes stilling. Tilbydere av eID på øverste sikkerhetsnivå tilbyr et nødvendig gode til allmennheten. Kontraheringsnektelse vil medføre at personen ikke har mulighet til å skaffe eID på øverste sikkerhetsnivå. Det må derfor stilles strenge krav til når slik nektelse er tillatt. Videre er ikke vilkåret for gyldig kontraheringsnektelse begrenset til forskjellsbehandling – det stilles bare krav om «saklig grunn». Det er tilstrekkelig at nektelsen ikke har saklig grunn for at kontraheringsnektelsen anses som ugyldig og i strid med kontraheringsplikten. Dette taler for at rekkevidden av kontraheringsplikten også gjelder utover de tilfellene som omfattes av diskrimineringsforbudet. På den måten vil all avvisning uten «saklig grunn» være i strid med kontraheringsplikten, uavhengig av om det foreligger en forskjellsbehandling som utgjør diskriminering.

Etter dette er ikke rekkevidden av den ulovfestede kontraheringsplikten for tilbydere av eID begrenset til rekkevidden av diskrimineringsforbudet. Det avgjørende for om kontraheringsnektelse er tillatt, er om det foreligger «saklig grunn» i det konkrete tilfellet. Likevel er diskrimineringsforbudet en grunnleggende menneskerettighet som også griper inn i privatrettslige spørsmål, slik som kontraheringsplikten. Som drøftelsen ovenfor har vist, påvirker diskrimineringsforbudet den privatrettslige kontraheringsplikten, herunder hva som utgjør «saklig grunn». Diskrimineringsforbudet slik det følger av likestillings- og diskrimineringsloven § 6, vil fungere som en «minstestandard» for når saklig grunn ikke foreligger. En kontraheringsnektelse som medfører brudd på diskrimineringsforbudet, vil ikke ha «saklig grunn» etter den ulovfestede kontraheringsplikten. Ettersom kontraheringsplikten er en privatrettslig regel som ikke knytter seg til forskjellsbehandling og diskrimineringsgrunnlag, vil en kontraheringsnektelse som ikke er diskriminerende, også kunne være ugyldig så fremt vilkåret om «saklig grunn» ikke er oppfylt.

3 «Saklig grunn» til kontraheringsnektelse – en vurdering med utgangspunkt i typetilfeller

3.1 Innledning

Hvorvidt det foreligger «saklig grunn» til kontraheringsnektelse, beror som nevnt på en konkret vurdering. Etter vurderingene av forholdet mellom kontraheringsplikten og tilbydernes øvrige forpliktelser kan det oppstilles noen retningslinjer for når tilbyderne har «saklig grunn» til kontraheringsnektelse. For det første vil tilbydere av eID ha «saklig grunn» når lovbestemte offentligrettslige krav pålegger tilbyderne kontraheringsnektelse. For det andre vil en kontraheringsnektelse som bryter diskrimineringsforbudet, *ikke* ha «saklig grunn». Utover dette er det vanskelig å si noe generelt om når det foreligger «saklig grunn» til kontraheringsnektelse.

For å kunne si noe nærmere om når det foreligger «saklig grunn» til kontraheringsnektelse, skal jeg i dette punktet foreta en konkret vurdering av når tilbyderne har «saklig grunn», med utgangspunkt i seks utvalgte typetilfeller. Disse typetilfellene utgjør noen av grunnlagene som de ulike tilbyderne påberoper seg ved nektelse av utstedelse av eID. At dette er grunnlag tilbyderne påberoper seg som grunnlag for nektelse, følger blant annet av en rapport fra Jussbuss, av avgjørelser fra Diskrimineringsnemnda og Finansklagenemnda og av tilbydernes egne uttalelser.[55] Enkelte av de påberopte grunnlagene for nektelse er begrunnet i lovbestemte krav. Andre er begrunnet i manglende oppfyllelse av tilbydernes egne vilkår for utstedelse. Kontraheringsnektelse har i slike tilfeller «saklig grunn» når kontraheringsvilkåret er saklig begrunnet.[56]

3.2 Nektelse på grunnlag av manglende legitimasjonsdokumenter

Et av grunnlagene som tilbyderne påberoper seg som grunnlag for kontraheringsnektelse, er manglende legitimasjonsdokumenter. Dette går særlig utover utenlandske statsborgere. Noen utenlandske statsborgere opplever problemer med å anskaffe legitimasjonsdokumenter.[57] For enkelte er det mulig å få utstedt reisebevis for flyktninger eller utlendingspass av norske myndigheter dersom vilkårene for dette er oppfylt.[58] Andre utenlandske statsborgere, herunder papirløse flyktninger, har ikke mulighet til å anskaffe legitimasjonsdokumenter overhodet. I tillegg opplever utenlandske statsborgere utfordringer knyttet til legitimasjonsdokumentenes notoritet. For å kunne vurdere hvorvidt tilbydernes kontraheringsnektelse begrunnet i en persons legitimasjonsdokumenter utgjør «saklig grunn», er det først nødvendig å undersøke hvilke krav til legitimasjonsdokumenter lovgiver har stilt. Dersom tilbydernes nektelse er begrunnet i lovbestemte krav som pålegger nektelse, vil det være saklig grunn til kontraheringsnektelse.

Lovgiver har i selvdeklarasjonsforskriften § 19 første ledd tatt stilling til hvilke legitimasjonsdokumenter som har tilstrekkelig notoritet for utstedelse av eID på sikkerhetsnivå høyt. Her heter det: «Som gyldig identitetsbevis regnes pass eller nasjonalt identitetskort. For utenlandsk identitetsbevis må entydig knytning til norsk identitetsnummer godtgjøres.» Gyldig identitetsbevis etter selvdeklarasjonsforskriften § 19 er norsk pass, utenlandsk pass, norsk utlendingspass, reisebevis for flyktninger og norsk eller utenlandsk nasjonalt identitetskort.[59]

En kontraheringsnektelse begrunnet i at legitimasjonskravet i selvdeklarasjonsforskriften § 19 ikke er oppfylt, har «saklig grunn». Tilbyderne praktiserer imidlertid legitimasjonskravet ulikt og oppstiller egne kontraheringsvilkår, herunder krever flere banker at passet har RFID-brikke.[60] Det er derfor nødvendig å vurdere hvorvidt nektelse på grunn av manglende RFID-brikke utgjør «saklig grunn».

RFID står for «radio frequency identification», som er en teknologi som brukes til å lagre og hente data. En RFID-brikke i et pass er en chip som lagrer biometriske data, slik som ansiktsfoto og fingeravtrykk.[61] Dette ble innført for alle norske pass i 2008. Ettersom norske pass har en maksimal gyldighetstid på ti år, har alle gyldige norske pass i dag RFID-brikke.[62] Alle personer med gyldig norsk pass vil derfor oppfylle krav om RFID-brikke. Tilsvarende gjelder derimot ikke for alle utenlandske pass.[63]

En RFID-brikke gjør det mulig å foreta en sammenlikning av biometriske data ved at biometriske data som avgis i kontrollen, kan kontrolleres opp mot biometriske data lagret i RFID-brikken.[64] Ved den fysiske legitimasjonskontrollen for utstedelse av BankID vil typisk ansiktsfoto og fingeravtrykk lagret i RFID-brikken sammenliknes med ansiktstrekkene og fingeravtrykket til personen. Dermed kan banken kontrollere at personen faktisk har den påståtte identiteten. Sikkerhetsmessige hensyn kan begrunne et slikt krav. At utsteder er sikker på personens identitet, er viktig ved utstedelse av eID på øverste nivå. Dette er det også tatt høyde for i både identifikasjonsnivåforordningen og selvdeklarasjonsforskriften.

Etter identifikasjonsnivåforordningen må det kontrolleres at personen er i besittelse av et anerkjent identitetsbevis, og at beviset dokumenterer den påståtte identiteten. Videre må det kontrolleres at identitetsbeviset er gyldig i henhold til en autoritativ kilde. Deretter må det kontrolleres at personen kan identifiseres med den påståtte identiteten ved sammenlikning av ett eller flere av personens fysiske kjennetegn med en autoritativ kilde. Etter identifikasjonsnivåforordningen godkjennes både fotografisk og biometrisk identifikasjonsbevis.[65] Det gjelder ikke et krav om RFID-brikke etter identifikasjonsnivåforordningen. Videre gjelder det i selvdeklarasjonsforskriften § 19 første ledd ikke et krav om at pass eller nasjonalt identitetskort har avlesbar RFID-brikke eller liknende.

I vurderingen av om en slik kontraheringsnektelse er saklig begrunnet, oppstår det spørsmål om krav om RFID-brikke er diskriminerende. Selv om bankenes praksis knyttet til krav om RFID-brikke varierer, stilles kravet om RFID-brikke i stor utstrekning for både norske og utenlandske pass. Kravet er tilsynelatende nøytralt. Ettersom alle gyldige norske pass har RFID-brikke, vil det imidlertid bare være utenlandske statsborgere som ikke oppfyller kravet. Kravet utgjør dermed indirekte forskjellsbehandling.[66] Videre er forskjellsbehandlingen knyttet til diskrimineringsgrunnlaget etnisitet, herunder nasjonal opprinnelse.[67] Det neste som må vurderes, er derfor om forskjellsbehandlingen er lovlig etter likestillings- og diskrimineringsloven § 9. For at forskjellsbehandlingen skal være lovlig, må den ha et saklig formål, være nødvendig for å oppnå formålet og ikke være uforholdsmessig inngripende, jf. § 9 første ledd bokstav a til c.

Et krav om RFID-brikke vil redusere risikoen for falsk identitetspåstand. Dette taler for at kravet har et saklig formål. Gjennom avlesing av RFID-brikke vil utsteder kunne kontrollere personens fysiske kjennetegn med de biometriske data som er lagret i RFID-brikken. Det er dermed en sikrere kontroll av en persons identitet enn en vanlig sammenlikning av passfoto og ansiktstrekkene til personen. Det er viktig at eID utstedes til rett person, både av hensyn til eID-ordningens troverdighet og på grunn av faren for misbruk. Forskjellsbehandlingen følger dermed et saklig formål.

Likevel er dette en risiko som er kjent for lovgiver. Lovgiver har i selvdeklarasjonsforskriften § 19 lagt til grunn at en persons identitet kan godgjøres på tilfredsstillende måte uten biometriske data. Ved personlig oppmøte for legitimering vil personen som foretar legitimasjonskontrollen, kunne foreta en sammenlikning av passfoto mv. og personens fysiske kjennetegn. Videre vil personens identitetspåstand kontrolleres opp mot opplysningene i folkeregisteret. På den måten sikres det at eID ikke utstedes til feil person. Ettersom lovgiver allerede har tatt hensyn til risikoen for falsk identitetspåstand gjennom å stille strenge krav til legitimasjonskontrollen, kan ikke dette hensynet gi bankene saklig grunn for å stille enda strengere krav til legitimasjonskontrollen. Forskjellsbehandlingen er derfor ikke nødvendig.

Ettersom kravet om RFID-brikke ikke er nødvendig for å oppnå formålet om ikke å utstede BankID til feil person, er ikke forskjellsbehandlingen lovlig etter likestillings- og diskrimineringsloven § 9. Kontraheringsvilkåret om RFID-brikke er dermed i strid med diskrimineringsforbudet. En kontraheringsnektelse begrunnet i at passet mangler RFID-brikke, vil derfor ikke ha «saklig grunn».

3.3 Nektelse på grunnlag av hvitvaskingsloven

Det neste typetilfellet som skal vurderes, er bankenes kontraheringsnektelse begrunnet i hvitvaskingsloven. At hvitvaskingsloven kan innebære en plikt til å nekte kontrahering, er lagt til grunn i forarbeidene til hvitvaskingsloven. Her heter det at manglende gjennomføring av kundetiltak etter hvitvaskingsloven er saklig grunn til kontraheringsnektelse etter både forsikringsavtaleloven § 1B-3 første ledd og finansavtaleloven § 4-1 første ledd.[68] Av de tre tilbyderne av eID på øverste sikkerhetsnivå er det bare bankene, som utsteder BankID, som er pliktsubjekter etter hvitvaskingsloven.[69] I dette punktet skal jeg derfor undersøke hvorvidt bankens forpliktelser etter hvitvaskingsloven kommer til anvendelse ved utstedelse av BankID. Dersom det er tilfellet, må det vurderes hvorvidt hvitvaskingsloven kan utgjøre «saklig grunn» til kontraheringsnektelse ved utstedelse av BankID.

Etter hvitvaskingsloven er bankene forpliktet til å forebygge og avdekke hvitvasking og terrorfinansiering.[70] Loven gjennomfører EUs fjerde hvitvaskingsdirektiv.[71] Hvitvasking er i hvitvaskingsloven § 2 bokstav a definert som handling som beskrevet i straffeloven §§ 332 og 337. Herunder omfattes handlinger som bidrar til å sikre utbyttet av en straffbar handling og gjennomføres for eksempel ved å oppbevare, overføre eller konvertere det.[72] Videre er terrorfinansiering definert som handling som beskrevet i straffeloven § 135 eller finansiering som beskrevet i straffeloven § 136 a, jf. hvitvaskingsloven § 2 bokstav b. Dette omfatter blant

annet å yte, motta, sende, fremskaffe eller samle inn penger elle andre formuesgoder med viten om at midlene skal brukes til terrorhandlinger, terrorforbund, terrortrusler, rekruttering til terror osv.[73] Fare for hvitvasking og terrorfinansiering oppstår dermed særlig ved tjenester knyttet til transaksjoner og andre økonomiske disposisjoner.

Fordi fare for hvitvasking og terrorfinansiering særlig oppstår ved økonomiske disposisjoner, må det vurderes hvorvidt hvitvaskingslovens regler kommer til anvendelse ved avtale om utstedelse av BankID. BankID er først og fremst et elektronisk identifikasjonsmiddel og en avansert elektronisk signatur. Det er imidlertid også mulig å bruke BankID ved overføringer i nettbank. I slike tilfeller blir BankID benyttet som et betalingsinstrument og vil derfor ha en tilknytning til økonomiske disposisjoner. Gitt at det ikke er noen tekniske hindringer for utstedelse eller bruk av BankID uten at det samtidig eksisterer eller samtidig gis tilgang til bankkonto mv. (andre banktjenester), kan BankID utstedes separat. Dersom BankID utstedes separat, vil BankID på utstedelsestidspunktet utelukkende fungere som en eID og en avansert elektronisk signatur på lik linje med Buypass. Lovgiver har avgrenset hvitvaskingslovens anvendelsesområde mot øvrige eID-ordninger, og loven kommer følgelig ikke til anvendelse ved utstedelse av Buypass eller Commfides.[74] Det kan derfor problematiseres hvorvidt lovgiver har ment at utstedelse av BankID utløser forpliktelser etter hvitvaskingsloven.

De relevante forpliktelsene etter hvitvaskingsloven er i dette tilfellet bankenes forpliktelse til å gjennomføre risikobaserte kundetiltak.[75] Etter hvitvaskingsloven § 10 første ledd bokstav a oppstår forpliktelsen ved «etablering av kundeforhold». Bestemmelsen svarer til EUs fjerde hvitvaskingsdirektiv, hvor det heter at «kundekendskabsprocedurer» («customer due diligence») skal gjennomføres når pliktsubjektene «etablerer forretningsforbindelser».[76]

Ordlyden «etablering av kundeforhold» er vid og taler for at etablering av ethvert kundeforhold omfattes. Dette taler for at også avtale om utstedelse av BankID er å anse som etablering av kundeforhold. Ettersom det er uklart hvorvidt BankID er ment å omfattes av hvitvaskingsregelverket, må det vurderes hvorvidt bestemmelsen må tolkes innskrenkende, slik at BankID likevel ikke omfattes.

I forarbeidene heter det: «Når et kundeforhold anses etablert, må vurderes med utgangspunkt i når kunden kan bruke den rapporteringspliktiges tjenester.»[77] Tilsvarende følger av hvitvaskingsforskriften § 4-1 første ledd, hvor det heter at kundeforhold anses som etablert når kunden «kan bruke den rapporteringspliktiges tjenester, for eksempel ved opprettelse av konto eller utstedelse av betalingskort». I Finanstilsynets veileder til hvitvaskingsloven listes det opp en rekke eksempler på når kundeforhold anses etablert. Herunder nevnes opprettelse av bankkonto.[78] Avtale om BankID nevnes ikke som eksempel. BankID er imidlertid en tjeneste bankene tilbyr, og kunden får tilgang til denne tjenesten når det inngås avtale om BankID. Dette taler for at hvitvaskingsloven kommer til anvendelse også ved avtale om utstedelse av BankID.

På den annen side er formålet med hvitvaskingsregelverket å forebygge og avdekke hvitvasking og terrorfinansiering.[79] De øvrige institusjonene som er forpliktet etter hvitvaskingsloven § 4, er institusjoner som har en tilknytning til transaksjoner eller andre økonomiske disposisjoner. Det er i slike tilfeller det er risiko for hvitvasking og terrorfinansiering. Når BankID utstedes uten at det allerede eksisterer et kundeforhold eller det samtidig gis tilgang til andre banktjenester, er BankID utelukkende en eID og en avansert elektronisk signatur. BankID kan riktignok benyttes som legitimasjon ved søknad om lån, men i slike tilfeller vil det være banken det søkes lån i, og ikke utstederbanken som er pliktsubjekt etter hvitvaskingsloven. I slike tilfeller vil det derfor være banken det søkes lån i, som er forpliktet til å gjennomføre risikobaserte kundetiltak, og plikten inntrer på tidspunktet for forespørsel om låneopptak. På tidspunktet for utstedelse av BankID uten samtidig tilgang til andre banktjenester vil det være liten risiko for hvitvasking eller terrorfinansiering. Formålet til hvitvaskingsloven taler derfor for at BankID ikke omfattes av bestemmelsen.

At de øvrige tilbyderne av eID på øverste sikkerhetsnivå ikke er forpliktet av hvitvaskingsloven, underbygger synet om at utstedelse av eID i utgangspunktet ikke representerer fare for hvitvasking og terrorfinansiering. Buypass er som nevnt også en avansert elektronisk signatur og kan blant annet benyttes til å signere vedtak om lån hos Lånekassen. Buypass kan dermed i likhet med BankID brukes som legitimering i tilknytning til låneopptak. Likevel er ikke Buypass pliktsubjekt etter hvitvaskingsloven. Dette kan være fordi risikoen for hvitvasking og terrorfinansiering ikke oppstår ved utstedelse, men først ved etterfølgende bruk av eID. I slike tilfeller er det som nevnt den som innvilger lånet mv., som er pliktsubjekt etter hvitvaskingsloven og ikke tilbyderen som har utstedt eID. Likhetsbetraktninger taler dermed også for at hvitvaskingsregelverket likevel

ikke kommer til anvendelse på avtale om utstedelse av BankID når BankID utstedes uten tilgang til andre banktjenester.

Etter ordlyden er det imidlertid klart at avtale om BankID er å anse som «etablering av kundeforhold» også i tilfeller hvor BankID utstedes separat. BankID er i slike tilfeller fortsatt en tjeneste som tilbys av bankene, og kunden får tilgang til denne ved å inngå avtale om BankID. En slik tolkning støttes av forarbeidene, hvor det heter at det sentrale er om kunden settes i stand til å bruke den rapporteringspliktiges tjenester.[80] Lovgiver har ikke uttrykkelig begrenset hvilke tilfeller som er å anse som «etablering av kundeforhold». At lovens formål og likhetsbetraktninger trekker i en annen retning enn ordlyden, er ikke tilstrekkelig til å tolke bestemmelsen innskrenkende når avtale om utstedelse av BankID klart omfattes av ordlyden i hvitvaskingsloven § 10 første ledd bokstav a. Ettersom det er lav risiko for hvitvasking i slike tilfeller, kan imidlertid den risikobaserte vurderingen bankene er forpliktet til å foreta, stille seg annerledes enn risikovurderingen ved etablering av andre banktjenester.

Siden avtale om utstedelse av BankID utløser forpliktelser for bankene etter hvitvaskingsloven, vil en kontraheringsnektelse begrunnet i reglene i hvitvaskingsloven kunne utgjøre «saklig grunn». Dette medfører problemer i praksis. At hvitvaskingsloven kommer til anvendelse, innebærer at bankene er forpliktet til å stille strengere krav for når BankID kan utstedes, enn det som er nødvendig etter de lovbestemte kravene for utstedelse av eID. Ett av grunnlagene som bankene påberoper seg ved kontraheringsnektelse, er at kundetiltak etter hvitvaskingsloven ikke kan gjennomføres. I det følgende vil jeg derfor vurdere hvorvidt en slik nektelse har «saklig grunn».

Etter hvitvaskingsloven § 9 første ledd skal kundetiltak og løpende oppfølging tilpasses risikoen for hvitvasking og terrorfinansiering knyttet til det enkelte kundeforholdet. Etter § 9 første ledd annet punktum skal risikoen vurderes ut fra blant annet kundeforholdets formål, mengden kundemidler som skal inngå i kundeforholdet, transaksjoners størrelse samt regelmessigheten og varigheten på kundeforholdet. Dersom kundetiltak ikke kan gjennomføres, skal den rapporteringspliktige ikke etablere kundeforholdet, jf. hvitvaskingsloven § 21.

I forarbeidene heter det at det i utgangspunktet må bero på kundens forhold at kundetiltak ikke kan gjennomføres; det er ikke tilstrekkelig at det er mer byrdefullt eller kostnadskrevende for den rapporteringspliktige. Som eksempel på når kundeforholdet kan avslås, nevnes tilfeller der formålet med kundeforholdet fremstår som illegitimt, eksempelvis ved at en konto skal misbrukes til å motta penger innbetalt som følge av bedrageri, og den rapporteringspliktige ikke tilfredsstillende kan håndtere den økte risikoen for at vedkommende misbrukes til hvitvasking eller terrorfinansiering.[81] Rapporteringspliktige har ikke adgang til på generelt grunnlag å avvise kunder som utgjør en høyere risiko for hvitvasking eller terrorfinansiering.[82]

Etter både finansavtaleloven § 4-1 første ledd og forsikringsavtaleloven § 1B-3 er utgangspunktet at manglende gjennomføring av kundetiltak utgjør «saklig grunn».[83] Tilsvarende må gjelde for den ulovfestede kontraheringsplikten ved utstedelse av eID. Avslag etter hvitvaskingsloven § 21 som følge av at kundetiltak ikke kan gjennomføres, vil derfor være saklig grunn til kontraheringsnektelse. En forutsetning for at vilkåret om saklig grunn er oppfylt, er imidlertid at bankene faktisk har grunnlag for å avvise etter hvitvaskingsloven § 21. For eksempel vil ikke det at en person har kriminelt rulleblad, i seg selv være nok til å kunne avvise kunden etter § 21.[84]

Hvitvaskingslovens anvendelse ved utstedelse av BankID kan medføre problemer knyttet til utstedelse av BankID for samtlige brukergrupper. En avgjørelse fra Finansklagenemnda avsagt i 2022 er et illustrerende eksempel på denne problematikken.[85] Saken gjaldt spørsmål om hvorvidt en bank kunne si opp klagers brukskonto, nettbank, kort og BankID etter hvitvaskingsloven § 24 fjerde ledd, jf. § 21. Banken hadde bedt klageren om å gjøre rede for kontantinnskudd på 333 000 kroner og overførsel på 110 000 kroner fra sin konto til egen konto i en annen bank. Klageren opplyste om at pengene var lønn fra lovlig prostitusjon. Finansklagenemnda uttalte at selv om det ikke var grunn til å tvile på klagers forklaring, kan ikke banken etter hvitvaskingsregelverket utelukkende basere seg på kundens egen forklaring av midlenes opprinnelse. Manglende dokumentasjon på midlenes opprinnelse gjorde at banken ikke kunne gjennomføre lovpålagte kundetiltak etter hvitvaskingsloven § 24. Finansklagenemnda konkluderte derfor med at banken var berettiget til å si opp klagers brukskonto, kort, nettbank og BankID.

Det er ingen opplysninger i denne klagesaken som tilsier at personen ikke kan ha BankID etter reglene i eIDAS-forordningen og tilhørende regelverk som påvirker utstedelse av eID. Gitt at BankID utstedes separat, uten at det samtidig gis tilgang til andre banktjenester, er det tvilsomt hvorvidt dette faktumet ville ha dannet grunnlag for å si opp avtale om BankID. Kundetiltakene i det konkrete tilfellet var knyttet til kontroll av

kontantinnskudd og overføringer. Dersom banken kun hadde sagt opp kontoavtalen mv., ville ikke personen lenger hatt mulighet til å foreta kontantinnskudd og kontooverføringer i utstederbanken selv om avtalen om BankID ble opprettholdt. Dette taler for at banken i så fall ikke ville ha hatt grunnlag for kontraheringsnektelse etter hvitvaskingsloven.

Det ovennevnte eksemplet illustrerer at det er problematisk at bankene er forpliktet av hvitvaskingsloven ved utstedelse av BankID. At hvitvaskingsloven kommer til anvendelse ved utstedelse av BankID, medfører at bankene har legitime grunner til nektelse som oppfyller vilkåret om «saklig grunn» utover det som følger av de lovbestemte kravene for utstedelse av eID. Dette gjelder selv om hensynene bak hvitvaskingsregelverket ikke gjør seg gjeldende når BankID utstedes separat. Personer som har problemer med å få utstedt BankID på grunn av kravene etter hvitvaskingsloven, har mulighet til å få utstedt Buypass eller Commfides dersom de øvrige kontraheringsvilkårene er oppfylt. Denne gruppen står derfor ikke uten tilgang til eID på øverste sikkerhetsnivå.

3.4 Nektelse på grunnlag av manglende folkeregistrert fødselsnummer eller d-nummer

Et annet påberopt grunnlag for kontraheringsnektelse er krav om folkeregistrert fødselsnummer eller d-nummer. Fødselsnummer og d-nummer er norske identifikasjonsnummer bestående av elleve siffer. Buypass og Commfides aksepterer både fødselsnummer og d-nummer ved utstedelse av sine respektive eID-ordninger.[86] Etter bransjenormen «Regler om BankID» er utgangspunktet at BankID kan utstedes til fysiske personer, og det stilles ingen krav om fødselsnummer og d-nummer.[87] Bransjenormen er dermed ikke til hinder for at bankene aksepterer både fødselsnummer og d-nummer. En rapport fra Jussbuss om utlendingers tilgang til banktjenester fra 2022 viser imidlertid at bankenes praksis varierer på dette punktet. Av rapporten følger det at fire av de seks bankene som deltok i undersøkelsen, krevde norsk fødselsnummer for utstedelse av BankID. To banker godkjente også d-nummer, men den ene av disse godkjente kun d-nummer for nordiske borgere over 18 år.[88] Spørsmålet er om manglende folkeregistrert fødselsnummer eller d-nummer utgjør «saklig grunn» til kontraheringsnektelse.

I selvdeklarasjonsforskriften § 18 første punktum heter det at identitetspåstanden må gjelde en person som finnes i Folkeregisteret. Videre heter det i annet punktum at eID-tilbyderen må kunne gi en sikker og entydig kobling til denne personens identifikator i Folkeregisteret, herunder fødselsnummer eller d-nummer. Kontraheringsnektelse begrunnet i at en person mangler folkeregistrert fødselsnummer eller d-nummer, vil dermed ha «saklig grunn». Buypass og Commfides overholder dermed kontraheringsplikten på dette punktet. Som nevnt krever imidlertid flere banker norsk fødselsnummer. Det neste spørsmålet er derfor om kontraheringsnektelse av personer med d-nummer har «saklig grunn».

Det første som må vurderes, er om kontraheringsnektelse av personer med d-nummer begrunnet i et krav om norsk fødselsnummer er i strid med diskrimineringsforbudet. Et vilkår om norsk fødselsnummer er en tilsynelatende nøytral betingelse, ettersom kravet gjelder for alle. I praksis vil kravet likevel innebære forskjellsbehandling av personer som ikke har mulighet til å skaffe seg norsk fødselsnummer. Det relevante diskrimineringsgrunnlaget er etnisitet, herunder nasjonal opprinnelse.[89] Det er bare personer med en annen nasjonal opprinnelse som kan mangle mulighet til å oppfylle vilkåret om norsk fødselsnummer. Et kontraheringsvilkår som stiller krav om norsk fødselsnummer, vil dermed utgjøre indirekte forskjellsbehandling.[90]

Det neste som må vurderes, er derfor hvorvidt vilkårene for lovlig forskjellsbehandling i likestillings- og diskrimineringsloven § 9 er oppfylt. Etter § 9 første ledd bokstav a til c vil forskjellsbehandlingen være lovlig dersom den følger et saklig formål, er nødvendig for å oppnå formålet og ikke er uforholdsmessig inngripende overfor den eller de som forskjellsbehandles.

For å kunne vurdere hvorvidt forskjellsbehandlingen er lovlig, er det nødvendig å undersøke grunnlagene som bankene påberoper seg for denne kontraheringsnektelsen, nærmere. En sak fra Diskrimineringsnemnda gir et innblikk i hvilke grunnlag dette kan være.[91] Saken gjaldt en svensk statsborger som ble fratatt sin BankID fordi hun ikke hadde norsk pass eller norsk fødselsnummer. Banken uttalte at den hadde valgt å legge seg på en strengere linje enn regelverket, slik at den som hovedregel kun utstedte BankID til kunder med norsk personnummer som legitimerte seg med norsk pass. Banken anførte tre grunnlag for denne strengere linjen. For det første viste banken til forpliktelsen til å forhindre hvitvasking og terrorfinansiering. Videre argumenterte banken med at BankID ikke er en del av grunnleggende banktjenester, slik at det ikke gjelder en

kontraheringsplikt. Til slutt viste den til at det er knyttet stor risiko for misbruk og svindel til BankID. Diskrimineringsnemnda uttalte at krav om norsk pass eller personnummer utgjorde indirekte forskjellsbehandling på grunnlag av etnisitet. Nemnda kom til at forskjellsbehandlingen ikke var lovlig, og at banken hadde diskriminert personen på grunnlag av etnisitet.

Bankens anførsel om at enhver person ikke har rett til å få BankID, kan klart nok ikke være et argument for at et krav om norsk fødselsnummer er saklig begrunnet. Som det følger av det ovennevnte, gjelder det en ulovfestet kontraheringsplikt for tilbydere av eID. Utgangspunktet er derfor at bankene er forpliktet til å inngå avtale om BankID med enhver person som ønsker dette, så fremt det ikke foreligger «saklig grunn» til kontraheringsnektelse. En kontraheringsnektelse i strid med diskrimineringsforbudet vil ikke oppfylle vilkåret om «saklig grunn».

Videre begrunnet banken kravet om norsk fødselsnummer med bankens forpliktelser etter hvitvaskingsloven. Som nevnt gjelder bankenes forpliktelser etter hvitvaskingsloven også ved utstedelse av BankID. Dermed kan en kontraheringsnektelse begrunnet i hvitvaskingsloven medføre at forskjellsbehandlingen er lovlig. Dette gjelder så fremt hvitvaskingsloven faktisk gir hjemmel for slik avvisning. For forskjellsbehandling som følge av krav om norsk fødselsnummer er det hvitvaskingslovens legitimasjonskrav som er relevant.

Et av kundetiltakene etter hvitvaskingsloven er å innhente informasjon om kundens identitet og bekrefte kundens identitet gjennom legitimering, jf. hvitvaskingsloven § 12. Etter hvitvaskingsloven § 12 første ledd bokstav a til c skal følgende opplysninger om kunden innhentes: navn, fødselsnummer eller d-nummer, eller annen entydig identitetskode, og adresse. Dermed er både fødselsnummer og d-nummer gyldig identitetsnummer etter hvitvaskingsregelverket, i tillegg til annen gyldig identitetskode. Hvitvaskingslovens krav til legitimasjonskontrollen ved etablering av kundeforhold er altså lavere enn de kravene som gjelder for utstedelse av eID på øverste sikkerhetsnivå. Det gir derfor lite mening å begrunne en praksis som er strengere enn selvdeklarasjonsforskriften § 18, med reglene i hvitvaskingsloven. Et krav om norsk fødselsnummer kan derfor ikke begrunnes i hvitvaskingsloven.

Den tredje begrunnelsen som ble påberopt av banken i den nevnte saken, er risiko for misbruk og svindel. For at dette skal være et saklig formål etter likestillings- og diskrimineringsloven § 9 første ledd bokstav a, må begrunnelsen være sann og legitim i det konkrete tilfellet.[92] Risiko for misbruk og svindel taler for at visse tiltak må gjennomføres for å sikre at BankID utstedes til rett person. Selv om risikoen for misbruk og svindel er størst ved etterfølgende bruk av BankID, er det en viss risiko knyttet til at BankID utstedes til feil person. Denne risikoen er det imidlertid tatt høyde for i regelverket. De kravene som gjelder for legitimering etter selvdeklarasjonsforskriften og eIDAS-forordningen, skal forhindre at eID utstedes til feil person. Risikoen for misbruk og svindel er derfor ikke et legitimt formål for krav om norsk fødselsnummer.

Etter dette er ikke krav om norsk fødselsnummer lovlig forskjellsbehandling etter likestillings- og diskrimineringsloven § 9. Å nekte å utstede BankID til en person med d-nummer begrunnet i at personen ikke har norsk fødselsnummer, utgjør diskriminering på grunnlag av etnisitet. En slik kontraheringsnektelse vil derfor ikke ha «saklig grunn». Bankene er derfor forpliktet til å tilby BankID til personer med d-nummer så fremt de oppfyller øvrige kontraheringsvilkår. For det tilfellet at en person hverken har norsk fødselsnummer eller d-nummer, er ikke det lovbestemte kravet i selvdeklarasjonsforskriften § 18 oppfylt. I slike tilfeller vil det derfor være «saklig grunn» til kontraheringsnektelse.

3.5 Nektelse på grunnlag av manglende etablering av kundeforhold

Et kontraheringsvilkår som bankene ofte stiller, er krav om at det eksisterer eller opprettes et kundeforhold i den aktuelle banken, herunder et samtidig krav om at det eksisterer eller inngås avtale om andre banktjenester, som bankkonto mv. At et slikt krav kan forekomme, er det lagt til rette for i avtaledokumentet «Avtale om BankID», som er utarbeidet av Bits med sikte på å fungere som avtale om BankID mellom utstederbanken og personen som får utstedt BankID.[93] I punkt 7 i denne avtalen følger det at avtalen kan sies opp dersom kundeforhold avsluttes. Et samtidig krav om andre banktjenester følger ikke av de lovbestemte reglene for utstedelse av eID. Det må derfor vurderes hvorvidt et slikt kontraheringsvilkår er saklig begrunnet.

Kravet er trolig begrunnet i forretningsmessige hensyn. Bankene kan se seg tjent med at det inngås avtale om andre banktjenester i tillegg til BankID. Forretningsmessige hensyn kan medføre at et kontraheringsvilkår er saklig begrunnet. Dette ble blant annet lagt til grunn av Høyesterett i den tidligere nevnte Rt-2014-36. I avsnitt 81 tok førstvoterende til orde for at et krav om at personer som benyttet seg av heisanlegget til egen

næringsvirksomhet, skulle betale mer enn forbrukere, var saklig begrunnet.[94] Dommen gjaldt spørsmål om bruk av heisanlegg i en skibakke til næringsvirksomhet. Faktum i dommen skiller seg dermed fra vårt tilfelle, hvor det er spørsmål om utstedelse av eID på øverste sikkerhetsnivå – en tjeneste som gir tilgang til en rekke nødvendige digitale tjenester. Til forskjell fra i dommen er det derfor flere tungtveiende motstående hensyn som må tas i betraktning ved vurderingen av om vilkåret er saklig begrunnet.

Selv om det fortsatt er mulig for personen å anskaffe Buypass eller Commfides dersom vilkårene for dette er oppfylt, er BankID den klart ledende aktøren.[95] I tillegg er det enkelte private tjenester som kun aksepterer BankID.[96] Å ikke få utstedt BankID medfører ulempe for enkeltindividet. Videre medfører krav om eksisterende banktjenester eller opprettelse av andre banktjenester at hvitvaskingslovens regler for etablering av banktjenester kommer til anvendelse. Ved separat utstedelse av BankID er det isolert sett lav risiko for hvitvasking og terrorfinansiering. Når det stilles krav om samtidig tilgang til andre banktjenester, vil kundeforholdet representere en høyere risiko for hvitvasking på utstedelsestidspunktet, ettersom personen gis tilgang til bankkonto mv. Dette vil igjen ha betydning for når bankene har grunnlag for å nekte kontrahering, og når det er grunnlag for å si opp avtalen. Kontraheringsvilkåret vil dermed medføre en innskrenkning i hvem som kan få utstedt BankID, og samtidig gi bankene en større adgang til senere å si opp avtale om BankID.

Hvorvidt bankene har «saklig grunn» til å stille et slikt kontraheringsvilkår, er usikkert. Når det legges vekt på at kontraheringsvilkåret vil føre til en innskrenkning i hvem som kan få utstedt BankID, taler det for at forretningsmessige hensyn ikke er tilstrekkelig tungtveiende til å begrunne et slikt kontraheringsvilkår. Dersom en slik forståelse legges til grunn, vil følgelig en kontraheringsnektelse på grunnlag av manglende oppfyllelse av dette kravet ikke ha «saklig grunn».

3.6 Nektelse på grunnlag av manglende språkkunnskaper

Det neste som skal vurderes, er hvorvidt kontraheringsnektelse på grunnlag av manglende språkkunnskaper i norsk eller engelsk utgjør «saklig grunn». I rapporten fra Jussbuss vises det til en avisartikkel hvor to banker uttaler at de krever at personen forstår norsk eller engelsk.[97] Dette begrunner bankene med at de må være helt sikre på at personen skjønner innholdet i avtalen om BankID og hva BankID er. Et slikt krav kan ikke utledes av eIDAS-forordningen og de tilhørende reglene som påvirker utstedelse av eID på øverste sikkerhetsnivå. Det må derfor vurderes hvorvidt det er andre grunner som medfører at en slik kontraheringsnektelse oppfyller vilkåret om «saklig grunn». Det første spørsmålet er om kontraheringsnektelse på grunnlag av manglende språkkunnskaper i norsk eller engelsk utgjør diskriminering.

Bankens krav om språkkunnskaper i norsk eller engelsk medfører at personer som ikke kan norsk eller engelsk, stilles dårligere enn personer som oppfyller språkkravet, ettersom de ikke har mulighet til å få utstedt BankID. Kontraheringsnektelsen utgjør dermed direkte forskjellsbehandling, jf. likestillings- og diskrimineringsloven § 7. Det relevante diskrimineringsgrunnlaget er etnisitet, herunder språk, jf. likestillings- og diskrimineringsloven § 6 første ledd. Slik forskjellsbehandling er bare tillatt dersom vilkårene for lovlig forskjellsbehandling i likestillings- og diskrimineringsloven § 9 er oppfylt: Forskjellsbehandlingen må følge et saklig formål, være nødvendig for å oppnå formålet og ikke være uforholdsmessig inngripende overfor dem som forskjellsbehandles. Det neste spørsmålet er derfor om kontraheringsnektelsen oppfyller vilkårene for lovlig forskjellsbehandling.

Vilkåret om saklig formål innebærer at begrunnelsen må være sann og legitim i det konkrete tilfellet. Å sikre at personen forstår innholdet i avtalen om BankID, er et saklig formål. Videre vil kravet medføre at bankene selv kan kontrollere at personen faktisk forstår innholdet i avtalen, og det er dermed egnet til å oppnå formålet. Det finnes eksempler fra praksis på at personer har blitt svindlet av nærstående som har fungert som tolk ved inngåelse av avtale om BankID. Enkelte har i slike tilfeller blitt lurt av den nærstående til å oppgi passord eller fått en uriktig forklaring av hva BankID kan brukes til. Ved å stille krav om norsk- eller engelskkunnskaper vil man kunne unngå dette.[98]

Det neste vilkåret er at forskjellsbehandlingen må være nødvendig for å oppnå formålet. Det kreves mer enn at forskjellsbehandlingen er ønskelig, men samtidig behøver den ikke å være uunnværlig.[99] Forskjellsbehandlingen må også være egnet til å oppnå formålet. Å nekte utstedelse av BankID til personer som ikke kan norsk eller engelsk, vil være egnet til å forhindre at BankID utstedes til en person som ikke forstår innholdet i avtalen. Dette formålet kan imidlertid oppnås med andre ikke-diskriminerende handlingsalternativer som ikke vil være uforholdsmessig ressurskrevende for bankene. For eksempel kan formålet oppnås ved å

bruke en uavhengig tolk. Alternativt, eller i tillegg, kan BankID-avtalen oversettes til flere språk, og det kan utarbeides informasjonsmateriale på flere språk. Forskjellsbehandlingen er derfor ikke nødvendig for å oppnå formålet.

Til slutt må det vurderes hvorvidt kontraheringsnektelse på grunnlag av manglende språkkunnskaper er uforholdsmessig inngripende overfor den eller dem som forskjellsbehandles. Kontraheringsnektelse er svært inngripende overfor den enkelte. Riktignok stiller hverken Buypass eller Commfides tilsvarende krav om språkkunnskaper, slik at personer som blir nektet BankID på grunnlag av språk, fortsatt vil ha mulighet til å skaffe seg eID på øverste sikkerhetsnivå. At andre tilbydere ikke stiller det samme kravet, kan imidlertid ikke være avgjørende for bankenes forpliktelser til å opptre på en ikke-diskriminerende måte. Formålet bankene ønsker å oppnå ved å nekte utstedelse av BankID til personer som ikke snakker norsk eller engelsk, kan oppnås gjennom ikke-diskriminerende handlingsalternativer. Disse handlingene vil ikke være uforholdsmessig ressurskrevende for bankene. Det er dermed uproporsjonalt å nekte å utstede BankID til personer som ikke snakker norsk eller engelsk.

Etter dette er ikke forskjellsbehandlingen lovlig etter unntaket i likestillings- og diskrimineringsloven § 9 første ledd. Bankenes krav om språkkunnskaper i norsk eller engelsk utgjør direkte diskriminering på grunnlag av etnisitet, herunder språk. En kontraheringsnektelse begrunnet i manglende språkkunnskaper i norsk eller engelsk har følgelig ikke «saklig grunn».

3.7 Nektelse på grunnlag av vergemål

3.7.1 Generelt om kontraheringsnektelse begrunnet i en persons vergemål

Det siste typetilfellet som skal vurderes, er kontraheringsnektelse begrunnet i at en person bistås av verge. I bransjenormen «Regler om BankID» punkt 3.4 heter det at BankID ikke skal utstedes til personer som helt eller delvis er fratatt sin rettslige handleevne.[100] I tillegg følger det av praksis fra Diskrimineringsnemnda at enkelte banker også nekter utstedelse til personer som bistås av verge, med den rettslige handleevnen i behold.[101] Tilsvarende opplyser Buypass om at det ved identifikasjonskontrollen hos Posten fremkommer at personen bistås av verge. Disse personene anses av Buypass for ikke å ha gyldig identitetsbevis.[102] Commfides opplyser om at de ikke kontrollerer om personen helt eller delvis har blitt fratatt rettslig handleevne.[103] Vurderingene i dette punktet gjør seg derfor ikke gjeldende for Commfides.

Diskrimineringslovgivningens krav om tilgjengelighet og plikt til universell utforming er ikke til hinder for at det foreligger «saklig grunn» til kontraheringsnektelse.[104] Spørsmålet er derfor hvorvidt bankene og Buypass har «saklig grunn» til kontraheringsnektelse når nektelsen begrunnes i at personen bistås av verge.

Ettersom vurderingen av om det foreligger «saklig grunn», vil avhenge av vergemålets omfang, er det nødvendig først å si litt om de ulike typene vergemål: Dagens vergemålsordning opererer med et minste middels prinsipp. Dette innebærer at vergemålet ikke skal gjøres mer omfattende enn nødvendig.[105] Omfanget av hvert enkelt vergemål skal derfor tilpasses individuelt ut fra en konkret vurdering av den enkeltes behov.[106] Som følge av dette kan en person være under vergemål med den rettslige handleevnen i behold, eller være helt eller delvis fratatt rettslig handleevne. Når en person med den rettslige handleevnen i behold settes under vergemål, står vedkommende fritt til å foreta rettslige handlinger og råde over egne midler.[107] Dette innebærer at en avtale inngått av en person under vergemål vil være gyldig med mindre den rammes av alminnelige ugyldighetsregler. Vergen og personen med den rettslige handleevnen i behold som er satt under vergemål, har parallell kompetanse.[108] Vergemålsloven er dermed ikke til hinder for å utstede eID til personer under vergemål med den rettslige handleevnen i behold.

Videre kan en person settes under vergemål med fullstendig eller delvis fratakelse av den rettslige handleevnen etter vergemålsloven § 22. Det kan gjelde økonomiske eller personlige forhold eller begge deler. «Økonomiske forhold» omfatter blant annet bistand til å ta hånd om løpende utgifter og inntekter eller til forvaltning av fast eiendom ved utleie, salg eller på annen måte. Det kan også omfatte at vergen tar hånd om næringsvirksomhet som den vergetrengende driver.[109] Med «personlige forhold» menes alle former for representasjon og ivaretakelse av rettigheter utover økonomiske forhold.[110]

Som utslag av det minste middels prinsipp skal vergemål med fratakelse av den rettslige handleevnen skreddersys ut fra den enkeltes behov på samme måte som ved ordinært vergemål. Fratakelsen av den rettslige handleevnen kan være begrenset helt ned til bestemte eiendeler eller bestemte disposisjoner.[111] Som eksempel nevnes det i forarbeidene at en person kan fratas den rettslige rådigheten over faste eiendommer, bestemte bankkonti, bestemte aksjeposter mv., men kan beholde rådigheten over andre bankkonti, inntekter fra arbeid, trygd, pensjoner eller liknende.[112] På det området eller for den disposisjonen personen er fratatt rettslig handleevne for, vil ikke personen kunne foreta rettslige handlinger uten samtykke fra verge. Hvorvidt en person som bistås av verge, og som delvis er fratatt den rettslige handleevnen, kan inngå en avtale om utstedelse av eID og selv bruke eID til å foreta rettslige handlinger, beror derfor på en konkret vurdering av omfanget av den enkeltes vergemål. Dersom fratakelsen av den rettslige handleevnen gjelder forhold som påvirker utstedelse eller bruk av eID på øverste sikkerhetsnivå vil ikke personen kunne ha en eID på øverste sikkerhetsnivå slik eID-ordningene er utformet i dag.

Det neste som må vurderes, er hvorvidt kontraheringsnektelse begrunnet i at en person bistås av verge, er i strid med diskrimineringsforbudet. Å nekte personer som bistås av verge, utstedelse av eID er direkte forskjellsbehandling på grunnlag av funksjonsnedsettelse.[113] Det avgjørende er derfor om forskjellsbehandlingen er lovlig etter likestillings- og diskrimineringsloven § 9. Som nevnt gjelder det her tre kumulative vilkår: Forskjellsbehandlingen må ha et saklig formål, være nødvendig for å oppnå formålet og ikke være uforholdsmessig inngripende overfor dem som forskjellsbehandles. Denne vurderingen vil variere for de ulike vergemålstypene, og de vurderes derfor hver for seg i det følgende.

3.7.2 Personer med rettslig handleevne som bistås av verge

Det første som skal vurderes, er hvorvidt kontraheringsnektelse av personer med rettslig handleevne som bistås av verge, er lovlig forskjellsbehandling. Det første vilkåret som må være oppfylt, er at nektelsen følger et saklig formål. Dette beror dels på om begrunnelsen er sann, og dels på om den er legitim i det konkrete tilfellet.[114] For personer med rettslig handleevne som bistås av verge, begrunner tilbyderne av eID avslaget med at eID er strengt personlig.[115] Et avslag begrunnet i at en person ikke kan benytte seg av eID-en på egen hånd, kan utgjøre et saklig formål. Et krav om selvstendig bruk vil forhindre misbruk og styrke tilliten til eID som identifikasjonsbevis. Begrunnelsen ivaretar dermed en beskyttelsesverdig interesse.

Formålet må også være legitimt i det konkrete tilfellet. Som nevnt ovenfor er ikke vergemålsloven til hinder for at en person med rettslig handleevne som bistås av verge, inngår avtale om utstedelse av eID og heller ikke om bruk av eID. Kontraheringsnektelse vil derfor ikke ha et saklig formål i et slikt tilfelle.

At kontraheringsnektelse av personer som bistås av verge uten å være fratatt rettslig handleevne, ikke er lovlig forskjellsbehandling, ble også lagt til grunn av Diskrimineringsnemnda i en klagesak fra 2021.[116] Saken gjaldt spørsmål om en bank hadde handlet i strid med diskrimineringsforbudet i likestillings- og diskrimineringsloven § 6 når den nektet å utstede BankID til en person som hadde bistand av verge uten å være fratatt den rettslige handleevnen. Banken begrunnet avslaget med kravet om «sole control» i eIDAS-forordningen artikkel 26 og kravet om selvstendig bruk som kommer til uttrykk i avtalen mellom banken og klager. Nemnda kom til at nektelsen utgjorde direkte forskjellsbehandling på grunnlag av funksjonsnedsettelse. I vurderingen av om forskjellsbehandlingen var lovlig, uttalte Diskrimineringsnemnda at ettersom klageren hadde den rettslige handleevnen i behold, kom ikke punkt 3.4 i «Regler om BankID» om at BankID ikke kan utstedes til personer som helt eller delvis er fratatt rettslig handleevne, til anvendelse. At personen hadde rettslig handleevne, gjorde det også tvilsomt om prinsippet om «sole control» i eIDAS-forordningen ville bli brutt. Nemnda kom videre til at forskjellsbehandlingen ikke kunne begrunnes i antesipert mislighold av kravet om selvstendig bruk i avtalen mellom banken og klageren. Diskrimineringsnemnda konkluderte med at det ikke forelå saklig grunnlag for å nekte å inngå avtale om BankID, og at forskjellsbehandlingen derfor var i strid med forbudet mot diskriminering av personer med funksjonsnedsettelse i likestillings- og diskrimineringsloven § 6.

Det er først når en person helt eller delvis er fratatt rettslig handleevne, at det oppstår problemer knyttet til selvstendig bruk av eID. En person med rettslig handleevne som bistås av verge, har kompetanse til å foreta rettslige handlinger på lik linje med personer som ikke bistås av verge. Det er derfor ikke større fare for at kravet om selvstendig bruk ikke blir overholdt i slike tilfeller, enn det er ved utstedelse til en funksjonsfrisk person. En kontraheringsnektelse begrunnet i kravet om enekontroll vil ikke ha et saklig formål etter likestillings- og diskrimineringsloven § 9 for personer med rettslig handleevne som bistås av verge, slik Diskrimineringsnemnda også kom til.

En kontraheringsnektelse av personer med rettslig handleevne som bistås av verge, oppfyller dermed ikke vilkårene for lovlig forskjellsbehandling i likestillings- og diskrimineringsloven § 9. En slik kontraheringsnektelse er i strid med diskrimineringsforbudet. Kontraheringsnektelse begrunnet i at en person bistås av verge uten å være fratatt den rettslige handleevnen, har ikke «saklig grunn».

3.7.3 Personer som bistås av verge, og som helt eller delvis er fratatt den rettslige handleevnen

Det neste som skal vurderes, er om kontraheringsnektelse av personer som bistås av verge, og som helt eller delvis er fratatt den rettslige handleevnen, utgjør lovlig forskjellsbehandling etter likestillings- og diskrimineringsloven § 9. Dette innebærer for det første at forskjellsbehandlingen må ha et saklig formål. At eID ikke kan utstedes til personer som helt eller delvis er fratatt den rettslige handleevnen, er begrunnet i at eID er strengt personlig. Som det fremgår av drøftelsen i punkt 2.2, kan kravet om enekontroll i eIDAS-forordningen være grunnlag for kontraheringsnektelse. Dette taler for at nektelsen har et saklig formål.

Kravet om saklig formål innebærer imidlertid også at begrunnelsen må være legitim i det konkrete tilfellet. I «Regler om BankID» heter det at BankID ikke skal utstedes til personer som helt eller delvis er fratatt den rettslige handleevnen.[117] Buypass har som nevnt tilsvarende praksis. Tilbyderne avviser tilsynelatende personer som bistås av verge, og som helt eller delvis er fratatt den rettslige handleevnen, uten å foreta en konkret vurdering av omfanget av det aktuelle vergemålet. Som nevnt skal vergemålet skreddersys til den enkeltes behov for bistand. Dette innebærer at en person kan være fratatt deler av den rettslige handleevnen uten at det påvirker personens evne til å inngå avtale om eID og bruk av eID.[118] I slike tilfeller vil personen være i stand til å bruke eID på egen hånd. Dersom tilbyderne nekter utstedelse til disse personene, vil ikke forskjellsbehandlingen følge et saklig formål. Når tilbyderne ikke foretar en konkret vurdering av hvert enkelt vergemål, vil avgjørelsen ikke bygge på et korrekt faktum. Vilkåret om saklig formål vil derfor ikke være oppfylt.

Gitt at det foretas en konkret vurdering, og tilbyderne kommer til at personen som bistås av verge, er fratatt den rettslige handleevnen på en slik måte at eID-en ikke kan brukes av personen på egen hånd, vil nektelsen ha et saklig formål som er av en slik art at prinsippet om likebehandling bør vike. I slike tilfeller vil vilkåret om saklig formål være oppfylt.

Videre gjelder det krav om at forskjellsbehandlingen skal være nødvendig og egnet til å oppnå det saklige formålet. Dersom det er foretatt en konkret vurdering hvor det konkluderes med at personen ikke har tilstrekkelig rettslig handleevne til å kunne benytte seg av en eID, vil nektelse være egnet til å oppnå formålet om å forhindre misbruk og styrke tilliten til eID. Formålet kan også oppnås på en ikke-diskriminerende måte ved for eksempel å gi tilgang via vergens egen eID.[119] En slik løsning finnes ikke på øverste sikkerhetsnivå i dag, men det er teknisk mulig.[120] Når det p.t. ikke eksisterer, kan imidlertid ikke dette medføre at kravet om nødvendighet ikke er oppfylt.

I tillegg kan ikke forskjellsbehandlingen være uforholdsmessig inngripende overfor den som forskjellsbehandles. Å ikke ha tilgang til eID på øverste sikkerhetsnivå er svært inngripende overfor den enkelte. Uten eID på øverste sikkerhetsnivå er det en rekke digitale offentlige og private tjenester som personen ikke får tilgang til. Å sikre at eID forblir personlig, er på den annen side et tungtveiende hensyn. Konsekvensene vil kunne være misbruk og en svekkelse av tilliten til eID som identifikasjonsmiddel. Formålet om å sikre at eID-en forblir personlig, er et legitimt formål. For personer som bistås av verge, og som helt eller delvis er fratatt den rettslige handleevnen slik at personen ikke kan inngå avtale om utstedelse av eID eller bruke eID personlig, vil nektelse kunne være forholdsmessig.

Etter dette kan kontraheringsnektelse av personer som bistås av verge, og som helt eller delvis er fratatt den rettslige handleevnen, være lovlig etter likestillings- og diskrimineringsloven § 9. Dette beror imidlertid på en konkret vurdering av omfanget av det enkelte vergemålet. Dersom bankene nekter kontrahering begrunnet i punkt 3.4 i «Regler om BankID» uten at det foretas en konkret vurdering, vil nektelsen være i strid med diskrimineringsforbudet i likestillings- og diskrimineringsloven § 9. Buypass opplyser om at det fremkommer at en person bistås av verge ved identifisering og utlevering av Buypass ID, og at disse ikke anses for å ha gyldig identitetsbevis.[121] Det tilsvarende vil derfor gjelde for Buypass. Det må foretas en konkret vurdering av vergemålets omfang for personer som bistås av verge, og som helt eller delvis er fratatt den rettslige handleevnen. Når kontraheringsnektelse begrunnes i at en person helt eller delvis er fratatt den rettslige

handleevnen, uten at det foretas en konkret vurdering, utgjør ikke kontraheringsnektelsen lovlig forskjellsbehandling etter likestillings- og diskrimineringsloven § 9. En slik kontraheringsnektelse vil være i strid med diskrimineringsforbudet og følgelig ikke ha «saklig grunn».

Et argument som blir benyttet av tilbyderne mot at det må foretas en konkret vurdering, er at opplysningene om omfanget av vergemålet er taushetsbelagte.[122] Etter vergemålsloven § 46 har oppnevnt verge som hovedregel taushetsplikt. Etter § 46 tredje ledd tredje punktum heter det at forvaltningsloven § 13 a gjelder tilsvarende. I forvaltningsloven § 13 a nr. 1 heter det at taushetsplikten i forvaltningsloven § 13 ikke er til hinder for at «opplysninger gjøres kjent for dem som de direkte gjelder, eller for andre i den utstrekning de som har krav på taushet samtykker». Henvisningen innebærer at så fremt personen som bistås av verge, er samtykkekompetent, kan personen samtykke til at opplysninger om vergemålets eksistens og rekkevidde gjøres kjent. I forarbeidene heter det: «Er den vergetrengende samtykkekompetent, vil han eller hun både kunne gi relevante opplysninger selv og samtykke til at vergen fritas for taushetsplikt.»[123] Taushetsplikten er derfor ikke til hinder for en konkret vurdering av vergemålets omfang så fremt personen som bistås av verge, samtykker til dette.

4 Oppsummering og rettspolitiske betraktninger

4.1 Oppsummering

Gjennom artikkelen er det fastlagt at det eksisterer en ulovfestet partiell kontraheringsplikt for tilbydere av eID på øverste sikkerhetsnivå. Tilbyderne har adgang til å avvise forespørsel om utstedelse av eID dersom det foreligger «saklig grunn» til kontraheringsnektelse. Ettersom «saklig grunn» er en rettslig standard, er det ikke mulig å gi en uttømmende beskrivelse av når tilbyderne har saklig grunn til kontraheringsnektelse. Gjennom artikkelen har jeg imidlertid kartlagt noen retningslinjer for når saklig grunn kan – og ikke kan – foreligge.

For det første påvirkes tilbydernes kontraheringsplikt av de lovbestemte kravene som gjelder for utstedelse av eID. Dersom utstedelse av eID vil være i strid med lovbestemte krav for utstedelse, vil tilbyderne ha «saklig grunn» til kontraheringsnektelse, siden en privatrettslig kontraheringsplikt ikke kan foreligge samtidig som et offentligrettslig krav pålegger kontraheringsnektelse.

For det andre påvirkes tilbydernes kontraheringsplikt av deres forpliktelser etter diskrimineringsforbudet. Selv om rettsvirkningene av diskriminering etter likestillings- og diskrimineringsloven primært er oppreisning og erstatning, eksisterer det en plikt til å kontrahere når plikten til ikke å diskriminere sees i sammenheng med den ulovfestede kontraheringsplikten. Selv om pliktene delvis sammenfaller, står de ikke i et én-til-én-forhold. Gjennom artikkelen er det blitt klart at en kontraheringsnektelse kan være i strid med kontraheringsplikten selv om den ikke er i strid med diskrimineringsforbudet. Tilbydernes forpliktelser etter den ulovfestede kontraheringsplikten strekker seg dermed lenger enn forpliktelsene etter diskrimineringsforbudet.

Med disse retningslinjene fastsatt er det mulig å vurdere konkret hvorvidt begrunnelsene tilbyderne påberoper seg, utgjør saklig grunn til kontraheringsnektelse. I artikkelen har jeg sett nærmere på seks utvalgte typetilfeller, herunder påberopte grunnlag for kontraheringsnektelse. Gjennom tolkning av lovbestemte krav til utstedelse av eID, tolkning av diskrimineringsregelverket og konkrete vurderinger har jeg kommet frem til at tilbyderne har saklig grunn til kontraheringsnektelse dersom personen ikke oppfyller legitimasjonskravet i selvdeklarasjonsforskriften, dersom personen er fratatt rettslig handleevne på en slik måte at det påvirker bruk av eID, eller dersom bankenes forpliktelser etter hvitvaskingsloven danner grunnlag for avvisning. Nektelse på grunnlag av manglende RFID-brikke, manglende norsk fødselsnummer eller fordi en person med rettslig handleevne bistås av verge, er ikke saklig begrunnet. Samtlige av de tre sistnevnte kontraheringsnektelsene vil også utgjøre diskriminering. Det er også tvilsomt hvorvidt bankenes nektelse på grunn av manglende opprettelse av kundeforhold utgjør saklig grunn.

Artikkelen avdekker en rekke svakheter knyttet til dagens ordning, hvor staten har overlatt utstedelse av eID på øverste sikkerhetsnivå til private aktører. Som det fremgår av det ovennevnte, eksisterer det flere tilfeller hvor tilbydere av eID har saklig grunn til kontraheringsnektelse. Myndighetenes mål om at alle innbyggere i Norge skal ha mulighet til å få utstedt eID på øverste sikkerhetsnivå, kan dermed ikke nås gjennom dagens system. Videre avdekker artikkelen manglende sammenheng i dagens regelverk. I det følgende vil jeg redegjøre for et utvalg av problemstillingene som oppstår, og drøfte disse i ett rettspolitisk perspektiv.

4.2 Rettspolitiske betraktninger

4.2.1 Problemer knyttet til at private aktører er ansvarlig for utstedelse av eID på øverste sikkerhetsnivå

En svakhet ved at eID på øverste sikkerhetsnivå er overlatt til private aktører, er at man som innbygger i Norge er tvunget til å inngå en privatrettslig avtale dersom man ønsker eID på øverste sikkerhetsnivå. BankID er den klart største aktøren, men er samtidig den tilbyderen som er pålagt de strengeste lovbestemte kravene. BankIDs tilknytning til økonomiske disposisjoner medfører at det er vanskelig eller umulig å få utstedt BankID for enkelte grupper. For det første gjør denne tilknytningen at personer som har fått oppnevnt verge, og som er helt eller delvis fratatt den rettslige handleevnen i økonomiske forhold, ikke kan få utstedt BankID. For det andre gjør denne tilknytningen at hvitvaskingsloven kommer til anvendelse. Dette innebærer at en kontraheringsnektelse begrunnet i hvitvaskingsloven kan ha «saklig grunn».

At finansnæringen er ansvarlig for utstedelsen av den mest brukte eID-ordningen i Norge, fører dermed til ytterligere begrensninger i når bankene er forpliktet til å kontrahere, utover de begrensningene som følger av reglene i eIDAS-forordningen. Dette er problematisk når eID på øverste sikkerhetsnivå er nødvendig for å få tilgang til en rekke offentlige tjenester. Disse problemene kan løses ved at staten oppretter en statlig eID på øverste sikkerhetsnivå. På den måten vil staten kunne begrense bruksområdet og gjøre nødvendige tilpasninger.

Et annet problem knyttet til at eID på øverste sikkerhetsnivå utstedes av private, er at tilbyderne stiller ulike vilkår for utstedelse. Det er ikke bare variasjon i vilkårene mellom de ulike aktørene; også bankene har ulike kontraheringsvilkår seg imellom. Dette leder til usaklig forskjellsbehandling. Siden tilbyderne har en ulovfestet kontraheringsplikt, er det adgang til å føre offentlig kontroll av kontraheringsvilkår gjennom domstolene. Å bringe en sak inn for domstolene er imidlertid ressurskrevende, og det vil derfor trolig sjelden være aktuelt for en person som har blitt nektet utstedelse, å bringe saken inn for domstolene for å overprøve kontraheringsnektelsen. Manglende domstolskontroll av tilbydernes kontraheringsnektelse vil igjen føre til at sakligheten av kontraheringsvilkår og kontraheringsnektelser ved avtale om utstedelse av eID sjelden blir kontrollert av det offentlige.

Dette taler for at den ordningen som gjaldt etter prisloven § 23, ville vært en bedre løsning for prøvelse av gyldigheten til en kontraheringsnektelse for avtale om utstedelse av eID. Etter denne regelen kunne forvaltningsorganet Prisrådet forby en næringsdrivende å nekte forretningsforbindelse med en annen. Ved vurderingen av opphevelse av ordningen argumenterte lovgiver blant annet med at Prisrådets virksomhet hadde vært ressurskrevende, og at det offentlige hadde båret kostnadene.[124] Argumentet gjør seg imidlertid først og fremst gjeldende når det er spørsmål om nektelse overfor en som driver næringsvirksomhet. I vårt tilfelle dreier det seg om kontraheringsnektelse overfor en privatperson. Videre er tjenesten som nektes, en tjeneste som staten gjennom digitaliseringen av den offentlige forvaltningen har gjort til en nødvendig forutsetning for den enkelte å ha for å kunne utøve sine rettigheter. Det er da lite rimelig at det er enkeltpersoner som potensielt må bære kostnadene for kontroll av gyldigheten av en kontraheringsnektelse.

Alternativt kan også dette problemet løses ved å opprette en statlig eID på øverste sikkerhetsnivå. Da vil det være opp til staten å bestemme vilkårene for utstedelse, og på den måten vil staten kunne forhindre at det stilles usaklige kontraheringsvilkår. Gjennom en statlig eID på øverste sikkerhetsnivå vil staten kunne sikre at alle har mulighet til å skaffe eID på øverste sikkerhetsnivå.

4.2.2 Dagens system kan utgjøre dobbelt diskriminering fra statens side

Gjennom dagens system for eID har staten overlatt viktig offentlig infrastruktur til private aktører. Staten har tatt i bruk et system som de private tilbyderne har legitime grunner til å utforme som de har gjort, uten å gjøre tilpasninger. Samtidig har staten satt innlogging med eID på øverste sikkerhetsnivå som krav for en rekke digitale offentlige tjenester. På den måten har staten gjort det til en nødvendighet å ha eID på øverste sikkerhetsnivå.

Samtidig fører statens bruk av private aktører til utstedelse av eID på øverste sikkerhetsnivå til at en rekke grupper ikke har mulighet til å få utstedt eID. Som artikkelen illustrerer, vil ikke en privatrettslig kontraheringsplikt avhjelpe alle problemene knyttet til utstedelse av eID på øverste sikkerhetsnivå i dagens system. Papirløse flyktninger har ikke mulighet til å skaffe seg legitimasjonsdokumenter som oppfyller kravene i selvdeklarasjonsforskriften. Videre har ikke tilbyderne kontraheringsplikt for personer som bistås av verge, og som helt eller delvis er fratatt den rettslige handleevnen på en slik måte at det påvirker bruk av eID. Etter diskrimineringsforbudets krav om tilgjengelighet og plikten til universell utforming er tilbyderne forpliktet til å utvikle en alternativ løsning for denne gruppen. Manglende oppfyllelse av disse kravene har imidlertid ikke blitt fulgt opp av staten. Dette fører til digital ekskludering. Personer som faller utenfor systemet, har ikke mulighet til å utøve sine rettigheter og ta del i samfunnet slik de har rett til. Gjennom diskrimineringsforbudet er staten forpliktet til å sikre lik tilgang til offentlige tjenester. Ulik eller manglende tilgang til offentlige tjenester som den enkelte har krav på, vil kunne utgjøre brudd på diskrimineringsforbudet. Det kan derfor argumenteres for at dagens system medfører diskriminering på to nivåer: For det første er det diskriminerende i seg selv at staten har tatt i bruk et system som ikke alle innbyggere har mulighet til å få tilgang til. For det andre har ikke staten gjort nok for å sikre den enkeltes rett til ikke å bli diskriminert ved utstedelse av eID fra private tilbydere.

4.2.3 Det er behov for et samlet regelverk som regulerer utstedelse av eID

Artikkelen illustrerer at utstedelse av eID på øverste sikkerhetsnivå påvirkes av en rekke ulike regelsett, uten at det er sammenheng mellom disse. Det gjelder ulike regler for de ulike tilbyderne. For eksempel virker det lite hensiktsmessig at hvitvaskingsloven skal komme til anvendelse på utstedelse av BankID selv når dette utstedes separat, samtidig som hvitvaskingsloven ikke kommer til anvendelse for hverken Buypass eller Commfides.

Videre er de reglene som påvirker utstedelse av eID på øverste sikkerhetsnivå, først og fremst rettet mot staten og tilbyderne. Det er ingen regler utover den ulovfestede kontraheringsplikten som direkte regulerer forholdet mellom tilbyderne og personer som ønsker å få utstedt eID. At forhold mellom to private parter ikke er lovregulert, er normalt på avtalerettens område. Dette avtaleforholdet skiller seg imidlertid fra tradisjonell avtaleinngåelse. Det er her tale om spørsmål om tilgang til samfunnskritisk infrastruktur for personer som ønsker å delta i det norske samfunnet. Utstedelse av eID på øverste sikkerhetsnivå er overlatt til det private, samtidig som det er helt nødvendig å ha eID for å delta digitalt i samfunnet. Ved slike avtaletyper er ofte forholdet mellom tilbyder og enkeltperson lovregulert, slik som for eksempel for forsikring og grunnleggende banktjenester.

Videre illustrerer artikkelen at dagens ordning medfører at personer blir diskriminert ved utstedelse av eID på øverste sikkerhetsnivå, og at dagens system fører til digital ekskludering. Dette tyder på at det er et behov for et samlet regelverk som stiller klare krav til tilbydere om når de er forpliktet til å utstede eID, og som enkelt kan håndheves av staten.

4.2.4 Ny nasjonal strategi for eID

I slutten av april 2023 publiserte Kommunal- og distriktsdepartementet en nasjonal strategi for eID i offentlig sektor. Her er et av de fem overordnede målene for strategien at alle relevante brukergrupper skal kunne skaffe seg en eID på det sikkerhetsnivået de har behov for.[125] Et av tiltakene for å realisere dette målet er at staten skal utrede hvordan eID på høyt sikkerhetsnivå kan gjøres tilgjengelig for flere. Her uttaler departementet at det både skal utredes i hvilken grad det skal lages en statlig eID på øverste sikkerhetsnivå, og det skal utredes i hvilken grad tilbyderne kan pålegges å utstedes til flere grupper med grunnlag i kontraheringsplikten og diskrimineringsforbudet.[126]

Litteraturliste

Norske rettskilder

Lov

1814	Lov 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven)
1918	Lov 31. mai 1918 nr. 4 om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer [avtaleloven]
1953	Lov 26. juni 1953 nr. 4 om kontroll og regulering av priser, utbytte og konkurranseforhold (prisloven) [opphevet]
1967	Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven)
1989	Lov 16. juni 1989 nr. 69 om forsikringsavtaler (forsikringsavtaleloven)
1990	Lov 29. juni 1990 nr. 50 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven)
1992	Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven)
1993	Lov 11. juni 1993 nr. 65 om konkurranse i ervervsvirksomhet (konkurranseloven) [opphevet]
1997	Lov 19. juni 1997 nr. 82 om pass (passloven)
2000	Lov 2. juni 2000 nr. 39 om apotek (apotekloven)
2005	Lov 20. mai 2005 nr. 28 om straff (straffeloven)
2008	Lov 15. mai 2008 nr. 35 om utlendingers adgang til riket og deres opphold her (utlendingsloven)
2010	Lov 26. mars 2010 nr. 9 om vergemål (vergemålsloven)
2017	Lov 16. juni 2017 nr. 50 om Likestillings- og diskrimineringsombudet og Diskrimineringsnemnda (diskrimineringsombudsloven)
2017	Lov 16. juni 2017 nr. 51 om likestilling og forbud mot diskriminering (likestillings- og diskrimineringsloven)
2018	Lov 1. juni 2018 nr. 23 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven)
2018	Lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)

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

Forskrift

2019	Forskrift 21. november 2019 nr. 1578 om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften)
2019	Forskrift 21. november 2019 nr. 1577 om tillitstjenester for elektroniske transaksjoner
2020	Forskrift 9. oktober 2020 nr. 2012 om pass og nasjonalt ID-kort (pass- og ID-kortforskriften)

Forarbeider

Ot.prp.nr.43 (1989–1990)	*Om lov om produksjon, omforming, overføring, omsetning og fordeling av energi m.m. (Energiloven)*
Ot.prp.nr.41 (1998–1999)	*Om lov om finansavtaler og finansoppdrag (finansavtaleloven)*
Ot.prp.nr.110 (2008–2009)	*Om lov om vergemål (vergemålsloven)*
Prop.80 L (2016–2017)	*Lov om Likestillings- og diskrimineringsombudet og Diskrimineringsnemnda (diskrimineringsombudsloven)*
Prop.81 L (2016–2017)	*Lov om likestilling og forbud mot diskriminering (likestillings- og diskrimineringsloven)*
Prop.40 L (2017–2018)	*Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven)*
Prop.92 LS (2019–2020)	*Lov om finansavtaler (finansavtaleloven) og samtykke til godkjennelse av EØS-komiteens beslutninger nr. 125/2019 og 130/2019 av 8. mai 2019 om innlemmelse i EØS-avtalen av direktiv 2014/17/EU om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål (boliglåndirektivet) og delegert kommisjonsforordning (EU) nr. 1125/2014*
NOU 1991:27	*Konkurranse for effektiv ressursbruk*
NOU 2009:14	*Et helhetlig diskrimineringsvern*

Rettspraksis

Rt-2010-291 (Vangen Eiendom)

Rt-2014-36

Forvaltningspraksis

Rundskriv mv.

Finanstilsynet (2022)

Kommunal- og distriktsdepartementet (2023)

Kommunal- og moderniseringsdepartementet (2019)

Høringsnotat

Justis- og beredskapsdepartementet (2022)

Nemnd- og ombudspraksis

Diskrimineringsnemnda (2021)

Finansklagenemnda Bank (2022)

Likestillings- og diskrimineringsnemnda (2020)

Internasjonale rettskilder

Direktiver og forordninger

Direktiv (EU) 2015/849	*Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF* [Fjerde hvitvaskingsdirektiv]
Forordning (EU) nr. 910/2014	*Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske*

	transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF [eIDAS-forordningen]
Forordning (EU) 2015/1502	*Kommissionens gennemførelsesforordning (EU) 2015/1502 af 8. september 2015 om fastlæggelse af tekniske minimumsspecifikationer og procedurer for fastsættelse af sikringsniveauer for elektroniske identifikationsmidler i henhold til artikel 8, stk. 3 i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked* [Identifikasjonsnivåforordningen]

Konvensjoner og erklæringer

FNs verdenserklæring om menneskerettigheter	*Universal Declaration of Human Rights*, Paris, 10. desember 1948

Litteratur

Arnholm (1974)	Arnholm, Carl Jacob. *Lærebok i avtalerett*. Oslo: Tanum, 1974.
Bull (2003)	Bull, Hans Jacob. *Innføring i forsikringsrett – utkast til en lærebok*, 9. utg. Oslo: H.J. Bull, 2003.
Buypass (u.å.a)	Buypass. «Aldersgrense og andre betingelser» (u.å.) https://www.buypass.no/hjelp/hjelp-til-smartkort/bestilling-og-fornying/aldersgrense-og-andre-betingelser. Hentet 25. mars 2022.
Buypass (u.å.b)	Buypass. «Aldersgrense og andre betingelser» (u.å.) https://www.buypass.no/hjelp/buypass-id-i-mobil/bestilling/aldersgrense-og-andre-betingelser. Hentet 25. mars 2022.
Capgemini Invent (2019)	Capgemini Invent. *Områdegjennomgang av ID-forvaltningen* (6. september 2019). https://www.regjeringen.no/contentassets/fc0f9e0edef4440cb1ef5e8dd8ffad0e/07-09-2021-hovedrapport.pdf.
Commfides (u.å.)	Commfides. «Hvem kan få privat e-ID?» (u.å.). https://www.commfides.com/faq/4870/. Hentet 25. mars 2022.
Digitaliseringsdirektoratet (2021)	Digitaliseringsdirektoratet. *Behovsanalyse eID. Sluttbrukere. Sluttrapport* (2. juli 2021). [Tilsendt på e-post etter forespørsel om innsyn.]

Digitaliseringsdirektoratet (u.å.)	Digitaliseringsdirektoratet. «Hvilke e-ID støtter elektronisk signering?» (u.å.). https://eid.difi.no/nb/esignering/hvilke-e-id-stotter-elektronisk-signering. Hentet 21. mars 2022
Falch (2004)	Falch, Ingvald. *Rett til nett*. Oslo: Universitetsforlaget, 2004.
Giertsen (2021)	Giertsen, Johan. *Avtaler*, 4. utg. Oslo: Universitetsforlaget, 2021.
Haaskjold (2013)	Haaskjold, Erlend. *Kontraktsforpliktelser*. Oslo: Cappelen Damm, 2013.
Hellum og Strand (2022)	Hellum, Anne og Vibeke Blaker Strand. *Likestillings- og diskrimineringsrett*. Oslo: Gyldendal, 2022.
Helsenorge (u.å.)	Helsenorge. «Koronasertifikat for ikke-digitale brukere» (u.å.). https://www.helsenorge.no/koronasertifikat/om/ikke-digitale-brukere/ Hentet 12. februar 2023.
Dyrud mfl. (2022)	Lisa Dyrud, Lise Stefanussen og Sveinung Liland Hartveit. *Utlendingers tilgang til banktjenester*. Oslo: Jussbuss, 2022. [https://foreninger.uio.no/jussbuss/publikasjoner/masteroppgaver/jussbuss-rapport-om-utlendingers-tilgang-til-grunnleggende-banktjenester-og-bankid.pdf.].
Krüger og Møgelvang-Hansen (2001)	Krüger, Kai og Peter Møgelvang-Hansen. *Reklamens bindende virkning*. *TemaNord* 2001:549. Nordisk ministerråd, 2001.
Nasjonalt ID-senter (u.å.)	Nasjonalt ID-senter. *Biometri og identitet – utfordringer og nye muligheter for utlendingsforvaltningen*. Oslo: Nasjonalt ID-senter, u.å. https://www.nidsenter.no/globalassets/dokumenter/publikasjoner/nid-rapporter/rapport_biometri.pdf. Hentet 2. mai 2022.
Samarbeidsportalen (2022)	Samarbeidsportalen. «ID-porten 2022 – Statistikk og nøkkeltal for ID-porten – året som gjekk» (2022). https://samarbeid.digdir.no/id-porten/id-porten-2022/1142. Hentet 12. februar 2023.
Selvig (1993)	Selvig, Erling. «Kontraktsretten», i Birger Stuevold Lassen mfl. (red.), *Knophs oversikt over Norges rett*, 10. utg. Oslo: Universitetsforlaget, 1993, s. 298-553.
Sivertsen (2022)	Sivertsen, Erle Katrine. *Kontraheringsplikt for tilbydere av elektronisk identifikasjonsbevis (eID)*. Masteravhandling, Universitet i Oslo. DUO Vitnearkiv. http://urn.nb.no/URN:NBN:no-98966.
Stang (1935)	Stang, Fredrik. *Innledning til formueretten*. 3. utg., Oslo: Aschehoug, 1935.
Vipps (u.å.)	Vipps. «Trenger jeg BankID for å bruke Vipps?» (u.å.) https://vipps.no/hjelp/vipps/kom-i-gang-med-vipps/trenger-jeg-bankid-for-a-bruke-vipps/. Hentet 23.

mai 2022.

Wilhelmsen (1995) — Wilhelmsen, Trine-Lise. «Forsikringsselskapenes kontraheringsplikt». *Norsk forsikringsjuridisk forenings publikasjoner* nr. 69, Oslo, 1995.

Woxholth (2021) — Woxholth, Geir. *Avtalerett*, 11. utg. Oslo: Gyldendal, 2021.

Andre kilder

Private avtaledokumenter

Bits (2021) — Bits. «Regler om BankID» (26. mars 2021) https://www.bankid.no/globalassets/dokumenter/apne-sider/regler-om-bankid/regler-om-bankid-15.03.2018.pdf. Hentet 29. mai 2022.

Bits (u.å.) — Bits. «Avtale om BankID» (u.å.) https://www.bits.no/document/avtale-om-bankid. Hentet 19. april 2022.

Noter

1 Tall fra Samarbeidsportalen (2022) viser at BankID og BankID på mobil ble brukt i til sammen 267 millioner av totalt 286 millioner innlogginger via ID-porten i 2021. Dette utgjør 93,5 prosent av innloggingene.

2 Etter eIDAS-forordningen artikkel 8 gjelder det tre ulike sikkerhetsnivåer: «lavt», «betydelig» og «høyt». Klassifiseringen etter sikkerhetsnivå gjøres for å angi graden av tillit til at den påståtte identiteten er korrekt.

3 Kommunal- og moderniseringsdepartementet (2019) s. 35.

4 Capgemini Invent (2019) punkt 11.1 på s. 187.

5 Dette gjelder blant annet Helsenorge.no, NAV, Lånekassen, betalingstjenesten Vipps og billettkjøp i Ruter-appen.

6 Tall oppgitt på e-post fra Digitaliseringsdirektoratet mottatt 30. mars 2022. Her opplyste Digitaliseringsdirektoratet om at av totalt 4950 tjenester som på det tidspunktet var tilgjengelig via ID-porten, var det krav om innlogging med eID på øverste sikkerhetsnivå for 1040 av disse. ID-porten er en felles innloggingsløsning ved bruk av eID for offentlige tjenester på internett.

7 Dette gjelder for eksempel for tilbydere av forsikring og tilbydere av grunnleggende banktjenester, jf. forsikringsavtaleloven § 1B-3 første ledd og finansavtaleloven § 4-1 første ledd.

8 Giertsen (2021) s. 42.

9 Se for eksempel finansavtaleloven § 4-1 første ledd.

10 Apotekloven § 6-2.

11 Blant annet er tilbyderne forpliktet av kravene til eID-ordninger i selvdeklarasjonsforskriften og eIDAS-forordningen. I tillegg er bankene forpliktet av hvitvaskingsregelverket.

12 Grunnloven § 98 annet ledd.

13 Plikten til å forhindre diskriminering, herunder krav om tilgjengelighet for personer med funksjonsnedsettelse og plikt til universell utforming, er en del av diskrimineringsforbudet. Fordi personer som bistås av verge, er en av brukergruppene som opplever problemer med anskaffelse av eID, har jeg vurdert forholdet mellom kontraheringsplikten og den aktive plikten til å forhindre diskriminering i masteravhandlingen min, se Sivertsen (2022) s. 48-56.

14 Apotekloven § 6-2; forsikringsavtaleloven § 1b-3 første ledd; finansavtaleloven § 4-1 første ledd.

15 Helsenorge (u.å.).

16 Selvdeklarasjonsforskriften § 18.

17 Prisloven § 23 første ledd første punktum.

18 Falch (2004) s. 162-163 og Krüger og Møgelvang-Hansen (2001) s. 125-126.

19 NOU 1991:27 s. 160-161.

20 Se i samme retning Falch (2004) s. 162-163.

21 Wilhelmsen (1995) s. 47 flg. og Bull (2003) s. 105-107.

22 Forsikringsskadenemnda er i dag en del av Finansklagenemnda.

23 Wilhelmsen (1995) s. 48-51.

24 For eksempel forsikringsforetak og banker, jf. forsikringsavtaleloven § 1B-3 og finansavtaleloven § 4-1 første ledd.

25 Energiloven § 3-1.

26 Ot.prp.nr.43 (1989–1990) s. 87-88.

27 Se blant annet Stang (1935) s. 306; Arnholm (1974) s. 76; Selvig (1993) s. 356; Woxholth (2021) s. 29.

28 Stang (1935) s. 306.

29 Arnholm (1974) s. 76-77.

30 Selvig (1993) s. 356 og Falch (2004) s. 165.

31 Forskrift om tillitstjenester for elektroniske transaksjoner § 6.

32 eIDAS-forordningen artikkel 8 jf. artikkel 9.

33 Identifikasjonsnivåforordningen bilag 1 punkt 2.1.2.

34 Digitaliseringsdirektoratet (u.å.).

35 Se blant annet bankens anførsler i DIN-2021-168, hvor banken anfører at den som utsteder av BankID er forpliktet til å sikre at BankID er personlig i henhold til prinsippet om *sole control*.

36 Se i samme retning Haaskjold (2013) s. 49.

37 Prop.92 LS (2019–2020) s. 375, jf. Ot.prp.nr.41 (1998–1999) s. 98.

38 Prop.40 L (2017–2018) s. 89.

39 Likestillings- og diskrimineringsloven § 6.

40 Grunnloven § 98 annet ledd.

41 Likestillings- og diskrimineringsloven § 2.

42 Grunnloven § 98 annet ledd.

43 Denne tanken kommer direkte til uttrykk i FNs verdenserklæring om menneskerettigheter artikkel 1.

44 Rt-2010-291 (Vangen Eiendom) avsnitt 38.

45 Se Sivertsen (2022) s. 34-36 for en nærmere drøftelse av betydningen av at tilbyderne kun er forpliktet av likestillings- og diskrimineringsloven § 6, som har en uttømmende liste over diskrimineringsgrunnlag.

46 Likestillings- og diskrimineringsloven §§ 7 og 8.

47 Prop.81 L (2016–2017) s. 100.

48 Se Hellum og Strand (2022) s. 230-286 for en nærmere gjennomgang av innholdet i de tre grunnvilkårene for diskriminering. Se også Sivertsen (2022) s. 40-47 for en presentasjon av vilkårene knyttet opp mot artikkelens tema.

49 Jf. blant annet Grunnloven § 98.

50 Diskrimineringsombudsloven § 11 første og annet ledd.

51 Prop.80 L (2016–2017) s. 105.

52 Straffeloven § 186 første ledd.

53 Selvig (1993) s. 356.

54 NOU 2009:14 s. 37.

55 Se blant annet Dyrud mfl. (2022) s. 48 flg., Diskrimineringsnemndas vedtak av 30. juni 2021 (DIN-2021-168), Likestillings- og diskrimineringsnemndas vedtak og uttalelse av 28. september 2020 (DIN-2019-439) og Finansklagenemnda Banks avgjørelse i klagesak av 15. mars 2022 (FinKN-2022-234).

56 Rt-2014-36.

57 Se Dyrud mfl. (2022) om utlendingers tilgang til banktjenester for en nærmere gjennomgang av problemene knyttet til utstedelse av reisedokumenter fra norske myndigheter til utenlandske statsborgere.

58 Utlendingsloven § 64.

59 Se Sivertsen (2022) s. 58-59 for en nærmere drøftelse av dette.

60 Dyrud mfl. (2022) s. 49-56.

61 Passloven § 6 annet ledd.

62 Pass- og ID-kortforskriften § 6-1 første ledd.

63 Dyrud mfl. (2022) s. 52 og Digitaliseringsdirektoratet (2021) s. 22.

64 Nasjonalt ID-senter (u.å.) s. 9-10.

65 Identifikasjonsnivåforordningen punkt 2.1.2, sikringsniveau «høj» nr. 1 bokstav a.

66 Likestillings- og diskrimineringsloven § 8.

67 Likestillings- og diskrimineringsloven § 6 første ledd.

68 Prop.40 L (2017–2018) s. 89.

69 Hvitvaskingsloven § 4 første ledd bokstav a.

70 Hvitvaskingsloven § 1 første ledd.

71 Direktiv (EU) 2015/849.

72 Straffeloven § 337 første ledd.

73 Straffeloven § 135.

74 Hvitvaskingsloven § 4.

75 Hvitvaskingsloven § 9.

76 Fjerde hvitvaskingsdirektiv artikkel 11 første ledd bokstav a.

77 Prop.40 L (2017–2018) s. 173-174.

78 Finanstilsynet (2022) punkt 4.1.2.1.

79 Hvitvaskingsloven § 1.

80 Prop.40 L (2017–2018) s. 173-174.

81 Prop.40 L (2017–2018) s. 177.

82 Prop.40 L (2017–2018) s. 90.

83 Prop.40 L (2017–2018) s. 89.

84 Sivertsen (2022) s. 68.

85 Finansklagenemnda Banks avgjørelse av 15. mars 2022 (FinKN-2022-234).

86 Buypass (u.å.a), Buypass (u.å.b) og Commfides (u.å.).

87 Bits (2021) punkt 3.4.

88 Dyrud mfl. (2022) s. 55.

89 Likestillings- og diskrimineringsloven § 6 første ledd.

90 Likestillings- og diskrimineringsloven § 8.

91 Likestillings- og diskrimineringsnemndas vedtak og uttalelse av 28. september 2020 (DIN-2019-439).

92 Prop.81 L (2016–2017) s. 315.

93 Bits (u.å.) punkt 2. Bits er bank- og finansnæringens infrastrukturselskap og er eid av Finans Norge.

94 Se punkt 2.1 for en nærmere analyse av dommen.

95 Tall fra Samarbeidsportalen (2022) viser at BankID og BankID mobil i 2022 ble brukt i 93,51 prosent av innloggingene gjennom ID-porten.

96 Dette gjelder blant annet for betalingstjenesten Vipps, se Vipps (u.å.).

97 Dyrud mfl. (2022) s. 53-54.

98 Disse opplysningene har kommet frem i samtaler om erfaringer med JURK, Jussbuss og Gatejuristen.

99 Prop.81 L (2016–2017) s. 315.

100 Bits (2021) punkt 3.4.

101 Diskrimineringsnemndas vedtak av 30. juni 2021 (DIN-2021-168).

102 E-post fra Buypass mottatt 23. november 2021, hvor det står: «Vi har i våre retningslinjer eller kundeavtale ikke eksplisitt skrevet om begrensninger knyttet til personer med helt eller delvis manglende rettslig handleevne, da det [ved] identifisering og utlevering av Buypass ID kommer frem [...] at slike personer ikke har gyldig identitetsbevis, men har verge. Verge må selv bestille og få utstedt eID på seg selv som egen person, som igjen skal gi vedkommende tilgang til tjenester på vegne av personen han/hun er verge for.»

103 E-post fra Commfides mottatt 9. mai 2022, hvor det på svar på spørsmål om vilkår for utstedelse av Commfides eID heter: «Her gjelder kun alderskravet [...] Vi kontrollerer ikke om en person for eksempel skulle ha blitt fratatt rettslig handleevne.»

104 Sivertsen (2022) s. 53-56.

105 Vergemålsloven § 21 tredje ledd annet punktum.

106 Ot.prp.nr.110 (2008–2009) s. 52.

107 Vergemålsloven § 21 første ledd annet punktum.

108 Ot.prp.nr.110 (2008–2009) s. 179.

109 Ot.prp.nr.110 (2008–2009) s. 179.

110 Ot.prp.nr.110 (2008–2009) s. 179.

111 Vergemålsloven § 22 annet ledd annet punktum.

112 Ot.prp.nr.110 (2008–2009) s. 181.

113 Likestillings- og diskrimineringsloven §§ 6 og 7.

114 Prop.81 L (2016–2017) s. 315.

115 Se for eksempel DIN-2021-168.

116 DIN-2021-168.

117 Bits (2021) punkt 3.4.

118 Vergemålsloven §§ 20 til 23.

119 Spørsmålet om utvikling av digitale fullmaktløsninger, hvor løsningen med at vergen kan bruke egen eID når vergen utfører oppgaver på vegne av personen som vedkommende er oppnevnt som verge for, spesifikt ble nevnt, har vært på høring og er under pågående vurdering, jf. Justis- og beredskapsdepartementet (2022) s. 3.

120 Diskrimineringsforbudets krav om tilgjengelighet og plikt til universell utforming kan medføre en plikt for tilbyderne til å utvikle en alternativ løsning. Se Sivertsen (2022) s. 53-56.

121 E-post fra Buypass mottatt 23. november 2021.

122 At dette argumentet påberopes av tilbyderne, har kommet frem under samtaler med representanter for tilbyderne og med personer i støtteorganisasjoner for personer med funksjonsnedsettelse.

123 Ot.prp.nr.110 (2008–2009) s. 200.

124 NOU 1991:27 s. 160.

125 Kommunal- og distriktsdepartementet (2023) s. 7.

126 Kommunal- og distriktsdepartementet (2023) s. 26.

Prosessbyrden ved betalingssvindel – Om bankens tilbakeføringsplikt ved ikke-godkjente betalingstransaksjoner

Vebjørn Wold[1]

Fagfellevurdert artikkel

1 Innledning

1.1 Tema og problemstilling

Misbruk av elektroniske betalingsinstrumenter, som betalingskort eller kombinasjonen BankID og nettbank, er blitt en vanlig måte å svindle privatpersoner på. Slik svindel er gjerne et resultat av at uvedkommende får tilgang til betalingsinstrumentet, inkludert eventuelle koder eller passord som er nødvendig for å iverksette transaksjoner. En bankkunde lures kanskje av en e-post som leder kunden til en falsk nettside. Kunden taster inn sikkerhetsinformasjon på denne nettsiden, og svindleren bruker informasjonen til å logge inn i kundens nettbank og tappe kundens konto. I Norge er omfanget av slik svindel betydelig. Finanstilsynet rapporterte i 2021 om årlige tap på 346 millioner kroner for kontooverføringer alene.[2]

Tapsfordelingen for denne typen hendelser reguleres av finansavtaleloven 2020,[3] som på dette punktet gjennomfører deler av EUs reviderte betalingstjenestedirektiv (PSD II).[4] Utgangspunktet, som fremgår av lovens § 4-30 første ledd, er at det er banken som må bære tapet etter ikke-godkjente betalingstransaksjoner og eventuelt forsøke å stille svindleren til ansvar.[5] Den angitte begrunnelsen for en slik hovedregel har vært at banken kan pulverisere tapene gjennom å spre dem over kundemassen, og at befolkningen skal kunne ha tillit til elektroniske betalingssystemer.[6] Videre har det vært et mål i den europeiske reguleringen at bransjen får insentiver til å utvikle sikre betalingsløsninger.[7]

For å motvirke skjødesløs eller svikaktig adferd som setter betalingssystemene i fare, legger reglene også noe risiko på kunden. Hvis tapet skyldes «tap, tyveri eller uberettiget tilegnelse» av kundens betalingsinstrument, reduseres bankens ansvar med inntil 450 kroner, jf. finansavtaleloven § 4-30 annet ledd første punktum.[8] Om tapet også skyldes at kunden ved «grov uaktsomhet» har brutt sentrale plikter som følger med bruk av det

elektroniske betalingsinstrumentet – typisk plikten til å verne instrument og/eller passord eller pinkode fra uvedkommende – svarer kunden for 12 000 kroner etter samme bestemmelses tredje ledd.[9] Kunder som *forsettlig* eller *vedsvik* bryter de ovennevnte pliktene, svarer på sin side for hele tapet, jf. fjerde ledd.

Selv om lovgiver har tatt sikte på å begrense kundenes ansvar ved svindeltransaksjoner, er det praktiske utgangspunktet at tapet ligger hos kunden. Hvis ingen av partene foretar seg noe i etterkant av svindelen, vil kontoen bli stående slik svindleren etterlot den. Ved siden av de nevnte reglene om ansvarsfordeling oppstiller derfor finansavtaleloven § 4-32 første ledd en plikt for banken til å tilbakeføre det omstridte beløpet til kunden. Denne gjelder som utgangspunkt også i saker der kunden har vært grovt uaktsom eller har handlet med forsett.[10] Finansavtalelovens system er altså at man på den ene side har regler som fordeler det endelige ansvaret, og på den annen side har regler som pålegger banken tilbakeføring etter å ha blitt varslet om en ikke-godkjent transaksjon. Den endelige fordelingen av tapet fra transaksjonen avgjøres ut fra hvilken grad av skyld kunden eventuelt har utvist, jf. § 4-30.[11] Men også en kunde som har utvist høy grad av skyld, kan ha rett til å få kreditert sin konto «straks», jf. § 4-32.

Tema for denne artikkelen er tilbakeføringsregelen i finansavtaleloven § 4-32. Artikkelen tar opp to problemstillinger. Den første er rettsdogmatisk – nemlig hvilket virkeområde og innhold plikten til å tilbakeføre har, samt hvilke rettsvirkninger brudd på plikten innebærer. Den andre er mer rettspolitisk – nemlig hvilken rolle tilbakeføringsplikten spiller i fordelingen av risiko for eID-misbruk i betalingssystemet.

Fremstillingen er avgrenset til tilfeller der kunden er forbruker og lovens regulering av spørsmålet følgelig er ufravikelig.[12] Jeg vil gjøre en del tilbakeblikk til finansavtaleloven av 1999,[13] fordi det bidrar til å klarlegge innholdet i den nye finansavtaleloven. Retts- og bransjepraksis rundt 1999-loven utgjør også en viktig del av bakteppet for diskusjonen av tilbakeføringspliktens funksjon i tapsfordelingen mellom bank og kunde ved svindel. Finansavtalelovens regler om betalingstransaksjoner må for øvrig tolkes i lys av EØS-retten, ettersom finansavtaleloven 2020 §§ 4-30 og 4-32 gjennomfører det andre betalingstjenestedirektivet (PSD II) artikkel 73 og 74. Det vil i den sammenheng bli gjort enkelte sideblikk til andre lands gjennomføringer av PSD II, særlig til svensk rett. Målet er ikke å foreta noen fullverdig komparativ analyse, men å skissere ulike tolkningsmuligheter innenfor den felleseuropeiske reguleringen.

Opplegget videre er som følger: I resten av innledningen vil jeg si noe nærmere om problemstillingens aktualitet og betydning og forklare sammenhengen mellom tilbakeføringsregelen og det såkalte prosessbyrdespørsmålet. I artikkelens punkt 2 gjennomgår jeg bakgrunnen for bestemmelsen om tilbakeføring, inkludert hensynene den er ment å ivareta, og gjør noen observasjoner om bransjepraksis. Punkt 3 er en kort rettsdogmatisk fremstilling av plikten til tilbakeføring. Punkt 4 beskriver hvilke offentlige eller privatrettslige reaksjoner som kan følge av brudd på tilbakeføringsplikten. Punkt 5 drøfter hvilken rolle tilbakeføringsplikten spiller i fordelingen av risiko for eID-misbruk i betalingssystemet.

1.2 Tilbakeføringsplikten, prosessbyrden og risikofordelingen i betalingssystemet

I juridisk diskurs virker det å være en utbredt antakelse at den såkalte *søksmålsbyrden* – hvem som må reise sak om et rettsforhold – er et praktisk viktig spørsmål.[14] Den parten som ikke behøver å bringe saken inn for rettsapparatet for å oppnå det han eller hun ønsker, sies å ha en prosesstaktisk fordel.[15] I denne artikkelen vil jeg, i tråd med lovgivers egen språkbruk for betalingstransaksjonstilfellene, bruke betegnelsen «prosessbyrde» i stedet for «søksmålsbyrde».[16] Begrepet «prosessbyrde» fremstår for så vidt også mer presist, da førsteinstans ofte er Finansklagenemnda, hvor det ikke tas ut søksmål. Når jeg i det følgende diskuterer hvem som skal ha prosessbyrden, viser jeg altså til spørsmålet om hvilken part som må reise sak for å få gjort gjeldende at den andre parten skal bære hele eller deler av tapet fra transaksjonen.[17]

De fleste vil nok intuitivt foretrekke at det er motparten og ikke en selv som må ta initiativet for at det skal komme til tvist. Kostnaden i tid og penger ved å forfølge et krav kan virke avskrekkende. Det er heller ikke sikkert at den parten som har et krav, har tilstrekkelig kunnskap om rettsreglene til å forstå at man har en rettighet å gjøre gjeldende. Og inntil søksmål eller klage eventuelt blir reist, vil saken ha samme praktiske realitet som om man hadde vunnet. Spørsmålet om prosessbyrde kan sies å ha en særlig relevans i saker hvor partene har ulike forutsetninger hva gjelder ressurser og kunnskap, slik som i forbrukersaker.

Et eksempel på betydningen av antakelsen om at manglende kunnskap og ressurser hos forbrukere medfører at de ikke foretar nødvendige prosesshandlinger, ser vi i EU-domstolens saker om effektiv gjennomføring av forbrukerdirektiver.[18] I disse sakene har spørsmålet typisk vært om forbrukeren har tilgjengelig en tilstrekkelig

enkel prosess for å gjøre gjeldende sine EU-baserte rettigheter. I EU-domstolens saker har det dreid seg om nasjonale prosessregler for tvist og tvangsfullbyrdelse, men begrunnelsen treffer også prosessbyrdespørsmål. Resonnementet er at forbrukernes relativt sett svake stilling ikke bare har konsekvenser for utformingen av avtalevilkår og forhandlinger om pris; de påvirker også den *reelle muligheten* til å hevde sin rett for nasjonale rettsinstanser.[19] De samme skjevhetene som begrunner preseptorisk kontraktlovgivning begrunner derfor også et særlig prosessrettslig vern for forbrukerne.

I betalingssvindelssaker kan man argumentere for en at plikt for banken til å tilbakeføre det omstridte beløpet vil kompensere for et ujevnt styrkeforhold mellom partene. Det kan hevdes at en slik plikt derfor vil bidra til at forbrukeren i større grad får en reell mulighet til å nyte godt av sitt vern etter finansavtaleloven § 4-30. Hvis banken blir tvunget til å tilbakeføre de omstridte kronene til kundens konto i etterkant av svindelen selv om den mener kunden har det endelige ansvaret for tapet etter finansavtaleloven § 4-30 tredje eller fjerde ledd, må banken eventuelt reise sak mot kunden om dette beløpet. Banken vil da måtte vurdere om ressursene den bruker på å forfølge kravet, er regningssvarende i lys av prosessrisikoen saken reiser. Dersom banken i stedet «avgjør» at kunden har vært grovt uaktsom eller har handlet med forsett, jf. § 4-30, og sikrer sin rettsposisjon ved å la kundens konto bli stående helt eller delvis tom, blir det kunden, med sin antatt begrensede kunnskap og sine antatt begrensede ressurser, som må vurdere om han eller hun vil forsøke å få bankens vurdering overprøvd av en rettsinstans.

Tilbakeføringsregelen avgjør dermed om en kunde – i en situasjon der man har blitt svindlet, og varsler banken om dette – skal måtte reise sak mot banken dersom banken mener kunden skal bære tapet. Hvis de kundene som må «vinne pengene tilbake», blir sittende med tapet oftere enn de som bare trenger å «forsvare seg» mot et krav fra banken, vil plasseringen av prosessbyrde måtte antas å påvirke den reelle risikofordelingen for eID-misbruk i det norske betalingssystemet. Dermed berøres også hensynene til tillit, innovasjon og tapspulverisering som ligger til grunn for de materielle reglene om ansvar. Samlet sett kan vi derfor anta at rekkevidden av bankens plikt til å tilbakeføre omstridte beløp langt på vei avgjør hvem som må bære prosessbyrden, noe som i alle fall *kan* få konsekvenser for hvordan tap ved misbruk av eID til å gjennomføre betalinger fordeles mellom banker og kunder.

2 Nærmere om bakgrunnen for tilbakeføringsreglene

2.1 Kort om lovhistorien og nærmere om tilbakeføringsregelens formål

Den særskilte reguleringen av prosessbyrde i saker om omstridte betalingstransaksjoner kom inn i norsk rett gjennom finansavtaleloven 1999 § 37. Banklovkommisjonen uttalte blant annet følgende som begrunnelse for hvorfor det måtte være en tilbakeføringsplikt:

> «I dag er det kontohaveren som må ta prosessinitiativet dersom institusjonens belastning av kontoen bestrides. Kommisjonen antar at prosesskostnader forbundet med tvist ikke sjelden medfører at kontohaveren unnlater å anlegge sak for domstolene selv om denne mener at en belastning av konto er uhjemlet. Institusjonen har på sin side økonomisk evne til å forskuttere prosesskostnader og vil kunne pulverisere eventuelle tap ved misbruk på brukernes betaling for tjenesten. Kommisjonen har på denne bakgrunn vært opptatt av å legge prosessbyrden på institusjonen og har foreslått regler om dette i § 2-29.»[20]

Ifølge Banklovkommisjonen var det et problem at det falt på kunden å reise sak, fordi det kunne medføre at kunder ikke forfulgte mulige krav mot bankene.

Banklovkommisjonens begrunnelse for å regulere prosessbyrden særskilt er relativt knapp. Med «prosesskostnader forbundet med å reise sak» viser Banklovkommisjonen tilsynelatende til kostnader ved å rette krav mot banken. Det kan her nevnes at kunden ved en klage til Finansklagenemnda ikke behøver å betale rettsgebyr eller ta risiko for motpartens sakskostnader.[21] Kundens manglende kjennskap til de relativt vanskelige vurderingene rundt «grov uaktsomhet» og «forsett» i finansavtalelovens regler om tapsfordeling kan også ha en avskrekkende effekt, særlig om banken fremstår sikker i sin sak når kunden reklamerer. Rettshjelp kan derfor fort bli nødvendig. I tillegg er det selvfølgelig en god del tid som kan gå med også i en sak hos Finansklagenemnda, noe det ikke er gitt at forbrukere føler at de kan avse. Dette forsterkes av at en uttalelse fra nemnda aldri har gitt kunden noen sikkerhet for å vinne frem med kravet sitt, ettersom avgjørelsene ikke er

bindende. Om banken vil overprøve nemdas vurdering, kan det bli en lang prosess før kunden eventuelt vinner frem én gang for alle.[22]

Uavhengig av hva som var den dypere begrunnelsen, kan vi trygt slå fast at det umiddelbare formålet bak tilbakeføringsplikten var å «legge prosessbyrden på institusjonen», jf. sitatet ovenfor. I proposisjonen til finansavtaleloven 1999 foreslo departementet derfor at bankene ble pålagt å tilbakeføre det omstridte beløpet, med mindre den innen fire uker reiste sak mot kunden.[23] Dette ble vedtatt av Stortinget som 1999-lovens § 37. Da det første betalingstjenestedirektivet (PSD I)[24] ble gjennomført i 2009, antok departementet at denne ordningen kunne bestå, selv om det var klare spenninger mellom ordlyden i direktivet, som bestemte at tilbakeføring skulle skje «straks» og den særnorske løsningen med en fire ukers «betenkningstid» for banken.[25] I finansavtaleloven 2020 har utgangspunktet om tilbakeføring til kunden ved betalingssvindel blitt videreført.

Forarbeidene gir ingen indikasjoner på at intensjonen bak tilbakeføringsregelen skal forstås annerledes i finansavtaleloven av 2020 enn hva Banklovkommisjonen i sitatet ovenfor la til grunn for 1999-loven. I både høringsnotatet og proposisjonen til finansavtaleloven av 2020 omtales tilbakeføringsregelen som en regel om «prosessbyrde».[26] Én viktig endring fulgte imidlertid av PSD II: I direktivet ble det presisert at plikten til å tilbakebetale beløpet til kunden måtte oppfylles «innen utløpet av neste virkedag» – med andre ord kunne ikke «straks» lenger bety innen fire uker. Unntaket der banken kunne reise sak innen fire uker, ble derfor ikke opprettholdt, utover tilfeller der banken har «rimelige grunde til at have mistanke om svig» – tilfeller som direktivet i sin helhet unntar fra tilbakeføringsplikten på nærmere vilkår.[27] I tillegg ble det gjort enkelte språklige justeringer.[28]

Det umiddelbare formålet med bestemmelsen om tilbakeføring er altså å legge prosessbyrden på banken. Banklovkommisjonen og Justis- og beredskapsdepartementet har antatt at banken ved ensidig å tilbakeholde beløpet og overlate til kunden å reise sak, skaffer seg et prosessuelt overtak som vil avskrekke kunder fra å gjøre krav gjeldende.[29] Vi kan som nevnt se dette i sammenheng med hensynene som ligger til grunn for de materielle reglene som begrenser kundens ansvar for svindeltransaksjoner. Dersom kunder avskrekkes fra å gjøre bankens ansvar for svindeltransaksjoner gjeldende, vanskeliggjøres realisering av de nevnte formålene om pulverisering, tillit og innovasjon.

Prosessbyrdesynspunktene kan også ses i sammenheng med hensynet til kundens økonomiske situasjon i etterkant av svindelen.[30] Kunden vil ofte ha et ganske umiddelbart behov for å ha tilgang til kontomidlene mens tvisten pågår. Det kan være snakk om midler som er nødvendige for mat, husly, familieforsørgelse og annet livsopphold. Dersom prosessbyrden ligger på kunden, vil kunden kunne få umiddelbare betalingsproblemer som følge av en svindel som banken kanskje egentlig skal bære risikoen for. I motsetning til i andre tilfeller der forbrukere havner i skyldforhold, vil kunden stå uten beskyttelse fra regler om rett til livsopphold ved gjeldsforfølgelse, slik som dekningsloven § 2-5.[31] Tilbakeføringsregelen kan derfor ses som et utslag av et mer overordnet prinsipp om at banker som tvister med kunder, ikke skal kunne bruke sin råderett over kundens betalingskanaler til å styrke sin posisjon i tvist eller forhandling.[32]

Det er vanskeligere å finne eksplisitte uttalelser om formål og hensyn som ligger til grunn for den EU-rettslige reguleringen av selve tilbakeføringsspørsmålet. Som det vil bli vist under punkt 3.1, er det ikke ubestridt at den europeiske regelen faktisk regulerer prosessbyrden. I noe europeisk litteratur virker likevel forståelsen av regelens grunnleggende innhold og formål å være tilsvarende som den norsk lovgiver har lagt til grunn.[33]

Dessuten kan det sies at en plikt til tilbakeføring er en teknisk gjennomføring av det formelle utgangspunktet: Innestående på kundens konto er ikke en kontantkasse, men en fordring på kundens hånd.[34] Sagt på en enklere måte: Saldoen på min bankkonto gir meg ikke disposisjonsrett over visse fysiske penger, men representerer et krav jeg har mot banken.[35] Når jeg trekker bankkortet på butikken, foretar banken en betaling og skriver ned min saldo – min fordring – med grunnlag i det samtykket jeg avga ved å trekke bankkortet og taste koden. Selv om vi dagligtale sier at «kundens penger er borte», «kontoen er tom» eller liknende ved betalingssvindel, er i alle fall det formelle forholdet at banken har iverksatt en betalingstransaksjon overfor mottakerens bank uten et gyldig grunnlag for å skrive ned kundens kontofordring. Det faller seg da, kan man hevde, mest naturlig at det blir opp til banken å rette et krav mot kunden for å dekke dette tapet.[36] Løsningen på praktiske rettsspørsmål som oppstår, må nok bero på en tolkning av de aktuelle bestemmelsene heller enn på slike mer tekniske synspunkter.[37] Det er likevel verdt å ha i mente at det i utgangspunktet er *banken* som har betalt, og at bildet av at «kundens penger er tapt», er nettopp det – et språklig bilde.

2.2 Har prosessbyrden blitt snudd i praksis?

I Norge har vi altså hatt regler som skal plassere prosessbyrden, fra og med den forrige finansavtalelovens ikrafttredelse i 2000. Likevel tyder tilgjengelig informasjon på at mange banker, i strid med § 37 i 1999-loven, ofte lot være å tilbakeføre beløp til kunden og heller ikke reiste sak innen fire uker (som var et alternativ til tilbakeføring under 1999-loven, jf. ovenfor). Det foreligger for det første en del rettspraksis der det fremgår at bankene ikke har tilbakeført det omstridte beløpet.[38] Videre har Finansklagenemnda også i sin årsrapport fra 2021 påpekt at reglene om tilbakeføring kun har blitt fulgt i varierende grad:

> «Enkelte finansforetak har ikke fulgt opp sine plikter etter bestemmelsen. Dette er tatt opp med finansforetakene flere ganger fra 2019 og de aller fleste bankene har etter hvert innrettet sin praksis etter lovverket. Dette gjelder ikke DNB, som også i 2021 konsekvent har unnlatt å sende slike klager til Finansklagenemnda.»[39]

At en del banker ikke har fulgt opp sine plikter etter bestemmelsen, stemmer overens med erfaringer innhentet fra rettshjelptiltaket *ID-juristen*, som ble opprettet i 2021 med formål om å gi gratis rettshjelp til personer utsatt for ID-tyveri og svindel.[40] Erfaringene fra ID-juristen tyder riktignok ikke på at «de aller fleste bankene» førte tilbake midlene eller reiste sak i tilfeller av ikke-godkjente betalingstransaksjoner fra og med 2019.[41] Tvert imot tyder ID-juristens saker på at tilbakehold har forekommet hos relativt mange banker også utover dette.[42] De samme sakene indikerer at noen banker synes å ha praktisert en ordning der de tilbakeførte midlene, men forbeholdt seg retten til å «gjenbelaste» kundens konto, enten uten en konkret hjemmel eller på grunnlag av vilkår kunden «samtykket» til ved innlevering av reklamasjon via bankens reklamasjonssystem.[43] Dette har samme praktiske realitet som manglende tilbakeføring – ved uenighet havner prosessbyrden hos kunden. På bakgrunn av at ID-juristen varslet Forbrukertilsynet om sine funn, gjennomførte Forbrukertilsynet en undersøkelse av praksis hos norske banker. Undersøkelsen konkluderte med at banker i mange tilfeller har latt være å tilbakeføre det omstridte beløpet til kunden.[44]

De undersøkelser som er gjort, indikerer altså at en del av bankene har praktisert ordninger der spørsmål om kundens materielle ansvar håndteres internt: Kunden informeres om bankens beslutning, og banken holder tilbake det omstridte beløpet i tråd med sin egen konklusjon om kundens grove uaktsomme eller forsettlige pliktbrudd. Det blir i så fall opp til kunden å bringe saken inn for et tvisteløsningsorgan. Et blikk på andre lands gjennomføring av betalingstjenestedirektivene indikerer at liknende praksiser også forekommer utenfor Norge – også i land med en liknende gjennomføring av tilbakeføringsregelen i PSD II. I Danmark er det etablert en tilbakeføringsplikt som man – i alle fall etter undertegnedes forståelse av lovens bokstav – skulle tro omfatter det omstridte beløpet.[45] I nemndspraksis virker det likevel som det faller på kundene å reise sak.[46] I en artikkel som analyserer gjennomføringen av PSD II i henholdsvis Portugal og Belgia, hevdes det at tilbakeføring «invariably» nektes, og at regelen om «pay first, argue later» ikke har fått særlig realitet i disse landene.[47] Samlet sett virker det derfor som prosessbyrden ofte ikke har vært snudd likevel – verken i Norge eller andre steder i EØS.

3 Nærmere om tilbakeføringspliktens anvendelsesområde, innhold og vilkår

3.1 Overordnet om de EØS-rettslige rammene og kort om gjennomføringen i svensk rett

I det videre undersøker jeg nærmere hvilke krav finansavtaleloven § 4-32 stiller til norske betalingstjenesteytere. Spørsmålene er hvilket *virkeområde* regelen har, hvilke *vilkår* som må være oppfylt for å utløse plikten til å tilbakeføre midler, og hvilket *innhold* som ligger i plikten.

Først må noe sies om de EØS-rettslige rammene. PSD IIs regler om ansvar ved betalingstransaksjoner er fullharmoniserende, slik at medlemsstatene i utgangspunktet verken kan pålegge bankene lempeligere eller strengere regler enn direktivet legger opp til.[48]

Plikten til å tilbakeføre midlene til kunden ved ikke-godkjente betalingstransaksjoner følger av PSD II artikkel 73 nr. 1. PSD II artikkel 74 nr. 1 tredje og fjerde avsnitt angir samtidig enkelte tilfeller der kunden kan eller skal hefte for tapet grunnet høy grad av skyld – som nevnt er de norske skyldansvarsreglene i finansavtaleloven § 4-30 tredje og fjerde ledd en gjennomføring av denne bestemmelsen. Systemet i direktivet svarer altså til

finansavtaleloven, med én regel om kundens ansvar for tapet og en annen regel som oppstiller en plikt for banken til å tilbakeføre midlene umiddelbart i etterkant av svindelen. Et spørsmål som da reiser seg, er om direktivet skal forstås slik at tilbakeføring skal skje også der kunden har utvist høy grad av skyld. Tilbakeføringsregelen i PSD II artikkel 73 nr. 1 annet punktum krever etter sin ordlyd at medlemsstatene

> «med forbehold av artikel 71,[49] [sikrer] at en betalers betalingstjenesteudbyder i tilfælde af en uautoriseret betalingstransaktion tilbagebetaler betaleren beløbet for den uautoriserede betalingstransaktion straks og under alle omstændigheder inden afslutningen af den følgende arbejdsdag efter at have konstateret eller være blevet underrettet om transaktionen, medmindre betalerens betalingstjenesteudbyder har rimelige grunde til at have mistanke om svig og skriftligt underretter den relevante nationale myndighed om disse grunde. Betalerens betalingstjenesteudbyder skal i givet fald føre den debiterede betalingskonto tilbage til den situation, der ville have været gældende, hvis den uautoriserede betalingstransaktion ikke var blevet gennemført».

Norsk lovgivers forståelse har vært at både PSD I og PSD II oppstiller en tilbakeføringsplikt som omfatter *det fulle beløpet* (eventuelt minus 50 euro / 450 kroner, jf. PSD II artikkel 74 nr. 1 og finansavtaleloven § 4-30 annet ledd første punktum) for transaksjonen, inkludert det kunden eventuelt hefter for etter ansvarsreglene i artikkel 74 nr. 3. Det er dette som gjør at den norske regelen fungerer som en prosessbyrderegel: Kundens ansvar grunnet grov skyld blir ikke et unntak fra tilbakeføringsplikten, men noe banken eventuelt må gjøre gjeldende *etter* å ha refundert beløpet til kunden.

Dette er tilsynelatende en annen tilnærming enn den som ble lagt til grunn av Den europeiske bankføderasjonen (*European Banking Federation*, EBF) ved tolkningen av tilsvarende regel i PSD I. EBF skrev i sin veiledning at det er en «balance to be struck» mellom prinsippet om øyeblikkelig tilbakeføring og behovet for eventuelt å fastslå om kunden har oppfylt sine plikter ved håndtering av betalingsinstrumentet.[50] Dette kan i alle fall forstås som at tilbakeføringsplikten kan begrenses av kundens plikt til å dekke egenandeler.

En slik oppfatning har også vært lovgivers forståelse i Sverige. I utredningen som lå til grunn for gjennomføringen av PSD II, kommenterte det svenske lovutvalget gjeldende rett, altså gjennomføringen av PSD I, slik:

> «Utredningen delar regeringens uppfattning att det indirekt framgår av den nuvarande regleringen att återbetalning ska göras omedelbart *om det inte förhåller sig så att betalaren ska ansvara för hela eller delar av det belopp som avser den obehöriga transaktionen*.»[51]

Her var altså det beløpet som kunden hadde ansvar for, tilsynelatende unntatt fra tilbakeføringsplikten. En slik løsning virker fremdeles å være gjeldende rett, jf. lag (2010:751) om betaltjänster 5 a kap. 1 § første ledd:

> «Har det genomförts en obehörig transaktion från en kontohavares konto, ska kontohavarens betaltjänstleverantör återställa kontot till den ställning som det skulle ha haft om transaktionen inte hade genomförts, *om inte annat följer av 2-6 §§*.»(Min kursiv.)

Kundens ansvar for uautoriserte transaksjoner grunnet egen skyld (tilsvarende finansavtaleloven § 4-30 tredje og fjerde ledd, som gir kunden økende grad av ansvar for det endelige tapet i takt med økende grad av skyld)[52] fremgår av lag (2010:751) om betaltjänster 5 kap. 3 §. Dermed tillater tilsynelatende det svenske regelverket at tilbakeføring helt eller delvis nektes fordi forbrukeren utviste «grov oaktsamhet», og derfor er ansvarlig for inntil 12 000 kroner, eller utviste «särskild klandervärd», og derfor ansvarlig for hele beløpet.[53] Ordlyden i lag om betaltjänster og de tilhørende forarbeidene gir altså inntrykk av at svenske banker *ikke* har blitt pålagt noen forpliktelse til å tilbakeføre beløp utover hva kunden faktisk har krav på etter reglene om det endelige ansvar for tapet.[54] I Sverige er PSD II artikkel 73 nr. 1 med andre ord altså tilsynelatende ikke gjennomført som en prosessbyrdebestemmelse.[55]

I lys av disse ulike synspunktene er det verdt å se litt nærmere på direktivteksten for å vurdere forholdet mellom ansvarsreglene og tilbakeføringsplikten. Det virker klart at PSD II artikkel 73 i alle fall stadfester et *utgangspunkt* om full tilbakeføring så lenge det ikke er rimelig grunn for mistanke om svik fra kunden; «beløpet for den uautoriserte betalingstransaksjonen» leses mest intuitivt som en henvisning til hele beløpet svindleren har lyktes i å ta ut fra kundens konto. Artikkel 73 nr. 1 siste punktum om at kontoen skal settes i samme situasjon som før transaksjonen, underbygger denne forståelsen; gjenopprettelse av den opprinnelige situasjonen forutsetter nødvendigvis at hele beløpet fra svindelen tilbakeføres.

Spørsmålet om hvorvidt direktivet pålegger en bestemt prosessbyrdeordning, er derfor i realiteten et spørsmål om hvordan *sammenhengen* mellom artikkel 73 og 74 skal forstås. Nærmere bestemt må man klarlegge i hvilket omfang artikkel 74 nr. 1 tredje avsnitt om kundens ansvar ved høy grad av skyld utgjør et unntak fra artikkel 73 nr. 1 om tilbakeføring. Innledningsvis stadfester artikkel 74 nr. 1 første avsnitt at egenandelen på 50 euro gjelder «[u]anset artikel 73» – eller på engelsk: «By way of derogation from Article 73». At det skal kunne gjøres et fradrag for denne egenandelen i tilbakeføringen, slik norsk lovgiver også har forutsatt, fremstår derfor ikke tvilsomt.

Det er imidlertid ingen tilsvarende ordlyd i regelen om kundens ansvar grunnet «forsæt eller ... grov forsømmelse» i artikkel 74 nr. 1 tredje avsnitt, en taushet som kan forstås i begge retninger. Fraværet av en eksplisitt ordlyd om unntak kan tas til inntekt for at disse bestemmelsene er uten betydning for omfanget av tilbakeføringsplikten, slik at reglene gjelder parallelt: Det skal skje tilbakeføring, men kunden kan senere holdes til ansvar. Motsatt kan man argumentere for at den innledende formuleringen «[u]ansett artikel 73» gjelder hele artikkel 74, og at regelen i tredje avsnitt om at «[b]etaleren skal dække alle tab ...» derfor også skal forstås som en unntaksregel fra utgangspunktet om tilbakeføring.

Noe klart svar på dette tolkningsproblemet kan ikke gis, men etter mitt syn er det eksplisitte unntaket som er gitt for tilfeller med «rimelige grunde til at have mistanke om svig» i artikkel 73 nr. 1, en indikasjon på at det kun er første avsnitt i artikkel 74 – altså den objektive egenandelen – som er ment å utgjøre et unntak fra utgangspunktet om tilbakeføring. Det systemet direktivet skisserer, fremstår mest koherent dersom bankens vurdering av kundens eventuelle skyld i betalingstransaksjonen er begrenset til å vurdere om det foreligger en rimelig mistanke om svik. Den tilhørende plikten til å varsle relevante myndigheter i tilfeller der slik mistanke foreligger, vil i praksis miste mye av sin notoritetsfunksjon dersom tilbakebetaling i stedet kan nektes med hjemmel i de øvrige skyldreglene i artikkel 74.[56] EU-kommisjonen har gitt uttrykk for et liknende syn i tilknytning til den tilsvarende regelen i PSD I artikkel 58,[57] og en viss støtte for synspunktet kan man også finne i europeisk litteratur.[58]

Jeg oppfatter det da slik at direktivets system legger opp til at plikten etter artikkel 73 skal oppfylles (med fradrag for 50 euro) selv om banken mener kunden har vært grovt uaktsomt eller utvist forsett, så lenge det ikke er «rimelige grunde til at have mistanke om svig». Det virker i alle fall pr. i dag ikke å være grunnlag for å konkludere med at bestemmelsen utelukker at medlemsstatene kan oppstille en regel med et slikt innhold. Men skulle EU- eller EFTA-domstolen klart konkludere med at også artikkel 74 nr. 3 skal gjelde «by way of derogation» fra artikkel 73, tilsier kravet til fullharmonisering at den norske ordningen vil kunne bli EØS-problematisk. Tilbakeføringsplikten slik den skisseres i direktivet, inntrer «straks» kunden har «underrettet» betalingstjenesteyteren om misbruket i samsvar med artikkel 71 – tilsvarende finansavtaleloven § 4-24.

3.2 Tilbakeføringspliktens materielle virkeområde

3.2.1 Ikke-godkjente betalingstransaksjoner

Temaet videre er tilbakeføringsbestemmelsens virkeområde, altså hvilke transaksjoner tilbakeføringsregelen regulerer. Finansavtaleloven § 4-32 første ledd første punktum fastsetter at tilbakeføring skal skje i den utstrekning en kunde bestrider ansvar for en «ikke godkjent betalingstransaksjon» og har varslet om denne i tråd med § 4-24.[59] En «betalingstransaksjon» er videre definert som «en handling som iverksettes av betaleren eller på dennes vegne eller av betalingsmottakeren for å innbetale, overføre eller ta ut betalingsmidler».[60] Betaling fra en innskuddskonto i kundens navn vil altså helt klart være en betalingstransaksjon. Ved tolkning av tilsvarende bestemmelse i 1999-loven er det antatt at denne definisjonen også omfatter overføringer ut fra kredittkontoer og bruk av kredittkort,[61] men ikke kredittstiftelse i seg selv.[62] Denne rettstilstanden ligger fast også i ny finansavtalelov.[63]

En betalingstransaksjon er ikke godkjent når kunden ikke har «samtykket» til den, jf. finansavtaleloven § 4-2 første ledd. Utgangspunktet etter ordlyden må være at samtykket – for eksempel inntasting av personlig passord og kode fra BankID-brikke – skal være gjort av kunden selv eller med samtykke fra kunden.[64] Den alminnelige avtaleretten åpner iblant for binding også utenfor tilfeller av et eksplisitt samtykke. En bank vil derfor kanskje anføre at et «samtykke» jf. § 4-2 første ledd har kommet i stand gjennom passivitet eller konkludent adferd – det som tradisjonelt har blitt betegnet som «uegentlige» dispositive handlinger.[65] I norsk rett er det imidlertid

ingen sterk tradisjon for å fingere avtalebinding på et slikt grunnlag ved tilfeller av falsk. Der «pseudoavgivere» kan anklages for å uaktsomt ha lagt forholdene til rette for falskneren, har oppfatningen i teorien vært at dette kun kan føre til erstatningsansvar.[66] Det er vanskelig å se noen grunn til å fravike dette her, hvor ordlyden gir anvisning på et eksplisitt «samtykke». Tvert imot tilsier direktivets og finansavtalelovens system, hvor kundens økonomiske ansvar fastsettes ut fra grad av utvist skyld, at kundens handlemåte ved tredjepersoners misbruk vurderes opp mot lovens særskilte skyldregler.[67] Tilfeller der kunden kan anføres å ha samtykket implisitt ved uaktsom handlemåte eller liknende, bør derfor også som den klare hovedregel behandles som ikke-godkjente transaksjoner, jf. § finansavtaleloven § 4-32. De vil da også uten tvil omfattes av tilbakeføringsplikten.

I noen saker vil banken også kunne påstå at kunden er bundet til svindlerens godkjenning av transaksjonen gjennom en *fullmakt* – først og fremst der kunden faktisk har delt betalingsinstrument og/eller sikkerhetsinformasjon i den hensikt at en tredjeperson skal gjøre disposisjoner, men svindleren har utnyttet denne tilliten. Igjen er mitt syn at lovens system med definerte skyldgrader i de fleste slike tilfeller er bedre egnet enn den ulovfestede avtaleretten som grunnlag for å vurdere kundens ansvar for transaksjonen, men det er antakelig et visst rom for fullmaktsbetraktninger i denne typen tilfeller.[68] Det er ikke anledning her til å gjøre en fullstendig vurdering av spørsmål om hvorvidt «samtykke» etter § 4-2 første ledd kan gis på andre måter enn ved eksplisitt godkjenning fra kunden selv. En slik vurdering vil også måtte ta stilling til om betalingstjenestedirektivets ordlyd og system – samt det EU/EØS-rettslige effektivitetsprinsippet – legger noen føringer for hvordan nasjonal avtalerett eventuelt kan anvendes i slike tilfeller.[69]

> Spørsmålet om hvorvidt det foreligger samtykke, kan også aktualiseres der kunden selv har foretatt en godkjenningshandling, *men ikke forsto hva som ble godkjent*. I nyere nemndspraksis om finansavtaleloven 1999 er det antatt at kunden for å «samtykke» må ha forstått at hen samtykket til gjennomføring av en betaling.[70] Ofte vil dessuten den viktigste uklarheten være det faktiske hendelsesforløpet – banken tviler rett og slett på forbrukerens forklaring om at hen ikke samtykket til transaksjonen.

Det fremstår ikke helt klart om loven regulerer prosessbyrden for en tvist om hvorvidt forbrukeren har «samtykket» på slike grunnlag. To tolkninger er mulig: Man kan hevde at reglene om tilbakeføring kommer til anvendelse så fort kunden *gjør gjeldende* at en transaksjon er «ikke godkjent», jf. ordlyden «[i] den utstrekning kunden ... *bestrider å ha ansvar* for en ikke godkjent betalingstransaksjon».[71] I så fall må banken legge til grunn kundens pretensjon om at transaksjonen ikke er godkjent – den må tilbakeføre midlene og senere gjøre gjeldende at kunden må anses å ha samtykket. Ordlyden kan imidlertid også, og kanskje mer intuitivt, leses slik at det forutsettes at transaksjonen er godkjent, for at tilbakeføringsplikten skal inntre. Dette skulle tilsi at banken ikke bryter noen plikt dersom det ved domstols- eller nemndsbehandling av kravet viser seg at transaksjonen blir vurdert å være godkjent. Tolkningsspørsmålet belyses best når man også ser hen til unntaket for «svik» i § 4-32 annet ledd, og behandles derfor lenger ned.[72]

3.2.2 Unntaket for svik

Selv der det foreligger en ikke-godkjent betalingstransaksjon, pålegger ikke PSD II banken å tilbakeføre midlene når den har «rimelige grunde til at have mistanke om svig» fra kunden, så fremt banken varsler den «relevante nationale myndighed» om tilbakeholdelsen og grunnlaget for den.[73] Den norske tilnærmingen til dette unntaket har, for tilfeller der det er slike rimelige mistankegrunner, vært å opprettholde 1999-lovens ordning[74] med unntak fra tilbakeføringsplikt dersom banken innen fire uker reiser sak for domstolen eller Finansklagenemnda. Lovgiver har med andre ord lagt til grunn at Finansklagenemnda eller domstol i sviktilfellene er «relevant myndighet» for Norge, der for eksempel svenske myndigheter har antatt at det er tale om en melding til en regulatorisk myndighet.[75]

Poenget med å stille krav om en melding fra banken til en nasjonal tilsynsmyndighet ved mistanke om svik er tilsynelatende å sikre at bankene ikke kan omgå hovedregelen om tilbakeføring ved å anføre svik. De norske forarbeidene legger særlig vekt på at saken skal bringes inn for et tvisteløsningsorgan for å bli vurdert.[76] I Sverige virker det å bli lagt mer vekt på at det sikres notoritet over bankenes bruk av dette unntaket.[77]

Hva som regnes som svikaktig adferd, er ikke nærmere presisert i direktivet og heller ikke utbrodert i de norske forarbeidene. En intuitiv forståelse av hva svik («fraud» i den engelske versjonen av direktivet) innebærer, er at man sikter til tilfeller der kunden med vitende og vilje har bidratt til å svindle betalingstjenesteyteren eller forsøker å svindle betalingstjenesteyteren ved å påberope seg et fiktivt misbruk. Dette samsvarer med

Høyesteretts og lovgivers tilnærming i saker om svikaktig tilbakehold av opplysninger ved inngåelse av forsikringsavtaler.[78] Svikbegrepet kan derfor ikke omfatte tilfeller av «ordinære» forsettlige rettsbrudd (jf. § 4-30 fjerde ledd), der kunden har overtrådt et utstedelsesvilkår ved en villet handling og er sterkt å bebreide, men ikke har hatt til hensikt å bidra til svindelen.[79] Banken må derfor tilbakeføre beløpet innen neste virkedag også i tilfeller hvor den mener det foreligger forsettlige pliktbrudd fra kunden, jf. § 4-30 fjerde ledd. Mye taler for at unntaket for svik først og fremst omfatter tilfeller der kunden i realiteten har samtykket til betalingen, men nå forsøker å gjøre gjeldende at banken skal hefte for den.

At banken skal ha *rimelig* mistanke om svik, forutsetter at det finnes objektive grunner for mistanken utover at kundens sikkerhetsanordninger har blitt benyttet.[80] Det er ikke grunn til å være svært streng med hensyn til hvilke bevis banken må besitte – tanken bak en slik begrensning i tilbakeføringsplikten må nettopp være at bankene får en rimelig mulighet til å undersøke at man ikke utbetaler penger til noen som egentlig forsøker å svindle banken. At kunden fullstendig mangler en realistisk forklaring på hvordan svindelen kan ha skjedd, må etter mitt syn kunne være en tilstrekkelig objektiv grunn for å nekte tilbakeføring. Det sentrale er at banken må gå lojalt frem for å oppklare faktum etter beste evne, og ikke bruke unntaket for å skaffe seg et prosessuelt overtak i en tvist som egentlig handler om en kunde som hefter grunnet uaktsomme, men ikke svikaktige forhold.

Loven angir at det hefter forsinkelsesrenter fra og med tidspunktet da tilbakeføring skulle skjedd, dersom en domstol senere konkluderer med at det *ikke* var rimelig grunnlag for mistanke om svik fra kunden.[81] Dersom banken får avkreftet mistanken, må tilbakeføring skje straks, ettersom man da vil være tilbake i hovedregelen i § 4-32 første ledd.

3.2.3 Forholdet mellom unntaket for svik og inngangsvilkåret om «ikke godkjent»

Forholdet mellom inngangsvilkåret «ikke godkjent» og unntaket for svik fremstår ikke helt klart. Om banken mener transaksjonen var godkjent, og kunden likevel gjør gjeldende et tilbakeføringskrav, vil det jo ofte være nærliggende å også mistenke kunden for å prøve å bedra banken.[82] Kan banken i så fall la være å tilbakeføre midlene, og også la være å bringe saken inn for et tvisteløsningsorgan innen fire uker, under henvisning til at transaksjonen er godkjent? Som indikert ovenfor blir spørsmålet praktisk sett om banken må legge til grunn kundens *pretensjon* om at transaksjonen er «ikke godkjent». I så fall vil tilbakeføringsplikten ikke bare regulere prosessbyrden for ansvarsforholdet etter finansavtaleloven § 4-30 tredje og fjerde ledd, men også spørsmålet om hvorvidt samtykke foreligger, jf. § 4-2.

Om man leser PSD II som en videreutvikling av PSD I på dette punktet, er det nærliggende å tenke at intensjonen bak direktivets regel var å lage en alternativ prosedyre for saker der banken mente kunden i realiteten hadde samtykket til transaksjonen.[83] I så fall kan ikke banken gjøre noen egen intern vurdering av om «inngangsvilkåret» om «ikke godkjent» er oppfylt. Direktivets ordlyd kan imidlertid anføres å tale sterkest for det motsatte – plikten til å melde til den «relevante nationale myndighed» gjelder kun når svik mistenkes i forbindelse med en uautorisert («ikke godkjent») transaksjon.[84] Tilsvarende kan ordlyden i finansavtaleloven definitivt leses slik at den ikke pålegger banken noen plikt til tilbakeføring, ei heller til å reise sak innen fire uker, så lenge betalingstransaksjonen er godkjent. I praksis ville dette innebære at banken *ikke* anses å ha brutt tilbakeføringsplikten dersom den senere vinner frem med at kunden har samtykket til transaksjonen

Fra et systemperspektiv er sistnevnte en lite tilfredsstillende konklusjon. I svært mange saker vil banker prinsipalt påberope seg at det foreligger en form for godkjenning fra kunden, og subsidiært gjøre gjeldende ansvarsreglene. Om bankene ikke tilbakefører midlene i disse tilfellene, risikerer man at svært mange tvister som i realiteten handler om kundens ansvar grunnet skyld, går tapt i dragsuget av denne prinsipale anførselen. I så fall fyller reglene om at påstått svik skal meldes til myndighetene, bare en notoritetsfunksjon så lenge banken aksepterer at transaksjonen ikke er godkjent, men likevel mistenker kunden for svik – en ganske snever kategori saker. Det virker her å være en klar spenning mellom loven og direktivets formål på den ene siden, og den ordlyden som i begge tilfeller er benyttet, på den andre.[85] Den mest systemtro og formålsorienterte tolkningen ville vært at man forsto vilkåret om «rimelige grunner til mistanke om svik» som først og fremst å vise til tilfeller der forbrukeren har samtykket, men nå gjør gjeldende at banken skal bære tapet.

Etter mitt syn har derfor en tolkning hvor unntaket for svikaktige forhold «sluker» en eventuell vurdering av kundens samtykke, mye for seg. Banken må i så fall reise sak innen fire uker også dersom den mener at kunden skal anses å ha godkjent transaksjonen, men nå benekter ansvar.[86] I den nylig avsagte FinKN-2022-1006, som

ble løst etter finansavtaleloven 1999, legges det (tilsynelatende uten protester fra banken) til grunn at tilbakeføringsregelen gjelder så lenge kunden bestrider å ha samtykket til transaksjonen. Kunden ble ansett å ha samtykket til betaling, men banken ble ansett å ha brutt tilbakeføringsplikten. Forbrukertilsynet la til grunn samme rettsoppfatning i sin orientering til bankene i 2022.[87] Vi kan imidlertid ikke vite om domstolene vil se det på samme måte, ordlyden tatt i betraktning.

3.2.4 Sammenfatning

Rettstilstanden skissert ovenfor kan oppsummeres med tre eksempler:

(I) Om banken tilbakeholder beløpet, og transaksjonen senere anses «ikke godkjent», har banken brutt tilbakeføringsplikten, selv om kunden senere skulle bli vurdert forsettlig og dermed være ansvarlig for hele beløpet, jf. finansavtaleloven § 4-30 fjerde ledd.

(II) Om banken tilbakeholder beløpet og reiser sak innen fire uker fordi den mener det forelå rimelig grunnlag for svik, og retten eller nemnda finner at kunden hadde utvist forsett, men at det ikke forelå noe grunnlag for å mistenke kunden for svik, er også tilbakeføringsplikten etter § 4-32 brutt.

(III) Om banken tilbakeholder beløpet og senere vinner frem med en anførsel om at kunden har godkjent transaksjonen, er det mer uklart om banken brutt tilbakeføringsplikten etter finansavtaleloven § 4-32 første ledd.

I alle disse tilfellene er det fullt mulig for banken å gjøre gjeldende at kunden til slutt skal hefte for beløpet. Poenget er at prosessbyrden, i alle fall i de to første eksemplene, skal overføres ved at beløpet først tilbakeføres til kunden.

3.3 Vilkårene for at tilbakeføringsplikten skal inntre

3.3.1 Kundens varsel

Spørsmålet er videre hva som ellers skal til for at en transaksjon skal bli gjenstand for tilbakeføring. Det sentrale vilkåret for at banken skal bli pålagt tilbakeføringsplikt, er at det er fremsatt et rettidig «varsel», jf. finansavtaleloven § 4-24, og at kunden bestrider ansvar i det aktuelle omfang, jf. finansavtaleloven § 4-32 første ledd første punktum. Dette er ikke et krav om to separate meldinger eller handlinger. Den indre sammenhengen i regelverket – så vel som forholdet til EØS-retten – tilsier at kunden ved å varsle også bestrider ansvar.[88] Loven pålegger med andre ord ikke kunden å formulere sin melding slik man påkaller en rettighet eller et krav. Det gjelder heller ikke noen særskilte formkrav for varselet.[89] Den avgrensningen man må lese inn i ordlyden «bestrider», er i stedet at det ikke foreligger noen tilbakeføringsplikt der kunden *erkjenner* ansvar.[90] Varselet må fremsettes senest 13 måneder fra betalingstidspunktet og «uten ugrunnet opphold etter at kunden ble oppmerksom på at transaksjonen kan kreves rettet», jf. finansavtaleloven § 4-24 annet ledd.

Et spørsmål er hvor presis meldingen må være med hensyn til hvilke transaksjoner det er snakk om. Etter ordlyden i finansavtaleloven § 4-32 første ledd første punktum virker det som om hver enkelt transaksjon må meldes. PSD II viser til «transaksjoner» i flertall, men kan også sies å gi krav om en viss spesifikasjon, da kunden må «underrette betalingstjenesteudbyderen snarest muligt efter at have konstateret *en sådan transaktion, der giver anledning til krav*».[91] Det er altså ikke tilstrekkelig at kunden viser til at hen har blitt svindlet; det må ut fra meldingen være mulig for banken å identifisere hvilken konto eller hvilke kontoer som er rammet, og hvor store beløp det er snakk om. Man må imidlertid forvente at banken stiller nødvendige oppfølgingsspørsmål for å oppklare hvilke transaksjoner som bestrides, dersom dette er nødvendig. Hvis kunden ikke har kunnskap om konkrete transaksjoner i samme svindelkompleks som det hen varsler om, vil selvsagt heller ikke den relative transaksjonsfristen («uten ugrunnet opphold») for de «ukjente» transaksjonene etter finansavtaleloven § 4-24 begynne å løpe.[92]

3.3.2 Særlig om «skriftlig innsigelse» i tilfellene der kunden mistenkes for svik

I tilfellene hvor banken mener det foreligger rimelig grunnlag for svik, og derfor tilbakeholder midler i inntil fire uker fra kundens «skriftlige innsigelse» etter finansavtaleloven § 4-32 annet ledd, oppstår det et spørsmål om hva denne skriftlige innsigelsen henviser til. Er dette et særskilt dokument kunden må levere, eller har kunden rettet en «innsigelse» ved å varsle om transaksjonen? Med andre ord: Må kunden etter å ha varslet avvente bankens vurdering av ansvarsfordelingen og deretter fremsette en eventuell «skriftlig innsigelse» mot denne, i samsvar med den omtalte bransjepraksisen rundt 1999-lovens § 37?

Lovens system taler mot en slik forståelse. Det følger klart av ordlyden at *tilbakeføringsplikten* utløses av kundens varsel alene. Om fristen på fire uker ikke skulle begynne å løpe på dette tidspunktet, ville det gitt et implisitt unntak fra finansavtaleloven § 4-32 første ledd som gikk på tvers av sammenhengen i bestemmelsen. Lovgiver forutsatte for 1999-loven at kundens rettidige reklamasjon utløste fireukersfristen, som på dette tidspunktet var relevant uavhengig av påstått svikaktighet.[93] Denne tolkningen av 1999-loven var også støttet av Finans Norge.[94] Den mest nærliggende tolkningen er at kundens varsel etter § 4-24, i alle fall så langt den er skriftlig, må utgjøre en «skriftlig innsigelse». Banken kan altså ikke avvente med å bringe saken inn for et tvisteløsningsorgan med den begrunnelse at det bare er fremsatt et skriftlig varsel, ikke en innsigelse. [95]

3.4 Innholdet i plikten til tilbakeføring

3.4.1 Tilbakeføring av innskuddsmidler på konto

Til slutt er spørsmålet hva plikten til å tilbakeføre går ut på. Når det foreligger en ikke-godkjent betalingstransaksjon, og kunden har varslet om denne, jf. punkt 3.3 ovenfor, påbyr loven «tilbakeføring» av det aktuelle «beløpet» til kunden, jf. finansavtaleloven 2020 § 4-32 første ledd første punktum. I saker der transaksjonen innebærer betalinger ut av en innskuddskonto, oppfylles plikten typisk ved å tilføre kundens konto hele det beløpet som ble betalt eller tatt ut i den ikke-godkjente transaksjonen, eventuelt med unntak av 450 kroner. Loven fastslår at beløpet som skal tilbakeføres, også omfatter eventuelle rentetap kunden har hatt som følge av tapt likviditet. Om kunden ikke lenger skulle ha en konto i den aktuelle banken, eller den aktuelle kontoen er avviklet, fritar ikke dette banken fra tilbakeføringsplikten. Ordlyden er klar på at det er «kunden» («betaleren» i direktivet) som skal motta beløpet, og dette må bety at tilbakeføring om nødvendig må skje ved vanlig betaling til kunden.[96]

3.4.2 Tilbakeføring i ikke-godkjente transaksjoner med et kredittelement

Et spørsmål som imidlertid kan reises, er om en kunde under henvisning til finansavtaleloven § 4-32 første ledd også kan kreve kreditering av en kredittkonto eller kredittkortsaldo. Betraktningene rundt prosessbyrden slår her litt annerledes ut enn i saker om innskudd på konto, fordi man kan se det slik at tapet allerede ligger på bankens side. Dette kommer blant annet til uttrykk i en avgjørelse fra Asker og Bærum tingrett fra 2014. Her fant retten at tilbakeføringsplikten i 1999-lovens § 37 ikke fikk anvendelse ved misbruk av kredittkort. Det ble vist til at det ikke var «noe beløp å tilbakeføre».[97] Samtidig er det i dagens kredittavhengige samfunn åpenbart at kunden har interesse av å få kreditert det aktuelle beløpet for å gjøre bruk av den avtalte likviditeten uten å måtte gå til sak mot banken.

Der et kredittkort er knyttet til en konto hos betalingstjenesteyteren, består kredittstiftelsen i praksis av et kredittopptak og deretter en transaksjon ut av konto. Antakelig må derfor beløpet fra transaksjonen tilbakeføres på samme måte som ved tapping av en konto med positiv saldo. I tråd med PSD II artikkel 73 nr. 1 annet punktum skal banken i slike tilfeller føre «den debiterede betalingskonto tilbage til den situation, der ville have været gældende, hvis den uautoriserede betalingstransaktion ikke var blevet gennemført». Kunden har derfor i slike tilfeller krav på at kontoen bringes i den stand den var før den ikke-godkjente transaksjonen. Det samme må gjelde for nettbankoverføringer ut av en kredittkonto.

Hva så med kredittkort som *ikke* er knyttet til en konto i kundens navn, men hvor betalingen går rett fra kredittyter til betalingsmottaker?[98] Lovens «tilbakeføre» og direktivets «tilbagebetale» passer tilsynelatende dårligere her, rent ordlydsmessig.[99] Samtidig er vi innenfor pliktens virkeområde ellers, ettersom kortutstederen er «betalingstjenesteyter», og det har skjedd en ikke-godkjent betalingstransaksjon.[100] I lys av målene om en enhetlig og betryggende regulering som fremgår i PSD IIs fortale og er vektlagt ved liknende tvilstilfeller i EU-

domstolens praksis, er det ikke sikkert at en streng ordlydstolkning av tilbakeføringsplikten er riktig tilnærming.[101] Disse hensynene virker å tale for at kunden også i slike tilfeller bør ha krav på å bli stilt som om transaksjonen ikke hadde skjedd. I så fall plikter den kortutstedende banken å kreditere kundens saldo og på ny tilgjengeliggjøre den aktuelle kreditten.[102] Sikker kan konklusjonen imidlertid ikke være.

3.4.3 «Gjenbelastning»

Et annet spørsmål er om banken har adgang til å belaste kundens konto på ny etter at den har tilbakeført det omstridte beløpet, dersom den finner at kunden har opptrådt grovt uaktsomt eller forsettlig. Dette er ikke en upraktisk problemstilling – enkelte banker virker som nevnt å ha praktisert en slik ordning under 1999-loven.[103] Etter en ordlydsforståelse må «tilbakeføre» innebære å sette kontoen i den stand den var før transaksjonen ble gjennomført, slik direktivet også impliserer. Det skjer dermed ingen reell «tilbakeføring» når banken samtidig belaster kunden for det omstridte beløpet. Forarbeidene er som nevnt tydelige på at tilbakeføringsplikten gjelder uavhengig av kundens eventuelle ansvar etter finansavtaleloven § 4-30 tredje eller fjerde ledd.[104] Lovgivers klare føringer om at regelen skal regulere prosessbyrden og ivareta kundens behov for likviditet, ville også ha blitt fullstendig undergravd om en slik ordning var lovlig. Ettersom finansavtalelovens regler om tilbakeføring er ufravikelige i forbrukerforhold,[105] vil en eventuell avtale med kunden som autoriserer gjenbelastning, være uten betydning. Kun dersom kunden ikke lenger bestrider ansvar, jf. finansavtaleloven § 4-32 første ledd, vil en slik avtale om gjenbelastning kunne stå seg mot lovens bestemmelser om ufravikelighet.[106]

3.5 Oppsummering

Det er, basert på gjennomgangen ovenfor, klart at kundens rettidige varsel om misbruk utløser en plikt for banken til å stille kunden i den situasjon vedkommende hadde vært i om den aktuelle transaksjonen ikke hadde skjedd. Det er mer uklart om loven krever at det objektivt sett ikke foreligger et gyldig samtykke fra kunden, eller om det er tilstrekkelig at kunden *hevder* dette, men etter mitt syn taler i alle fall formåls- og systembetraktninger for sistnevnte løsning. Bestemmelsen gir videre ikke i noe tilfelle rom for en intern vurdering fra banken av kundens ansvar etter finansavtaleloven 2020 § 4-30 tredje og fjerde ledd. Praksisen med manglende tilbakeføring som er beskrevet i punkt 2 vil ikke være lovlig etter den nye bestemmelsen i finansavtaleloven § 4-32. Med tanke på at det har vært relativt vanlig blant bankene heller ikke å bringe saker inn for et tvisteløsningsorgan i tråd med 1999-lovens § 37 annet ledd, har denne praksisen også vært i strid med det som var gjeldende rett før 2020-loven.

4. Rettslige konsekvenser av brudd på tilbakeføringsplikten

4.1 Offentligrettslige reaksjonshjemler

Jeg vil videre se på hvilke privatrettslige og offentligrettslige reaksjoner det er hjemmel for når en bank lar være å tilbakeføre det omstridte beløpet. Klare brudd på tilbakeføringsplikten kan sanksjoneres av tilsynsmyndighetene. Finansavtaleloven 1999 § 37 hadde ingen direkte rettsgrunnlag for reaksjoner, men lovstridig praksis overfor forbrukere kan i sin alminnelighet utgjøre brudd på markedsføringsloven § 6 om urimelig handelspraksis, noe som kan medføre overtredelsesgebyr fra Forbrukertilsynet, jf. markedsføringsloven § 42. Under ny finansavtalelov har Forbrukertilsynet fått direkte tilsyn med forbrukerbestemmelsene i loven, jf. § 3-55 første ledd. Dette omfatter tilsyn med regelen om tilbakeføring.

I tillegg har Finanstilsynet mulighet til å treffe pålegg om retting av forhold som strider mot finansforetaksloven,[107] og klare brudd på tilbakeføringsplikten vil nok kunne utgjøre brudd på kravet til god forretningsskikk i denne lovens § 13-5. Brudd på slike pålegg kan i siste instans medføre mulkt eller straff.[108] Det har imidlertid i skrivende stund aldri blitt truffet noen tilsynsvedtak fra Finanstilsynet eller Forbrukertilsynet på grunnlag av brutt tilbakeføringsplikt. På bakgrunn av undersøkelsen Forbrukertilsynet foretok etter varselet fra ID-juristen omtalt i punkt 2.1, sendte tilsynet i desember 2022 et brev til samtlige

norske banker.[109] Her ble det i ganske harde ordelag fremsatt kritikk av rådende bransjepraksis. Det ble imidlertid ikke vedtatt noe overtredelsesgebyr.

4.2 Privatrettslige sanksjoner – om praksis under 1999-loven

Loven angir ikke direkte hvilken betydning brudd på finansavtaleloven § 4-32 første ledd får *mellom partene*. Steennot har for Belgias del påpekt at mangelen på sivilrettslige sanksjoner bidrar til å gjøre brudd på tilbakebetalingsplikten attraktivt:

> «Belgian PSPs do not always comply with this requirement. PSPs fear that they will not be able to recover the reimbursed amounts from the payer, if at a later stage it is found that the payer is liable. This behaviour is stimulated by the lack of a specific civil remedy, that payers can invoke if PSPs do not comply with this rule.»[110]

Spørsmålet om privatrettslige sanksjoner får en særlig aktualitet når offentligrettslige tilsyn ikke har resultert i noen sanksjoner, på tross av at ganske mange banker virker å ha brutt bestemmelsen relativt ofte.[111]

Hva gjelder tilbakeføringsplikten og/eller den tilhørende søksmålsfristen på fire uker i 1999-lovens § 37, finnes det et lite utvalg saker – først og fremst i Finansklagenemnda Bank – der kunden har gjort gjeldende at brudd på denne bestemmelsen avskjærer banken fra å gjøre gjeldende kundens ansvar ved grov uaktsomhet eller forsett. Så vidt jeg kan se, har slike anførsler ved alle anledninger blitt avvist. I FinKN-2016-326 fikk banken medhold i at kunden måtte dekke 12 000 kroner selv om det var klargjort at banken ikke oppfylte sin plikt til å tilbakeføre eller reise sak innen fire uker, jf. § 37. I FinKN-2017-652 og FinKN-2021-907 fulgte nemnda opp dette standpunktet. I sistnevnte sak uttalte nemnda at bankens manglende oppfyllelse av plikten til tilbakeføring etter § 37 hadde «ingen betydning for det endelige ansvaret for de omtvistede betalingene». At manglende tilbakeføring var uten preklusiv betydning, ble også lagt til grunn en tingrettssak fra 2014.[112]

Et annet spørsmål er om kunden kan ha krav på erstatning for sakskostnader som følge av brutt tilbakeføringsplikt. I FinKN-2021-907 ble det indikert at manglende tilbakeføring kan få betydning for sakskostnader, men tilsynelatende kun for sakskostnader som knytter seg til tilbakeføringskravet i seg selv og ikke til spørsmålet om kundens endelige ansvar for transaksjonsbeløpet etter § 4-30 tredje eller fjerde ledd. Det vil sjelden være betydelige sakskostnader knyttet til å rette et tilbakeføringskrav, og det var det etter nemndas mening heller ikke i denne saken.

Endelig har det vært et spørsmål om hvorvidt brudd på tilbakeføringsplikten kan sanksjoneres med forsinkelsesrenter, også der kunden eventuelt skulle være ansvarlig for tapet grunnet grov uaktsomhet eller forsett. Forsinkelsesrenteloven innebærer at det løper forsinkelsesrente når et «pengekrav» ikke «innfris ved forfall», jf. §§ 1 og 2.[113] I FinKN-2016-326 blir det tilsynelatende hintet til at en kunde som *vinner frem* i spørsmålet om ansvar for tapet ved transaksjonen, skal ha krav på forsinkelsesrenter fra tilbakeføring skulle skjedd.[114] Dette samsvarer med forsinkelsesrenteloven § 2, gitt at man antar at kundens krav på at banken skal dekke tapet, forfaller når fristen for å reise sak utløper. Men kunden ble i den aktuelle saken ansett holdt ansvarlig for det omstridte beløpet og ble ikke tilkjent forsinkelsesrenter. I FinKN-2021-907 var utfallet det samme.[115] I den nylig avsagte FinKN-2022-1006 ble imidlertid kunden tilkjent forsinkelsesrenter selv om kunden ble ansett ansvarlig for hele tapet.[116] Denne avgjørelsen representerer så vidt jeg har sett, det første eksempelet i rettspraksis på en privatrettslig konsekvens av brudd på tilbakeføringsplikten.

4.3 Hvilken virkning skal brutt tilbakeføringsplikt få når kunden er ansvarlig for tapet fra transaksjonen, jf. finansavtaleloven § 4-30 tredje og fjerde ledd?

4.3.1 Innledende bemerkninger

I det følgende ser vi nærmere på hvilke privatrettslige virkninger bankens brudd på tilbakeføringsplikten skal få etter den nye finansavtaleloven. Dette forutsetter en nærmere undersøkelse av forholdet mellom reglene om den endelige fordelingen av tapet og reglene om tilbakeføring. For enkelhets skyld forholder vi oss her til tilfeller der det er overført midler ut av kundens konto, og avgrenser mot rene kredittkortmisbrukssaker som nevnt i punkt 3.4.3.

Spørsmålet om privatrettslige virkninger er først og fremst interessant der banken har vurdert spørsmålet om kundens ansvar «riktig», og kunden etter finansavtaleloven § 4-30 hefter for tapet i samme størrelsesorden som banken tilbakeholder. Der hvor kunden vinner frem i spørsmålet om endelig ansvar for tapet, angir tilbakeføringsregelen simpelthen bare tidspunktet da banken må oppfylle sin plikt til å dekke tapet overfor kunden, jf. § 4-30 første ledd. Hvis en bank ikke tilbakefører under henvisning til kundens ansvar for 12 000 kroner for grov uaktsomhet, og en kunde deretter reiser sak og vinner frem med at hen ikke var grovt uaktsom og derfor bare hefter for 450 kroner, har kunden krav på forsinkelsesrenter på de mellomværende 11 550 kroner fra dagen etter at banken ble varslet om transaksjonen, jf. § 4-32 første ledd.

Spørsmålet om hvorvidt brudd på tilbakeføringsplikten får preklusive virkninger for banken, er mindre aktuelt etter ny finansavtalelov. Det fremsto etter mitt syn prosedabelt at fireukersfristen i 1999-lovens § 37 første ledd måtte overholdes for å gjøre gjeldende kundens ansvar etter § 35 tredje ledd, selv om den ikke ble lest slik i nemndspraksis.[117] Når banken i 2020-loven ikke lenger gis noen slik fire ukers «betenkningstid», men må tilbakeføre «straks», blir det imidlertid helt klart for strengt mot banken å tillegge brudd på denne plikten preklusive virkninger.

Spørsmålet som står igjen, er derfor om tilbakeføringsplikten gir opphav til et krav det kan løpe forsinkelsesrenter på, også der kunden anses ansvarlig for tapet grunnet grov uaktsomhet eller forsett, jf. finansavtaleloven § 4-30. Dette vurderes nærmere i det følgende.

4.3.2 Etablerer tilbakeføringsregelen et formuerettslig krav for kunden?

Først kan vi spørre om tilbakeføringsregelen gir kunden et *formuerettslig krav* på hele det omstridte beløpet, der kunden er ansvarlig for tapet etter § 4-30 tredje eller fjerde ledd. Svaret kan virke opplagt – banken har en plikt til å tilbakeføre hele det omstridte beløpet uansett kundens skyldansvar, og man skulle da tro at kunden må ha et korresponderende krav på dette. En del av den nemnds- og rettspraksis som foreligger om 1999-lovens § 37, gjør det likevel nødvendig å se nærmere på spørsmålet. I FinKN-2021-907 får man ikke inntrykk av at nemnda ser tilbakeføringskravet som et motstående pengekrav:

> «Nemnda er enig med klageren i at banken ikke har oppfylt sin plikt til tilbakeføring etter § 37, etter at tilbakeføring ble krevd skriftlig 2.12.20. Når nemnda nå, etter klage fra kunden, ikke har gitt kunden medhold i sakens hovedspørsmål om ansvar for betalingene, er det heller ikke grunnlag for å konkludere med tilbakeføring etter § 37.»

Der saken blir avgjort, og forbrukeren anses ansvarlig for beløpet, legges med andre ord spørsmålet om tilbakeføringsplikten dødt. Fra et pragmatisk ståsted kan det selvsagt fremstå som unødvendig anstaltmakeri å gi kunden et krav på et beløp som uansett skal betales tilbake. Én måte å se det på er derfor at kunden har krav på betaling i det omfang man kan få medhold i at banken skal bære tapet etter § 4-30 første ledd, men at tilbakeføring utover dette er en plikt som eventuelt sanksjoneres av Forbrukertilsynet.

Det er imidlertid viktig å være klar over at ny finansavtalelov, i motsetning til 1999-loven, uttrykkelig fastsetter forsinkelsesrenter der en nemnd eller domstol mener at banken uriktig har lagt til grunn at det var rimelig grunnlag for svik, jf. § 4-32 annet ledd siste punktum, og derfor ikke har tilbakeført. Etter ordlyden er det tilstrekkelig at banken etter retten eller nemndas vurdering ikke hadde rimelig mistanke om svik fra kunden – forsinkelsesrenter løper tilsynelatende også dersom kunden materielt sett viser seg å være ansvarlig etter § 4-30 tredje eller fjerde ledd. Dette samsvarer best med et syn om at tilbakeføringsplikten hjemler et krav på *hele det omstridte beløpet*, noe som forutsetter at kravet i et slikt tilfelle bygger på tilbakeføringsplikten og ikke på regelen om bankens ansvar i § 4-30 første ledd (som jo kunden i et slikt tilfelle ikke kan gjøre gjeldende).

Forarbeidene gir ellers ingen inngående forklaring på hvordan forholdet mellom tilbakeføringsplikten og reglene om endelig ansvar for tapet etter § 4-30 skal forstås, ut over at tilbakeføringsplikten også omfatter beløpet kunden eventuelt hefter for etter § 4-30 tredje og fjerde ledd.[118] Ordlyden i § 4-30 første ledd («banken er ansvarlig overfor kunden») gir inntrykk av at det er denne bestemmelsen som er ment å være den bestemmelsen kunden bygger et krav på, og at samme bestemmelses tredje og fjerde ledd gir grunnlag for eventuelle innsigelser banken kan rette mot et slikt krav. Dette samsvarer med hvordan 1999-loven ofte har blitt anvendt i praksis, jf. ovenfor.

Samtidig stemmer en slik lesning dårlig overens med departementets beskrivelse av selve svindelsituasjonen. I proposisjonen omtaler departementet reglene om ansvarsfordeling og tilbakeføring slik:

> «Det er kunden som har lidt tapet, slik at ansvarsreglene i §§ 4-30 og 4-32 må forstås i relasjon til den egenandelen som kunden vil måtte bære selv. Reglene gjelder når kunden har lidt et tap som følge av misbruket.»[119]

I høringsnotatet til ny finansavtalelov het det:

> «Betalingstjenesteyteren har en plikt til å tilbakebetale beløpet i alle tilfeller der det ikke foreligger rimelige grunner til å ha mistanke om svik fra kundens side. ... Det er imidlertid mulig å ta rettslige skritt for å kreve disse pengene tilbake.»[120]

Departementets oppfatning av hendelsesforløpet virker dermed å være slik: Når penger blir flyttet ut av kundens konto ved en ikke-godkjent betalingstransaksjon, har kunden lidd et tap. Dette tapet skal banken umiddelbart dekke, jf. § 4-32 første ledd. Om banken deretter mener kunden helt eller delvis bærer ansvar etter § 4-30 tredje og fjerde ledd, kan banken likevel ta «rettslige skritt» for å kreve tapet dekket fra kunden.

Dersom saken løper slik departementet har sett for seg (og slik loven foreskriver), vil altså § 4-30 første ledd om at banken som utgangspunkt er ansvarlig overfor kunden, kun utgjøre en ansvarsbegrensning når banken i sin tur retter sitt krav mot kunden. Det vil unektelig være paradoksalt om lovens system baseres på den antakelse om at banken *ikke* etterlever plikten til tilbakeføring, slik at tapet forblir hos kunden frem til det endelige spørsmålet om ansvar for tapet, jf. § 4-30, avgjøres. Forarbeidenes omtale av selve svindelsituasjonen kan derfor i en viss grad underbygge at § 4-32 første ledd gir kunden et formuerettslig krav.

Et videre poeng å være oppmerksom på, er at PSD II, i motsetning til finansavtaleloven, ikke inneholder noen selvstendig regel (à la finansavtaleloven § 4-30 første ledd) om bankens prinsipale ansvar som ikke også innebærer en øyeblikkelig plikt til tilbakeføring. Direktivet bestemmer bare at banken skal tilbakeføre, men at kunden likevel skal bære det endelige tapet i visse tilfeller.[121] Man har ikke «splittet» regelen i en ansvarsregel og en tilbakeføringsregel. Dette gjelder også på vilkårssiden – dersom kunden ikke har rett til tilbakeføring, har kunden heller ikke krav på at banken skal dekke tapet.[122] Direktivets system syn harmonerer derfor godt med at kunden gis et selvstendig krav etter § 4-32 første ledd.[123]

Totalt sett virker det i alle fall å være et visst grunnlag i rettskildene for å se det slik at § 4-32 første ledd gir kunden et selvstendig krav på hele det omstridte beløpet. Tilbakeføringskravet forfaller i så fall ved utløpet av neste virkedag etter kunden har varslet, jf. finansavtaleloven § 4-32 første ledd – eller, for sviktilfellene, fra utløpet av fireukersfristen i § 4-32 annet ledd. Regelen om forsinkelsesrenter § 4-32 annet ledd siste punktum gjelder bare tilfeller der et klageorgan «kommer til at det ikke foreligger rimelig mistanke om at kunden hadde opptrådt svikaktig». I andre tilfeller – for eksempel der banken ikke tar saken til domstol eller etablert klageorgan i det hele tatt – må det likevel løpe forsinkelsesrenter på kravet, jf. forsinkelsesrenteloven § 2.[124] Kundens ansvar etter § 4-30 tredje og fjerde ledd kan ikke utgjøre noen innsigelse mot dette tilbakebetalingskravet, fordi forarbeidene er helt klare på at tilbakeføringskravet *ikke* er begrenset av disse bestemmelsene. Det blir i så fall et separat krav banken kan rette mot kunden.

4.3.3 Kan banken innfri tilbakeføringskravet ved motregning?

På bakgrunn av konklusjonen ovenfor kan altså situasjonen der kunden krever tilbakeføring, men banken mener kunden er ansvarlig for tapet etter finansavtaleloven § 4-30 tredje eller fjerde ledd, forstås som en situasjon der det foreligger to motstående krav: Kunden har et krav på tilbakeføring på hele beløpet, typisk med unntak av 450 kroner, jf. § 4-30 annet ledd. Banken gjør på sin side gjeldende at kunden skal betale 12 000 kroner (ved grov uaktsomhet) eller tilsvarende hele tapet (ved forsett).[125]

Dermed aktualiseres et spørsmål om motregning. Motregning er en oppgjørsform som innebærer at man avregner motstående krav «så langt de dekker hverandre».[126] Kan banken, når kunden har vært grovt uaktsom, innfri tilbakeføringsplikten ved å motregne med sitt krav etter § 4-30 tredje ledd? Kan en kunde som retter et tilbakeføringskrav på 100 000 kroner mot banken etter finansavtaleloven § 4-32 første ledd, bli avspist med en motregningsinnsigelse i stedet for en faktisk kreditering av kontoen?[127] For vårt tilfelle ville motregning resultert i at banken var berettiget til å la være å *betale* til kunden i tråd med § 4-32 første ledd i de tilfeller hvor banken hadde et krav mot kunden etter finansavtaleloven § 4-30 tredje eller fjerde ledd. Bankens krav om at kunden skulle ta det endelige ansvaret for betalingen ville i stedet kunne brukes til å innfri kravet om tilbakeføring.

Ettersom manglende oppfyllelse av tilbakeføringsplikten så langt ikke har blitt forstått som en motregningssituasjon i Norge, har det ikke – verken i teori, rettspraksis eller forarbeider – blitt sagt noe om hvordan motregningsreglene får anvendelse på et slikt tilfelle. En viss føring ligger det likevel i at departementet i høringsnotatet til ny finansavtalelov antok at bankene etter å ha tilbakeført må ta «rettslige skritt» for å holde kunden ansvarlig – motregning er jo nettopp en måte å unnslippe «rettslige skritt» på.[128]

Etter mitt syn vil lovgivers ambisjon om å regulere prosessbyrden måtte tale klart imot å tillate banken å motregne i tilbakeføringskravet. Ved vurderinger av om motregning skal tillates, er nettopp oppgjørsrekkefølgen i forgrunnen – blant annet på grunn av motregningens effekt på prosessbyrden. Ved å la være å innfri et motkravkan debitoren for *hovedkravet* sørge for at det faller på motparten å reise sak. En illustrativ uttalelse om motregning finner vi hos Krüger:

> «Motregning endrer meget effektivt partenes prosesstaktiske status i tvisten: Foretar motregningsdebitor seg intet, blir motregningsresultatet definitivt og jevngodt med dom. Og uansett hva han gjør, blir han fratatt likviditet han tilkommer i henhold til sitt krav mot motregningskreditor ....»[129]

Loven regulerer ikke motregningsspørsmålet direkte,[130] slik at utgangspunktet må tas i de ulovfestede reglene om motregning. De alminnelige vilkårene for motregning sies gjerne å være *komputabilitet* (at de avkrevde ytelsene er av lik karakter, typisk penger), *gjensidighet* (at partene er de samme i hovedkravet og motkravet) og *oppgjørsmodenhet* (at kravene har forfalt eller kan bringes til forfall ved kreditors påkrav).[131]

For en situasjon som nevnt ovenfor her, der kunden har et krav på tilbakeføring, og banken har et krav mot kunden grunnet kundens grove uaktsomhet eller forsett, jf. § 4-30, vil vilkårene om gjensidighet og komputabilitet være oppfylt. Men det er kanskje ikke helt åpenbart at bankens krav er *oppgjørsmodent*.[132] For at dette vilkåret skal være oppfylt, må bankens krav enten ha forfalt eller kunne bringes til forfall av banken.[133] At banken skal kunne rette krav etter § 4-30 tredje eller fjerde ledd, kan sies å forutsette at banken har lidt et «tap», og derfor at banken har kreditert kundens konto – vi kan se det som et betinget krav hvis betingelse ikke er inntrådt. Et mulig standpunkt er derfor at banken først må legge ut overfor kunden før det blir snakk om et krav som kan gjøres gjeldende andre veien.[134]

Det er også alminnelig antatt å gjelde et forbud mot å motregne på en måte som har karakter av *rettsmisbruk*.[135] Denne regelen bygger på et synspunkt om at man ikke skal skaffe seg en bedre dekningsmulighet ved rettsstridig eller utilbørlig opptreden. Den har blitt utledet av eldre høyesterettspraksis, fått bred støtte i juridisk teori[136] og synes også å ha blitt lagt til grunn av underrettene og Høyesterett også i «nyere tid».[137] I saker om ikke-godkjente betalingstransaksjoner er det etter mitt syn gode grunner for å se bankens tilbakeholdelse av det aktuelle beløpet som en form for rettsmisbruk – ved å bryte en helt klar forpliktelse oppnår man dekning for et krav man mener å ha etter finansavtaleloven § 4-30 tredje og fjerde ledd.[138]

> Selv om rettsstridsreservasjonen vanligvis kommer på spissen når debitor for motkravet har gått konkurs, er det – som påpekt av Arntzen med et for vår del talende eksempel – gode grunner til å nekte rettsstridig motregning også utenfor konkurs: «Man kan ellers risikere at rettsbrudd begås i den hensikt å skaffe til veie et hovedkrav som det kan kompenseres i. *Banken vet f.eks. at den senere vil få et motkrav mot kunden, og den sperrer derfor kundens konto for å skaffe et hovedkrav å motregne i.*»[139]

Videre er det også andre reservasjoner mot motregning som kan bli relevante. Det er for eksempel antatt at man ofte ikke kan motregne på en måte som beskjærer midler til kundens livsopphold sml. dekningsloven § 2-5 og § 2-7 første ledd.[140] En kan lett tenke seg at bankens manglende oppfyllelse av tilbakeføringsplikten går ut over kundens mulighet til å dekke livsopphold – kunden kan ha fått kontoen tømt og stå uten likvide midler. I noen tilfeller antas det også å gjelde begrensninger i adgangen til å motregne med omtvistede krav, noe bankens krav på at kunden skal hefte grunnet høy grad av skyld, gjerne vil være.[141] Blant begrunnelsene for en slik regel er nettopp at skyldner ikke skal kunne spekulere i at motparten ikke «vil ta bryet med å reise sak».[142]

De mange relevante motregningsbegrensningene, sett i sammenheng med lovgivers klare forutsetninger om oppgjørsrekkefølge, tilsier totalt sett at banken ikke vil kunne påberope seg motregning basert på kundens ansvar etter § 4-30 tredje og fjerde ledd.

4.3.4 Samlet om rettsvirkningene av manglende tilbakeføring

Det ovennevnte kan oppsummeres med at tilbakeføringskravet er et selvstendig krav kunden har mot banken dersom vilkårene i § 4-32 er oppfylt. At kunden eventuelt bærer det endelige ansvaret etter § 4-30 tredje eller fjerde ledd, utgjør ingen holdbar innsigelse mot dette kravet, ei heller gir det grunnlag for et krav som banken kan bruke til å motregne i tilbakeføringskravet. Man kan kritisere løsningen for å være rettsteknisk komplisert. Det er imidlertid viktig å huske at spørsmålet om tilbakeføringskravets «selvstendige liv» bare blir aktuelt når banken bryter den stort sett klare, lovfestede plikten til tilbakeføring. Hvis lovens ordning følges, trenger vi bare å behandle ett krav – nemlig bankens krav om at kunden skal holdes ansvarlig grunnet grov uaktsomhet eller forsett, jf. § 4-30 tredje og fjerde ledd.

Løsningen Finansklagenemnda valgte for 1999-loven i FinKN-2022-1006, er derfor den riktige også for ny lov – kunden har krav på forsinkelsesrenter for tilbakebetalingskravet selv om hen taper i spørsmålet om det endelige ansvaret for transaksjonen. Tilbakeføringskravet forfaller ved utløpet av neste virkedag etter at kunden har varslet om at transaksjonen ikke var godkjent, jf. § 4-32 første ledd og § 4-24 annet ledd. Det vil derfor løpe forsinkelsesrenter på tilbakebetalingskravet fra dette tidspunktet og frem til det innfris ved betaling, selv om kunden skulle vise seg ansvarlig i henhold til § 4-30 tredje eller fjerde ledd. Selv om man skulle mene at bankens krav er forfalt eller kunne bringes til forfall før kunden har mottatt tilbakebetalingskravet, er det neppe grunnlag for å legge forsinkelsesrenter på dette kravet før beløpet er tilbakeført til kunden, ettersom banken i et slikt tilfelle selv må bære risikoen for det forsinkede oppgjøret, jf. forsinkelsesrenteloven § 2 annet ledd.

Etter mitt syn vil en slik rettstilstand gi et resultat som harmonerer med bestemmelsens formål; bankene får et reelt oppfyllelsespress for tilbakeføringsplikten, og kundens ansvar etter § 4-30 realiseres gjennom et krav banken skal gjøre gjeldende på vanlig måte. Man skal ikke overdrive den praktiske betydningen av at det tilkjennes forsinkelsesrenter – det dreier seg om små beløp sammenliknet med beløpet kunden eventuelt blir idømt. Men med tanke på at de fleste banker vil ha mange slike saker i løpet av år, vil forsinkelsesrentene i praksis medføre en ikke ubetydelig «avgift» som banken må betale uavhengig av om den til slutt får rett i det materielle spørsmålet om ansvar etter § 4-30. Det vil ha en kostnad å forsøke å få «dekning» på en måte som omgår loven.

Banker som systematisk lar være å tilbakeføre, vil risikere forsinkelsesrentekrav som til sammen kan få en viss størrelse. For eksempel må det på bakgrunn av Finansklagenemndas (etter mitt syn riktige) oppfatning i FinKN-2022-1006 være slik at alle kunder som har reklamert over svindeltransaksjoner og blitt møtt med ensidig tilbakehold i stedet for at saken ble brakt inn for nemnda, i utgangspunktet ha krav på forsinkelsesrente – begrenset av foreldelsesfristen på tre år.[143] Dette vil gjelde selv om bankens konklusjon om at kunden var ansvarlig for tapet, skulle vise seg korrekt. Forbrukertilsynets stikkprøver indikerer at dette kan utgjøre mange kunder.[144] Opptil tre år med forsinkelsesrenter på tilbakeføringskravene kan da innebære ganske store beløp samlet sett.[145] Dette avhenger selvsagt av at forbrukere vil gjøre forsinkelsesrenter gjeldende, noe mange antakelig ikke vil gjøre. Men kanskje skal det ikke veldig mange kranglevillige kunder til før bankene opplever det som en unødig risiko å forsøksvis legge saken død med et strengt brev til kunden i stedet for å tilbakeføre og reise sak.

5 Avsluttende diskusjon – tilbakeføringsregelens rolle i tapsfordelingen

Foran har jeg skissert innholdet av regelen om tilbakeføring, og sett på reelle og potensielle konsekvenser ved at bestemmelsen brytes. I lys av de observasjoner jeg har gjort av bransjepraksis rundt § 37 i 1999-loven i punkt 2, kan det virke som det enkle prinsippet om tilbakeføring har vist seg vanskelig å gjennomføre i praksis. Muligens har det vært for lite oppmerksomhet rundt problemstillingen, på tross av at Banklovkommisjonen i sin tid så prosessbyrdespørsmålet som viktig. Forarbeidene til ny finansavtalelov gir hvert fall ingen indikasjoner på at lovgiver har vært klar over at regelen om prosessbyrde ofte ikke følges. Økt press fra tilsynsmyndighetene vil antakelig kunne skjerpe bransjepraksis noe. Etter min mening bør også § 4-32 første ledd i den nye finansavtaleloven tolkes slik at brudd på bestemmelsen får konsekvenser, i form av forsinkelsesrenter og en rett for kunden til isolert oppgjør, også der kunden ikke får medhold i at banken skal bære tapet etter § 4-30 første ledd.

Noen vil kanskje mene at brudd på tilbakeføringsplikten er av begrenset betydning; til syvende og sist vil en kunde med en rettmessig sak kunne få prøvd denne uansett. Det er imidlertid et poeng at lovgiver har lagt til grunn at å plassere prosessbyrden på kunden vil medføre at en del krav om tilbakeføring aldri vil bli gjort gjeldende.[146] Saker om svindeltransaksjoner reiser ofte vanskelige grensedragninger mellom simpel og grov uaktsomhet og mellom grov uaktsomhet og forsett.[147] Det er derfor for bankkunder vanskelig å vite om det er

mulig å få overprøvd bankens «konklusjon» om at man skal bære hele eller deler av tapet. I sitt orienteringsbrev til bankene i 2022 har Forbrukertilsynet også «funnet eksempler på at banker oppgir feilaktig og potensielt villedende informasjon om finansavtalelovens regler om ansvar for tap ved uautoriserte transaksjoner overfor forbrukere».[148] Slik praksis er i så fall ytterligere egnet til å villede forbrukeren om sin rettsstilling.

Selv om forbrukerne jevnt over skulle ta en del saker til et tvisteløsningsorgan, er det neppe kontroversielt å si at hvilken part som pålegges prosessbyrden, i mange tilfeller kan ha betydning for hvor det endelige tapet plasseres i de mange tvilsomme sakene. Det er ikke mulig å få klare svar på hvor mange og hva slags saker som blir «endelig avgjort» av bankene selv i perioden fra 1999-loven trådte i kraft til tilsynsmyndighetene kom på banen i 2022. Overblikket i punkt 2.2 indikerer imidlertid at det kan utgjøre en betydelig andel av saker hvor kunder varsler om svindeltransaksjoner. En undersøkelse fra det europeiske banktilsynet (EBA) indikerer at tapsfordelingen ved ikke-godkjente betalingstransaksjoner i alle medlemsland i EØS slår ut slik at kundene relativt ofte blir sittende med en betydelig del av tapet.[149] Kanskje kan disse funnene delvis forklares med det praktiske utgangspunktet at kundens konto blir stående «tømt», og at dette har endt opp med å trumfe det rettslige utgangspunktet om at banken skal bære tapet?

Regimet for fordelingen av tap, som i dag følger av finansavtaleloven § 4-30, var ment å stimulere til utvikling av sikrest mulige betalingsløsninger samt til at tapet ble plassert hos den parten med best forutsetninger for å pulverisere tapet.[150] Dersom det over tid har vært en regelstridig praksis i deler av norsk finansbransje, som har til virkning å snu prosessbyrden, vil dette på systemnivå kunne forskyve tapsrisiko vekk fra bankene og over på kundene.[151] Om man skal legge lovgivers forutsetninger til grunn, må man da konkludere med at denne praksisen er egnet til å svekke utviklingen av sikrere betalingsløser og til å øke den økonomiske risikoen kundene utsettes for når de bruker betalingsløsninger. Ettersom ny finansavtalelov nå er i kraft, bør derfor lovgiver og tilsynsmyndigheter følge med på om ambisjonen om «snudd prosessbyrde» får realitet, og løpende vurdere behovet for ytterligere grep som sikrer etterlevelse.

Kilder

Litteratur

Arntzen, Siri K. *Bankenes motregningsrett.* Norges råd for anvendt samfunnsforskning, 1991.

Augdahl, Per. *Den norske obligasjonsretts almindelige del*, 3. utg. Aschehoug, 1963.

Bergsåker, Trygve. *Pengekravsrett*, 3. utg. Gyldendal, 2015.

Cherednychenko, Olha O. «Two sides of the same coin: EU financial regulation and private law». *European Business Organization Law Review,* 2021, *22*, s. 147-172. https://doi.org/10.1007/s40804-020-00202-y

Christensen, Lars. «Felles foreldreansvar for alle foreldre?». *Kritisk Juss*, 2004, *30*, s. 345-347.

Flock, Hans og Joakim Bakke-Nielsen. *Lov 25. juni 1999 nr. 46om finansavtaler og finansoppdrag (finansavtaleloven).* Karnov Lovkommentarer, Lovdata Pro, ajourført 1. april 2021.

Guimarães, Maria Raquel. «The transposition of PSD2: Decree-Law 91/2018 of 12 November, the Portuguese experience and what may (or may not) change», i Elisabetta Bani, Vincenzo De Stasio, Antonella Sciarrone Alibrandi, red., *The transposition of PSD2 and open banking.* Bergamo University Press, 2021., s 141-167 (tilgjengelig via https://aisberg.unibg.it/retrieve/e40f7b89-e356-afca-e053-6605fe0aeaf2/Vol_DeStasio_Banking_ebook.pdf)

Guimarães, Maria Raquel og Reinhard Steennot. «Allocation of liability in case of payment fraud: Who bears the risk of innovation? A comparison of Belgian and Portuguese law in the context of PSD II». *European Review of Private Law*, 2022, *30*(1), s. 29-72 https://doi.org/10.54648/erpl2022003

Habibija, Admir. *Ansvarsfordelingen mellom forbruker og bank ved ikke-godkjente betalingstransaksjoner. Grensen for grovt uaktsomme og forsettlige pliktbrudd ved misbruk av elektroniske betalingsinstrumenter etter ny finansavtalelov.* Masteroppgave, Universitetet i Oslo, 2021, http://hdl.handle.net/10852/87051

Hagstrøm, Viggo. *Obligasjonsrett*, 2. utg. Universitetsforlaget, 2011.

Hov, Jo og Høgberg, Alf Petter. *Alminnelig avtalerett*. Calax, 2009

Iversen, Torstein. *Obligationsret3. del*, 3. utg., Djøf forlag, 2018.

Kjørven, Marte Eidsand, «Who pays when things go wrong? Online financial fraud and consumer protection in Scandinavia and Europe»*, European Business Law Review*, 2020, *31*(1), s. 77-110. (http://urn.nb.no/URN:NBN:no-87668)

Kjørven, Marte Eidsand, Herman Bruserud, Håvard H. Holde, Jon Vegard Lervåg, Mona Nygård og Espen Nyland. *Foreldelse av fordringer.* Universitetsforlaget, 2011.

Kjørven, Marte Eidsand, Alf Petter Høgberg og Geir Woxholth. «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)». *Lov og Rett*, 2021, *60*(6), s. 335-366. http://urn.nb.no/URN:NBN:no-94987

Krüger, Kai. «Hvor langt kan rettstvister løses midlertidig og betryggende i påvente av endelig dom?», i Anders Bratholm mfl., red., *Lov og frihet. Festskrift til Johs. Andenæs på 70-årsdagen.* Universitetsforlaget, 1982, s. 603-615 (FEST-1982-ja-603).

Law, Stephanie. «The transformation of consumer law in times of crisis: The ex officio control of unfair contract terms»*,* i Alan Uzelac og Cornelis H.R. van Rhee, red., *Transformation of civil justice. Unity and diversity*. Springer, 2018, s.283-309

Lenaerts, Koen og José A. Gutiérrez-Fons. «To say what the law of the EU is. Methods of interpretation and the European Court of Justice», *EUI AEL, 2013/09, Distinguished Lectures of the Academy*.http://hdl.handle.net/1814/28339

Lindskog, Stefan. *Betalning. Om kongruent infriande av penningskulder och andra betalningsrättsliga frågor*, 2. utg. Norstedts, 2018.

Lindskog, Stefan. *Kvittning. Om avräkning av privaträttsliga fordringar,* 3. utg. Norstedts, 2014.

Løvold, Vibeke Irene. «Motregning i trygdeytelser til innkreving av tilbakebetalingskrav etter folketrygdloven – beskyttelse av midler til livsopphold og forholdet til utleggstrekk». *Lov og Rett*, 2021, *60*(5), s. 265-277. https://doi.org/10.18261/issn.1504-3061-2021-05-03

Martinson, Claes. «Det nordiska funktionalistiska angreppssättet och obehörig vinst – Dieselfallet»*, Juridisk Tidskrift (JT)*, 2019, *2019-2020*(1), s. 148-170.

Norland, Line og Marte Eidsand Kjørven. «Elektroniske signaturer og avtalebinding»,i Marte Eidsand Kjørven, Maria Astrup Hjort og Tone Linn Wærstad, red., *Bruk og misbruk av elektronisk identifikasjon*, Karnov Group Norway, 2022.

Norros, Olli. *Obligationsrätt.* Alma Talent, 2018.

Oleownik, Sonja. «Phishing in online banking. An overview of the development and the European and German legal positions», i Georg Borges og Christoph Sorge, red., *Law and technology in a global digital society*. Springer, 2022, s. 257-286. https://doi.org/10.1007/978-3-030-90513-2_13

Røed, Anne Cathrine. *Foreldelse av fordringer*, 3. utg. Cappelen Damm, 2010.

Steennot, Reinhard. «Liability for unauthorized payment transactions: The transposition of PSD2 in Belgium», i Elisabetta Bani, Vincenzo De Stasio, Antonella Sciarrone Alibrandi, red., *The transposition of PSD2 and open banking.* Bergamo University Press, 2021, s 167-189 (https://aisberg.unibg.it/retrieve/e40f7b89-e356-afca-e053-6605fe0aeaf2/Vol_DeStasio_Banking_ebook.pdf)

Steennot, Reinhard. «Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2)». *Computer Law & Security Review*, 2018, *34*(4), s. 954-964, https://doi.org/10.1016/j.clsr.2018.05.008

Steennot, Reinhard. «Allocation of liability in case of fraudulent use of an electronic payment instrument: The new directive on payment services in the internal market». *Computer Law & Security Review*, 2008, *24*(6), s. 555-561. https://doi.org/10.1016/j.clsr.2008.09.005

Storvik, Marius. «Er studentsamskipnadenes depositumspraksis lovlig?». *Kritisk Juss,* 2022, *48*(2), s. 148-163, https://doi.org/10.18261/kj.48.2.2

Sæbø, Rune. *Motregning.* Fagbokforlaget, 2013.

Torvund, Olav. *Betalingsformidling i et rettslig perspektiv.* TANO, 1993.

Wallin-Norman, Karin. «Kontopengar och kontorätter: Några reflektioner med anledning av ett aktuellt rättsfall». *Ny Juridik*, 2011, 4(11), s. 29-44.

Wold, Vebjørn og Petter Omland. «I rimelighetens navn, Finansforetakenes betalingssøksmål mot forbrukere og EØS-forbrukerrettens prosessuelle side», i Anders Løvlie, Axel Hodnefjeld og Kristine-Petrine Olthuis, red., *Festskrift. Jussbuss 50år*, RennessanseMedia, 2021, s. 68-89.

Ørjasæter, Jo. «Foreldelse, ugyldighet og vindikasjon», *Jussens Venner*, Vol 50. utg 3, 2015 s 119-149

Norsk rettspraksis

Høyesterett

Rt-2000-59

Rt-2008-385

HR-2020-2021-A

HR-2022-1752-A

Underretter

TOSLO-2011-65228

TAHER-2014-21993

LB-2014-127752

TSUMO-2017-145582

LE-2021-19671

Finansklagenemnda Bank

FinKN-2016-326

FinKN-2017-281

FinKN-2017-652

FinKN-2021-326

FinKN-2021-907

FinKN-2022-490

FinKN-2022-1006

Norske forarbeider

NOU 1994:19

NOU 2008:21

Ot.prp.nr.49 (1988–1989)

Ot.prp.nr.94 (2008–2009)

Prop.62 L (2015–2016)

Prop.92 LS (2019–2020)

*Høring*snotat ny finansavtalelov, Justis- og beredskapsdepartementet, 7. september 2017 https://www.regjeringen.no/no/dokumenter/horing---revisjon-av-finansavtaleloven/id2569865/

Norske lover

Lov 31. mai 1918 nr. 4 om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer (avtaleloven)

Lov 17. desember 1976 nr. 100 om renter ved forsinket betaling m.m. (forsinkelsesrenteloven)

Lov 18. mai 1979 nr. 18 om foreldelse av fordringer (foreldelsesloven)

Lov 8. juni 1984 nr. 59 om fordringshaveres dekningsrett (dekningsloven)

Lov 26. juni 1992 nr. 86 om tvangsfullbyrdelse (tvangsfullbyrdelsesloven)

Lov 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag (finansavtaleloven)

Lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven)

Lov 10. april 2015 nr. 17 om finansforetak og finanskonsern (finansforetaksloven)

Lov 18. desember 2020 om finansavtaler (finansavtaleloven)

EU-rettsakter

PSD II (Europaparlaments- og rådsdirektiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF)

PSD I (Europaparlaments- og rådsdirektiv 2007/64/EF af 13. november 2007 om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF)

Rådsdirektiv 93/13/EØF av 5. april 1993 om urimelige vilkår i forbrukeravtaler

Utenlandske lover

Lag (2010:751) om betaltjänster (Sverige)

Lov nr 652 af 08/07/2018 om betalinger (Danmark)

Bürgerliches Gesetzbuch (BGB) (Tyskland) (tilgjengelig via https://www.gesetze-im-internet.de/bgb/)

EU-rettspraksis

Sak C-565/12*LCL Credit Lyonnais SA* (ECLI:EU:C:2014:190)

Sak C-176/17*Profi Credit Polska I* (ECLI:EU:C:2018:711)

Sak C-295/18*Mediterranean Shipping Company* (ECLI:EU:C:2019:320)

Sak C-337/20*DM, LR mod Caisse régionale de Crédit agricole mutuel (CRCAM) – Alpes-Provence*, (ECLI:EU:C:2021:671)

Annen skandinavisk rettspraksis

Almänna reklamationsnämnden

ARN 2019-08258

ARN 2019-11253

ARN 2019-14354

ARN 2022-04140

Det finansielle ankenævn

Sag 569/2021

Sag 369/2021

Øvrige forarbeider

Prop.2009 /10:220*Betaltjänster*

SOU 2016:53*Betaltjänster, förmedlingsavgifter och grundläggande betalkonton*

LFF 2017-03-15 nr. 157, *Forslag til lov om betalinger*

Annet

EU-kommisjonen, «*Your questions on PSD Payment Services Directive 2007/64/EC Questions and answers*»

European Banking Authority (EBA), *Discussion Paper on the EBA's preliminary observations on selected payment fraud data under the Payment Services Directive,* 17. januar 2022 *(https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/discussion-paper-payment-fraud-data-received-under-psd2)*

European Banking Federation (EBF), European Banking Industry, PSD Expert Group, *Guidance For The Implementation Of The Payment Services Directive Version 1.0 – august 2009*. (https://www.ebf.eu/wp-content/uploads/2017/01/Brochure-_24-08-09-PSD-Web-2009-01152-01-E.pdf)

Finans Norge, rundskriv nr. 10/22, «Tilbakeføringsplikten etter finansavtaleloven § 37».

Finansklagenemnda, *Årsrapport 2021* (tilgjengelig via https://www.finkn.no/Aktuelt?id=80#80)

Forbrukertilsynet, «Krav om oversendelse av dokumentasjon – kartlegging av bankenes praktisering av tilbakeføringsplikten ved uautoriserte transaksjoner», brev av 24. juni 2022 (https://www.forbrukertilsynet.no/wp-content/uploads/2022/06/krav-om-oversendelse-av-dokumentasjon-kartlegging-av-bankenes-praktisering-av-tilbakeforings.pdf)

Finanstilsynet, Risiko- og sårbarhetsanalyse (ROS) 2022 (https://www.finanstilsynet.no/contentassets/d6c5910b41044d1b89f7a50a7b7315db/ros-2022.pdf)

Forbrukertilsynet, «Orientering til bankene», brev av 7. desember 2022 https://www.forbrukertilsynet.no/wp-content/uploads/2022/12/orientering-til-bankene-krav-til-bankenes-tilbakeforing-av-forbrukers-tap-ved-uautoriserte-transaksjoner.pdf

ID-juristen ved Petter Omland, «Finansforetaks brudd på tilbakeføringsplikt etter finansavtaleloven § 37», brev til Forbrukertilsynet og Finanstilsynet av 21. april 2021. (https://www.forbrukertilsynet.no/wp-content/uploads/2022/06/brev-fra-id-juristen-med-vedlegg.pdf)

Norges Bank, *Det norske finansielle systemet*, 2022 (https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/det-norske-finansielle-systemet/2022-dnfs/innhold/

Finansklagenemda, Saksbehandlingsregler for Finansklagenemda, (https://www.finkn.no/Om-oss/Regelverk/Saksbehandlingsregler-for-Finansklagenemnda)

Vedtak 29. mars 2022 nr. 4849 om delegering av myndighet fra Finansdepartementet til Finanstilsynet

Noter

1 Forfatteren er stipendiat ved Institutt for privatrett ved Universitetet i Oslo. Takk til redaksjonen (særlig til professor Marte Eidsand Kjørven), så vel som til den anonyme fagfellen, for innspill på tidligere utkast. Takk også til Petter Omland og Vegard Kleven for gjennomlesning og diskusjon underveis. Eventuelle feil og unøyaktigheter er mine egne.

2 Finanstilsynet (2022) s. 5. Dette kommer i tillegg til 159,3 millioner kroner knyttet til misbruk av betalingskort (s. 37).

3 Lov 18. desember 2020 nr. 146 om finansavtaler (finansavtaleloven).

4 Europaparlaments- og rådsdirektiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF.

5 For enkelhets skyld bruker jeg i det videre betegnelsen «bank» i stedet for lovens «betalingtjenesteyter». I noen tilfeller kan man tenke seg at betalingstjenesteyter ikke har konsesjon som bank, men for eksempel som kredittforetak etter finansforetaksloven § 2-8, slik som for kredittkorttilfellene omtalt i punkt 3.4.2 siste avsnitt.

6 Ot.prp.nr.94 (2008–2009)s. 129.

7 Se for eksempel PSD II fortale punkt 4, jf. Justis- og beredskapsdepartementets forståelse av direktivet i Prop.92 LS (2019–2020)s. 19.

8 Dette gjelder ikke hvis kunden ikke kunne ha oppdaget tilegnelsen på forhånd og heller ikke har opptrådt svikaktig, jf. § 4-30 annet ledd annet punktum.

9 Etter det formelle utgangspunktet (§ 4-30 tredje ledd første punktum) hefter kunden for hele beløpet ved grov uaktsomhet, men ansvaret begrenses altså til 12 000 kroner når det aktuelle betalingsinstrumentet er et elektronisk betalingsinstrument, jf. annet punktum.

10 *Høringsnotat ny finansavtalelov*s. 84.

11 Spørsmål rundt aktsomhetsvurderingen har blant annet vært behandlet i Kjørven (2020), Kjørven mfl. (2021), Habibija (2021).

12 Finansavtaleloven (2020) § 1-9.

13 Lov 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag (finansavtaleloven).

14 Se for eksempel Storvik (2022) s. 156 om søksmålsbyrden i husleieforhold, Prop.62 L (2015–2016) s. 142-143 om søksmålsbyrden ved administrative sanksjoner, og Christensen (2004) s. 346 om søksmålsbyrden i samværssaker.

15 Se for eksempel Krüger (1982) s. 606 om motregning og partenes «prosesstaktiske status».

16 For eksempel NOU 1994:19s. 146.

17 Den begrensede økonomiske kostnaden ved å bringe en sak inn for Finansklagenemnda er selvsagt et poeng og vil bli tatt i betraktning i analysen videre i artikkelen (se punkt 2.1 og 5).

18 Se blant annet sak C-176/17*Profi Credit Polska I* (avsnitt 69), med videre henvisninger til en lang rekke avgjørelser. Se nærmere Wold og Omland (2021) om EU-domstolens doktrine og praktiske implikasjoner for norsk rett.

19 Se Law (2018) s. 290, som fremhever at EU-domstolens praksis springer ut av at nasjonale domstoler i medlemsstatene (som kan forelegge spørsmål for EU-domstolen) «have recognised that these procedural rules constitute obstacles that shape the relationship between the parties and affect the possibility for the effective enforcement of EU consumer protection at the domestic level. That is to say, given the imbalances in economic, political and social power-essentially in terms of a lack of knowledge, time and economic resources-consumers are deemed to be less likely to engage their consumer rights of their own motion before their national courts, or even to appear before a court to defend themselves ...».

20 NOU 1994:19s. 146.

21 Finansklagenemnda var allerede da Banklovkommisjonen skrev, tilgjengelig som lavterskelorgan for kundene i slike saker. Se for eksempel Torvund (1993) s. 428 flg., som omtaler en rekke nemndssaker om betalingstransaksjoner.

22 Det er tilstrekkelig å vise til saksgangen i HR-2022-1752-A («Olga-svindel»), som omhandlet et spørsmål om hvorvidt kunden hadde opptrådt forsettlig etter finansavtaleloven § 35 tredje ledd og derfor heftet for hele beløpet for en svindelbetaling. Kunden vant i Finansklagenemnda, men banken brakte saken inn for tingretten og vant. Kunden vant deretter i både lagmannsretten og Høyesterett, jf. dommens avsnitt 7-9.

23 Finansavtaleloven 1999 § 37 første ledd, jf. annet ledd. Banklovkommisjonen foreslo opprinnelig tre uker, men fristen ble justert etter høringen.

24 Europa-Parlamentets og Rådets direktiv 2007/64/EF af 13. november 2007 om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF

25 Ot.prp.nr.94 (2008–2009)s. 131 mv.

26 Høringsnotat ny finansavtalelov s. 84, Prop.92 LS (2019–2020)s. 169.

27 PSD II artikkel 73.

28 Navnlig ble omtalen i 1999-lovens § 37 første ledd av et «krav om tilbakeføring» fra kunden endret til et «varsel» fra kunden i finansavtaleloven § 4-32 første ledd, jf. § 4-24 annet ledd.

29 Se noter 20 og 26

30 At Banklovkommisjonen bruker pulveriseringshensynet som et argument for å oppstille en prosessbyrderegel, jf. sitatet ovenfor, må vel forstås dit hen at kommisjonen mener at banken i større grad enn kunden kan bære tapet mens saken pågår.

31 Lov 8. juni 1984 nr. 59 om fordringshaveres dekningsrett (dekningsloven). Dekningsloven § 2-5 bestemmer at beslag «ikke [kan] tas i skyldnerens penger, bankinnskudd og andre fordringer eller forråd av varer, for så vidt de er nødvendige til underhold av skyldneren og husstanden inntil lønn eller annen inntekt neste gang forfaller, likevel ikke utover to måneder med mindre særlige hensyn tilsier det».

32 Se også finansavtaleloven § 4-13 om tilbakehold og motregning i innestående på konto, som hviler på liknende betraktninger.

33 Guimarães og Steennot (2022) s. 46 og 47, Steennot (2018) s. 958 og Steennot (2008) s. 559.

34 Norges Bank (2022), se faktaboksen «Hva er penger?», og Torvund (1993) s. 150.

35 I norsk rett er det tilsynelatende liten tradisjon for å problematisere forskjellen på kontopenger og vanlige penger, jf. Ørjasæter (2015) s. 136 (note 66). Se imidlertid behandlingen hos Torvund (1993) s. 150 flg. Se også diskusjonen mellom Lindskog (2018) s. 439-444, særlig note 1564, og Wallin-Norman (2011) s. 30 flg., med utgangspunkt i svensk rett.

36 I den tyske reguleringen er dette tilsynelatende formalisert, jf. Oleownik (2022) s. 265 mv. Her ser man det slik at som utgangspunkt blir banken sittende med tapet som følge av at den – på grunn av manglende godkjenning – mangler rett til å belaste kundens konto (altså nedskrive kundens kontofordring).

37 Dette kan sies å være i tråd med den skandinaviske «funksjonalistiske» innfallsvinkelen til rettskonflikter, se Martinson (2019) s. 159-160, hvor vi er opptatt av å løse den reelle interessekonflikten heller enn å utlede begrepsperfekt juss. Det vil imidlertid være tilsvarende i strid med en funksjonalistisk tilnærming å komme til rettsdogmatiske konklusjoner ut fra et tankebilde om kontopenger som fysiske ting som kunden har «tapt» eller «brukt».

38 Eksempelvis TAHER-2014-21993 (Tingrettsdom fra Asker og Bærum tingrett), FinKN-2016-326, FinKN-2021-326.

39 Finansklagenemnda, *Årsrapport 2021* s. 22

40 https://www.id-juristen.no/. For ordens skyld: ID-juristen er finansiert gjennom forskningsprosjektet *Samfunnssikkerhet og digitale identiteter*, hvor forfatteren også er ansatt. Forfatteren bisto ID-juristen med faglige råd i forbindelse med redegjørelsen som ble oversendt Forbrukertilsynet om daværende finansavtalelov § 37.

41 Brev fra ID-juristen til Forbrukertilsynet og Finanstilsynet av 21. april 2021. Sakene fra ID-juristen gir også inntrykk av at kundene jevnlig fortelles at det er de som må bringe forholdet inn for Finansklagenemnda dersom de er uenige i foretakets interne konklusjoner.

42 Brev fra ID-juristen til Forbrukertilsynet og Finanstilsynet av 21. april 2021. (Se sak fra Eika Bank).

43 Brev fra ID-juristen til Forbrukertilsynet og Finanstilsynet av 21. april 2021. En praksis bygget på samtykke synes å ha vært standard hos DNB, jf. DNBs prosesskriv i FinKN-sak 2022-2585 (DNB trakk saken før den gikk til avgjørelse). I prosesskrivet angir DNB at de kan gjenbelaste kundekontoer i tråd med følgende klausul: «Jeg gir herved fullmakt til å gjenbelaste kontoen min for eventuelle krediteringer gjort i anledning denne reklamasjonen, dersom utfallet av reklamasjonsprosessen er at transaksjonene likevel kan dokumenteres som korrekte, brukerstedet har refundert beløpet til kontoen min *eller jeg for øvrig er ansvarlig for beløpet.*» (Min kursiv.)

44 Forbrukertilsynet, «Orientering til bankene» (2022).

45 Betalingsloven § 99 nr. 1. Se fra forarbeidene: «Udbyderen kan kun tilbageholde beløbet indtil mistanken om svig er bekræftet eller afkræftet» (se *LFF 2017-03-15 nr 157, Bemærkninger til § 99*).

46 Se for eksempel sag 569/2021 og sag 369/2021 hos Det finansielle ankenævn.

47 Guimarães og Steennot (2022) s. 46 og 47. Forfatterne forstår altså PSD II artikkel 73 på samme måte som norsk lovgiver – som en prosessbyrderegel. Det er tilsynelatende også slik den har blitt gjennomført i både Belgia og Portugal, men angivelig da bare på papiret.

48 PSD II artikkel 107.

49 Artikkel 71 hjemler kundens plikt til å underrette banken om misbruk sml. finansavtaleloven § 4-24.

50 European Banking Federation (EBF), European Banking Industry, PSD Expert Group (2009) s. 25-26.

51 SOU 2016:53 s. 267 (min kursiv).

52 Se punkt 1.

53 «Grov oaktsamhet» medfører ansvar for 12 000 kroner, mens «särskild klandervärd» medfører ansvar for hele beløpet, tilsvarende de norske kategoriene «grov uaktsomhet» og «forsett» jf. finansavtaleloven § 4-30 tredje og fjerde ledd.

54 Se note 52

55 Se også Allmänna reklamationsnämndens (ARN) redegjørelse under overskriften «Allmänt om regleringen» i ARN 2022-04140.

56 Se nærmere om plikten til å varsle nasjonale myndigheter ved mistanke om svik i punkt 3.2.2 og 3.2.3.

57 Se her EU-kommisjonen s. 187: «If the payment service provider of the payer can exclude on a prima facie basis that the payer has acted fraudulently, it should refund the user immediately.»

58 Se tilsvarende syn hos Guimarães og Steennot (2022) s. 47 og 48 og Steennot (2021) s. 174, Steennot (2018) s. 958 og Steennot (2008) s. 559.

59 Dette gjelder en absolutt reklamasjonsfrist på 13 måneder. Tilbakeføringsplikten omfatter ikke den objektive egenandelen på 450 kroner.

60 Finansavtaleloven (2020) § 1-5 sjette ledd.

61 Se 1999-lovens § 24 annet ledd og FinKN-2016-326 og FinKN-2017-281, jf. omtale i *Høringsnotat ny finansavtalelov* s. 26.

62 Se Høyesteretts uttalelser i HR-2020-2021-A (avsnitt 36 og 37) og Prop.92 LS (2019–2020)s. 175.

63 Prop.92 LS (2019–2020)s. 175.

64 Avtale mellom kunden og banken kan angi hvilken form et samtykke skal ha, og måten samtykke kan gis på, jf. PSD II artikkel 64 nr. 2 og finansavtaleloven § 4-2 annet ledd. Det virker imidlertid ikke å være vanlig praksis i Norge å fastsette nærmere retningslinjer i kontovilkår eller utstedelsesvilkår utover bruk av det aktuelle betalingsinstrumentet. Merk at finansavtaleloven § 4-2 i likhet med PSD II viser til at samtykket må gjøres av «betaleren». Slik «betaler» er definert i direktivet (artikkel 4 nr. 8), vil kunden teknisk sett ikke være «betaleren» i relasjon til den aktuelle transaksjonen, fordi kunden ikke initierer transaksjonen. Dette må forstås som et rent arbeidsuhell fra den europeiske lovgiverens side, slik Guimarães (2021) s. 148 note 27 har påpekt. «Betaleren» i § 4-2 må derfor forstås som «kunden».

65 Jf. begrepsbruken i Hov og Høgberg (2009) s. 97-98.

66 Se Norland og Kjørven (2022) med videre henvisninger (blant annet note 39 om passivitet).

67 Sml. Norland og Kjørven (2022) om finansavtaleloven § 3-20.

68 Se for eksempel Banklovkommisjonens uttalelser i NOU 2008:21s. 98 om at ansvar kan bygges på «fullmaktsbetraktninger». Ifølge Oleownik (2022) s. 267 mv. har kunder i Tyskland ofte blitt bundet av samtykker gitt av tredjepersoner uten kundenes tillatelse, på grunnlag av «apparent authority», noe likt en kombinasjonsfullmakt.

69 Se for eksempel EU-domstolens sak C-565/12 om forholdet mellom effektiv gjennomføring av direktiver og nasjonal privatrett som supplerer gjennomførende rettsregler – i dette tilfellet restitusjonsregler.

70 FinKN 2022-490. I svensk nemndspraksis er forståelsen tilsynelatende den motsatte, se ARN 2019-08258, ARN 2019-11253 og ARN 2019-14354. Dette trenger ikke utelukkende å bunne i veldig ulike syn på hensynene som gjør seg gjeldende, men kan ha sammenheng med ulike tekniske spesifikasjoner for henholdsvis norsk og svensk mobil BankID.

71 Finansavtaleloven (2020) § 4-32 første ledd første punktum. Min utheving.

72 Se punkt 3.2.3.

73 PSD II artikkel 73 nr. 1.

74 Se punkt 2.1

75 Se lag om betaltjänster 5 a kap. 1 § første ledd.

76 *Høringsnotat ny finansavtalelov* s. 84.

77 Se fra SOU 2016:53 s. 268: «Att betaltjänstleverantören är skyldig att redovisa sina misstankar bör minska risken för att leverantörer slentrianmässigt hänvisar till en misstanke om att betalaren har handlat svikligt för att undkomma betalningsansvar.»

78 Se Rt-2000-59 og Ot.prp.nr.49 (1988–1989) s. 63-64. Her er det presisert at svikaktighet forutsetter at et forsettlig mislighold begås med hensikt om å få en bedre forsikringsavtale på forsikringsselskapets bekostning. En annen forskjell for finansavtalelovens del er at forsettskravet er knyttet til kundens forpliktelser etter loven og utstedelsesvilkårene, mens kundens ansvar for svik i prinsippet er uavhengig av dette – man kan forsøke å begå svik mot banken ved å rette et krav om tilbakeføring for en fiktiv svindel selv om man har etterlevd pliktene i BankID-avtalen.

79 Finans Norge virker å ha vært av motsatt oppfatning under høringsrunden, se Prop.92 LS (2019–2020)s. 172, hvor det vises til at svikaktighet omfatter forsett. Dette kan imidlertid ikke være riktig, ettersom et forsettlig brudd på kundens plikter helt klart kan foreligge som følge av uforsiktig bruk/oppbevaring av personlig sikkerhetsinformasjon, uten at kunden har hatt til hensikt å berike seg på bankens bekostning.

80 Finansavtaleloven (2020) § 3-7 tredje ledd jf. PSD II fortale avsnitt 71, «objektive grunne».

81 Jf. finansavtaleloven § 4-32 annet ledd siste punktum.

82 Tilsvarende svensk lovgivers observasjoner i Prop. 2009/10:220 s. 29 og SOU 2016:53 s. 268.

83 EU-kommisjonen har for PSD Is del forutsatt at betalingstjenesteyter har en kort periode tilgjengelig for å «etterforske» om det foreligger «svindel» fra kunden før tilbakebetaling må skje, en etterforskningsperiode som tilsynelatende skal brukes til å avdekke om transaksjonen faktisk var uautorisert, jf. EU-kommisjonen, «*Your questions on PSD Payment Services Directive 2007/64/EC Questions and answers*» s. 187. En sammenlikning mellom PSD I og PSD II kan gi inntrykk av at unntaket for svik er ment å konsumere det som tidligere inngikk i vurderingen av om kunden i realiteten hadde samtykket til transaksjonen.

84 PSD II fortalen avsnitt 71.

85 Også her kan vi se til den svenske direktivgjennomføringen for en alternativ tilnærming. I den svenske lag om betaltjänster 5 a kap. 1 § tredje punktum har unntaket for svik blitt knyttet til om betalingene er godkjente («behöriga») eller ikke. I Sverige skal altså bankene ikke ta stilling til om kunden kan mistenkes for svik, men til om det er grunnlag for mistanke om at transaksjonen i realiteten var godkjent. I alle tilfellene der banken nekter tilbakebetaling med påstand om at transaksjonen er godkjent, skal dette meldes til Finansinspektionen. Som nevnt er ikke den svenske regelen noen prosessbyrderegel, men den bygger på et liknende ønske om å forhindre «slentrianmässig» bruk av unntak fra tilbakeføringsplikten, jf. SOU 2016:53 s. 267-268.

86 Domstolen må selvsagt også vurdere samtykkespørsmålet når den skal ta stilling til hvem som må bære tapet.

87 Forbrukertilsynet, «Orientering til bankene» (2022) s. 5.

88 PSD I artikkel 60 nr. 1 krevde at tilbakeføring skulle skje «straks» etter kundens rettidige varsel.

89 Direktivet oppstiller et krav om «underretning», jf. PSD II artikkel 71. Etter PSD II artikkel 73 nr. 1 skal medlemsstatene sikre at kundene får tilbakebetalt midlene så lenge («med forbehold af» at) de har gitt slik underretning. Et krav om for eksempel skriftlighet i underretning ville derfor brutt med ordlyden i direktivet.

90 Se også finansavtaleloven 1999 § 37 annet ledd bokstav a.

91 PSD I artikkel 58 nr. 1, PSD II artikkel 71 nr. 1.

92 Se også her annet punktum om at friststart for kundens absolutte 13 måneders varslingsfrist forutsetter at betalingstjenesteyter har oppfylt sine opplysningsplikter i loven, jf. finansavtaleloven § 4-24 annet ledd siste punktum.

93 Ot.prp.nr.94 (2008–2009) s. 118. Se også Flock og Bakke-Nielsen (2021) note 2 til finansavtaleloven 1999 § 37.

94 Finans Norge, rundskriv nr. 10/22, «Tilbakeføringsplikten etter finansavtaleloven § 37».

95 Et avsluttende spørsmål er da om kravet om «skriftlig» innsigelse medfører at fristen ikke begynner å løpe der kunden *kun varslet muntlig*. At bestemmelsen som helhet skal skape rom for en situasjon der kunden anses å ha varslet rettidig, men fristen ikke har begynt å løpe, samsvarer dårlig med bestemmelsens formål og fratar regelen mye av sin logiske sammenheng. Skriftlighetskravet og det særskilte kravet til «innsigelse» er ikke begrunnet i forarbeidene – verken til 1999-loven eller dagens lov. En mulig tilnærming her, som kanskje rimer best med hensynene bak bestemmelsen og med bankens ansvar for å tilrettelegge for varsling etter finansavtaleloven § 4-23 annet ledd, er å la skriftlighetskravet stå i de tilfeller der banken etter muntlig varsel har veiledet kunden om behovet for skriftlig innsigelse, men ikke ellers. Dette er selvsagt ikke en helt tilfredsstillende løsning, ordlyden tatt i betraktning, og spørsmålet må totalt sett anses uavklart.

96 PSD II artikkel 73 nr. 1

97 TAHER-2014-21993 fra Asker og Bærum Tingrett. Saken ble resultatsløst anket til Lagmannsretten (se sak LB-2014-127752).

98 Også denne typen betalinger er betalingstransaksjoner. Utstederen av kortet yter en betalingstjeneste, jf. finansavtaleloven § 1-5 første ledd bokstav e. Den aktuelle transaksjonen blir dermed en «ikke godkjent betalingstransaksjon» selv om betalingen ikke skjer fra en konto i kundens navn, jf. finansavtaleloven § 1-5 sjette ledd.

99 Finansavtaleloven § 4-32 første ledd og PSD II artikkel 73 nr. 1.

100 Finansavtaleloven § 1-5 første ledd bokstav e jf. sjette ledd og § 4-2 første ledd.

101 Se EU-domstolens sak C-295/18 avsnitt 47. Det er verdt å nevne at enkelte språkversjoner av PSD II fremstår mer åpne med hensyn til dette spørsmålet, jf. engelske «the payer's payment service provider *refunds* the payer» og tyske «der Zahlungsdienstleister des Zahlers diesem den Betrag des nicht autorisierten Zahlungsvorgangs unverzüglich...*erstattet*». I møte med denne typen språklige uklarheter, og særlig ved betydningsfulle nyanser mellom språkversjoner, er tolkningstradisjonen i EU at man legger stor vekt på rettsakters formål og system, jf. Lenaerts og Gutiérrez-Fons (2011) s. 10.

102 Implikasjonen av et slikt synspunkt må da også være at kundens ansvar for uautoriserte kredittkorttransaksjoner som banken mener er svikaktige, skal bringes inn for et tvisteløsningsorgan innen fire uker fra kundens rettidige varsel dersom en slik kreditering ikke finner sted, jf. finansavtaleloven § 4-32 annet ledd.

103 Se punkt 2.2 og Forbrukertilsynet, «Orientering til bankene» (2022) s. 9.

104 Jf. blant annet *Høringsnotat ny finansavtalelov* s. 84 flg.

105 Jf. finansavtaleloven (1999) § 2 og finansavtaleloven (2020) § 1-9.

106 Selv om man skulle mene at finansavtalelovens ufravikelighet ikke er til hinder for at kunden inngår en slik avtale, ville denne typen vilkår i alle tilfelle være ugyldig etter avtaleloven § 36, jf. § 37. Et slikt vilkår setter forbrukeren i en vesentlig svakere stilling enn bakgrunnsretten (jf. vilkåret om «betydelig skjevhet» til forbrukerens ugunst i direktiv 93/13/EØFartikkel 3 nr. 1, jf. f.eks. sak C-415/11 avsnitt 68. En slik praksis vil være i strid med de retningslinjer direktiv 93/13/EØF setter for tolkningen av avtaleloven § 36 jf. § 37 og vil ikke binde forbrukerne, jf. direktivets artikkel 6 nr. 1.

107 Lov 10. april 2015 nr. 17 om finansforetak og finanskonsern (finansforetaksloven). Vedtakskompetansen ligger etter loven hos Finansdepartementet, jf. finansforetaksloven § 22-2, men er delegert til Finanstilsynet, jf. vedtak om delegering av myndighet fra Finansdepartementet til Finanstilsynet (forskrift 29. mars 2022 nr. 484).

108 Finansforetaksloven § 22-2 annet ledd og § 22-1.

109 Forbrukertilsynet, «Orientering til bankene» (2022).

110 Steennot (2021) s. 174. «PSPs» sikter her til betalingstjenesteyter, altså banken.

111 Se punkt 2.2.

112 TAHER 2014-21993 fra Asker og Bærum tingrett.

113 Lov 17. desember 1976 nr. 100 om renter ved forsinket betaling m.m. (forsinkelsesrenteloven)

114 Nemnda understreket i alle fall at «Banken har godtatt å betale forsinkelsesrenter for tiden etter utløpet av fireukersfristen i § 37 for det tilfelle at kunden skulle få medhold i saken». «Banken har ikke oppfylt sin plikt etter finansavtalel. § 37 til enten å føre tilbake beløpet med dekning av rentetap, eller å ta ut søksmål eller klage til Finansklagenemnda, innen fire uker fra mottakelse av skriftlig reklamasjon fra kunden. Banken har godtatt å betale forsinkelsesrenter for tiden etter utløpet av fireukersfristen i § 37 for det tilfelle at kunden skulle få medhold i saken.»

115 Dette kan kanskje skyldes at forsinkelsesrenter muligens ikke ble krevet. Finansklagenemnda er ikke bundet av partenes anførsler og rettsgrunnlag, jf. *Saksbehandlingsregler for Finansklagenemnda* punkt 13. Det kan fremstå uklart om «anførsler» kan innebære at man trekker inn nye krav, slik som et krav om forsinkelsesrenter.

116 For ordens skyld: undertegnede bisto klagers prosessfullmektig hos rettshjelpstiltaket *ID-juristen* (se fotnote 37) med enkelte faglige råd i forbindelse med saken.

117 Se punkt 4.2 om FinKN-2016-326, FinKN-2017-652 og FinKN-2021-907.

118 *Høringsnotat ny finansavtalelov* s. 84 og 85.

119 Prop.92 LS (2019–2020)s. 172.

120 *Høringsnotat ny finansavtalelov* s. 84 og 85.

121 PSD II artikkel 73 nr. 1 og artikkel 74 nr. 1 tredje og fjerde ledd.

122 Se EU-domstolens sak C-337/20 (se avsnitt 30-52).

123 At finansavtaleloven 1999 § 35 første ledd – tilsvarende dagens § 4-30 første ledd – har blitt forstått som å utgjøre grunnlaget for at kunden kan holde banken ansvarlig for svindeltransaksjoner, må ses i sammenheng med at forarbeidene til 1999-loven la til grunn at kunden hadde et krav i behold der banken ikke pliktet å tilbakeføre – typisk fordi kunden reklamerte for sent (se NOU 1994:19s. 147). Det er da åpenbart at regelen om bankens materielle ansvar har et «eget liv» som grunnlag for et krav fra kunden. Dette synspunktet har imidlertid vist seg å være i strid med den underliggende EU-retten (jf. sak C-337/20), og etter ny finansavtalelov vil dette helt klart ikke være gjeldende rett – vilkårene for tilbakeføring må være oppfylt for at banken skal bære tapet, jf. § 4-24 første ledd.

124 Selv om det er en melding fra kunden som utløser bankens tilbakebetalingsplikt, må man vel se det slik at forfallsdatoen er «fastsatt i forveien», jf. forsinkelsesrenteloven § 2 første ledd annet punktum, ved at loven angir tidspunktet tilbakebetalingskravet skal betales på.

125 Dersom kunden har opptrådt svikaktig, vil det ikke foreligge noen plikt til tilbakeføring med mindre banken oversitter fristen på fire uker for å reise sak, jf. § 4-32 annet ledd.

126 Hagstrøm (2011) s. 728.

127 Til illustrasjon er tysk rettspraksis ifølge Oleownik slik at banken tillates å innfri tilbakeføringsplikten ved motregning, se Oleownik (2022) s. 271 (avgjørelser listet i note 75).

128 *Høringsnotat ny finansavtalelov* s. 185.

129 Krüger (1982) s. 606.

130 Det kan kanskje argumenteres for at en slik motregning uansett rammes av motregningsforbudet i finansavtaleloven § 4-13. Imidlertid vil nok bankens krav måtte legges til grunn å «springe ut av kontoavtalen» slik at forbudet ikke får direkte anvendelse. I tillegg motregnes det, kan det i alle fall hevdes, ikke i innskuddsfordringen, men i et selvstendig tilbakeføringskrav med hjemmel i § 4-32 første ledd.

131 Jf. Sæbø (2003) s. 48 flg.

132 Jf. Sæbø (2003) s. 80.

133 Jf. Sæbø (2003) s. 83 med videre henvisninger.

134 Analogt med hva Hagstrøm (2011) s. 740 uttaler om regressfordringer. Hvis man ikke anser kravet for å være forfalt, vil det for øvrig også kunne være i strid med finansavtaleloven § 4-13 å bruke det til motregning, se note 131.

135 Dette følger en eldre lære som blant annet er begrunnet av Augdahl (1963), som på s. 76-77 påpekte at der A «urettmessig og på utilbørlig måte enten setter sig i besiddelse av midler tilhørende B eller tilvender sig andre fordeler på Bs bekostning», bør ikke A kunne «kompensere med sin fordring på B; ellers vilde han jo som følge av sin utilbørlige optreden opnå en dekningsadgang som han ikke før hadde.» At man ikke kan begå rettsbrudd for å skaffe seg motregningsrett, virker å være anerkjent i dansk rett (Iversen (2018) s. 286) og finsk rett (Norros (2018) s. 516). Lindskog (2014 s. 285), som omtaler svensk rett, er noe mer restriktiv, men virker å anerkjenne at motregning ikke kan godtas når motregningskreditoren har foretatt en utilbørlig handling med den hensikt å foreta motregning («kvitningssyfte»). Reservasjon mot motregning grunnet på forsettlige rettsbrudd er lovfestet i tysk rett, se Bürgerliches Gesetzbuch (BGB) § 393.

136 Hagstrøm (2011) s. 753, Sæbø (2003) s. 302-306, Bergsåker (2015) s. 255.

137 Se Rt-2008-385. Se også LE-2021-19671, TSUMO-2017-145582, TOSLO-2011-65228.

138 En mulig innvending mot å anvende rettsmisbruksreservasjonen er at også bankens krav vil kunne bygge på grovt uaktsomt eller forsettlig pliktbrudd fra kunden (jf. resonnementet i Sæbø (2003) s. 305). Dette synspunktet har antakelig mye for seg generelt, men neppe her, hvor kundens forsett knytter seg til overtredelse av detaljerte utstedelsesvilkår kunden vedtar som standardvilkår, mens bankens ansvar bygger på overtredelse av en svært klar lovbestemmelse. Kundens forsett vil derfor (foruten de svikaktige tilfellene, hvor det uansett ikke gjelder noen umiddelbar plikt til tilbakeføring) ikke gå ut på et forsøk på å berike seg på bankens bekostning. Bankens rettsbrudd vil normalt være begått i den hensikt å sikre at den – i strid med lovens klare intensjon – får dekning hos kunden.

139 Arntzen (1991) s. 71. Min kursiv.

140 Det virker å være en viss uklarhet om rekkevidden av denne reservasjonen, se Løvold (2021) s. 270, Sæbø (2003) s. 256, Hagstrøm (2011) s. 752-753, Arntzen (1991) s. 45.

141 Sæbø (2003) s. 290 mv. Et særlig poeng i denne sammenheng er departementets synspunkt om at kundens eventuelle ansvar skal fastslås av et uavhengig tvisteløsningsorgan – et moment som taler for at kravets omtvistede karakter skal bli et hinder for motregning. Et annet spørsmål i seg selv er om bankenes svar på kundens varsel i det hele tatt oppfyller kravene man stiller til en motregningserklæring, jf. Hagstrøm (2011) s. 730-731.

142 Sæbø (2003) s. 281.

143 Forsinkelsesrenter foreldes suksessivt, slik at det beregnes renter for de siste tre år, jf. Røed (2010) s. 193 og Kjørven mfl. (2011) s. 119.

144 Forbrukertilsynet, «Orientering til bankene» (2022).

145 Når selve tilbakeføringskravet eventuelt foreldes er et spørsmål i seg selv. Det kan argumenteres med at det er snakk om en alminnelig pengefordring som foreldes etter tre år fra tilbakeføringsplikten oppsto, men det kan kanskje innvendes at særregelen for bankinnskudd i foreldelsesloven § 4, hvor fristen er 20 år, bør komme til anvendelse.

146 Ot.prp.nr.41 (1998–1999)s. 44 jf. NOU 1994:19s. 146.

147 Kjørven (2020), Kjørven mfl. (2021), Habibija (2021).

148 Forbrukertilsynet, «Orientering til bankene» (2022) s. 11.

149 European Banking Authority (EBA) (2022) s. 26 og 27.

150 Se punkt 1 med henvisninger.

151 Betydningen av systemrisikobetraktninger i privatretten er mye diskutert på europeisk nivå, se blant annet Cherednychenko (2021).

Empiriske funn om misbruk av eID

Ellen Bennin Brataas , Amelia Ella Svensson og Mira Stokke

1 Introduksjon

Norge er et av verdens mest gjennomdigitaliserte samfunn. Både privat og offentlig sektor har i løpet av kort tid introdusert mange digitaliseringsprosjekter og reformer som har gjort den norske befolkningen til mer digitale borgere. Bruk av elektronisk identifisering (eID) har blitt en grunnleggende del av befolkningens hverdag.[1] Finanssektoren i Norge har vært en pådriver for digitaliseringen gjennom utvikling og innføring av BankID, som med over fire millioner brukere er den mest utbredte eID-en i Norge.[2] BankID brukes til autentisering og signering av både offentlige og private aktører.

Implementering av eID har gitt mer effektive muligheter til å tilby og motta private og offentlige tjenester digitalt. Innføring av elektroniske identiteter medfører imidlertid også en risiko for misbruk for så vel individer som organisasjoner og bedrifter og endog stater. Trusselbildet må tas på alvor for å beskytte befolkningens digitale sikkerhet. Det krever at beslutningstakere i finanssektoren, rettssystemet og samfunnssikkerhetsfaglige instanser utvikler kunnskap om gjeldende risikoer og sårbarheter ved bruk av eID.

I norsk kontekst er det begrenset empirisk forskning på misbruk av elektroniske identifikasjonsløsninger. Dette var bakgrunnen for rapporten *Misbruk av eID*, skrevet av artikkelforfatterne.[3] Rapporten *Misbruk av eID* er den første i en serie av vitenskapelige publikasjoner i forskningsprosjektet *Samfunnssikkerhet og digitale identiteter (SODI)*.

Rapporten baserer seg på empirisk datainnsamling og formidler funn fra analyse av 300 saker som gjelder misbruk av eID, behandlet av rettshjelptiltakene Jussbuss, Juridisk rådgivning for kvinner (JURK) og Gatejuristen i perioden 2015-2021. Målet med rapporten var å bidra med en empirisk forståelse av hvordan ulike demografiske forhold påvirker sårbarheten for å bli utsatt for elektroniske identitetskrenkelser, og hvilke konsekvenser slike krenkelser kan ha for ofrene.

I denne artikkelen vil vi gjennomgå funnene fra rapporten basert på empirisk materiale fra de tre rettshjelptiltakene nevnt ovenfor. Vi vil presentere de demografiske aspektene hos svindelofferet og offerets relasjon til svindleren. Deretter presenterer vi trekk ved selve svindelen, herunder om det er snakk om lånesvindel eller betalingssvindel, hvordan svindleren fikk tilgang til sikkerhetsinformasjon, og det økonomiske omfanget av svindelen. Til sist viser vi til tendenser i de rettslige og utenomrettslige prosessene i de enkelte sakene.

2 Definisjoner

I dagligtale kalles misbruk av andres identitet ofte for «identitetstyveri». Det finnes ingen enhetlig konsensus på forskningsfeltet om hvordan identitetstyveri skal defineres. Av den grunn vil vi i denne artikkelen anvende det strafferettslige begrepet «identitetskrenkelse» i stedet for «identitetstyveri». «Identitetskrenkelse» forstås etter straffeloven § 202 som tilfeller hvor en annens identitet blir benyttet til å begå bedrageri med økonomisk

vinningsformål.[4] «Svindel» vil i denne artikkelen forstås som handlingen som påfører offeret økonomisk tap. Eksempler på identitetskrenkelse og svindel etter denne forståelsen er å overføre penger ut fra offerets bankkonto, signere låne- og kredittopptak, misbruke offentlige tjenester og sensitive personopplysninger eller på annen måte ta kontroll over en annens økonomiske liv for å oppnå økonomisk vinning.[5]

Når vi i denne artikkelen snakker om «identitetskrenkelse» og «svindel» menes tilfeller hvor det er skjedd uberettiget bruk av en eID.«eID» er forkortelse for «elektronisk identifikasjon». Elektronisk identifikasjon benyttes for identitetskontroll i elektroniske tjenester.[6] Det finnes mange eID-ordninger som kan brukes som elektroniske identifikasjonsmiddel. Per 2023 er det i Norge seks ulike eID-ordninger.[7]

3 Rapportens empiriske datagrunnlag

Vi ønsket å undersøke identitetskrenkelser fra privatpersoners perspektiv. For å få innsikt i hele den rettslige prosessen undersøkte vi sakene til personer som har oppsøkt rettshjelp. Vi tok utgangspunkt i saker fra de frivillige rettshjelptiltakene Jussbuss, JURK og Gatejuristen fra perioden 2015-2021.

Selve datainnsamlingen ble gjennomført i 2021 og 2022. Vi brukte datainnsamlingsverktøyet *Nettskjema* for å registrere data om den enkelte saken anonymt og sikkert. Vi registrerte opplysninger fra alle arkiverte saker der klienten påstod å ha blitt utsatt for en identitetskrenkelse. Datamaterialet består av totalt 292 observasjoner, hvorav 136 observasjoner er fra Jussbuss, 113 fra JURK og 43 fra Gatejuristen.[8] Vi brukte kvantitativ metode til å utarbeide beskrivende statistikk om ofrene, svindelen og det rettslige utfallet.

Datautvalget og metoden for datainnsamling byr både på styrker og svakheter. Siden vi bare har sett på saker der svindelofferet har valgt å oppsøke rettshjelp, kan det antas at sakene er av høyere alvorlighetsgrad enn identitetskrenkelser generelt. Sakene er av en slik karakter at partene ikke har klart å løse dem på egen hånd, og må i noen tilfeller behandles i rettssystemet. I tillegg gir Jussbuss, JURK og Gatejuristen gratis rettshjelp til spesifikke demografiske grupper. Gatejuristen gir gratis rettshjelp til personer som har eller har hatt rusproblemer, og JURK gir gratis rettshjelp til kvinner. Når datamaterialet er basert på en gruppe som nødvendigvis ikke er representativ for alle svindelofre i Norge, bør man være forsiktig med å generalisere funnene.

4 Hvem er svindler, og hvem er svindeloffer?

Enkelte grupper har større risiko for å bli utsatt for identitetskrenkelser enn andre. Noen ganger skyldes dette ulike sosiale og demografiske egenskaper. En slik demografisk egenskap er *alder*.

Personer i alle aldre kan bli rammet av en identitetskrenkelse. Funnene fra vår undersøkelse viser allikevel en korrelasjon mellom lav alder og økt utsatthet for identitetskrenkelse.[9] I vårt datagrunnlag er aldersgruppen 18-30 år som var den mest utsatte gruppen for identitetskrenkelse (22 prosent), tett fulgt av aldersgruppen 31-40 år (20 prosent). Aldersgruppen 18-30 år var dobbelt så utsatt som aldersgruppen 61-67 år.

Dersom man kontrollerer for kjønn i sammenheng med alder, viser funnene at de kvinnelige svindelofrene kan være noe eldre enn de mannlige. Menn blir i noe større grad utsatt for svindel i de yngre aldersgruppene 18-30 år (9,5 prosent) og 31-40 år (9,5 prosent), mens kvinnene oftest ble utsatt i aldersgruppene 18-30 år (12 prosent) og 41-50 år (14,5 prosent). På tross av at utsattheten avtar i takt med økende alder hos både menn og kvinner, er det samtidig en større andel av menn i aldersgruppen 61-67 som er utsatt for identitetskrenkelse (6,7 prosent) enn kvinner i samme aldersgruppe (4,6 prosent).

I norske medier er tendensen å portrettere det typiske svindelofferet som en eldre person.[10] Et eksempel i Norge som har fått mye oppmerksomhet, er sakene som blir benevnt som såkalt Olga-svindel. I «Olga-svindlene» ble eldre kvinner kontaktet av personer som hevdet å være kunderådgivere hos personens dagligbank og som følge av dette fikk kvinnene til å oppgi sensitiv sikkerhetsinformasjon til svindleren.[11] En typisk antakelse er at eldre er attraktive mål, og at svindlere har som strategi å rette seg mot eldre, mer uerfarne digitale brukere for å lure til seg sensitiv sikkerhetsinformasjon.[12]

At de yngre aldergruppene er noe mer utsatt for identitetskrenkelse i vårt utvalg, kan forklares av kriminologiske teorier. Kriminologiske studier som ser på hvordan digitale aktiviteter og adferd kan påvirke utsatthet for identitetskrenkelse, peker på en vekselvirkning mellom økt bruk av digitale løsninger og økt sårbarhet for misbruk.[13] At svindelofre oftest er yngre, kan være en indikasjon på at de yngre aldersgruppene er

mer aktive brukere av elektroniske identiteter enn eldre. Tendensen nyanserer portretteringen av eldre som særlig sårbare for å bli utsatt for identitetskrenkelser. Det er derfor grunn å tro at både de yngre og de eldre digitale brukene er sårbare for identitetskrenkelser.

En annen demografisk egenskap som kan belyse sårbarhet for identitetskrenkelser, er *kjønn*. I vår undersøkelse var den klare majoriteten av ofrene kvinner. Kvinner sto for 64 prosent av ofrene av identitetskrenkelse i utvalget. Ettersom JURK bare bistår kvinner, tas det imidlertid forbehold om at funnet kan være et utslag av utvalget i datagrunnlaget. Funnet er likevel fortsatt av interesse, fordi det viser at kjønn kan innebære variasjoner i utsatthet for identitetskrenkelse. Tidligere studier som har undersøkt hvorvidt kvinner eller menn er mer utsatt for identitetskrenkelse, har ikke kommet til noen tydelige konklusjoner.[14] Det er dermed grunn til å tro at både menn og kvinner er sårbare for identitetskrenkelse i et digitalisert samfunn, men muligens av ulike grunner.

I tillegg til ofrenes alder og kjønn har vi undersøkt *relasjonen mellom svindeloffer og svindler*. Risikoen for identitetskrenkelser er ikke bare begrunnet i tekniske sikkerhetsbrister. Et eksisterende tillitsforhold mellom svindler og svindeloffer har vist seg å være en signifikant sårbarhetsfaktor ved misbruk av eID. Som følge av forbrytelsens natur vil imidlertid svindelofrene ofte ikke vite hvem som har misbrukt deres identitet.[15]

Våre funn viser at der offeret vet hvem som er svindleren, er svindleren oftest en nærstående person, som et familiemedlem, en venn eller en kollega.[16] Den klart største andelen identitetskrenkelser i vårt utvalg har skjedd i nære relasjoner (66 prosent), mens svindleren i 13 prosent av tilfellene var en annen bekjent og i 21 prosent av tilfellene en ukjent person. Våre funn taler for at nærstående er overrepresentert som svindlere blant ofre i alle aldersgrupper, men at forskjellen viskes ut i de høyere aldersgruppene. Disse funnene er i tråd med tidligere forskning.[17]

Et tydelig funn i våre undersøkelser er at svindelofferets kjønn har betydning for nærheten til svindleren. I vår studie har det klare flertallet av kvinner blitt utsatt for identitetskrenkelser av en nærstående person. Av det totale antall observasjoner i undersøkelsen utgjør kvinner som er utsatt for identitetskrenkelse av en nærstående, over halvparten av observasjonene (52,8 prosent). Innad i gruppen kvinner som er utsatt for identitetskrenkelse (65,8 prosent), er 80 prosent svindlet av en nærstående.

Menn blir i størst grad utsatt for identitetskrenkelse av en ukjent person. Innad i gruppen som blir utsatt for identitetskrenkelse av ukjente (21,3 prosent), står menn for nesten 80 prosent av observasjonene (16 prosent av totalen). Menn er i større grad utsatt for identitetskrenkelse i nære relasjoner i de lavere aldersgruppene 18-30 år (4,6 prosent) og 31-40 år (3,9 prosent), mens nærstående er de primære svindlerne for kvinner i alle aldre.

Tidligere forskning peker på at svindlere kan utnytte tillitsforhold i nære relasjoner til å gjennomføre identitetskrenkelsen. Identitetskrenkelse i nære relasjoner antas også å være en måte å utøve partnervold på.[18] Partnervold rammer som oftest kvinner.[19] Funnene fra rapporten i sammenheng med funn fra tidligere studier kan peke i retning av at tillit og økonomisk vold i nære relasjoner er to risikofaktorer som gjør kvinner sårbare for å bli utsatt for identitetskrenkelser.

Datagrunnlaget i denne undersøkelsen er ikke egnet til å si noe om hvorvidt kvinnene som er blitt utsatt for identitetskrenkelse av en nærstående, faktisk har levd med partnervold. Funnene belyser likevel et behov for å undersøke nærmere i hvilken grad nær relasjon med svindler har betydning for hvordan svindelen skjer, og hvilke metoder svindler bruker for å begå identitetskrenkelsen. Det er også behov for å undersøke hvilken innvirkning svindel fra en nærstående har på offeret, som eksempelvis på hvilke måter svindelen får betydning for familielivet og for eventuelle felles barn av svindelofferet og svindler. Det reiser seg også spørsmål om hvordan identitetskrenkelse som utslag av økonomisk vold skal bli vurdert rettslig.

5 Svindelen

5.1 Svindlerens tilgang til eID og sikkerhetsinformasjon

En svindel kan gjennomføres på mange måter. I arbeidet med å forhindre svindel og identitetskrenkelser er det viktig med kunnskap om hvordan misbruket kan skje. For å gjennomføre en digital identitetskrenkelse er svindleren avhengig av å skaffe seg tilgang til sikkerhetsinformasjonen til offerets eID.

Metodene for å få tilgang til sikkerhetsinformasjonen til eID kan variere. Én fremgangsmåte er svindel gjennom internettkanaler, som får offeret til å følge en lenke og legge inn sikkerhetsopplysninger via nettportaler.[20] En annen metode er at svindleren benytter seg av sosial manipulasjon eller utnytter relasjonen til svindelofferet for å lure til seg sikkerhetsinformasjon.[21]

Tabell 3. Hvordan svindleren har fått tilgang til sikkerhetsinformasjon, og hvilken BankID som ble benyttet ved misbruk av eID. Tall i prosent. 210 observasjoner.

BankID			**BankID-brikke**	**BankID på mobil**	**Annen**	**Vet ikke**	**Totalt**
Tilgang til sikkerhetsinformasjon							
Vedkommende gav passordet til svindleren	28,57	0,48	1,43	2,38	**32,86**		
Vedkommende oppgav passord over telefon	5,24	0	0,95	0,95	**7,14**		
Vedkommende tastet inn passord etter å ha fulgt lenke på nett/SMS/e-post	1,90	0	0	0,95	**2,86**		
Passord var skrevet ned og tilgjengelig for svindleren	2,86	0	0	0	**2,86**		
Passordet var likt andre passord	1,90	0	0	0	**1,90**		
Keylogger/hacking	0,95	0,48	0	0,48	**1,90**		
Svindler så på mens vedkommende la inn passordet	0	0,95	0	0	**0,95**		
Annen	10,00	0,48	0	1,43	**11,90**		
Ukjent / vet ikke	16,19	0,95	0	20,48	**37,63**		
Totalt			**67,62**	**3,33**	**2,38**	**26,19**	**100,00**

I vår undersøkelse fant vi at veldig mange ikke vet hvordan sikkerhetsinformasjonen er kommet på avveie. For tilnærmet 40 prosent av ofrene i datagrunnlaget var det *ukjent* hvordan svindleren kunne misbruke deres eID. En omtrent like stor andel hadde imidlertid *selv oppgitt sikkerhetsinformasjonen* til svindleren. I datagrunnlaget hadde offeret oppgitt sikkerhetsopplysninger til svindleren ansikt til ansikt i 32,9 prosent av tilfellene. I tillegg hadde 7,1 prosent oppgitt passord over telefon.

Funnet om at om lag 40 prosent hadde oppgitt sikkerhetsinformasjonen sin til svindleren, bør sees i sammenheng med funnet diskutert ovenfor om at 66 prosent av ofrene i datagrunnlaget er svindlet av en nærstående. Funnene sett i sammenheng kan indikere at svindlere utnytter relasjonen til svindelofferet for å få tilgang til offerets sikkerhetsinformasjon.

Det kan være vanskelig å vite hvorfor noen selv gir fra seg egen sikkerhetsinformasjon. Våre data gir ikke informasjon om hvorvidt svindelofferet *frivillig* har oppgitt sikkerhetsinformasjonen til svindleren. Vi kan likevel se til andre studier. Tidligere studier peker på at svindlere bruker sosiale mekanismer som spiller på ofrenes emosjoner for å gjennomføre identitetskrenkelsen.[22] Manipulasjonen kan utnytte både frykt, begeistring og etablering av et nært tillitsforhold.

En annen form for manipulasjon er utnyttelse av situasjoner hvor ofrene oppsøker hjelp. Situasjoner som kan nødvendiggjøre hjelp med å bruke eID er språkbarrierer, manglende digital kompetanse, eller mangelfull kjennskap til gjeldende digitale identitetsløsninger. Tillit i nære relasjoner og fysisk nærhet til det elektroniske autentiseringsverktøyet, kan på denne måten være to særlige risikofaktorer for å bli utsatt for identitetskrenkelser.

5.2 Svindelverktøy

Det er som tidligere nevnt seks forskjellige eID-ordninger i Norge: BankID, BankID på mobil, Buypass ID på smartkort, Buypass ID i mobil, Commfides eID og MinID.[23] Av alle formene for eID som finnes på det norske markedet, er BankID-brikken klart overrepresentert i datagrunnlaget som verktøy for å gjennomføre identitetskrenkelser. Brikken ble benyttet til å gjennomføre svindelen i hele 68 prosent av tilfellene, mens BankID på mobil ble benyttet i bare 3 prosent av tilfellene. Det er også verdt å merke seg at svindelofferet ofte ikke vet hvilken eID som er benyttet for å gjennomføre svindelen (26 prosent av tilfellene).

Funnet om at brikken er overrepresentert, trekker i retning av at det er iboende sikkerhetssvakheter ved løsningen. En svakhet ved brikken, til forskjell fra BankID på mobil, er at brikken ofte vil oppbevares tilgjengelig for andre i husstanden eller på kontoret. Overfor hustandsmedlemmer og kollegaer vil passordet være den eneste beskyttelsen mot misbruk. Den fysiske tilgjengeligheten til eID-en kan følgelig være en ytterligere risikofaktor for å bli utsatt for identitetskrenkelse, særlig overfor nærstående.

Funnene om hvordan misbruk av eID skjer, er relevant for juridiske vurderinger av svindelofferets ansvar for svindeltapet.

5.3 Svindelhandlingen

Elektroniske identiteter kan misbrukes til å utføre mange forskjellige handlinger. Overfor finansinstitusjoner kan eID misbrukes til å inngå avtaler om finansielle tjenester som bankkontoer og kredittavtaler, og til å utføre betalinger over internett, enten som overføring direkte ut av nettbanken eller gjennom kjøp av varer og tjenester over internett.[24]

Misbruk av eID kan også inngå i andre typer kriminalitet, eksempelvis arbeidslivskriminalitet. Økokrim beskriver i sin trusselvurdering for 2022 at eID misbrukes av stråmenn til å skjule sin tilknytning til foretak. På den måten unndrar de skatter og avgifter, begår hvitvasking, begår brudd på arbeidsmiljøloven eller benytter ulovlig arbeidskraft.[25] eID kan også misbrukes overfor myndighetene, eksempelvis til å utstede førerkort eller gjennomføre endring av skattekort.[26]I våre analyser har vi sett på tilfeller hvor eID misbrukes overfor en finansinstitusjon.

Den vanligste svindelhandlingen i datagrunnlaget er opptak av lån eller kreditt (61 prosent). Kjøp av varer eller tjenester og overføring ut av nettbank står for til sammen 35 prosent. Funnet skiller seg fra undersøkelser gjort i Norge av NorSIS og Skatteetaten, som baserer seg på representative utvalg av befolkningen. Deres

undersøkelse fra 2022 konkluderer med at svindel i form av at noen har kjøpt varer eller tjenester på internett i en annens navn, er den vanligste formen for identitetskrenkelser.[27] Bare litt under 3 prosent av respondentene i NorSIS og Skatteetatens undersøkelse hadde opplevd at andre hadde tatt opp lån eller kreditt i deres navn.

En viktig forskjell mellom datamaterialet vårt og undersøkelsen gjort av NorSIS og Skatteetaten er at vi har sett på saker hvor offeret har søkt rettshjelp. Våre funn kan derfor indikere at lånebedragerisvindlene er av en slik kompleksitet og alvorlighetsgrad at offeret i større grad vil oppsøke juridisk bistand. I tillegg kan funnet gi uttrykk for at kreditorer som tilbyr lån og kreditt, er mindre villige til å komme ofre for identitetskrenkelser i møte. At svindeltyper som omhandler opptak av lån og kreditt, innebærer den største økonomiske belastningen, blir også fremhevet i neste punkt.

5.4 Hvilken betydning har svindelhandlingen for svindelens økonomiske omfang?

Flere forhold kan påvirke svindelens økonomiske konsekvenser for offeret. Vi har undersøkt om, og i så fall hvordan, ulike typer *svindelhandlinger* påvirker den totale økonomiske belastningen.

I vårt datagrunnlag fant vi en særlig sammenheng mellom svindelens økonomiske omfang og visse typer svindelhandlinger.[28] Opptak av lån og kreditt er den svindelhandlingen som medfører de største og mest alvorlige økonomiske konsekvensene for svindelofferet. Der svindleren overfører penger ut av konto eller kjøper varer og tjenester, er kravenes hovedstol vanligvis maksimalt 50 000 kroner. Opp til en hovedstol på 50 000 kroner er det en relativt jevn fordeling i hvilken type svindel som har blitt utført. Der svindleren tar opp lån eller kreditt, kan den totale hovedstolen være helt opp til 5 000 000 kroner.

5.5 Hvilken betydning har relasjonen til svindleren for svindelens økonomiske omfang?

Vi fant videre at relasjonen mellom svindler og offer påvirker hvilken type svindel som blir gjennomført.[29] Det er de nærstående svindlerne som i vårt datagrunnlag påfører offeret den største økonomiske belastningen. Vi fant at der svindleren er ukjent for svindelofferet, er det ingen hovedstol som er på over 99 999 kroner. Hele 25,8 prosent av de nærstående svindlerne hadde påført offeret krav med en total hovedstol på mellom 250 000 og 799 999 kroner. Funnet bør også sees i sammenheng med at det i størst grad er kvinner som blir svindlet av nærstående. Det kan indikere at kvinner i størst grad er sårbare for å bli utsatt for de mest økonomisk belastende svindlene.

At svindel begått av nærstående innebærer større økonomiske konsekvenser, kan forklares med at vårt utvalg er basert på personer som har hatt behov for rettshjelp for å håndtere svindelens konsekvenser. At personene har oppsøkt rettshjelp, kan peke på svindelens alvorlighetsgrad. Potensielle årsaker til at nærstående svindlere kan tenkes å utføre mer alvorlige tilfeller av svindel, kan være at de kan ha tilgang til den digitale identiteten under en lengre periode, tar opp flere og større lån og har bedre muligheter for å skjule spor etter svindelen for offeret.

At svindleren er en nærstående, kan også påvirke hvor hurtig svindelofferet tar tak i problemet. Det kan være vanskelig å søke hjelp om man står i et avhengighetsforhold til svindleren. I tillegg til at identitetskrenkelser kan være et resultat av at svindleren utnytter et tillitsforhold,[30] har studier som har sett på svindleres motiver for å begå cyberkriminalitet, pekt på at svindelen kan være en måte for svindleren å svekke personens økonomiske situasjon på og med dette skape sosial isolasjon og avhengighet.[31] Det kan dermed tenkes at nærstående svindlere også kan handle ut fra en bevisst motivasjon om å ødelegge offerets finansielle situasjon.

Rapportens funn står ikke i motsetning til tidligere undersøkelser som utgår fra representative utvalg, som viser at svindel gjennom internettkanaler – som «phishing» – er mest utbredt.[32] På tross av at disse svindelmetodene er mest utbredt, er det ikke nødvendigvis de ukjente svindlerne som bruker internettkanaler til å utføre svindelen, som påfører offeret det største økonomiske tapet.

5.6 Svindelens økonomiske og øvrige konsekvenser

Å bli utsatt for en identitetskrenkelse kan for mange ha ødeleggende virkninger på så vel privatøkonomien som den private livssituasjonen og helsen. Vi har undersøkt den totale økonomiske størrelsen på svindlene sett i

sammenheng med offerets økonomiske situasjon. Vi så på svindelofferets årsinntekt det året klienten tok kontakt med rettshjelptiltaket.[33] Inntekt i sammenheng med svindelens størrelse gir en bedre indikasjon på hvor tyngende svindelen kan være for enkeltpersoner. I tillegg kan svindelofrenes årlige inntekt belyse om økonomisk status er en risikofaktor for å bli utsatt for identitetskrenkelse.

Tabell 6: Kravenes totale hovedstol per observasjon og det totale antallet krav som er rettet mot svindelofferet. Tall i prosent. 292 observasjoner.

Antall krav		**1-5**	**6-10**	**11-15**	**16-20**	**21-25**	**26-40**	**Ukjent**	**Totalt**
Total hovedstol									
0-9999	2,40	0,34	0	0	0	0	1,03	**3,77**	
10.000-49.999	7,88	0,34	0	0	0	0	1,37	**9,59**	
50.000-99.999	4,45	0,34	0	0	0	0	1,03	**5,82**	
100.000-249.999	1,71	1,03	0	0	0	0	0,34	**3,08**	
250.000-499.999	4,11	0,34	0	0	0	0	1,03	**5,48**	
500.000-799-999	2,74	1,71	0	0	0	0	3,42	**7,88**	
800.000-999.999	0	0	0	0	0	0	1,03	**1,03**	
1.000.000 - 1.999.999	0	0,68	0	0	0	0	2,05	**2,74**	
2.000.000 - 5.000.000	0	0	0	0,68	0	0	1,37	**2,05**	
Ukjent		25,68	5,48	2,40	0,68	0,34	1,71	22,26	**58,56**
Totalt		**48,97**	**10,27**	**2,40**	**1,37**	**0,34**	**1,71**	**34,93**	**100**

For å få en oversikt over svindelens omfang og konsekvenser har vi sett på hvor mange krav svindelofrene har rettet mot seg, og svindelens totale hovedstol. Den totale hovedstolen inkluderer summen av hovedstolene for samtlige krav et svindeloffer har rettet mot seg. Funnene illustrerer omfanget av den økonomiske påkjenningen og størrelsen på svindelen vedkommende er utsatt for.

Halvparten av svindelofrene har mellom 1 og 5 krav rettet mot seg. Det har ikke vært tilgjengelig informasjon om kravenes hovedstol i alle kravene. For kravene vi har hatt informasjon om, er flest svindlet for henholdsvis mellom 10 000 og 49 000 kroner (10 prosent) og mellom 500 000 og 799 999 kroner (8 prosent). Totalt er kravenes hovedstol under 100 000 kroner i 19 prosent av observasjonene. Det er verdt å merke seg at i 13,4 prosent av observasjonene er kravets hovedstol mellom 250 000 og 799 999 kroner.

Videre har vi sett på svindelofrenes årsinntekt det året klienten tok kontakt med rettshjelptiltaket. Gatejuristen registrerer ikke klientenes årlige inntekt. Observasjonene fra Gatejuristen er derfor inkludert i verdikategorien «Ikke registrert».

Over halvparten av svindelofrene hadde en årlig inntekt på under 350 000 kroner.[34] 13 prosent hadde en årlig inntekt på under 100 000 kroner. Rundt 36 prosent hadde en årlig inntekt som er under EUs lavinntektsgrense for enslige uten barn på 242 000 kroner.[35]

Funnene fra undersøkelsen antyder to mulige indikasjoner: For det første befinner majoriteten av utvalget seg i den nedre del av inntektsskalaen. Det indikerer at lav inntekt innebærer en sårbarhet for å bli utsatt for identitetskrenkelser. I tidligere forskning er både høy og lav inntekt anerkjent som en mulig risikofaktor.[36]

For det andre gir funnene uttrykk for at svindelen innebærer store økonomiske konsekvenser for det enkelte offeret. Samtidig som ofrene overveiende befinner seg på den lavere delen av inntektsskalaen, er det stor spredning i kravenes hovedstol. Sett hen til at majoriteten av ofrene har mer enn ett krav rettet mot seg, vil totalsummen av kravene som rettes mot offeret, utgjøre en betydelig økonomisk belastning. I tillegg til den økonomiske belastningen følger også indirekte økonomiske konsekvenser, som å slite med å betale løpende utgifter, og at den økonomiske belastningen innebærer en emosjonell og psykisk påkjenning.[37]

Siden datagrunnlaget er hentet fra Jussbuss, JURK og Gatejuristen, som tilbyr gratis rettshjelp, er ikke utvalgets årlige inntekt nødvendigvis representativ for den totale populasjonen av svindelofre i Norge. Funnene gir allikevel viktig innsikt i hvordan identitetskrenkelse påvirker den utsatte gruppen som søker seg til gratis rettshjelp. Det belyser konsekvensen av svindel for utsatte og sårbare grupper i samfunnet.

6 Straffeprosessen

Rapporten *Misbruk av eID,* som denne artikkelen tar utgangspunkt i, er den første i Norge til å gi en oversikt over kjennetegn ved de rettslige og utenrettslige prosessene i de enkelte svindelsakene. Funnene kan belyse nye viktige rettslige problemer på området og kan bidra til utviklingen av rettsregler og rettshjelp som gir bedre muligheter til å ivareta den enkeltes digitale beskyttelse.

En essensiell del av vår empiriske forskning er å få bedre oversikt over kjennetegn ved de rettslige prosessene som kan belyse behov for endringer i den rettslige håndteringen av identitetskrenkelser. Da misbruk av elektronisk identifikasjon er en relativt ny form for kriminalitet som innebærer en samfunnsmessig sikkerhetsrisiko, er det viktig å oppfordre til kontinuerlig granskning av hvilke rettslige problemer som kan oppstå, for å sikre borgenes digitale beskyttelse. I dette punktet undersøker vi derfor de strafferettslige prosessene som kravet har vært gjennom, og betydningen av straffeprosessen for den sivilrettslige tvisten mellom svindeloffer og kreditor.

Flere tidligere studier fra USA og Australia indikerer at så få som en tredjedel av ofrene anmelder identitetskrenkelser til politiet.[38] Det har blitt antydet at andelen er enda lavere blant ofre som har blitt svindlet gjennom internettkanaler i tilknytning til kjøp og salg på nett og «phishing».[39] Det kan være mange grunner til at et offer lar være å anmelde: at man ikke vet hvor man skal henvende seg, at man ikke tror anmeldelse nytter, at man ikke tror at saken er alvorlig nok, mangel på bevis, skam over å bli utsatt for svindel, frykt for ikke å bli trodd og et ønske om å holde saken skjult for sine omgivelser.[40] Der svindleren er en nærstående, er det grunn til å tro at det i seg selv vil utgjøre en terskel for å anmelde.

Identitetskrenkelse som kriminalitetsform særpreges av at det er et mangfold av steder et offer kan henvende seg, herunder politiet, forbrukermyndighetene, banker og andre finansinstitusjoner, i tillegg til innkrevingsselskaper, sosialtjenester og andre rettighetssentraler.[41] Denne jungelen av steder å henvende seg til kan potensielt utgjøre en kompliserende faktor for svindelofferet når vedkommende forsøker å rydde opp i svindelsaken sin. Et svindeloffer vil ofte oppleve å bli henvist fra ett sted til et annet og slik bli sendt på runddans i forvaltningen uten å få nødvendig hjelp.[42]

Det har også vist seg at anmeldelsesfrekvensen er betydelig høyere blant ofre som har tatt kontakt med et rettshjelpstilbud. Av ofrene som hadde fått bistand fra Identity Theft Resource Center (ITRC) i USA i starten av 2021, hadde over 80 prosent selv tatt kontakt med en finansinstitusjon, som sin dagligbank eller et kredittselskap, vedrørende svindelen.[43] På tross av at ofrene hos senteret hadde kontaktet en finansinstitusjon eller politiet for bistand, hadde 40 prosent av ofrene i april 2021 fremdeles økonomiske vansker som var knyttet til en svindel registrert hos rettshjelptiltaket i 2020, og for tilnærmet 40 prosent av ofrene var saken fremdeles ikke oppklart.

Europakommisjonens rapport om identitetskrenkelser og identitetsrelatert kriminalitet på nett fra 2022 peker også på svakheter ved de rettslige prosessene som omhandler identitetskrenkelser i Europa. I rapporten pekes

det på at det oppstår praktiske problemer ved etterforskning og rettsforfølgelse av nettbasert kriminalitet, for eksempel på grunn av svikt i internasjonalt samarbeid, utfordringer med å innhente nødvendige bevis i digitale miljøer eller for lite ressurser og sviktende kompetanse blant rettsutøvere.[44]

Av 262 observasjoner i vårt datagrunnlag ble 201 saker (76,72 prosent) anmeldt og 61 (23,28 prosent) ikke anmeldt.[45] Funnene samsvarer med undersøkelsen av Identity Theft Resource Center (ITRC) i USA, som gir grunn til å tro at dersom et svindeloffer får kontakt med et rettshjelptiltak, vil de fleste ofre anmelde forholdet.

Få anmeldelser resulterer imidlertid i at identitetskrenkelser blir etterforsket og oppklart. 56 prosent av sakene i vårt datamateriale ble henlagt, og bare 9 prosent av anmeldelsene ble etterforsket og oppklart. På tidspunktene for datainnsamlingen var det 30 prosent av sakenesom fremdeles var under etterforskning. Funnet indikerer en høy terskel å få identitetskrenkelser og eID-svindel til å bli etterforsket og oppklart.

På tross av at det er mange anmeldelser som resulterer i henleggelse, gir våre funn uttrykk for at etterforskning og oppklaring har en klar betydning for å få svindleren domfelt. Et klart flertall av sakene som blir etterforsket og oppklart, resulterer i en fellende dom mot svindleren. Av sakene som ble etterforsket og oppklart, ble 13 saker (77 prosent) avgjort med fellende dom mot svindleren, 2 saker (12 prosent) ble ikke avgjort med fellende dom mot svindleren, og 2 saker (12 prosent) er ikke kategorisert. Den lave andelen saker som blir etterforsket, sett opp mot at de sakene som faktisk blir etterforsket, i det store og hele også blir oppklart, kan indikere at politiet kun prioriterer å etterforske de helt klare sakene.

Tidligere undersøkelser viser til at en høy grad av henleggelser kan skyldes utfordringer ved å innhente bevis i digitale miljøer, for lite ressurser innenfor rettshåndhevelsen eller sviktende kompetanse om elektronisk kriminalitet.[46] Et spørsmål som reiser seg, er om den lave oppklaringsraten eventuelt kan medføre at færre velger å anmelde forholdet.[47]

Der straffesaken endte med fellende dom mot svindler (13 saker), har vi ingen tilfeller hvor kreditor i etterkant av avgjørelsen rettet kravet mot svindleren. I 8 av sakene fant vi at kreditor fortsatte å rette kravet mot svindelofferet, på tross av domfellelse. I resterende saker var det ikke tilstrekkelig informasjon i lagret saksmappe til å konkludere. På tross av få observasjoner viser analysen fortsatt en tydelig trend i retning at kreditorene forsøker å dekke sitt krav hos svindelofferet, uavhengig av om saken har blitt avgjort med fellende dom.

At fellende dom mot en svindler sjelden resulterer i at kreditor retter kravet mot svindleren, skaper videre spørsmål om hvorfor tendensen gjør seg gjeldende. En mulig forklaring kan være at kreditor ikke er pålagt å rette kravet utelukkende mot svindler som følge av fellende dom. I tillegg kan tendensen være et utslag av at kreditor ut fra en sannsynlighetsvurdering bedømmer at svindelofferet står i en bedre finansiell posisjon enn svindleren til å dekke kravet.

At kreditor kan holde svindelofferet ansvarlig etter fellende straffedom mot svindler, reiser viktige problemstillinger om i hvilken grad strafferettslig forfølgning har betydning for finansinstitusjonenes håndteringer av eID-svindel. Det er behov for å utforske samspillet mellom strafferettslig ansvar for svindler og sivilrettslig ansvar for svindelofferet videre.

Tabell 9: Tapsfordelingen mellom svindeloffer, kreditor og svindler, og utfall av politianmeldt forhold. Tall i prosent. 110 observasjoner.

Utfall av anmeldelse	Etterforsket og oppklart	Henlagt	Under etterforskning	Totalt
Tapsfordeling				
Svindeloffer	0	27,27	6,36	**33,64**
Kreditor	4,55	27,27	15,45	**47,27**
Svindeloffer og kreditor	0,91	6,36	2,73	**10,00**
Svindler	4,55	1,82	0,91	**7,27**

Svindeloffer og svindler	0,91	0	0,91	**1,82**
Totalt	**10,91**	**62,73**	**26,36**	**100**

Tabell 9 analyserer hvordan tapet ble fordelt på henholdsvis svindeloffer, kreditor og svindler, sett opp mot utfallet av politianmeldelsen. Det er verdt å minne om at undersøkelsen gjelder saker hvor offeret har fått bistand fra et rettshjelptiltak. Tapsfordelingen illustrerer her fordelingen på tidspunktet da svindelsaken ble avsluttet hos et av de tre rettshjelptiltakene.

Av i alt 110 tilfeller ble tapet dekket av kreditor i 47 prosent av tilfellene og av svindelofferet i 34 prosent av tilfellene. I 10 prosent av tilfellene ble tapet fordelt mellom svindelofferet og kreditor. Svindleren dekket tapet i 7 prosent av tilfellene. I 2 prosent av tilfellene ble tapet fordelt på svindler og svindeloffer.

Tabellen kan illustrere betydningen av straffesakens utfall for hvordan tapet blir fordelt på de ulike aktørene. Det mest fremtredende funnet er at i tilfellene hvor politianmeldelsen endte med at saken ble etterforsket og oppklart, er det ingen observasjoner hvor svindelofferet står med tapet alene. Det er en betydelig større tendens til at svindelofferet blir pålagt ansvaret for svindelbeløpet alene dersom saken blir henlagt.

Av den totale andelen tilfeller hvor svindleren dekket tapet (7,3 prosent), skjer dette i majoriteten av tilfellene som følge av at saken ble etterforsket og oppklart (totalt 4,55 prosent av tilfellene). I tilfellene hvor saken fremdeles er under etterforskning, dekker også kreditor tapet i stor utstrekning (15,5 prosent).

Analysen kan indikere betydningen av etterforskning for at enten den som faktisk utførte svindelen blir pålagt ansvaret for svindelbeløpet, eller at kreditor påtar seg ansvaret for tapet. Analysen er ikke egnet til å gi svar på hvorfor kreditor i større utstrekning påtar seg å dekke tapet i sakene som fremdeles er under etterforskning, eller som er etterforsket og oppklart.

Etterforskning av svindelsakene vil imidlertid bidra til å oppklare hendelsesforløpet. Det kan tenkes at kreditor er mer villig til å påta seg tapet i sakene som står seg bevismessig sterkere. En annen mulig forklaring er at sakene politiet velger å etterforske, er av en karakter hvor svindelofferet står sterkere.

Rapporten belyser flere interessante funn koblet til håndtering av identitetskrenkelse innenfor straffeprosessen. To funn som er interessante å se i sammenheng, er at et klart flertall av anmeldelsene resulterer i henleggelse, og at svindelofferet har betydelig høyere risiko for å måtte dekke det økonomiske tapet alene hvis politianmeldelsen blir henlagt. Funnene er nyttige for å forstå at strafferettslige prosesser har betydning for utfallet av straffesaker som gjelder identitetskrenkelse.

7 Rettsprosessen

En sentral del av SODI-prosjektet er å drive forskning om rettsprosessen koblet til identitetskrenkelser. Denne forskningen kan gi innsikt i hvordan det norske rettssystemet håndterer identitetskrenkelse i dag. I Europakommisjonens rapport fra 2022 ble det poengtert at det er krevende å innføre lovgivning rettet mot elektroniske identitetskrenkelser, fordi slik kriminalitet blir stadig mer kompleks.[48] I EUs medlemsstater eksisterer det verken en ensartet forståelse av identitetskrenkelse som lovbrudd eller et omfattende lovgivningsinstrument med sikte på identitetskrenkelse.[49]

Videre følger noen interessante funn koblet til rettsprosessen som understreker behovet for mer kunnskap på området. Analysen presenterer interessante aspekter ved kravene som blir tvangsinndrevet, og kravene som er rettslig avgjort på tidspunktet hvor saken avsluttes.

Som en del av å analysere rettsprosessen har vi sett på tilfeller der det er gjennomført tvangsinndrivelse, og hvordan tvangsinndrivelsen er gjennomført. Det er gjort gjennom å dele inn de tilfeller hvor det er begjært tvangsinndrivelse, i tre kategorier: begjæring om tvangsinndrivelse gjennom utleggstrekk, begjæring av tvangsinndrivelse ved tvangssalg og kombinasjonen av begjæring om utleggstrekk og tvangssalg.[50]

Utleggstrekk innebærer at namsmyndighetene gir kreditorene dekning i inntekt som lønn og trygd for å innfri det skyldige beløpet.[51] Tvangssalg innebærer at namsmyndighetene selger unna formuesgoder som bil, båt og fast eiendom til dekning for det skyldige beløpet, jf. tvangsfullbyrdelsesloven kapittel 8-12.[52] Kombinasjonen

av utleggstrekk og tvangssalg kan være et resultat av at en sak kan inneholde flere krav som har resultert i forskjellige typer tvangsinndrivelser.

Av sakene som tvangsinndrives, har kreditor i over halvparten av sakene begjært tvangssalg av svindelofferets eiendeler (56 prosent). I en tredjedel av sakene har kreditor begjært utleggstrekk (33 prosent). I de øvrige sakene har kreditor begjært både utleggstrekk og tvangssalg (11 prosent).

Vi har også delt inn saker som har gått til tvangsinndrivelse henholdsvis *uten å ha blitt rettslig avgjort* og *etter å ha blitt rettslig avgjort*. Av 102 saker der kravene har gått til tvangsinndrivelse, er det et klart flertall som har fått tvangsgrunnlag uten rettsavgjørelse (59 prosent). 31 prosent har fått tvangsgrunnlag ut fra en rettsavgjørelse.

Krav som har blitt rettslig avgjort, kan baseres på ulike typer rettsavgjørelser. Tabellen nedenfor viser kravenes endelige tapsfordelinger sett hen til hvilken type rettsavgjørelse kravet ble avgjort med. Siden en klient (observasjon) kan ha flere krav rettet mot seg, betyr det samtidig at en observasjon kan inneholde flere forskjellige rettsavgjørelser. Dermed inneholder tabellen kombinerte verdikategorier som representerer de observasjonene hvor kravet er avgjort for eksempel både ved fraværsdom i forliksrådet og dom i tingretten.

Tabell 11: Kravets rettsavgjørelse (og kravets tapsfordeling. Tall i prosent. 54 observasjoner.

Tapsfordeling		**Svindeloffer**	**Kreditor**	**Svindeloffer og kreditor**	**Svindler**	**Svindeloffer og svindler**	**Totalt**
Rettsavgjørelse							
Fraværsdom i forliksrådet		33,93	3,57	3,57	1,79	0	**42,86**
Dom i forliksrådet		3,57	19,64	0	7,14	1,79	**32,14**
Dom i tingretten		1,79	3,57	0	7,14	0	**12,50**
Fraværsdom og dom i forliksrådet	1,79	3,57	3,57	0		0	**8,93**
Dom i forliksrådet og tingretten	0	0	1,79	0		0	**1,79**
Fraværsdom og dom i lagmannsretten	0	1,79	0	0		0	**1,79**
Totalt			**41,07**	**32,14**	**8,93**	**16,07**	**1,79**

Tabell 11 viser at 43 prosent av rettsavgjørelsene ble avsagt med fraværsdom i forliksrådet. Av de sakene som ble avgjort ved fraværsdom i forliksrådet, ble svindelofrene pålagt å dekke tapet i 79 prosent av observasjonene. Motsatt ble kreditor eller svindler i saker der det ble avsagt dom etter rettsmøte i forliksrådet (32 prosent) eller i tingretten (13 prosent) pålagt å dekke hele eller deler av tapet i 84 prosent av observasjonene. Ved domsavsigelse i forliksrådet og domstolen var det primært kreditoren eller svindler som ble pålagt tapet. Av de 32,1 prosent av sakene som ble avgjort med dom i forliksrådet, ble tapet plassert hos kreditor eller svindler i 26,8 prosent av tilfellene. Av de 12,5 prosent av sakene som ble avgjort med dom i tingretten, ble tapet plassert hos kreditor eller svindler i 10,7 prosent av tilfellene.

Tapsfordelingen kan være avhengig av i hvor stor utstrekning svindelofferet har vært deltakende i rettsprosessen. Funnene gir uttrykk for at svindelofferet i større grad må bære den økonomiske byrden svindelen innebærer, dersom kravet er avgjort med fraværsdom i forliksrådet. De sakene hvor svindelofferet har vært deltakende i rettsprosessen og har fått anledning til å tale sin sak, er det større sannsynlighet for at kreditoren eller svindleren blir pålagt ansvaret for tapet. Dermed kan tapsfordelingen være avhengig av i hvor stor utstrekning svindelofferet har vært involvert i rettsprosessen. Funnene taler for at tilgang til rettsapparatet er nødvendig for å sikre beskyttelsen av svindelofrene.

Undersøkelsen er ikke egnet til å avdekke årsaken til at ofrene ikke er deltakende i rettsprosessene. Funnene indikerer likevel at det er behov for en praksisendring i rettsinndrivelsesprosessen som sikrer at svindelofre blir inkludert i rettsprosessen. Betydningen av, og reglene om, fraværsdommer i forliksrådet bør undersøkes nærmere, blant annet med tanke på om rettssikkerheten er tilstrekkelig ivaretatt. Analysen kan indikere at inndrivelsesprosessen ikke har nødvendige sikkerhetsmekanismer til å fange opp om debitor er offer for en identitetskrenkelse. I tillegg kan analysen tale for betydningen av tilgang til rettshjelp for kravets tapsfordeling.

8 Avslutning

I denne artikkelen har vi presentert funnene fra en datainnsamling fra 300 saker om elektroniske identitetskrenkelser i perioden 2015-2021 hvor offeret har fått rettshjelp fra Jussbuss, JURK eller Gatejuristen. Artikkelen baserer seg på rapporten *Misbruk av eID*, som er publisert av SODI-prosjektet. Målet er å bidra med empirisk kunnskap om elektroniske identitetskrenkelser.

I artikkelen har vi gjennomgått kjennetegn ved hvem henholdsvis svindelofferet og svindleren er, kjennetegn ved selve svindelen og svindelens økonomiske belastning. Videre har vi sett på den sivilrettslige inndrivelsesprosessen og straffeforfølgningen av svindler og på hvilke måter sivil- og straffeprosessene får betydning for den endelige tapsfordelingen av svindeltapet. Funnene fra rapporten kan brukes til å belyse nye problemstillinger ved implementeringen av eID. Artiklene i denne antologien om bruk og misbruk av elektronisk identifikasjon undersøker nærmere juridiske komplikasjoner ved misbruk av eID.

Det er noen funn vi særlig ønsker å fremheve. Et av rapportens viktigste funn er at det først og fremst er kvinner som blir svindlet av sine nærstående, og det er også kvinnene som blir rammet hardest. Menn blir i størst grad utsatt for identitetskrenkelse av ukjente. I tillegg gir fire av ti ofre fra seg sine sikkerhetsopplysninger til svindleren. Mulige årsaker til at svindelofferet gir fra seg sikkerhetsinformasjonen, kan være felles økonomi med svindleren, at offeret opplever trusler og vold fra svindleren, eller at man rett og slett stoler på sine nærstående. Tidligere forskning peker også på at svindlere utnytter allerede eksisterende tillitsforhold i nære relasjoner til å gjennomføre svindelen.[53]

Narrativet i mediene er gjerne at svindelofre blir svindlet fordi de er dumme eller er slepphendte med sine sikkerhetsopplysninger. Denne typen holdninger kan bidra til å legge skylden på offeret (*victim blaming*) og fjerner oppmerksomheten fra det underliggende problemet. Svindel som følge av en identitetskrenkelse er grov kriminalitet. Identitetskrenkelse er først og fremst svært økonomisk belastende for svindelofferet, men er også en påkjenning for resten av samfunnet: for bankene som utnyttes av svindlerne, for rettsapparatet og for velferdsstaten.

Slik situasjonen er i dag, opplever mange svindelofre å bli motarbeidet i møte med rettssystemet. Det økonomiske tapet som følge av svindelen pålegges i mange tilfeller den parten som er utsatt for den kriminelle handlingen. Ingen av sakene som ble avgjort med fellende dom mot svindler, førte til at kreditor rettet kravet mot svindleren direkte som en følge av dommen. Ut fra våre funn mener vi narrativet om identitetskrenkelse bør endres: I stedet for å legge vekt på svindelofferets ansvar for å beskytte seg selv mot svindel, bør det legges vekt på rettssystemets og bankenes ansvar for å beskytte mennesker som har blitt utsatt for svindel.

Litteratur

Anderson, K.B. (2006). «Who are the victims of identity theft? The effect of demographics», *Journal of Public Policy & Marketing 25*, nr. 2: 160-171.

Anderson, K.B. (2007). «Consumer Fraud in the United States: The Second FTC Survey», *Staff Report of the Bureaus of Economics and Consumer Protection Federal Trade Commission.*

Armiwulan, H. (2021) «Gender-based cyber violence: A challenge to gender equality in Indonesia», *International Journal of Cybercriminality,* 15/2: 102-111. doi: 10.5281/zenodo.4766547

BankID, *Om oss*. [Hentet 21. mars 2023] https://www.bankid.no/privat/om-oss/.

Brataas, E.B., Stokke, M.S. og Svensson A. (2022). *Rapport om misbruk av eID*, Universitetet i Oslo. Tilgjengelig fra: Rapport om misbruk av eID (uio.no)

Bergmann, M.C., Dreißigacker, A., Von Skarczinski, B. og Wollinger, G.R. (2018). «Cyber-dependent crime victimization: the same risk for everyone?», *Cyberpsychology, Behavior, and Social Networking*, Vol. 21 nr. 2: 84-90, doi: 10.1089/cyber.2016.0727.

Button, M., Lewis, C. og Tapley, J. (2009). *Fraud typologies and the victims of fraud. Literature review.* London: National Fraud Authority.

Button, M., Lewis, C. og Tapley, J. (2014). «Not a victimless crime: The impact of fraud on individual victims and their families». *Security Journal 27*, nr. 1: 36-54.

Clevenger, S. og Gilliam, M. (2020). «Intimate partner violence and the internet: perspectives», i Holt, T., Bossler, A. (red.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance,* Palgrave Macmillan, Cham, 1333-1351. Doi: 10.1007/978-3-319-78440-3_58

Cross, C., M. Dragiewicz og K. Richards. (2018). «Understanding romance fraud: Insights from domestic violence Research», *The British Journal of Criminology*, 58(6): 1303-1322. Doi: 10.1093/bjc/azy005

Cross, C. (2015). «No laughing matter: Blaming the victim of online fraud», *International Review of Victimology*, 21(2): 187-204. https://doi.org/10.1177/0269758015571471

Cross, C., Richards, K., og Smith, R. (2016). *The reporting experiences and support needs of victims of online fraud*. Canberra: Australian Institute of Criminology.

Europakommisjonen. (2020). *Survey on «Scams and Fraud Experienced by Consumers» – Final Report.* Brussel: European Commission.

Europakommisjonen. (2022). *Study on online identity theft and identity-related crime: final report.* Publications Office of the European Union.

Foley, L. og Foley, J. (2003). *Identity theft: The aftermath 2003.* Identity Theft Resource Center.

Forordning 910/2014 – Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF [eIDAS-forordningen]

Gordon, G.R., Donald, D., Rebovich, J. og Kyung-Seok Choo. (2007). *Identity fraud trends and patterns*. Utica College Center for Identity Management and Information Protection.

Harrell, E. (2019). *Victims of identity theft, 2016: Bulletin*. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Identity Theft Resource Center (ITRC). (2022). *2021 consumer aftermath reports: How identity crimes impact victims, their families, friends and workplaces.*

Kommunal- og distriktsdepartementet. (2022). *Utkast til ny strategi for eID i offentlig sektor*.

Lov 26. juni 1992 nr. 86 om tvangsfullbyrdelse (tvangsfullbyrdelsesloven).

Nasjonal kommunikasjonsmyndighet. «Elektronisk identifikasjon (eID)» (4. april 2023). https://nkom.no/internett/elektronisk-id-og-tillitstjenester/elektronisk-identifikasjon-eid

Newman, G.R. og McNally, M.M. (2005). *Identity theft literature review.* Washington: National Institute of Justice (NIJ).

(NorSIS) Norsk senter for informasjonssikring og Skatteetaten (2022). *ID-tyverirapporten2022*. *ID-tyveri rammer fortsatt mange – behov for flere tiltak og økt kunnskap.* Gjøvik: Skatteetaten.

Pratt, T.C., Holtfreter, K. og Reisig, M.D. (2010) «Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory», *The Journal of Research in Crime and Delinquency*, 47(3): 267-296. Doi: 10.1177/0022427810365903

Rebovich, D.J., Layne, J., Jiandani, J. og Hage, S. (2000). *The national public survey on white collar crime.* National White Collar Crime Center Morgantown, WV.

Rege, A. (2009). «What's love got to do with it? Exploring online dating scams and identity fraud». *International Journal of Cyber Criminology,* 3(2): 494-512. Retrieved from https://www.proquest.com/scholarly-journals/whats-love-got-do-with-exploring-online-dating/docview/763181753/se-2

Reyns, B.W., og Henson, B. (2016) «The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory», *International Journal of Offender Therapy and Comparative Criminology*, 60(10): 1119-1139. Doi: 10.1177/0306624X15572861

Schoepfer, A. og Piquero, N.L. (2009).«Studying the correlates of fraud victimization and reporting». *Journal of Criminal Justice 37,* nr. 2: 209-215

Smith, R.G. (2008). «Coordinating individual and organisational responses to Fraud». *Crime, Law and Social Change 49,* nr. 5: 379-396.

Statistisk sentralbyrå (2022). «Inntekts- og formuesstatistikk for husholdninger. Lavinntektsgrenser i kroner (EU- og OECD-skala), etter husholdningstype 2009-2020». *Statistikkbanken* (ssb.no). Hentet 7. februar 2023.

Stuart, A., Schuck, A.M. og Lersch, K.M. (2005). «Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics». *Journal of Criminal Justice 33*, nr. 1: 19-29.

Titus, R.M., Heinzelmann, F. og Boyle, J.M. (1995). «Victimization of persons by fraud». *Crime & Delinquency 41, nr. 1* (1995): 54-72.

Werenskjold, K.K. (2020). *BankID-svindel i nære relasjonar: Spørsmålet om avtalebinding i lys av det menneskerettslege vernet mot økonomisk vald*. Masteroppgave, Universitetet i Oslo.

Williams, Matthew L. «Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level.» British Journal of Criminology 56, no. 1 (2016): 21-48.

Økokrim (2022). Trusselvurdering 2022. https://www.okokrim.no/getfile.php/5017571.2528.q7zikqspuaaqqs/%C3%98kokrim+trusselvurdering+2022.pdf

Noter

1 Kommunal- og distriktsdepartementet (2022) punkt 2.1.

2 BankID (2023).

3 Brataas, Stokke og Svensson (2022).

4 En form for legaldefinisjon følger av straffebudet om identitetskrenkelse i straffeloven § 202. Identitetskrenkelse er straffbart dersom man «uberettiget setter seg i besittelse av en annens identitetsbevis, eller opptrer med en annens identitet eller med en identitet som er lett å forveksle med en annens identitet, med forsett om å a. oppnå en uberettiget vinning for seg eller en annen, eller b. påføre en annen tap eller ulempe». Etter straffeloven § 202 vil det følgelig være straffbart både å sette seg i besittelse av en annens identitet og å opptre med en annens identitet.

5 Stuart mfl. (2005) s. 19-29.

6 Forordning (EU) nr. 910/2014artikkel 3 nr. 1; Nasjonal kommunikasjonsmyndighet (2023).

7 BankID, BankID på mobil, Buypass ID på smartkort, Buypass ID i mobil, Commfides eID og MinID.

8 For nærmere beskrivelse av datamaterialet se Brataas, Stokke og Svensson (2022), s. 15 flg.

9 Graf tilgjengelig i fullstendig rapport, se Brataas, Stokke og Svensson (2022) s. 22.

10 Se for eksempel nettsaken «Eldre blir forsøkt svindlet på SMS»: https://www.gjensidige.no/godtforberedt/content/eldre-blir-forsokt-svindlet-pa-sms (lest 1. juni 2023)

11 HR-2022-1752-A.

12 Cross (2015) s. 188-189.

13 Bergmann mfl. (2018); Pratt mfl. (2010); Reyns og Henson (2016).

14 For eksempel Stuart mfl. (2005); Anderson (2006).

15 Newman og McNally (2005) s. 26-29: En gjennomgang av rapporterte identitetskrenkelser i perioden 2000-2006 til den amerikanske Secret Service, avdekket at 56 prosent av ofrene ikke var kjent med svindlerens identitet; Gordon mfl. (2007) s. 56.

16 Graf tilgjengelig i fullstendig rapport, se Brataas, Stokke og Svensson (2022) s. 25.

17 Se eksempelvis Anderson, K.B. (2007) s. 12, som gjennomgår svindelsaker behandlet av Federal Trade Commission i USA.

18 Foley og Foley (2003); Armiwulan (2021); Clevenger og Gilliam (2020); Cross, Dragiewicz og Richards (2018); Rege (2009).

19 Werenskjold (2020).

20 Denne metoden kalles ofte for «phishing».

21 Newman og McNally (2005) s. 44-45.

22 Newmann og McNally (2005) s. 44-45; Gordon et.al. (2007) s. 49.

23 Nasjonal kommunikasjonsmyndighet (2023).

24 Se legaldefinisjon av «finansiell tjeneste» i finansavtaleloven § 1-3 andre ledd.

25 Økokrim (2022) s. 61.

26 ITRC (2022).

27 Norsk senter for informasjonssikring (NorSIS) og Skatteetaten (2022) s. 4.

28 Graf tilgjengelig i fullstendig rapport, se Brataas, Stokke og Svensson (2022) s. 33.

29 Graf tilgjengelig i fullstendig rapport, se Brataas, Stokke og Svensson (2022) s. 35.

30 Foley (2003) s. 21-22.

31 Clevenger og Gilliam (2020) s. 1336 og 1344.

32 Europakommisjonen (2020) s. 30; Europakommisjonen (2022) s. 5.

33 For nærmere beskrivelse av hvordan vi har gjennomført datainnsamlingen, se Brataas, Svensson og Stokke (2022) s. 15 fl.

34 Graf tilgjengelig i fullstendig rapport, se Brataas, Stokke og Svensson (2022) s. 39.

35 Se Statistisk sentralbyrås årlige gjennomgang av Norges befolkning under EUs lavinntektsgrense: https://www.ssb.no/statbank/table/09593/tableViewLayout1/?loadedQueryId=10021621&timeType=top&timeValue=1.

36 Noen undersøkelser fra USA finner en sammenheng mellom høy inntekt og risiko for identitetskrenkelse, se eksempelvis Anderson (2006) s. 160-171 og Harrell (2019). Studier fra Europa viser at det å leve med lav sosial status i et høyinntektsland utgjør en risikofaktor for identitetskrenkelse, se Williams (2016) s. 21-48.

37 Europakommisjonen (2020) s. 15 og 18-19; Europakommisjonen (2022) s. 47; Identity Theft Resource Center (2022); Button mfl. (2009); Cross mfl. (2016) s. 806-828.

38 Rebovich mfl. (2000) (USA); Schoepfer og Piquero (2009) s. 209-215 (USA); Smith (2008) s. 379-396 (Australia); Titus mfl. (1995) s. 54-72 (USA).

39 Smith (2008) s. 379-396 (Australia).

40 Button mfl. (2009) s. 806-828.

41 Button mfl. (2014) s. 36-54.

42 Button mfl. (2009) s. 806-828.

43 Identity Theft Resource Center (2022).

44 Europakommisjonen (2022) s. 94.

45 Graf tilgjengelig i fullstendig rapport, se Brataas, Stokke og Svensson (2022) s. 42.

46 Europakommisjonen (2022) s. 94

47 Smith (2008) s. 387; Button mfl. (2009) s. 806-828.

48 Europakommisjonen (2022) s. 10.

49 Europakommisjonen (2022) s. 7 og 48.

50 Graf tilgjengelig i fullstendig rapport, se Brataas, Stokke og Svensson (2022) s. 48.

51 Tvangsfullbyrdelsesloven kapittel 7.

52 Tvangsfullbyrdelsesloven kapittel 8-12.

53 Foley (2003) s. 21-22.

Elektroniske signaturer og tinglysing

Erik Røsæg

Fagfellevurdert artikkel

1 Innledning

Med for eksempel BankID kan en signere et brev eller en avtale på liknende måte som man signerer med kulepenn. Dette er en form for elektronisk signatur. Rent praktisk får en opp en tekst i for eksempel BankID-vinduet på datamaskinen i stedet for eksempelvis en forespørsel om en vil betale et beløp i nettbanken, og en bekrefter det på samme måte som en betaling i nettbanken.

Etter EU-basert norsk rett skal en elektronisk signatur under visse forutsetninger få virkning som en håndskrevet signatur.[1] Men en elektronisk signatur er likevel ikke *mer* verd enn en håndskrevet.[2] Den påstått forpliktede har stadig innsigelsen om at det ikke var hen som underskrev, i behold, altså innsigelser om falsk og forfalskning. Selv om en elektronisk signatur er maskinlesbar, er det altså ingen mekanisk sammenheng mellom en elektronisk signatur og en forpliktelse for den som den elektroniske signaturen er utstedt til.

Mange av de rettslige problemene som gjelder håndskrevne signaturer, gjelder altså også for elektroniske signaturer. Det kan også være rettslige risikoaspekter med elektroniske signaturer i tillegg til risikoaspektene ved håndskrevne signaturer. Her skal risikobildet for elektroniske signaturer diskuteres nærmere i forbindelse med tinglysing av fast eiendom.

Fra 2015 kan tinglysingsdokumenter om for eksempel salg av fast eiendom signeres elektronisk. De fleste tinglysinger i grunnboken er nå elektroniske. Tinglysingsregisteret (grunnboken for fast eiendom og borettslagsrettigheter[3]) registrerer ikke bare rettigheter, men kan også gi grunnlag for at rettigheter tapes, eller ikke kan påberopes om de ikke er registrert.[4] Risiko forbundet med elektroniske signaturer i den sammenhengen kan altså innebære at retten til huset eller borettslagsleiligheten går tapt.

Dette er eventuelt en annen type risiko enn den en løper om en elektronisk signatur misbrukes til å trekke fra ens bankkonto. Er en bank involvert på denne måten, har lovgiveren muligheten til å la bankene bære en del av tapet ved misbruk av BankID, som dem som har formet systemet, eller simpelthen som dem med dypest lomme og flest kunder å fordele tapet på. Noen slik mulighet finnes ikke ved eiendomstransaksjoner, der banker kan hende ikke er involvert i det hele tatt. Da er det ingen bank å ty til, og en akseptabel fordeling av risikoen mellom for eksempel en kjøper og en selger, slik den fordeles mellom banken og bankkunden, er ikke mulig så lenge det bare er én familie som kan bo i huset som er kjøpt. Skyldsynspunkter er også vanskelige så lenge dette ikke bare dreier seg om den påstått uaktsommes rett til husvære, men også familien hens. Endelig har salg av fast eiendom enda større innvirkning på den allmenne tilliten til rettssystemet enn gjeldsforhold. Dels dreier det seg for de fleste av oss om beløp som er langt større enn de beløpene vi noen gang vil ha på en bankkonto eller få lånt. Og dels vil trolig de fleste av oss bli mer skeptiske til å investere dersom vi ikke har en følelse av at rettsordenen effektivt kan beskytte vår rett til investeringsobjektet.

Det finnes en rekke andre rettighetsregistre[5] over formuesgoder der tilsvarende problemer kan oppstå som de som kan oppstå i forbindelse med tinglysing i grunnboken. Disse registrene vil ikke bli diskutert her. Dette har sammenheng med at elektronisk kommunikasjon med disse registrene om rettighetsregistrering er lite brukt. Selv om slike registre nå vanligvis føres elektronisk, er kommunikasjonen med dem oftest på papir. Det finnes noen unntak, og noen registre godtar skannede papirdokumenter, iallfall om det ikke er tydelig at underskriften er limt inn fra et annet dokument. Rettslig sett er det ofte adgang for registrene til å motta kommunikasjon elektronisk fordi tinglysingsloven kapittel 2 er gitt tilsvarende anvendelse,[6] eller med basis i den alminnelige regelen om aksept av elektroniske signaturer i eIDAS-forordningen art. 25. For brukerne av disse registrene er det neppe bryet verd å opprette slike avtaler som kreves for å kunne bruke elektronisk kommunikasjon etter mønster av tinglysingsloven. Elektronisk signering av et registreringsskjema som sendes som e-post, ville for noen registres vedkommende kanskje kreve så mye forklaringer overfor og overtalelse av mottakerne at det er lettere å bruke papir. Svindlere vil iallfall ikke tiltrekke seg oppmerksomhet ved å gå inn i slike diskusjoner.

Noen plikt til å ta imot registreringer elektronisk uten spesiell avtale har verken tinglysingen (for grunnboken) eller andre rettighetsregistre. Plikten til å anerkjenne elektroniske signaturer på linje med håndskrevne er iallfall i Norge tolket innskrenkende, slik at plikten bare gjelder når det teknisk er tilrettelagt for elektronisk kommunikasjon.[7] Desto mindre er det noen plikt til å la den som skal registrere, få velge fritt hvilket «merke» elektronisk signatur hen skal bruke, og spesielt å velge en utenlandsk signatur.[8] Når det gjelder grunnboken, gjelder det visst uansett et generelt unntak fra eIDAS-forordningen for slike registre.[9]

Praktisk sett har tinglysingen et tosporet system. Privatpersoner og virksomheter kan, som før, sende inn dokumenter til tinglysing på papir via post eller bud. I så fall gjelder krav til bruk av særskilte blanketter, vedleggelse av en tinglysingskopi (som imidlertid bare arkiveres elektronisk) og vitnekrav etter

tinglysingsloven § 17.[10] Virksomheter, for eksempel banker, advokater og eiendomsmeklere, kan alternativt registrere seg som elektroniske innsendere og sende inn dokumenter elektronisk på vegne av seg selv eller andre. Ved siden av et enkelt opplegg for mindre virksomheter[11] kan større virksomheter få et opplegg tilpasset sine datasystemer.[12] Det er mitt inntrykk at systemet fungerer godt.

Nedenfor skal først den tekniske sikkerheten ved elektroniske signaturer forklares og diskuteres. Deretter diskuteres misbruk av elektroniske signaturer og noen andre risikoaspekter ved dem.

I et forarbeid til innføringen av elektronisk tinglysing blir de viktigste risikoene ved reformen klassifisert som risikoer for identitetssvikt (en annen enn den berettigede disponerer), viljesmangler (manglende disposisjonsvilje og fullmaktsinnsigelser) samt systemsvikt (tekniske tilkortkommenheter).[13] Her tas utgangspunkt i den sistnevnte risikotypen. Deretter drøftes viljesmangler og til slutt en rekke mindre risikospørsmål.

2 Teknisk forfalskningsrisiko

2.1 Innledning

En enkel måte å signere elektronisk på er at man skanner et dokument og knytter det til en elektronisk signatur, som for eksempel BankID. For eksempel programmet Adobe Acrobat har en funksjon som gjør dette mulig. Det elektroniske dokumentet vil da gi uttrykk for at det er signert, og ha en lenke for å verifisere signaturen.[14]

Noe liknende gjelder for dokumenter som skal tinglyses elektronisk. Dokumentet blir da enten fylt ut i en nettløsning eller lastet ned til et nettsted, og det blir i begge tilfeller signert elektronisk der.

En skannet underskrift for hånd teller vel ikke som elektronisk signatur. Uten en elektronisk signatur er en skannet kopi av et dokument underskrevet for hånd lett å forfalske. Den håndskrevne underskriften kan for eksempel være kopiert inn fra et annet dokument.

Spørsmålet her i avsnitt 2 er om forfalskningsrisikoen er større ved et elektronisk signert tinglysingsdokument enn ved et tilsvarende papirdokument signert for hånd. Risikoen for at en persons elektroniske signatur er brukt av en annen, diskuteres særskilt nedenfor i 3. Her i avsnitt 2 er det den tekniske sikkerheten det gjelder. Kan underskriften knyttes til et annet budskap enn den som fremstår som underskriver, ønsket?

Når en skal vurdere hvordan risikobildet endrer seg med hensyn til teknisk risiko ved bruk av elektroniske signaturer, er håndskrevne signaturer gullstandarden.[15] Like lite som en kan forvente at dokumenter underskrevet med hånd er helt umulige å forfalske, kan en forvente at elektronisk signerte dokumenter er det.

2.2 Hva tinglysningen krever

Etter tinglysingsforskriften kan underskrifter i tinglysingssammenheng være elektroniske om de bygger på en «eID-ordning» på nivå «høyt» – det høyeste – etter eIDAS-forordningens system.[16] I praksis utelukkes de fleste slike ordninger fordi det ikke er laget et brukergrensesnitt for dem, og bare de norske systemene BankID og Buypass kan brukes. De underliggende dokumentene kan imidlertid i prinsippet være signert ved hjelp av andre systemer, så lenge disse systemene er sikre nok.[17]

En «eID-ordning» gir en entydig identifikasjon av noen. Skal den gi mening i tinglysingssammenheng, må identifikasjonen knyttes til dokumentene som sendes til tinglysing, og til et eventuelt samtykke til tinglysing etter tinglysingsloven § 13. Uten slik tilknytning ville det være som å sende med passet til noen for å vise at passinnehaveren hadde godtatt dokumentene sendt i samme konvolutt. En slik tilknytning kan imidlertid skapes ved at «eID-ordningen» brukes som et ledd i en elektronisk underskrift.

Denne elektroniske underskriften som brukes i elektronisk tinglysing er ikke på det høyeste nivået for elektroniske underskrifter («kvalifisert»), og regelen i eIDAS-forordningen art. 25 nr. 2 om at slike elektroniske signaturer har samme rettsvirkning som håndskrevne, får ikke anvendelse.[18] Det spiller liten rolle. I norsk rett har selv en håndskrevet underskrift uansett ingen spesiell rettsvirkning.[19] Den er bare et bevis for identitet og disposisjonsvilje, og dette beviset kan vise seg utilstrekkelig i forhold til andre bevis.

Hadde underskrifter hatt slike rettsvirkninger i norsk rett, ville det kunne undergrave systemet i eIDAS om rettsvirkningene også ble tillagt ikke-kvalifiserte elektroniske signaturer.[20] Men slik er det altså ikke i norsk rett. Strengt tatt kan det kanskje sies at slik systemet med elektronisk tinglysing er laget, kan den ikke-«kvalifiserte» elektroniske signaturen få den rettsvirkningen at det kan tinglyses, og det kunne vært et problem med hensyn til synspunktet som drøftes her, om systemundergraving. Men i tinglysingssammenheng er ikke signaturen konstituerende for noen rett; den er bare et formkrav. Retten som tinglyses eksisterer er etter sikker rett uavhengig av tinglysingen. Og iallfall så lenge det ikke er tale om underskrifter som konstituerer en rett, må en fritt kunne bruke de enklere elektroniske signaturene. I motsatt fall ville jo elektroniske signaturer på lavere nivå en «kvalifisert» overhodet ikke kunne tillegges rettslig betydning, og dette ville være i strid med den uttrykkelige ordlyden i eIDAS art. 25 nr. 1.[21] Opplegget for elektronisk tinglysing er slik sett uproblematisk.

2.3 Etterlikning

Hvilken risiko innebærer så slike elektroniske signaturer i tinglysingssammenheng? Vi begynner med etterlikningsrisikoen.

Mens en håndskrevet signatur er lett å etterlikne, er dette mye vanskeligere med en elektronisk signatur. Elektroniske signaturer er basert på avanserte koder, som det ikke er praktisk mulig å knekke med dagens teknologi.

En teknisk presis beskrivelse av elektroniske signaturer hører ikke hjemme her.[22] Men det følgende kan kanskje gi leseren en brukbar ide om hva det dreier seg om:

Til hver elektronisk signatur hører det to koder, en offentlig og en hemmelig.[23] Brukeren ser ikke disse, men den hemmelige koden holdes hemmelig ved hjelp av for eksempel et passord.

Koder brukes vanligvis til å holde noe hemmelig. Det er ikke poenget her. Her er poenget at om du kan lese et kodet budskap fra meg med min offentliggjorte kode, så bekrefter det at budskapet er kodet med min hemmelige kode, og derfor formodentlig er fra meg. Det er omtrent som at om en nøkkel virker i låsen, så vet man at man har kommet til riktig dør, enten den har vært låst eller ikke.

Fra andre koder er man vant til at om man kan lese noe jeg har kodet, så kan man også kode et budskap slik at det ser ut som det kommer fra meg. Her bruker man imidlertid såkalte asymmetriske koder; en kan ikke gjette seg til hvordan man koder et budskap (med min hemmelige kode) selv om man har kodenøkkelen til å lese det (med min offentlige kode). Til anskueliggjøring av prinsippet: Selv om man vet alle minnetallene i et regnestykke der tall legges sammen, kan man ikke konstruere regnestykket. Det er likevel en nær nok sammenheng mellom regnestykket og minnetallene som kan brukes til å lage et sett med asymmetriske koder: én hemmelig til å signere med (som lages fra minnetallene) og én offentlig (som lages fra tallene som legges sammen) til å verifisere at signaturen er registrert på den som angivelig har signert. Detaljene kan ligge her.

Fordi elektroniske signaturer er basert på slike koder, vil det kunne verifiseres om en elektronisk signatur er utstedt til den personen det gjelder. Dette kan gjøres enkelt og rutinemessig om man har internettilgang med programvare som finnes på de fleste personlige datamaskiner.

Også underskrifter for hånd kan for så vidt verifiseres, men dette krever skrifteksperter, tid og penger, og sikkerheten i verifiseringen er langt dårligere enn man skulle tro.[24] En underskrift er tross alt en veldig begrenset skriftprøve.

Håndskrevne signaturer kan sammenliknes med tidligere underskrifter fra samme person, og for eksempel i bankvesenet har man tradisjonelt utvekslet underskriftsprøver samarbeidspartnere imellom. I tinglysingen kunne man tenke seg at man hentet frem gamle dokumenter og sammenliknet med underskriftene på dokumenter som foreligger til tinglysing. Dette gjøres likevel ikke, og slik sammenlikning av lekfolk ville uansett være nokså usikker, blant annet fordi folks underskrifter endres over tid. Sammenlikning gir lite økt sikkerhet.

Etter dette er det nokså klart at risikoen for etterlikning reduseres kraftig ved bruk av elektroniske signaturer.

2.4 Tekstendringer

Ved håndskrevet underskrift på papir knytter papirarket underskriften sammen med teksten det underskrives på, og etterfølgende endringer i teksten vil lett sette spor på papiret. Ved forutgående rettelser og når et dokument er skrevet på flere ark, verifiserer man gjerne endringene og de ikke underskrevne arkene med initialer («parafering») om dokumentet er viktig nok, og om det ikke er for kleint å be om det. På denne måten får en iallfall en viss sikkerhet mot at innholdet i det noen har skrevet under på, er endret etter underskriften.

Når innholdet som signeres, er laget elektronisk, kan det i utgangspunktet være enkelt å endre det etter signeringen, kanskje uten å etterlate spor. Det er derfor nødvendig at det signerte budskapet sikres sammen med signaturen. Det gjøres. Rent praktisk brukes en såkalt hashtag, som er en utregning basert på det signerte budskapet, og som ikke lett vil kunne gi samme sluttresultat om budskapet er endret.

Også i denne henseende reduserer elektroniske signaturer risikoen for at et signert budskapet endres etter signaturen. Underskrifter på papir gir en viss trygghet mot slikt, og parafering kan også ha en viss betydning om det gjøres, men sikkerheten ved elektroniske signaturer er langt større.

2.5 Usikre fremstillingssystemer

Selv om det teknisk sett er mulig å sikre at en tekst ikke blir endret, kan det som bruker være vanskelig å vite om disse mulighetene er brukt. Er fremstillingssystemene for den elektroniske signaturen gode nok?

Ved underskrifter for hånd er en avhengig av at blekket på det man skriver under på, ikke kan viskes bort, slik at teksten kan endres. Erfaringsmessig går det bra, skjønt de færreste sjekker utstyret som er brukt til å produsere dokumentet. Ofte har man også en kopi man stoler på.

Ved elektroniske signaturer er man nok enda mer avhengig av forhold man ikke kan kontrollere, som at de som tilbyr signeringstjenestene (for eksempel BankID), er ærlige og seriøse, og at programvaren som tilsynelatende verifiserer signaturene, virkelig gjør det. Erfaringsmessig går også dette bra, blant annet fordi det er et visst offentlig tilsyn med dem som tilbyr signeringstjenester,[25] og fordi det oftest er kjent og anerkjent programvare som brukes til å verifisere signaturene.

Risikonivået for underskrifter for hånd og for elektroniske signaturer er trolig omtrent det samme i denne henseende.

2.6 Kort oppsummering

Den tekniske forfalskningsrisikoen – om en underskrift knyttes til et annet budskap enn den angivelige underskriveren ønsket – reduseres snarere enn økes om håndskrevne signaturer erstattes av elektroniske.

3 Risiko for manglende sammenheng mellom person og signatur

3.1 Systemet

Den som er registrert i grunnboken som rettighetshaver i en fast eiendom, kontrollerer frivillige rettsstiftelser vedrørende rettigheten ved signaturen sin.[26] Signaturen er derfor avgjørende for kontrollen over rettigheter i fast eiendom, inklusiv eiendomsretten. Det har derfor stor betydning at det virkelig er rettighetshaveren som signerer.

Ovenfor i 2 er forfalskninger av signaturer drøftet. En håndskrevet signatur er uløselig knyttet til en person, og er den skrevet av en annen enn vedkommende person, er den falsk og derfor ugyldig. Dette er ikke like enkelt med elektroniske signaturer. På liknende måte som når noen skriver under på vegne av en virksomhet, må en etablere en sammenheng mellom signaturen og den det skrives under på vegne av.[27] De tekniske løsningene som er diskutert ovenfor i 2, etablerer ikke en slik sammenheng.

Her skal den ikke-tekniske risikoen for manglende sammenheng mellom signatur og person drøftes i samband med tinglysing. Samtykke og uaktsomhet vil bli drøftet særskilt i 3.5 nedenfor.

Utgangspunktet for både elektroniske signaturer og innføringen i grunnboken er fødselsnummer e.l.[28] Da har man identifisert en person så entydig og offisielt det lar seg gjøre. Men selv om en person kjenner et fødselsnummer og påberoper seg at det er hens, trenger selvsagt ikke dette være riktigere enn om hen kjenner et navn og påberoper seg at det er hens.[29]

Det gjør ting enklere om man bruker det samme utgangspunktet – altså typisk fødselsnummer – både når det gjelder elektroniske signaturer og i tinglysingen. Kan man knytte en person til en elektronisk signatur, kan man også knytte hen til rettigheten i grunnboken. Denne siden av systemet drøftes nedenfor i 3.2.

Bygger både elektroniske signaturer og tinglysingen på for eksempel fødselsnummer, etableres sammenhengen mellom person og en elektronisk signatur 1) ved at rett person tildeles brukerkoder mv. til en elektronisk signatur, og 2) ved at en sikrer seg at brukerkoder mv. er brukt av denne personen. Det første diskuteres nedenfor i 3.3 og det andre nedenfor i 3.4. Det er bare når det gjelder det siste punktet at de tekniske løsningene skissert ovenfor i avsnitt 2 er til hjelp. Også her er imidlertid teknikken sårbar for menneskelige feil.

Systemet her er ganske teknisert. Man trenger ikke å bry seg om for eksempel hvem som kan fremvise et skjøte, eller om en person er kjent som (har en sosial identitet som) den personen som er oppgitt i grunnboken. Dette er på mange måter betryggende når eiendomsrettigheter omsettes i en større verden. På den andre siden går en glipp av de enkle kontrollmekanismene et mindre teknisert system ga.

3.2 Nærmere om bruken av fødselsnummer o.l.

Det viktige med elektroniske signaturer i forbindelse med tinglysing er altså ikke å etablere hvem som signerer (hens sosiale identitet), men at den som signerer, er den samme som rettighetshaveren som er registrert i grunnboken. Et godt forbindelsesledd i så måte er norsk fødselsnummer. Bare et navn, eller et navn i kombinasjon med fødselsdato, er ikke like entydig.

Dersom man ikke har tilstrekkelig entydige forbindelseslinjer mellom en elektronisk signatur og den som er registrert i grunnboken som rettighetshaver, må tinglysingen behandles manuelt. En elektronisk signatur kan da være til hjelp, men bare som et av flere identitetsbevis og som en bekreftelse på disposisjonsvilje. Uansett vil det ikke være lagt til rette for elektronisk signering med mindre det er en entydig forbindelseslinje mellom den elektroniske signaturen og den som er registrert i grunnboken som rettighetshaver for eksempel ved hjelp av et fødselsnummer.

Vi skal nå se nærmere på de forskjellige forbindelseslinjene mellom elektroniske signaturer og den som er registrert i grunnboken som rettighetshaver.

Norsk fødselsnummer er som nevnt godt egnet, og trolig ganske sikkert.[30] Det kan visst tenkes at en person har fått to norske fødselsnumre ved en feil.[31] Dersom ikke samme fødselsnummer er brukt i grunnboken og i den elektroniske signaturen hens, må det ordnes opp i dette før det kan tinglyses elektronisk, for eksempel ved retting av grunnboken etter tinglysingsloven § 18.

Den som ikke kan få norsk fødselsnummer, kan få et såkalt D-nummer.[32] Dette gjelder for eksempel personer som ikke bor i Norge. Slike nummer rekvireres av myndigheten som skal bruke det, for eksempel tinglysingen, banker og Brønnøysundregistrene.[33] D-nummer kan utstedes uten identitetskontroll.[34] Et D-nummer utstedt uten identitetskontroll bør ikke kunne gi grunnlag for elektronisk tinglysing, fordi nummeret meget vel senere kan knyttes til en person med en annen identitet enn den som har legitimert seg overfor tinglysingen.[35]

En forutsetning for å kunne bruke D-nummer ved elektronisk tinglysing er at brukere med D-nummer kan få elektronisk signatur, og at slike elektroniske signaturer godtas av tinglysingen. Det synes å være tilfellet.

De elektroniske signaturene som kan brukes til tinglysing, er norske,[36] og norske elektroniske signaturer kan ikke utstedes for andre enn dem som er registrert i folkeregisteret.[37] En utlending uten D-nummer kan da ikke tinglyse elektronisk.

En tredje variant, ved siden av fødselsnummer og D-nummer, er norsk organisasjonsnummer. Et utenlandsk selskap kan få norsk organisasjonsnummer, men kan få registrert rettigheter også uten et slikt nummer. For elektronisk tinglysing kreves det norsk organisasjonsnummer, og virksomhetssertifikater (elektronisk ID for en virksomhet) godtas bare fra finansforetak.[38] Alternativt kan det registreres en fullmakt, slik at en person kan disponere på vegne av virksomheten ved sin personlige elektroniske signatur.[39]

3.3 Risiko ved utstedelse av bruker til elektronisk signatur

Som nevnt ovenfor i avsnitt 3.1 er det av avgjørende betydning for systemet med elektronisk tinglysing at elektroniske signaturer blir utstedt til riktig person.[40] For formålene her betyr det først og fremst at den elektroniske signaturen ikke må knytte seg til galt fødselsnummer, D-nummer eller organisasjonsnummer. Som en ekstra sikkerhet får en heller ikke tinglyst elektronisk om navnet er galt.[41]

Utstedelsen av brukere til elektroniske signaturer skjer i to faser. Først bringes søkerens identitet på det rene. Deretter får søkeren brukerkoder mv., som er nødvendig for å kunne bruke den elektroniske signaturen. Brukerkodene sikrer at det er rett person som bruker signaturen. Det dreier seg typisk om kombinasjoner av et passord («noe man vet»), en kodebrikke som genererer en engangskode, en mobiltelefon («noe man har») eller gjenkjenning av iris, ansikt eller fingeravtrykk («noe man er»).

Hva som skal til for å verifisere identitet, er forbausende nok ikke klart definert, verken i eIDAS-forordningen eller i reglene til de elektroniske signaturene som brukes ved elektronisk tinglysing. I eIDAS-forordningen faller en tilbake på formuleringer som at identiteten skal kontrolleres «ved bruk av ... identifikasjonsmetoder anerkjent på nasjonalt plan som garanterer pålitelighet som tilsvarer fysisk tilstedeværelse».[42] Man kan bygge på pass,[43] men det er ikke veldig lenge siden pass ble utstedt på grunnlag av førerkort[44] eller dåpsattest[45] , og er pass først utstedt, vil det gamle kunne danne grunnlag for et nytt pass og altså en elektronisk signatur. Man kan ikke alltid bygge på en tidligere utstedt elektronisk signatur alene, men dette kan ha med andre forhold enn sikkerhet å gjøre.[46]

Det er altså en viss risiko for at det utstedes en bruker til elektronisk signatur til feil person, slik at vedkommende for eksempel kan disponere over andres rettigheter i grunnboken ved elektronisk tinglysing. Elektronisk tinglysing representerer imidlertid neppe en økt risiko, fordi for eksempel pass ville blitt godtatt som identifikasjon også ved papirtinglysing. Tvert imot kan det være at risikoen reduseres ved elektronisk tinglysing sammenliknet med papirtinglysing fordi det normalt kreves fremmøte ved utstedelse av bruker til en elektronisk signatur,[47] mens en ikke har noen praktisk ordning for personlig fremmøte i forbindelse med papirtinglysing.

Når identiteten til den som søker om å få en bruker til en elektronisk signatur, er brakt på det rene, er det avgjørende at brukerkoder mv. for den elektroniske signaturen som utstedes, blir overbrakt søkeren og ingen annen. Her gjelder tilsvarende krav til identifikasjon som ved identifiseringen av søkeren. I dag kreves typisk fremmøte med ID-kontroll på Posten, og er således gjennomførbart for dem som befinner seg i Norge.[48]

Dersom slike rutiner følges, er bruk av elektronisk signatur etter mitt skjønn trolig iallfall like sikkert som papirtinglysing. Helt sikre er systemene imidlertid ikke, og det kan være at rutinene fra tid til annen ikke følges, og at dette medfører tap av rettigheter eller verdier. En må da i tilfelle falle tilbake på erstatningsreglene, som er behandlet nedenfor i avsnitt 6. Utstederens ansvar for feil er etter avtalene svært begrenset, særlig sett i lys av de verdiene tinglysing av fast eiendom ofte gjelder.

3.4 Risiko ved brukerkoder brukt av feil person

I mediene har det vært mye omtale av saker der en person A er forsøkt gjort ansvarlig for gjeld stiftet av andre ved å bruke hens elektroniske signatur. Som nevnt ovenfor i avsnitt 1 dreier disse sakene seg om As ansvar overfor långiveren, typisk en bank. Tilsvarende problemer kan reise seg om noen har misbrukt As elektroniske signatur til for eksempel å selge eiendommen hens og tinglyse salget.

Når en elektronisk signatur er misbrukt, kan det være et ledd i et mer omfattende identitetstyveri. For formålene her spiller det ingen rolle om man kan snakke om identitetstyveri. Karakteristikken «identitetstyveri» har intet juridisk innhold, men brukes vel gjerne om omfattende misbruk av blant annet signaturer i vinnings hensikt.[49]

Juridisk sett er dette falsk (falskneri, forfalskning). Avtalen er ugyldig og kan ikke gjøres gjeldende overfor signaturhaveren. Det er ingen rettsregel som tilsier at en elektronisk signatur virker uavhengig av viljen til signaturhaveren.

Tinglysingen spiller ingen rolle mellom partene; i Norge har vi ingen regel om at tinglysing reparerer ugyldighet mellom to avtaleparter.[50] Tinglysingen kan da kreves rettet etter tinglysingsloven § 18: «Dersom

registerføreren blir oppmerksom på at en innføring i grunnboken er uriktig, eller at det på annen måte er gjort feil, ...» Dersom registerføreren er i tvil om det virkelig dreier seg om falsk, kan det tinglyses krav om retting (tinglysingsloven § 18 tredje ledd), og for eksempel den historiske eieren kan reise sak mot kjøperen for å få dette avklart. Tinglysingen av rettingskravet kan skje før stevning og uten rettslig beslutning, i motsetning til hovedregelen at bare saker som er brakt inn for tingrett eller høyere rett, kan tinglyses (tinglysingsloven § 19).

Reglene er slik sett like for håndskrevne og elektroniske signaturer. Bevissituasjonen er likevel svært forskjellig om det er tvil om det er rette vedkommende som har underskrevet elektronisk. Ved en underskrift for hånd har man iallfall en skriftprøve (underskriften) å gå ut fra, om enn meget begrenset.[51] Ved en elektronisk signatur er det ikke upraktisk at det ikke finnes noe som helst å ta tak i for å bekrefte eller avkrefte at det er rette vedkommende som har brukt den elektroniske signaturen – heller ikke elektroniske spor. Et skoleeksempel er sønnen som betaler sin gamle (men åndsfriske) mors regninger, og derfor har tilgang til hennes BankID. Dersom BankID-en er brukt til å selge huset (til sønnen eller til andre), kan det være vanskelig eller umulig å vite om det er sønnen eller moren som har tastet koden til den elektroniske signaturen hennes. Dersom moren dør eller blir mentalt svekket før spørsmålet kommer opp, har en ikke engang hennes vitneprov å bygge på.

Moren i eksempelet burde selvsagt gitt sønnen fullmakt i stedet for kodene til den elektroniske signaturen, men det har hun altså ikke gjort. Dette er visst vanlig.[52] En av grunnene til dette kan være at fullmakt ikke gir adgang til fullmaktsgiverens e-fakturaer og avtalegiroer, slik at det blir dyrt å bruke fullmakt og upraktisk for fullmektigen. Og har fullmektigen adgang til fullmaktsgiverens koder i nettbanksammenheng, gir de også mulighet til å tinglyse disposisjoner over fast eiendom. Det er i dag dessverre ikke mulighet til å begrense digitale signaturer til å gjelde bare visse typer disposisjoner.[53]

Det er i dag ingen mekanismer som sikrer bevis i slike situasjoner som i eksempelet.[54] Man kunne tenke seg at det krevdes irisskanning, ansiktsgjenkjenning eller fingeravtrykk for å bruke elektroniske signaturer, men det brukes ikke i Norge i dag, og det er uansett usikkert hvor mye en kunne få ut av slikt bevismessig i tilfeller som i eksempelet i forrige avsnitt. Tinglysingen sender varsel til den offisielle adressen til den registrerte rettighetshaveren i en del tilfeller,[55] men slike meldinger vil typisk sønnen i vårt eksempel håndtere. Endelig kunne man tenke seg at de bankene etc. som tilrettelegger for elektronisk signering, undersøkte hvem som faktisk signerte. Noen plikt til dette har de ikke etter avtalene med tinglysingen.[56] Hvitvaskingsreglene krever at mellommenn, som eiendomsmeklere om det brukes, skal klargjøre partenes identitet, men ikke at disposisjonsviljen skal undersøkes.[57] Resultatet er at elektronisk signering har medført et bevisvakuum i tilfeller som i eksempelet ovenfor.

Det var tidligere i slike tilfeller den som den elektroniske signaturen er utstedt til, som hadde bevisbyrden for at det var en annen som tastet brukerkodene mv.[58] I vårt eksempel ville dette altså si den senile eller døde moren. Hun – eller arvingen hennes – kunne[59] føre bevis for at det ikke var hun som tastet brukerkodene mv., eller at brukerkodene mv. har kommet på avveier uten hennes medvirkning. Bevisbyrdereglene er nå kraftig modifisert, iallfall på finansavtalelovens område.[60] Det synes uansett mer formålstjenlig å sørge for bevis enn å bruke bevisbyrderegler.

Arbeidsgruppen som utredet rettslige spørsmål om elektronisk tinglysing, foreslo at dette bevisvakuumet kunne avhjelpes ved et krav om vitner.[61] Vitner kan selvsagt vitne falsk, men det er iallfall bevis å ta utgangspunkt i. Dersom sønnen i eksempelet ovenfor viser til to utenlandske gjestearbeidere som vitner, og disse ikke kjente moren, kunne norsk eller kan identifiseres, ville en ikke stå helt på bar bakke bevismessig i vurderingen av om det faktisk var moren som underskrev. Selv ville jeg iallfall tro at moren ikke hadde valgt slike vitner.

Dette forslaget var forskjellig fra vitnekravene ved papirtinglysing etter tinglysingsloven § 17, som tiden på mange måter har løpt fra etter at underskriverens alder lettere kan dokumenteres på annen måte (for eksempel ved fødselsnummer). De foreslåtte vitnekravene kunne oppfylles uten at vitnene var til stede sammen med underskriveren (men for eksempel hadde snakket med hen på telefon), og vitnepåtegningen kunne skje ved elektronisk signatur.

Vitnekravet har selvsagt en ulempe- og kostnadsside, om enn begrenset, og bør neppe gjennomføres for all bruk av elektroniske signaturer. For transaksjoner vedrørende fast eiendom kan imidlertid kostnadene og ulempene lett forsvares, siden det er relativt få transaksjoner det dreier seg om, og verdiene kan være store, både økonomisk og emosjonelt.

I lovforslaget ble dette vitnekravet ikke tatt med, og det ble ikke foreslått alternative metoder for å avhjelpe bevisvakuumet ved elektroniske signaturer. Det gamle vitnekravet ble opphevet for dokumenter med

elektroniske signaturer, men bemerkelsesverdig nok opprettholdt for papirdokumentasjon.[62] Departementet synes å ha forstått forslaget om vitner slik at det skulle bekrefte hvem den elektroniske signaturen var utstedt til, og ikke hvem som hadde brukt den.[63]

Høyesterett har sett problemet med bevisvakuumet som kan oppstå ved elektroniske signaturer, og krever at en bank som vil påberope seg en slik signatur, i mange tilfeller må ha en viss kontakt med underskriveren.[64] Det er imidlertid uklart hvor langt denne plikten går, og noen slik plikt er ikke etablert for for eksempel en kjøper av fast eiendom som vil stole på en elektronisk signatur.

Alt i alt er ordningen med elektroniske signaturer i tinglysingen slik den er utformet, temmelig uforsvarlig, bevismessig sett.

3.5 Samtykke og uaktsomhet

Selv om brukeren til en elektronisk signatur ikke blir forpliktet om noen andre har brukt den, kan det likevel tenkes at hen blir ansvarlig på grunn av den falske signaturen på annet grunnlag.[65] For den som den elektroniske signaturen er utstedt til, er dette et spørsmål om risiko for tap. Speilvendingen av dette er at den som har stolt på den elektroniske signaturen, risikerer tap om den som den elektroniske signaturen er utstedt til, ikke blir ansvarlig.

For det første kan det tenkes at situasjonen oppfattes slik at eieren av den elektroniske signaturen har tolerert eller bent frem ønsket at signaturen hens skal brukes av en annen, slik at vi får en fullmaktssituasjon.[66] Slik toleransefullmakt, kombinasjonsfullmakt eller hva en vil kalle det, er vel kjent i norsk rett.[67] Oppfattes bruken av den elektroniske signaturen som en disposisjon gjort etter toleransefullmakt e.l., blir den som den elektroniske fullmakten er utstedt til, bundet som om hen hadde undertegnet selv. Dette vil i tinglysingssammenheng si at huset hens kan regnes som solgt eller pantsatt.

Det er i strid med avtalene om den elektroniske signaturen å etablere fullmakt på denne måten.[68] Men avtalene binder ikke den som stoler på signaturen, så avtalebrudd er i seg selv ikke til hinder for fullmaktssynspunktet. Avtalene om elektroniske signaturer er imidlertid så vel kjente at en som ser at den elektroniske signaturen på for eksempel et skjøte ikke tilhører den som signerer, neppe kan være i god tro, og derfor ikke kan stole på fullmakten. Har den som signerer, utgitt seg for å være den personen som signaturen er utstedt til, kan den som stoler på signaturen, imidlertid meget vel være i god tro og kunne gjøre krav gjeldende mot for eksempel huseieren som den elektroniske signaturen er utstedt til.

Ofte vil det nok være slik i misbrukssituasjonene at den som den elektroniske signaturen er utstedt til, har latt en annen signere for seg i en bestemt situasjon (for eksempel til å betale regninger), mens denne har brukt signaturen også i andre situasjoner (for eksempel til å selge et hus). Siden den elektroniske signaturen gir legitimasjon utad – det ser ut som det er rette vedkommende som handler – kan det neppe komme på tale at slike avtaler mellom den som eier og den som bruker den elektroniske signaturen, skal kunne påberopes overfor den som stoler på signaturen. Dette likner mer på en skriftlig fullmakt enn en oppdragsfullmakt.[69]

Ved håndskrevne signaturer kan liknende situasjoner oppstå om en person ber om eller stadig tolererer at en annen underskriver med hens navnetrekk eller påfører en kopi av hens underskrift. Risikoen ved elektroniske signaturer er her verken større eller mindre enn ved håndskrevne. Det er kanskje mer fristende å gjøre slikt ved elektroniske signaturer, da motviljen mot å skrive falsk nok er større enn motviljen mot å taste falsk.

Alt i alt vil en falsk elektronisk signatur etter omstendighetene i prinsippet kunne tenkes å binde den signaturen er utstedt til, etter reglene om toleransefullmakt e.l.[70] En nærmere drøftelse av kriteriene faller utenfor denne fremstillingen; her er poenget at muligheten finnes.

En annen rettsvirkning av en falsk signatur kan være erstatningsansvar på uaktsomhetsgrunnlag for den som den elektroniske signaturen er utstedt til. Jeg går ikke inn på alle vilkårene for slikt ansvar her. Ved slikt ansvar får den som har stolt på den elektroniske signaturen i tinglysingen, ikke for eksempel huset, men den som den elektroniske signaturen er utstedt til, må dekke tapet hens. Siden den som har stolt på den elektroniske signaturen, kunne forventet å få huset i eksempelet, men ikke får det, vil tapet som skal erstattes, være verdien av huset om kjøpesummen er betalt til en svindler. Dette vil være alvorlig.

Etter norsk rett er det ikke grunnlag for å kreve erstatning av den som den elektroniske signaturen er utstedt til, i slike tilfeller med mindre hen har opptrådt uaktsomt. Det vil si at om man følger alle regler om hemmelighold

av personlig kode mv., skulle det ikke være noen risiko for at man må betale erstatning. I disse tilfellene vil heller ikke misbruk av den elektroniske signaturen kunne skje om systemet fungerer som man håper.

Nå kan det hende at den som den elektroniske signaturen er utstedt til, har vært aktsom, men ikke blir trodd, eller at hen uaktsomt har tatt feil av hvilke sikkerhetsforanstaltninger hen må sørge for. Da kan hen bli erstatningsansvarlig. Dette er risikoer man tar om man bruker systemet, og som man neppe kan unngå om man vil ha en bruker til en elektronisk signatur. Det første likner på risikoen med at noen forfalsker ens underskrift for hånd så godt at den blir tatt for å være ekte. Det siste har ingen parallell til håndskrevne signaturer – her er det ingen kjente eksempler på at man får erstatningsansvar for eksempel fordi man vanligvis undertegner på en måte som er lett å etterlikne. Totalt sett er nok slik sett risikoen for å bli erstatningsansvarlig større ved en elektronisk signatur enn ved en underskrift for hånd.

Det kan tenkes at den som den elektroniske signaturen er utstedt til, tolererer at en annen (som av en eller annen grunn kjenner koden) bruker den, eller bent frem gir hen kodene. Dette kan ses som kvalifisert uaktsomhet eller som fullmakt (som beskrevet ovenfor under denne overskriften). Erstatningskravet er et krav på penger for det tapet som er lidt, og foreldes etter tre år,[71] mens kravet etter fullmaktssynspunktet er et krav på avtalens innhold, som kan være å få huset som er solgt. Er kravet på eiendomsrett, foreldes kravet ikke.[72]

I Sverige og Finland, og i en rekke andre land, kan en som utgangspunkt ikke kreve erstatning for lidt tap med mindre en del av tapet er tings- eller personskade.[73] På denne måten holdes kontrakts- og erstatningskrav klarere fra hverandre. Dette fører nok til at fullmaktssynspunktet er mer naturlig i disse landene enn erstatningssynspunktet,[74] og kanskje også at en domstol nødig vil finne avtalebundet når det ikke foreligger intensjon om å binde seg, men bare uaktsomhet. I Norge er det ikke grunnlag for å hevde en slik regel, og den som behandler kodene til en elektronisk signatur uaktsomt, vil trolig lettere bli ansvarlig overfor en som er villedet, enn i disse nabolandene.

Aktsomhetsnormen – og de øvrige vilkårene for uaktsomhetsansvar – er imidlertid ikke nødvendigvis de samme i og utenfor kontrakt. Dette gjelder også i et tilfelle som dette, der utgangspunktet for plikten til å holde kodene etc. hemmelig er hjemlet i avtalen mellom den som har fått utstedt elektronisk signatur, og utstederen.[75] Den som stoler på den elektroniske signaturen og blir villedet fordi den er brukt av en som ikke var berettiget til det når den berettigede har vært uaktsom, er ikke part i denne avtalen og kan i utgangspunktet ikke påberope seg den.

I en serie dommer har Høyesterett drøftet i hvilken grad grunnlaget for uaktsomhetsansvar overfor tredjeperson sammenfaller med uaktsomhetsansvaret i kontrakt.[76] Dette dreier seg om situasjoner der fast eiendom o.l. blir overdratt fra A til B til C, og C krever A på grunnlag av brudd på de normene som gjelder mellom A og B.[77] Typisk kan det dreie seg om en C som har kjøpt en bolig av B, og som saksøker arkitekten A for ikke å ha fulgt opp byggingen som hen pliktet. I de tilfellene vi diskuterer her, dreier det seg for eksempel om en avtale mellom bankkunden A og banken B om å holde kodene hemmelige, og en C som påberoper seg denne avtalen når hen krever tapet sitt dekket av A. At det i våre tilfeller ikke er noen overdragelser, eller noen avtale overhodet mellom B og C, kan neppe spille noen rolle i de spørsmålene vi drøfter her, nemlig om C kan påberope seg avtalen mellom A og B, som hen ikke er part i.

I dommene er Høyesterett klart nok ikke fremmed for at C kan påberope seg avtalen mellom A og B når grunnlaget for erstatningskrav mot A skal avgjøres. Pliktene som var misligholdt, dreide seg for eksempel om plikter etter byggeforskriftene og plikter til å påse at byggingen ble forsvarlig gjennomført.

Spørsmålet om en norm gjeldende mellom A og B skal kunne påberopes av en tredjeperson C, vil etter dommene «bero på en bredere avveining, hvor tapssituasjonen, karakteren av pliktbruddet og de interesser som beskyttes og håndhevingssynspunkter vil inngå».[78] Dette trekker nok i retning av at også en tredjeperson C som lider tap fordi den A som den elektroniske signaturen er utstedt til, har røpet koden, kan påberope seg dette bruddet på avtalen mellom A og banken hens B. De aller fleste vil forstå at ved å bryte hemmeligholdet utsetter man ikke bare seg selv for å lide tap, men også en tredjeperson. Slik sett kunne regelen like gjerne vært en del av den ulovfestede aktsomhetsstandarden.[79] Det er i grunnen merkelig at regelen om hemmelighold ikke er generelt lovfestet eller skrevet inn i eIDAS-forordningen.[80]

I HR-2021-2201-Aavsnitt 73 fremholdes det at uaktsomhetsnormen, som C påberoper seg, ikke nødvendigvis sammenfaller helt med det som gjelder mellom A og B (altså i vårt tilfelle avtalen om hemmelighold av kodene). For at A skal bli ansvarlig overfor C, kreves det

«at tredjemann er blitt påført et betydelig tap og er satt i en vanskelig situasjon. Videre fremgår at ansvar er nærliggende der pliktbruddets karakter er grovt, for eksempel fordi det er knyttet til grunnleggende forhold .... Dette kan eksempelvis gjelde pliktbrudd av betydning for sikkerhet og helse. Det supplerende [erstatnings]ansvaret vil etter dette kunne virke som et sikkerhetsnett».

Etter mitt skjønn vil slike kriterier regelmessig være oppfylt om en tredjeperson C lider tap i tinglysingssammenheng fordi den A som den elektroniske signaturen er utstedt til, ikke overholder kravet til hemmelighold av brukerkoder mv. etter avtalen med B (typisk en bank på vegne av BankID eller Buypass). Det vil typisk dreie seg om store tap, og C vil lett kunne være satt i en vanskelig situasjon uten hus. Pliktbruddet må anses som temmelig grovt, og berører ofte grunnleggende forhold som rett til hjem og eiendom.[81] At slike forhold er grunnleggende, følger allerede av at de er beskyttet som menneskerettigheter.[82]

Etter dette er det mange muligheter til å holde den som den elektroniske signaturen er utstedt til, ansvarlig selv om det er noen andre som har misbrukt den, dersom hen ikke har holdt brukerkoder mv. hemmelig. Ansvaret kan være basert på en fullmaktskonstruksjon eller på erstatningansvar utenfor kontrakt. I det første tilfellet vil den som har stolt på signaturen og for eksempel kjøpt et hus, kunne kreve kjøpet gjennomført, mens i det siste tilfellet kan hen bare kreve tapet sitt dekket.

3.6 Konklusjon

Det svake punktet ved elektroniske signaturer er forbindelseslinjen mellom den tekniske signaturen og en person. Dersom det er en annen enn den signaturen er utstedt til, som har brukt kodene og derved signert, er signaturen i utgangspunktet falsk og i utgangspunktet uten rettsvirkning. Dette gjelder selv om den fremstår som ekte og noen har stolt på den.

Ved tinglysing av fast eiendom brukes de elektroniske signaturene ofte i disposisjoner som har svært stor betydning for den enkeltes økonomi og for grunnleggende behov, som retten til det hjemmet man har etablert. Selv i disse sammenhengene har ikke lovgiveren lagt opp til systemer som sikrer bevis for om det er rette vedkommende som har brukt den elektroniske signaturen. Det er en risiko både for den som holdes til et løfte hen ikke har avgitt, og for den som har stolt på et løfte som viser seg å være ugyldig.

Selv om også en elektronisk signatur kan være ugyldig på grunn av falsk, kan falsken være muliggjort ved at den som den elektroniske signaturen er utstedt til, har brutt pliktene om hemmelighold av brukerkoder mv. Dette kan føre til ansvar både som en fullmaktsgiver – altså som om hen selv skulle ha underskrevet – og til erstatningsansvar – altså plikt til å dekke det tapet andre måtte ha lidt. Dette krever imidlertid en form for uaktsomhet hos den som den elektroniske signaturen er utstedt til. Det er ikke noen regel i norsk rett om at om den elektroniske signaturen er brukt, så skal det formodes enten at rette vedkommende har brukt brukerkoder mv., eller så har hen vært uaktsom. Iallfall i tilfeller der kode er fralurt en rimelig aktsom innehaver av en elektronisk signatur eller falskneren har fått tak i den for eksempel ved datainnbrudd hos utstederen (BankID eller Buypass), kan ansvar ikke gjøres gjeldende.

4 Risiko for at ting går for raskt

At tinglysing skjer raskt i Norge, er et stort gode for dem som skal gjennomføre et prosjekt.[83] Papirbasert tinglysing tar omtrent fire dager i tillegg til postgangen. Elektronisk tinglysing går noe raskere. En del banker prøver også ut automatisert behandling av lånesøknader. Det å få et pantelån kan da gå særdeles raskt.

For noen kan dette gå for raskt og slik sett være en risiko. EU har derfor innført angrefrist for lån avtalt utenom fast forretningssted[84] og for forbrukerkredittavtaler,[85] uavhengig av om avtalen er gjort utenom fast forretningssted. De førstnevnte reglene gjelder imidlertid ikke for lån med pant i fast eiendom,[86] og lån med pant i fast eiendom kan unntas fra de sistnevnte i nasjonal rett.[87] Norge har bare unntatt boliglån.[88]

Man kan diskutere om denne adgangen til å gå fra låneavtaler er for vid eller for snever. Likevel er det slik at uansett om tinglysingen går raskt, forverrer det ikke långiverens situasjon. Det er uansett låneavtalen som avgjør om forbrukeren er bundet for eksempel til en avtale om urimelig høye renter. Om forbrukeren kan gå fra låneavtalen, vil tinglysingen ikke spille noen rolle i seg selv. Tinglysing av pant sikrer bare krav som kan gjøres gjeldende etter låneavtalen.[89]

Rask etablering av pantelån representerer ikke en økt risiko for låntakeren.[90]

5 Risiko for tap av prioritet

I tinglysing gjelder prinsippet om først tinglyst, best i rett.[91] Tinglyser man ikke i tide, risikerer man å miste en rettighet. Det er flere unntak fra og modifikasjoner av denne regelen, men det er generelt viktig at det blir tinglyst i tide, at en rettighet «får prioritet».

Dersom et dokument blir godtatt til tinglysing, regnes det som tinglyst den dagen det ble mottatt på tinglysingen.[92] Men mens dokumenter signert (og sendt) elektronisk blir regnet som mottatt på det klokkeslettet de ankommer, regnes dokumenter skrevet på papir først som innkommet kl. 21 den dagen de kommer inn.[93] Det vil si at om både du og jeg kjøper samme eiendom av A og dokumentene kommer frem til tinglysingen samtidig, går mitt kjøp foran ditt dersom jeg bruker elektronisk signatur mens du bruker håndskrevet signatur. Du mister da retten din til eiendommen, selv om du har kjøpt den.

En har vel tenkt seg at for det store flertallet av papirdokumenter som sendes med post, er det nokså tilfeldig akkurat når dokumentene ankommer tinglysingen og blir registrert der. En datamaskin kan selvsagt registrere elektroniske dokumenter automatisk akkurat idet de ankommer. Regelen sikrer at ingen papirdokumenter kommer foran andre papirdokumenter ved en tilfeldighet i håndteringen, og skaper slik sett rettferdighet, men sikrer samtidig at papirdokumentene uansett kommer etter det store flertallet av elektroniske dokumenter, og skaper slik sett urettferdighet.

Denne nyansen i prioritetsregelen er en liten risiko, for det er ikke ofte at dokumenter i konflikt med hverandre kommer inn til tinglysingen samtidig. Det kan imidlertid ha en viss prinsipiell interesse at man har valgt å la elektroniske dokumenter ha en forrang. Forrangen kommer først og fremst dem til gode som bruker elektronisk tinglysing, typisk virksomheter som banker, og ikke privatpersoner.[94]

Denne lille risikoen reduseres ytterligere ved en modifikasjon av regelen om at først tinglyst gir best rett. Er den ene rettighetshaveren en tvangskreditor, ville selv klokkeslettprioritet ikke ha hjulpet den konkurrerende rettighetshaveren som tinglyser på papir. Ved (tvangs)utlegg må nemlig den konkurrerende avtaleerververen ha tinglyst ikke bare rett før utleggstakeren, men dagen før.[95] Og ved konkursbeslag er det konkursåpningstidspunktet, og ikke tinglysingen av det, som teller;[96] tinglysingen av det konkurrerende ervervet må ha skjedd senest dagen før konkursåpningen for at det skal stå seg i forhold til konkursen.

Alt i alt er det en begrenset risiko for at en som tinglyser på gamlemåten, kommer dårligere ut etter regelen først tinglyst, best rett, enn en som tinglyser ved hjelp av en elektronisk signatur.[97]

6 Systemsviktrisiko og erstatning

Papirdokumentasjon og underskrifter for hånd oppfattes av de fleste som rimelig trygge systemer. Elektronisk dokumentasjon med elektroniske signaturer er man kanskje mer usikre på. Hva om hele systemet svikter, slik at det for eksempel blir lett urettmessig å fremstå som registrert eier av en annens eiendom? Regulerer tinglysingsloven denne typen risikoer på en god måte?

Systemet for risikohåndtering i tinglysingen er basert på en enkel forhåndskontroll supplert med erstatning for tinglysingsfeil, og ble ikke endret ved innføringen av elektronisk tinglysing. «Feil» i denne sammenhengen innebærer ikke nødvendigvis at man har brutt med de normene som gjelder for god tinglysing.[98] En kjøper av fast eiendom kan for eksempel få erstatning dersom hen har stolt på en tinglysingsattest som viste seg å være feil, eller om hen ikke får eiendommen hen har kjøpt og tinglyst rett til, fordi selgeren var registrert som eier på grunnlag av et dokument som overraskende viser seg å være falsk.[99]

Samlet sett begrenser systemet og erstatningsreglene publikums risiko ved papirtinglysing i stor grad. Selv med en begrenset kontroll i forbindelse med den enkelte tinglysing har erstatningsreglene skapt den nødvendige tilliten til systemet. Det har også stor betydning at saker om tinglysingsfeil er sjeldne.[100] Det kan imidlertid være tilfeller av tinglysingsfeil i form av falsk i tinglyste dokumenter som ingen kan eller vil rapportere om, for eksempel arvingers disposisjoner over arvelaters eiendom før arven har falt, men etter at hen har mistet rettslig handleevne. Tinglysingsfeil er derfor kanskje hyppigere enn vi tror.

Dette systemet virker også ved elektronisk tinglysing. Er en tinglysingsattest feil, får den som lider tap, erstatning uansett om feilen er en datafeil. Det er flere grunner til at dette kanskje ikke er tilstrekkelig til å opprettholde tilliten til tinglysingssystemet. Noen, til dels overlappende, eksempler:

- Brukerne har ennå ikke hatt mulighet til å erfare at de elektroniske systemene har liten risiko. Dette gjelder både risikoen ved at man selv anvender elektroniske signaturer, og ved at andre misbruker ens elektroniske signatur.
- Risikoprofilen kan være annerledes i papirbaserte og elektroniske systemer. Dersom det for eksempel skulle utvikles datamaskiner som kan knekke kodene som brukes ved elektroniske signaturer, vil dette være et mye mer omfattende problem enn enkeltstående forfalskninger. Når en ulykke rammer mange, kan det føre til bedre kompensasjon – eller dårligere. Denne usikkerheten kan oppleves som en risiko.
- Mens man klart nok kan unngå avtalebindinger ved å la være å undertegne for hånd, er det større usikkerhet knyttet til dette når det gjelder elektroniske signaturer. Kan man risikere at noen får tak i passordet ved et datainnbrudd uten at man kan bevise at det er det som har skjedd? Også dette kan oppleves som en risiko.
- Brukerne har ingen mulighet til innsyn i de sikkerhetsmekanismene som finnes; et slikt innsyn ville i seg selv kunne tenkes å være en sikkerhetsrisiko. De aller fleste brukere ville uansett ikke være i stand til å vurdere de tekniske løsningene. Manglende gjennomsiktighet kan oppleves som en risiko.
- Det kan være flere aktører involvert i et elektronisk tinglysingssystem enn i et papirbasert, og det kan oppleves som en risiko at aktørene skylder på hverandre dersom feil skjer. Ligger problemet hos leverandøren av den elektroniske signaturen eller hos tinglysingen? Muligheten for å bli en kasteball mellom forskjellige aktører når det kreves erstatning for feil, kan oppleves som en risiko.
- Leverandører av elektroniske signaturer har en begrenset undersøkelsesplikt når det gjelder identiteten til den signaturen utstedes til, og for eksempel feil i folkeregisteret kan lett forplante seg.[101] De garanterer selvsagt heller ikke mot misbruk av signaturene. Deres erstatningsansvar er uansett svært begrenset, selv når de tillates brukt i elektronisk tinglysing.[102] Har det skjedd feil ved utstedelsen av en signatur, kan da de som har stolt på den eller har måttet forholde seg til den, sitte igjen med en risiko, iallfall for å måtte ordne opp.

For å opprettholde tilliten til tinglysingen kan det etter dette være grunn til å supplere ansvarsregelen i tinglysingsloven § 35 (som er omtalt ovenfor) med et ansvar for systemsvikt. Poenget er ikke at risikoen for systemsvikt er stor, eller at et elektronisk system nødvendigvis må være helt vanntett. Poenget er at de som utformer systemet og har muligheten til å sikre kvaliteten av det, også skal ha risikoen for det i form av erstatningsansvar om noe går galt.

Noen grunn til å forsøke å lage veldig detaljerte erstatningsregler om dette er det neppe. Det er lang tradisjon i erstatningsretten for å bruke brede standardregler som for eksempel uaktsomhetsnormen som ansvarsgrunnlag. En konkretisering ville uansett neppe nytte. Siden de elektroniske systemene er laget for å være sikre, er det stort sett ikke noen konkrete hull en forsøker å tette.

Noe grunnlag for et helt objektivt ansvar utover det tingl. § 35 hjemler, er det vanskelig å se. Skadeserstatningsloven[103] § 2-1 synes imidlertid å hjemle et systemsviktansvar for staten, og det er ingen holdepunkter for å tolke tingl. § 35 slik at den utelukker ansvar etter skadeserstatningsloven. Ved vurderingen av statens ansvar etter skadeserstatningsloven § 2-1 for feil arbeidstakere har begått i tjenesten, skal det tas hensyn til «om de krav skadelidte med rimelighet kan stille til virksomheten eller tjenesten, er tilsidesatt». Etter rettspraksis trenger en ikke heller å finne en konket syndebukk ved et samvirke av tilkortkommenheter.[104] Selv om formuleringen opprinnelig ble tatt inn for å redusere det offentliges erstatningsansvar i visse tilfeller, er lovteksten ikke til hinder for en skjerpelse når rettspolitiske hensyn taler for det, som her.[105] Alt i alt skulle da alt ligge til rette for at (den hypotetiske) risikoen for systemsvikt i ordningen med elektronisk tinglysing legges der den bør ligge: på den staten som tilbyr tjenestene og utformer systemet.

Forarbeidene til endringene i tinglysingsloven, der elektronisk tinglysing ble lovregulert, synes å støtte en slik tankegang og la til grunn at dette allerede fulgte av lovteksten i skadeserstatningsloven.[106] Den systemrisikoen som måtte være forbundet med elektronisk tinglysing, ligger da hos staten i form av erstatningsansvar. Dette opprettholder den nødvendige tilliten til systemet, og risikoen for systemsvikt er slik sett i stor grad eliminert.

7 Risiko for godtroerverv av eiendommen

Det er som nevnt[107] slik at tinglysing ikke reparerer en ugyldig kontrakt eller er en gyldighetsbetingelse. Blir en ugyldig kontrakt tinglyst, kan likevel den som stoler på den, få rett etter det tinglyste på tross av ugyldigheten. Dette kalles godtroerverv (ekstinksjon). Poenget med dette er at en skal kunne stole på det som står i grunnboken, selv om det unntaksvis er galt. Dette gjør det mindre risikabelt å kjøpe fast eiendom, og den historiske eieren kan oftest beskytte seg ved å melde fra om ugyldigheten.

I forbindelse med elektronisk tinglysing kan det tenkes at for eksempel et salg av en fast eiendom blir tinglyst på grunnlag av en falsk elektronisk signatur, altså når det er en annen enn den signaturen er utstedt til, som har tastet brukerkoder mv. I slike tilfeller risikerer altså den historiske eieren å miste eiendommen ved godtroerverv etter hovedregelen skissert ovenfor, uansett om vilkårene for å gjøre hen ansvarlig etter drøftelsene ovenfor i 3.5 (uaktsomhet) ikke er til stede. Her skal det diskuteres nærmere om dette er en reell risiko ved elektroniske signaturer.

Hjemmel for godtroerverv i disse tilfellene er tinglysingsloven § 27. Bestemmelsen beskytter ikke den som har stolt på en elektronisk signatur, men den som har stolt på uriktigheter i grunnboken. Dersom en A tror hen har kjøpt en eiendom av den historiske eier H og tinglyst kjøpet, har hen ikke stolt på uriktigheter i grunnboken (men bare på den elektroniske signaturen). Det som sto i grunnboken, var jo ikke galt; det var virkelig H som var eier. Problemet var at A kjøpte av en annen. Dersom A deretter selger videre til B, stoler B på at A virkelig er eier, slik det da uriktig fremgår av grunnboken. B kan da ved godtroerverv etter omstendighetene vinne bedre rett til eiendommen enn den historiske eier H. Det er i slike tilfeller tinglysingsloven § 27 gir grunnlag for godtroerverv, slik at kjøperen B vinner rett over den historiske eieren H.

Et vilkår for godtroerverv er naturlig nok aktsom god tro. Dersom B visste eller burde vite bedre, kan hen ikke påberope seg at A uriktig sto oppført som eier i grunnboken.

Det er sikker rett (og følger av ordlyden «rett ... ervervet ved avtale») at regelen i tinglysingsloven § 27 ikke kan påberopes av tvangskreditorer, som As konkursbo. Noen tilsvarende regler finnes ikke for dem. Det vil si at tvangskreditorene til A ikke er noen risiko for den historiske eier H, heller ikke om en elektronisk signatur er misbrukt.[108] As tvangskreditorer kan bare beslaglegge det A rettmessig eier.

Avgjørende for om reglene om godtroerverv er en risiko ved elektroniske signaturer, er likevel at det er gjort unntak for «falsk» og «forfalskning» i tinglysingsloven § 27 andre ledd. Skyldes ugyldigheten (blant annet) falsk eller forfalskning, gjelder ikke hovedregelen om godtroerverv ved ugyldighet, og reglene representerer ingen spesiell risiko ved elektroniske signaturer.

Selv om jeg ovenfor har brukt uttrykket «falsk» om misbruk av elektroniske signaturer, er det ikke opplagt at unntaket i § 27 andre ledd for regelen om godtroerverv gjelder. Felleskjennetegnet for unntakene i § 27 andre ledd er nemlig at det er forhold den historiske eieren ikke lett kan beskytte seg mot, som grov tvang.[109] Men falsk ved elektroniske signaturer kan en vanligvis lett beskytte seg mot om systemet fungerer som man håper – ved å holde brukerkoder mv. hemmelig. Det er derfor ikke opplagt at falskunntaket gjelder i disse tilfellene.

Uaktsomhet er imidlertid ikke til hinder for at unntakene påberopes og godtroerverv utelukkes. Vurderingstemaet er ikke om den historiske eieren i det enkelte tilfellet lett hadde kunnet beskytte seg mot falsk, tvang o.l., men om dette typisk er vanskelig i tilfeller av falsk, tvang o.l. Falskunntaket fra godtroervervsregelen gjelder for eksempel klart nok også når forfalskningen er muliggjort av et dokument som er lett å forfalske, for eksempel fordi det var god plass til å endre eiendomsadressen (gårds- og bruksnummer). Og det har (så vidt jeg vet) aldri vært antydet at unntaket for grov tvang gjelder selv om den historiske eieren har innlatt seg med lyssky individer. På liknende måte kan det heller ikke spille noen rolle i samband med godtroerverv om den historiske eieren har vært slepphendt med brukerkoder mv.

Den uaktsomme eieren kan da påberope seg unntakene fra hovedregelen om godtroerverv, og kommer bedre ut av det enn for eksempel en eier som har blitt utsatt for tvang som ikke er grov. Slike skjevheter finnes det mange av i tingl. § 27; et annet eksempel er eieren H som kan miste eiendommen sin om den er solgt ved en avtale som er ugyldig på grunn av hens sinnssykdom. Disse skjevhetene har ingenting spesielt med elektroniske signaturer å gjøre, og bør ikke være avgjørende for tolkingen av tinglysingsloven § 27 akkurat i samband med disse.

Alt i alt må en ta ordlyden på alvor. Om en elektronisk signatur er misbrukt av en annen enn den som har brukeren til den, er det falsk. Da gjelder ikke regelen om godtroerverv i tingl. § 27 første ledd. Godtroerverv representerer da ikke noen spesiell risiko for den historiske eieren.

Noen garanti mot at den historiske eieren taper i en konflikt med en godtroende erverver, er bruk av elektroniske signaturer likevel selvsagt ikke. Blir eierens overlatelse av brukerkoder mv. til en annen ansett som en fullmakt, hefter hen selvsagt.[110] Og får eieren av en eiendom varsel for eksempel fra tinglysingen om at den er solgt uten at hen vet om det, må hen reagere enten salget har skjedd ved elektronisk tinglysing eller papirtinglysing. Eieren kan her løpe en risiko ved passivitet, men dette er ikke en risiko ved elektroniske signaturer.

8 Risiko ved automasjon

Det kan godt tenkes at en datamaskin fatter en automatisert beslutning om for eksempel å innvilge et pantelån på vegne av en bank, og besørger tinglysing av dette. Hvordan skal tinglysingslovens regler om godtroerverv anvendes i disse tilfellene, altså at man kan stole på det som står i grunnboken? Vil banken miste sin mulighet til å påberope seg reglene om godtroerverv ved automasjon, eller vil den tvert imot alltid anses for å ha vært i god tro? Iallfall oftest er det jo ikke meningsfylt å si at datamaskiner er i god eller ond tro,[111] selv om beslutninger av den typen som diskuteres her, gjerne er skjønnsmessige beslutninger basert på kunstig intelligens.

Hvis dette virkelig er et problem, er det ikke egentlig et problem ved bruk av elektroniske signaturer i tinglysing. For mens det er den som gir fra seg en rettighet, som eventuelt bruker en elektronisk signatur, er det den som får (erverver) en rettighet, som etter omstendigheten kan påberope seg reglene om godtroerverv. Denne erververen trenger vanligvis ikke å signere dokumentene som tinglyses, verken på papir eller elektronisk. Spørsmålet om en datamaskin kan være i god tro ved automasjon, oppstår derfor ikke på grunn av elektronisk tinglysing.

Automasjon er imidlertid mer og mer praktisk. Beslutninger som at banken skal be om pant i en eiendom og sende pantedokumentene til tinglysing, kan meget vel bli tatt av en maskin, særlig ved elektronisk tinglysing. Da melder spørsmålene om datamaskinens gode tro seg med full styrke.

Hadde det vært en medarbeider i banken som hadde en slik tilknytning til saken som skissert i forrige avsnitt, ville hens gode eller onde tro klart nok være relevant. Hovedsynspunktet bør være at banken (eller hvem det måtte være) ikke skal komme bedre ut ved å bruke en datamaskin i stedet.[112] Om datamaskinen «kan» være i god eller ond tro, er for så vidt irrelevant.

Utgangspunktet for datamaskinen, som for den ansatte, bør generelt være at den skal regnes som å være i god tro, altså at grunnboken er riktig. Det er først når det foreligger omstendigheter som gjør at man skjønner eller bør skjønne at grunnboken kan være gal, at man ikke lenger er i aktsom god tro. Videre undersøkelser kan imidlertid selvsagt synes å bekrefte utgangspunktet om at grunnboken er riktig. Dette innebærer at om en datamaskin som brukes til automatiserte beslutninger, ikke er slik innrettet at den ser faresignalene som et menneske ville sett, eller den ikke sørger for at det blir gjort nærmere undersøkelser når dette er nødvendig, bør dette likestilles med at den som erverver rettigheten, ikke var i aktsom god tro.[113]

Alt i alt innebærer dette at den som erverver en rettighet, verken får større eller mindre risiko ved automasjon. Speilvendingen av dette er at en konkurrerende rettighetshaver med en utinglyst rett ikke risikerer å miste rettigheten sin i større grad om det tinglyses ved hjelp av automasjon, enn om man bruker konvensjonelle rutiner. Risikobildet ved automasjon er nøytralt.

9 Avslutning

Gjennomgangen ovenfor har vist at det er en viss risiko ved elektroniske signaturer i tinglysingssammenheng, slik det også er ved underskrifter for hånd. Den tekniske risikoen er mindre ved elektroniske signaturer enn ved underskrifter for hånd. Risikoen ved at noen andre pådrar meg en forpliktelse ved å bruke min signatur, er nok noe større ved elektroniske signaturer enn ved underskrifter for hånd, men om systemet fungerer som man håper, er det mulig å beskytte seg ved å holde brukerkoder mv. hemmelig. Beskyttelsen for alle involverte ville

være bedre om det ble innført vitnekrav ved bruk av elektroniske signaturer, iallfall i en del tinglysingssammenhenger.

Systemet med elektroniske signaturer er helt avhengig av at signaturene ikke blir utstedt til feil person. Ansvaret for dette er overlatt til private utstedere, som riktignok bygger på offentlige dokumenter. Feil kan likevel skje. Det er da bemerkelsesverdig hvor begrenset ansvaret for dem som tildeler brukere til elektroniske signaturer, er, selv når det gjelder elektroniske signaturer som kan brukes i tinglysingssammenheng.

Er man bekymret, er det mulig å unngå risikoen ved elektroniske signaturer i tinglysingssammenheng ved å la være å ha rettigheter i fast eiendom eller ved ikke å få en bruker til en elektronisk signatur. Begge deler er upraktisk. En hensiktsmessig og rimelig ordning ville være om en kunne kreve å få en bruker til en elektronisk signatur med beløpsbegrensning, eller slik at den ikke kan brukes til tinglysing. En kunne også tenke seg en ordning der den som hadde to elektroniske signaturer utstedt til seg, kunne kreve at begge måtte brukes i tinglysingssammenheng.

Selv er jeg ikke bekymret. Etter å ha gått gjennom og vurdert risikoene mener jeg systemet er rimelig trygt.

Litteratur

Mads Bryde Andersen: Grundlæggende aftaleret (København: Gjellerup 2021)

Erling Eide: Bevisvurdering: usikkerhet og sannsynlighet (Oslo: Cappelen Damm 2016)

Faigman et al.: Modern scientific evidence: the law and science of expert testimony (Eagan: Thomson West 2022) s. 625-924

Thor Falkanger og Aage Thor Falkanger: Tingsrett (Oslo: Universitetsforlaget 2022)

Finansdepartementet: Høringsnotat – Forslag til ny personidentifikator, saksnr. 13/812, 23.03.

Johan Giertsen: Avtaler (Oslo: Universitetsforlaget 2021)

Viggo Hagstrøm og Are Stenvik: Erstatningsrett (Oslo: Universitetsforlaget 2019)

Study on online identity theft and identity-related crime. Final Report. A report submitted by ICF SA in cooperation with Wavestone, Center for the Study of Democracy, University of Trento, and Victims Support Europe (https://tinyurl.com/erikro145)

ITU-T Recommendation X.1254. International Standard ISO/IEC DIS 29115 (2011). Information technology – Security techniques – Entity authentication assurance framework.

Jan Kleineman: Robotrådgivning – finns det?, i Torsten Iversen et al. (red.): Festskrift til Bent Iversen (København: Adlibris 2019) s. 151

Kommunal- og distriktsdepartementet: Nasjonal strategi for eID i offentlig sektor (2023

Lantmäteriet: Lagfartskapningar – förekomst och åtgärder (dnr u2007/10895/L1, Ju2007/3171/L1) 21.10.2008

Birger Stuevold Lassen: Kontraktsrettslig representasjon: en lærebok med et avsnitt om kommisjon (Oslo: Universitetsforlaget 1992)

Förhandlingarna vid det 34:e nordiska juristmötet i Stockholm 21-23 augusti 1996: 2 (Stockholm 1997) s. 713-742

Utne Norland og Marte Eidsand Kjørven: Elektroniske signaturer og avtalebinding (https://tinyurl.com/erikro138)

Alexander Roßnagel: Beweiswirkungen elektronischer Vertrauensdienste. Neue Regelungen durch die eIDAS-Verordnung der Europäischen Union, MMR Zeitschrift für IT-Recht und Recht der Digitalisierung 2016 s. 647

Erik Røsæg: IT: Avtaleslutning og behovet for lovreform, i Lars Gorton (red.): Festskrift till Gunnar Karnell (Stockholm: Carlsson 1999) s. 657

Rundskriv for tinglysingen (https://tinyurl.com/erikro126), sist oppdatert 24.10.

Victor Titov et al.: Digital Transformation of Signatures: Suggesting Functional Symmetry Approach for Loan Agreements, 10 Computation (2022) 106 https://doi.org/10.3390/computation10070106

Olav Torvund: Formueretten i informasjonssamfunnet (Oslo: Universitetsforlaget 2022)

Amund Bjøranger Tørum: Direktekrav: særlig om direktekrav ved kjøp, tilvirkning og entreprise: formuerettslige analyser i komparativ belysning (Oslo: Universitetsforlaget 2007)

Henrik Udsen: Den digitale signatur: ansvarsspørgsmål (København: Thomson 2002)

Peer Philip Wagner: Das elektronische Dokument im Zivilprozess, Juristische Schulung 2016 s. 29.

Geir Woxholth: Avtalerett (Oslo: Gyldendal 2021)

Alessio Zaccaria et al. (red.): EU eIDAS regulation: Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market. Article-by-article commentary (München: Nomos/Beck/ Hart 2020)

Marianne M. Rødvei Aagaard: Kreditgivares ersättningsanspråk efter obehörig användning av bank-id. Kommentar till Høyesteretts avgörande HR-2020-2021-A, SvJT 2021 s. 235

Thea Melsbø Aarseth et al.: Trygge forbrukere: Sluttrapport analysefasen (BITS 2023, upublisert)

1 Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF (eIDAS-forordningen) art. 25, som gjennomført ved lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester) § 1.

2 Art. 25 er tolket av EU-domstolen i sak C-362/21«'Ekofrukt' EOOD», se særlig premiss 35.

3 Lov 7. juni 1935 nr. 2 om tinglysing (tingl.) kap. 2, lov 6. juni 2003 nr. 39 om burettslag (burettslagslova) kap. 6.

4 Se f.eks. tingl. §§ 20 og 27.

5 Se https://tinyurl.com/erikro123.

6 Se f.eks. lov 17. juni 2005 nr. 79 om akvakultur (akvakulturloven) § 18 fjerde ledd.

7 Ot.prp.nr.82 (1999–2000) Om lov om elektronisk signatur s. 50-51 med støtte i eIDAS-forordningen avsnitt 23 i fortalen.

8 Dette gjør at det blir lite fri flyt av elektroniske signaturer over landegrensene, i strid med et av formålene for eIDAS, og at det blir dårlig konkurranse mellom tilbyderne av tillitstjenester som elektroniske signaturer, i strid med konkurranserettslige prinsipper.

9 «Land registers» – eIDAS-forordningen avsnitt 21 i fortalen. Unntaket er med i forslaget til revisjon av forordningen som sirkulerer, se Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity COM(2021) 281 final 3.6.2021 avsnitt 19 i fortalen.

10 Forskrift 3. november 1995 nr. 875 om tinglysing (tinglysingsforskriften) §§ 2 flg.

11 Se https://tinyurl.com/erikro128. Systemet er under avvikling.

12 Statens kartverk: Avtale om tilgang og bruk av system for elektronisk tinglysing (versjon 4 2017).

13 Elektronisk tinglysing. Forslag til endringer i tinglysingsloven mv. for å tilrettelegge for elektronisk tinglysing. Rapport avgitt til Justis- og politidepartementet 1.6.2010 (https://tinyurl.com/erikro125; heretter 2010-utredningen) kap. 5. Jeg ledet denne gruppen.

14 Et eksempel på et bilde av et elektronisk signert dokument og hvordan det ser ut i Acrobat Reader, finnes på https://tinyurl.com/erikro124.

15 Victor Titov et al.: Digital Transformation of Signatures: Suggesting Functional Symmetry Approach for Loan Agreements, 10 Computation (2022) 106 https://doi.org/10.3390/computation10070106 foreslår en sammenlikningsmetodikk basert på «fuzzy logic».

16 Tinglysingsforskriften § 3, jf. eIDAS- forordningen art. 8, Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market og Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Om sikkerhetsnivåene se Alessio Zaccaria et al. (red.): EU eIDAS regulation: Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market. Article-by-article commentary (München: Nomos/Beck/ Hart 2020) s. 217 flg.

17 I praksis tilbyr banker bare elektronisk signatur av typen BankID til kundene sine, og svært mange pantelån ytes av banker.

18 Disse signaturene bygger på sertifikater på nivå kvalifisert (https://tinyurl.com/erikro148), men mangler dokumentasjon på at metoden for å knytte sertifikatet sammen med det som signeres, og den som signerer, er på nivå kvalifisert (eIDAS-forordningen art. 29; https://tinyurl.com/erikro149). Denne siste begrensingen er underkommunisert både av myndighetene og av dem som selger de elektroniske signaturene. Takk til Marte Kjørven og forskningsprosjektet SODI, som har gjort meg oppmerksom på dette.

19 Se Prop.71 LS (2017–2018) Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), og samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordningen i EØS-avtalen s. 26 og motsetningsvis nedenfor i note 54 om tysk rett.

20 Slik EU-domstolens i sak C-362/21«'Ekofrukt' EOOD» premiss 37.

21 Slik også *ibid*. premiss 36 om at det er medlemsstatene som i utgangspunktet avgjør hvilket sikkerhetsnivå som trengs på elektroniske signaturer i forskjellige sammenhenger.

22 Se mer tekniske fremstillinger f.eks. på https://en.wikipedia.org/wiki/Digital_signature og NOU 2001:10 Uten penn og blekk – Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen punkt 3.2. 2010-utredningen (note 13) beskriver dette i kap. 4.

23 Plikten til hemmelighold følger av avtalen med utsteder, se f.eks. Sparebank 1: Avtalevilkår for PersonBankID (https://tinyurl.com/erikro127) art. 9 nr. 1. I de fleste praktiske tilfeller vil imidlertid plikt til hemmelighold følge også av lov 18. desember 2020 nr. 146 om finansavtaler (finansavtaleloven) § 3-19, som bare lovfester avtalens plikter innenfor sitt virkeområde (Prop.92 LS (2019–2020) Lov om finansavtaler (finansavtaleloven) og samtykke til godkjennelse av EØS-komiteens beslutninger nr. 125/2019 og 130/2019 av 8. mai 2019 om innlemmelse i EØS-avtalen av direktiv 2014/17/EU om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål (boliglåndirektivet) og delegert kommisjonsforordning (EU) nr. 1125/2014 s. 358). Plikten til hemmelighold er tatt inn i UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 (New York: United Nations 2002) art. 8.

24 Faigman et al.: Modern scientific evidence: the law and science of expert testimony (Eagan: Thomson West 2022) s. 625-924; Erik Røsæg: IT: Avtaleslutning og behovet for lovreform, i Lars Gorton (red.): Festskrift till Gunnar Karnell (Stockholm: Carlsson 1999) s. 657, 676; Erling Eide: Bevisvurdering: usikkerhet og sannsynlighet (Oslo: Cappelen Damm 2016) s. 64; Olav Torvund: Formueretten i informasjonssamfunnet (Oslo: Universitetsforlaget 2022) s. 151.

25 Se lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester) § 3.

26 Se tingl. § 13 første ledd, jf. § 14. I tinglysingsloven er terminologien for den som er registrert rettighetshaver, at hen har grunnbokshjemmel til rettigheten, og beskyttelsen gjelder den som tidligere har fått grunnbokshjemmel (på grunnlag av elektronisk tinglysing eller papirtinglysing).

27 Etter eIDAS-forordningen avsnitt 5 er det mulig å lage elektroniske segl for en virksomhet, som etter nasjonal rett kan overflødiggjøre behovet for å vise at den som brukte seglet, kunne representere virksomheten. Dette vil si at en bruker til en elektronisk signatur utstedes til en virksomhet som slik.

28 Jeg ser foreløpig bort fra «juridiske personer», som selskaper, jf. noten ovenfor. Kravet om fødselsnummer gjelder også ved papirtinglysing, jf. tinglysingsforskriften § 4. Ved behov, som f.eks. tinglysingen har, gir utstedere av elektroniske signaturer ut fødselsnummer, se f.eks. Sparebank 1 avtalevilkår art. 8(3) og e-post fra Statens kartverk 2.2.2023 punkt 1.

29 Fødselsnummer er ikke fortrolige opplysninger, se lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven) § 13 andre ledd. En annen sak er at man kan gjøre det vanskeligere for svindlere – og alle andre – om man holder det for seg selv. Slik sett er fødselsnummer litt i samme stilling som mellomnavn og bankkontonummer. Selv om man kjenner bankkontonummeret mitt, skal man jo ikke få tilgang til pengene på kontoen min. I rapporten Finansdepartementet: Høringsnotat – Forslag til ny personidentifikator, saksnr. 13/812, 23.03.2017 punkt 5.3 blir det nevnt at myndighetene har sett seg lei på at kjennskap til fødselsnummer brukes som legitimasjon.

30 Torvund, Formueretten s. 181. Kommunal- og distriktsdepartementet: Nasjonal strategi for eID i offentlig sektor (2023) punkt 2.6 erkjenner imidlertid: «Det er en risiko for at det kan være registrert falske eller uriktige identiteter i Folkeregisteret, og at det på grunnlag av dette kan bli utstedt et ID-bevis med uriktig identitet.»

31 Se Torvund, Formueretten s. 200; Nasjonal strategi for eID punkt 2.6.

32 D-en henger igjen fra gammelt av og står for Direktoratet for sjømenn (https://tinyurl.com/erikro129).

33 Forskrift 14. juli 2017 nr. 1201 til folkeregisterloven (folkeregisterforskriften) § 2-2-4.

34 Se ibid. § 3-2-1.

35 Tinglysingen kontrollerer i dag ikke om eksisterende D-nummer er utstedt etter identitetskontroll, men krever selv legitimasjon av dem som ikke har D-nummer, og som det derfor skal søkes om D-nummer for, jf. e-post fra Statens kartverk 2.2.2023 punkt 2. Selv denne siste ordningen er ansett utilfredsstillende, se brev fra Kartverket til Skattedirektoratet 30.10.2012 (Skattedirektoratets saksnr. 2011/1133940).

36 Se ovenfor i avsnitt 2.2.

37 Forskrift 21. november 2019 nr. 1578 om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften) § 18.

38 Jf. ibid. punkt 3.

39 Rundskriv for tinglysingen (https://tinyurl.com/erikro126), sist oppdatert 24.10.2022 punkt 3.2 problemstilling 2. Dette er noe annet enn fullmakter til å sende inn andres dokumenter til tinglysing, se om dette https://tinyurl.com/erikro130.

40 Torvund, Formueretten s. 243 flg.

41 E-post fra Statens kartverk 2.2.2023 punkt 1. EU-domstolen har tolket eIDAS-forordningen slik at man skal se bort fra transkriberingsproblemer, se sak C-362/21«'Ekofrukt' EOOD», konklusjonens avsnitt 4.

42 Slik eIDAS-forordningen art. 24. Tilsvarende regulering finnes i Kommisjonens gjennomføringsforordning (EU) 2015/1502 av 8. september 2015 om fastsettelse av tekniske minstespesifikasjoner og minstekrav til framgangsmåter for sikkerhetsnivåene for elektroniske identifikasjonsmidler i henhold til artikkel 8 nr. 3 i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked, som i noen grad bygger på den internasjonale standarden ITU-T Recommendation X.1254. International Standard ISO/IEC DIS 29115 (2011). Information technology – Security techniques – Entity authentication assurance framework.

43 Bits AS: Regler om BankID. Fastsatt av Finans Norge Servicekontor etter behandling i Bransjestyre betalingsformidling og infrastruktur 28.11.2013. Endret av Bits AS 18.05.2022 (https://tinyurl.com/erikro131) art. 10.3.

44 Den nå opphevede forskrift 9. desember 1999 nr. 1263 om pass (passforskriften) § 7.

45 Jeg bygger her på egen erfaring.

46 Se f.eks. Sparebank 1 avtalevilkår art. 6(2), men motsatt Buypass AS: Kundeavtale versjon 8.0, publisert 23.12.2020, gyldig fra 11.01.2021 (https://tinyurl.com/erikro132) art. 8.2.

47 Bits' kundeavtale art. 10.2.

48 Buypass' kundeavtale art. 8.2 godtar «elektronisk fremmøte».

49 Se om begrepet Study on online identity theft and identity-related crime. Final Report. A report submitted by ICF SA in cooperation with Wavestone, Center for the Study of Democracy, University of Trento, and Victims Support Europe (https://tinyurl.com/erikro145) s. 11 flg.

50 Om virkningen av tinglysing for andre enn avtalepartene (en «tredjeperson»), se nedenfor i 7.

51 Se ovenfor i 2.3.

52 Nasjonal strategi for eID punkt 3.1.

53 Muligheten er nevnt for BankID, men ikke prioritert, i Thea Melsbø Aarseth et al.: Trygge forbrukere: Sluttrapport analysefasen (BITS 2023, upublisert). Se om denne muligheten også Torvund, Formueretten s. 208 flg. I eIDAS-forordningen avsnitt 37 i fortalen synes man mest opptatt av slike begrensninger i utsteders interesse. I Henrik Udsen: Den digitale signatur: ansvarsspørgsmål (København: Thomson 2002) s. 68 fremholdes det at begrensninger bør kunne gjøres gjeldende på tross av at den som signerte elektronisk, ønsket å binde seg.

54 Det verserer et spørsmål for EU-domstolen om det skal presumeres at en elektronisk signatur har en spesiell beviskraft, se sak C-466/22«V.B. Trade». I Tyskland er det en viss tradisjon for en slik tenkemåte, når det gjelder både elektroniske og håndskrevne signaturer, se Alexander Roßnagel: Beweiswirkungen elektronischer Vertrauensdienste. Neue Regelungen durch die eIDAS-Verordnung der Europäischen Union, MMR Zeitschrift für IT-Recht und Recht der Digitalisierung 2016 s. 647; Peer Philip Wagner: Das elektronische Dokument im Zivilprozess, Juristische Schulung 2016 s. 29.

55 Se https://tinyurl.com/erikro137.

56 Statens kartverk: Avtale om tilgang og bruk av system for elektronisk tinglysing (versjon 4 2017).

57 Lov 1. juni 2018 nr. 23 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven) og forskrift 14. september 2018 nr. 1324 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften).

58 HR-2017-639-U.

59 En arving som eventuelt har misbrukt den elektroniske signaturen, er neppe interessert i å gjøre dette.

60 Finansavtaleloven § 3-7.

61 2010-utredningen punkt 8.3 (note 13).

62 Se tinglysingsforskriften § 3.

63 Kommunal- og moderniseringsdepartementet: Høringsnotat – forslag til endringer i tinglysingsforskriften m.m. (elektronisk tinglysing) 22.6.2015 punkt 3.3.3.

64 HR-2020-2021-Aavsnitt 104.

65 Se slik uttrykkelig UNCITRAL Model Law art. 8(2), jf. veiledningen avsnitt 129 og 141.

66 Se f.eks. Mads Bryde Andersen: Grundlæggende aftaleret (København: Gjellerup 2021) s. 52 flg.

67 Se f.eks. Geir Woxholth: Avtalerett (Oslo: Gyldendal 2021) s. 241 flg.; Johan Giertsen: Avtaler (Oslo: Universitetsforlaget 2021) s. 369 flg.; Birger Stuevold Lassen: Kontraktsrettslig representasjon: en lærebok med et avsnitt om kommisjon (Oslo: Universitetsforlaget 1992) s. 32-39.

68 Ovenfor i avsnitt 2.3 om hemmelighold av brukerkoder mv.

69 Woxholth, Avtalerett s. 253.

70 Denne muligheten er drøftet i denne antologien av Line Utne Norland og Marte Eidsand Kjørven: Elektroniske signaturer og avtalebinding (https://tinyurl.com/erikro138), som ikke anbefaler den.

71 Lov 18. mai 1979 nr. 18 om foreldelse av fordringer (foreldelsesloven) § 9.

72 HR-2012-672-A.

73 Svensk skadeståndslag (1972:207) 2 kap. 2 §; finsk skadeståndslag 412/74 5 kap. 1 §. Det er unntak for grov uaktsomhet.

74 Marianne M. Rødvei Aagaard: Kreditgivares ersättningsanspråk efter obehörig användning av bank-id. Kommentar till Høyesteretts avgörande HR-2020-2021-A, SvJT 2021 s. 235, 238 flg.

75 Se nærmere i avsnitt 2.3 ovenfor.

76 HR-2015-537-A Bori, HR-2017-1834-A Branncelle, HR-2020-312-A Solem og HR-2021-2201-A.

77 Disse sakene dreier seg også om andre spørsmål, som ikke skal drøftes her.

78 HR-2015-537-A Bori avsnitt 26, HR-2021-2201-Aavsnitt 66.

79 Altså en slik alminnelig handlingsnorm som gjelder alle og enhver, se Amund Bjøranger Tørum: Direktekrav: særlig om direktekrav ved kjøp, tilvirkning og entreprise: formuerettslige analyser i komparativ belysning (Oslo: Universitetsforlaget 2007) s.

499. I denne retningen HR-2020-2021-Apremiss 54.

80 Se ovenfor i avsnitt 2.3 om plikt til hemmelighold av brukerkoder mv.

81 Å forsettlig utstyre en annen med brukerkoder mv. til ens egen elektroniske signatur kan nok være medvirkning til og/eller forsøk på dokumentfalsk etter lov 20. mai 2005 nr. 28 om straff (straffeloven) § 361.

82 European Convention om Human Rights 1950 (https://tinyurl.com/erikro133) art. 8 om beskyttelse av hjem og familieliv og dens protokoll 1 art. 1 om beskyttelse av eiendom.

83 Se https://tinyurl.com/erikro134 om Verdensbankens Doing Business Project.

84 Europaparlaments- og rådsdirektiv 2002/65/EF av 23. september 2002 om fjernsal av finansielle tenester til forbrukarar, og om endring av rådsdirektiv 90/619/EØF og av direktiv 97/7/EF og 98/27/EF art. 6. Europaparlaments- og rådsdirektiv 2014/17/EU av 4. februar 2014 om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål og om endring av direktiv 2008/48/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 har ikke slike regler.

85 Europaparlaments- og rådsdirektiv 2008/48/EF av 23. april 2008 om forbrukerkredittavtaler og om oppheving av rådsdirektiv 87/102/EØF (forbrukerkredittdirektivet) art. 14.

86 Se ibid. art. 2(2)(a). Dette er foreslått opprettholdt i Proposal for a Directive of the European Parliament and of the Council on consumer credits COM(2021) 347 final 30.6.2021.

87 Direktiv 2002/65/EFart. 6(3).

88 Finansavtaleloven § 3-41.

89 Se slik forutsetningsvis lov 26. juni 1992 nr. 86 om tvangsfullbyrdelse § 11-2.

90 2010-utredningen kap. 10 (note 13) foreslår heller ikke regler i denne sammenheng, men peker på at reglene om dokumentavgift kan være et særlig problem ved rask tinglysing når angrefrist gjøres gjeldende. Departementet ser imidlertid ikke urimeligheten her, se Prop.53 L (2013–2014) Endringer i tinglysingsloven mv. (elektronisk tinglysing) s. 39.

91 Se tingl. § 20.

92 Se nærmere tinglysingsforskriften § 11.

93 Ibid.

94 De som bruker elektronisk tinglysing, har også den fordelen at de ikke trenger å bruke formularene for skjøter etc. som gjelder for papirdokumenter, se ibid. § 2. Det er ikke godt å si om en privatperson taper tid på å finne frem til og fylle ut et slikt formular.

95 Se tingl. § 20 andre ledd. Det samme gjelder etter ordlyden arrest og sikkert annen midlertidig sikring, jf. lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven) del 7.

96 Se tingl. § 23. Regelen om at rettigheter må tinglyses dagen før konkursåpning eller utlegg tas, skriver seg fra den tiden en slik regel var en måte en kunne sikre at de konkurrerende ervervene virkelig var tinglyst før utlegget eller konkursåpningen. Når regelen ble beholdt etter at klokkeslettprioritet ble innført, har nok dette å gjøre med en forestilling om at den ga tvangskreditorene en rettmessig fordel, se Prop.53 L (2013–2014)s. 46.

97 2010-utredningen (note 13) godtar også dette, se s. 39.

98 HR-2014-1465-Uavsnitt 23.

99 Se tingl. § 35.

100 I Sverige har en undersøkt forsøk på svindel systematisk, se Lantmäteriet: Lagfartskapningar – förekomst och åtgärder (dnr u2007/10895/L1, Ju2007/3171/L1) 21.10.2008. Der regner en med at det er omtrent fem tilfeller i året, se https://tinyurl.com/erikro136. I Norge og Danmark forekommer saker om falsk ved tinglysing i fast eiendom sjelden eller aldri (e-post fra Statens kartverk 10.11.2022, e-post fra Tinglysningsretten i Hobro 14.11.2022). En rundspørring ga inntrykk av at det samme gjelder andre norske rettighetsregistre (e-poster fra Skipsregistrene 18.11.2022, Plantesortsnemnda 18.11.2022, Brønnøysundregistrene 18.11.2022, Petroleumsregisteret 21.11.2022, Luftfartøyregisteret 23.11.2022 og Patentstyret 24.11.2022). Heller ikke det digitaliserte registeret for internasjonale rettigheter i luftfartøyer hadde hatt saker om falsk (e-post fra Aviareto Limited 18.11.2022).

101 Se ovenfor i avsnitt 3.3.

102 Se f.eks. Sparebank 1 avtalevilkår art. 14 om uaktsomhetsansvar (riktignok med omvendt bevisbyrde) begrenset til kr 100 000 i disse tilfellene. I Buypass' kundeavtale art. 3.2 er ansvarsgrensen enda lavere – kr 5000 pr. transaksjon.

103 Lov 13. juni 1969 nr. 26 om skadeserstatning (skadeserstatningsloven).

104 Viggo Hagstrøm og Are Stenvik: Erstatningsrett (Oslo: Universitetsforlaget 2019) s. 241 flg.

105 Se ibid. s. 253 flg.

106 Prop.53 L (2013–2014)kap. 14.

107 Ovenfor i avsnitt 3.4.

108 Ved beslag av fast eiendom av tvangskreditoren kreves for øvrig ikke den registrerte eierens underskrift, jf. tingl. § 13, som etter ordlyden bare gjelder frivillige disposisjoner.

109 Thor Falkanger og Aage Thor Falkanger: Tingsrett (Oslo: Universitetsforlaget 2022) s. 692.

110 Se ovenfor i avsnitt 3.5.

111 Torvund, Formueretten s. 89.

112 Se i denne retning fra andre områder f.eks. Røsæg i Förhandlingarna vid det 34:e nordiska juristmötet i Stockholm 21-23 augusti

1996: 2 (Stockholm 1997) s. 713-742, 735 og Jan Kleineman: Robotrådgivning – finns det?, i Torsten Iversen et al. (red.): Festskrift til Bent Iversen (København: Adlibris 2019) s. 151-165.

113 Torvund, Formueretten s. 247.