

Elektroniske signaturer og tinglysing

Forfatter: Røsæg, Erik

Publiseringsdato: 6. oktober 2023

Publisert av: Karnov forlag

Inngår i artikkelsamling: *Bruk og misbruk av elektronisk identifikasjon* – ISBN 978-82-93816-31-7

Lenke til hele publikasjonen i Lovdata Pro: <https://lovdata.no/pro/KARNOV/karnov-2022-03>

Fagfellevurdert artikkel

Artikkelen ble publisert 6. oktober 2023. Kilder det er lenket til, kan senere ha blitt erstattet eller fjernet.

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 forpliktete 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

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) artikkel 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 Artikkel 25 er tolket av EU-domstolen i sak C-362/21 «'Ekofrukt' EOOD», se særlig premiss 35.

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

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 borettslagsrettigheter³) 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 rettighetsregistre⁵ 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 som ser ut til å være undertegnet med penn på vanlig måte. Rettslig sett er det ofte adgang for registrene til å motta kommunikasjon elektronisk fordi

³ Lov [7. juni 1935 nr. 2](#) om tinglysing (tingl.) [kapittel 2](#), lov [6. juni 2003 nr. 39](#) om burettslag (burettslagslova) [kapittel 6](#).

⁴ Se f.eks. tingl. §§ [20](#) og [27](#).

⁵ Se [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.

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

tinglysingsloven [kapittel 2](#) er gitt tilsvarende anvendelse,⁶ eller med basis i den alminnelige regelen om aksept av elektroniske signaturer i [eIDAS-forordningen](#) artikkel 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 og få et opplegg tilpasset sine datasystemer.¹¹ Det er mitt inntrykk at systemet fungerer godt.

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 Europaparlaments- og rådsforordning [\(EU\) nr. 910/2014](#) av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked 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» – Europaparlaments- og rådsforordning [\(EU\) nr. 910/2014](#) av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked 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 Statens kartverk: [Avtale om tilgang og bruk av system for elektronisk tinglysing](#) (versjon 4 2017).

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

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 tilkorkommenheter).¹² 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.¹³

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 punkt 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 punkt 3. Her i punkt 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.¹⁴ Like lite

¹² [Elektronisk tinglysing. Forslag til endringer i tinglysingsloven mv. for å tilrettelegge for elektronisk tinglysing. Rapport avgitt til Justis- og politidepartementet 1.6.2010](#) (heretter 2010-utredningen) [kapittel 5](#). Jeg ledet denne gruppen.

¹³ Et eksempel på [et bilde av et elektronisk signert dokument og hvordan det ser ut i Acrobat Reader](#) finnes på nett.

¹⁴ Victor Titov mfl., [Digital Transformation of Signatures: Suggesting Functional Symmetry Approach for Loan Agreements](#), 10 Computation, 2022, s. 106 foreslår en sammenlikningsmetodikk basert på «fuzzy logic».

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 tinglysningsforskriften kan underskrifter i tinglysningssammenheng være elektroniske om de bygger på en «eID-ordning» på nivå «høyt» – det høyeste – etter eIDAS-forordningens system.¹⁵ 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.¹⁶

En «eID-ordning» gir en entydig identifikasjon av noen. Skal den gi mening i tinglysningssammenheng, må identifikasjonen knyttes til dokumentene som sendes til tinglysning, og til et eventuelt samtykke til tinglysning etter tinglysningsloven § 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 tinglysning er ikke på det høyeste nivået for elektroniske underskrifter («kvalifisert»), og regelen i [eIDAS-forordningen](#) artikkel 25 nr. 2 om at slike elektroniske signaturer har samme rettsvirkning som håndskrevne, får ikke anvendelse.¹⁷ Det spiller liten rolle. I norsk rett har selv en

¹⁵ Tinglysningsforskriften § 3, jf. Europaparlaments- og rådsforordning [\(EU\) nr. 910/2014](#) av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked artikkel 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 mfl., 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. Nomos/Beck/ Hart, 2020, s. 217 flg.

¹⁶ I praksis tilbyr banker bare elektronisk signatur av typen BankID til kundene sine, og svært mange pantelån ytes av banker.

¹⁷ Signaturene som tilbys i Norge, er avanserte signaturer som bygger på sertifikater på nivå kvalifisert, men er derimot ikke fremstilt ved hjelp av et «kvalifisert elektronisk signaturfremstillingssystem», og oppfyller derfor ikke kravene til å være kvalifiserte elektroniske signaturer etter Europaparlaments- og rådsforordning [\(EU\) nr. 910/2014](#) av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked artikkel 3 nr. 12, jf. artikkel 29. De er derfor ikke listet i [European Commission: Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices](#). Denne 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.

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

håndskrevet underskrift uansett ingen spesiell rettsvirkning.¹⁸ 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.¹⁹ 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](#) artikkel 25 nr. 1.²⁰ 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.²¹ 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.²² Brukeren ser ikke disse, men den hemmelige koden holdes hemmelig ved hjelp av for eksempel et passord.

¹⁸ 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.

¹⁹ Slik EU-domstolens i sak [C-362/21](#) «'Ekofrukt' EOOD» premiss 37.

²⁰ Slik også [C-362/21](#) premiss 36 om at det er medlemsstatene som i utgangspunktet avgjør hvilket sikkerhetsnivå som trengs på elektroniske signaturer i forskjellige sammenhenger.

²¹ Se mer tekniske fremstillinger f.eks. på [Wikipedia, oppslagsord 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](#) beskriver dette i [kapittel 4](#).

²² Plikten til hemmelighold følger av avtalen med utsteder, se f.eks. [Sparebank 1: Avtalevilkår for PersonBankID](#) punkt 4.1. I de fleste praktiske tilfeller vil imidlertid plikt til hemmelighold følge også av lov [18. desember](#)

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

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 skriftekspert, tid og penger, og sikkerheten i verifiseringen er langt dårligere enn man skulle tro.²³ 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

[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 godkjenning 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](#). United Nations, 2002, artikkel 8.

²³ Faigman mfl., *Modern scientific evidence: the law and science of expert testimony*, Thomson West, 2022, s. 625–924, Erik Røsæg, «IT: Avtaleslutning og behovet for lovreform», i Lars Gorton, red., *Festskrift till Gunnar Karnell*, Carlsson, 1999, s. 657, Erling Eide, *Bevisvurdering: usikkerhet og sannsynlighet*, Cappelen Damm, 2016, s. 64 og Olav Torvund, *Formueretten i informasjonssamfunnet*, Universitetsforlaget, 2022, s. 151.

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

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, sjønt 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

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

med dem som tilbyr signeringstjenester,²⁴ 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.²⁵ 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 punkt 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.²⁶ De tekniske løsningene som er diskutert ovenfor i punkt 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 punkt 3.5 nedenfor.

Utgangspunktet for både elektroniske signaturer og innføringen i grunnboken er fødselsnummer e.l.²⁷ Da har man identifisert en person så entydig og offisielt det lar seg

²⁴ 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](#).

²⁵ 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).

²⁶ Etter Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked 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.

²⁷ 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

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

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.²⁸

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 punkt 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 punkt 3.3 og det andre nedenfor i punkt 3.4. Det er bare når det gjelder det siste punktet at de tekniske løsningene skissert ovenfor i punkt 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 annen side 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 o.l.²⁹ 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

utstedere av elektroniske signaturer ut fødselsnummer, se f.eks. [SpareBank 1 avtalevilkår](#) punkt 8.2 og e-post fra Statens kartverk 2.2.2023 punkt 1.

²⁸ 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.

²⁹ Forskrift [3. november 1995 nr. 875](#) om tinglysing § 4 sjette ledd.

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

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.

³⁰ Olav Torvund, *Formueretten i informasjonssamfunnet*, Universitetsforlaget, 2022, 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 Olav Torvund, *Formueretten i informasjonssamfunnet*, Universitetsforlaget, 2022, s. 200 og Kommunal- og distriktsdepartementet, [Nasjonal strategi for eID i offentlig sektor](#), 2023, punkt 2.6.

³² D-en henger igjen fra gammelt av og står for Direktoratet for sjømenn, se [Wikipedia, oppslagsord Fødselsnummer](#).

³³ Forskrift [14. juli 2017 nr. 1201](#) til folkeregisterloven (folkeregisterforskriften) [§ 2-2-4](#).

³⁴ Se forskrift [14. juli 2017 nr. 1201](#) til folkeregisterloven (folkeregisterforskriften) [§ 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 punkt 2.2.

³⁷ Forskrift [21. november 2019 nr. 1578](#) om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften) [§ 18](#).

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

En tredje variant, ved siden av fødselsnummer og D-nummer, er organisasjonsnummer. For elektronisk tinglysing kreves det norsk organisasjonsnummer. Et utenlandsk selskap kan få norsk organisasjonsnummer ved registrering i Enhetsregisteret om det ikke er registrert i et annet register og har fått norsk organisasjonsnummer i den forbindelsen.³⁸ At den som sender inn noe til tinglysing, kan handle på vegne av selskapet, kan dokumenteres ved at virksomhetens egen elektroniske signatur (virksomhetssertifikat) brukes, men det kan 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 punkt 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

³⁸ Forskrift [9. februar 1995 nr. 114](#) om registrering av juridiske personer m.m. i Enhetsregisteret [§ 8](#).

³⁹ [Statens kartverk: Rundskriv for tinglysing](#), sist oppdatert 11.04.2025 [punkt 3.2](#) problemstilling 2. Dette er noe annet enn fullmakter til å sende inn andres dokumenter til tinglysing, se om dette [Statens kartverk: Fullmakter ved elektronisk tinglysing](#), sist oppdatert 19.06.2024.

⁴⁰ Olav Torvund, *Formueretten i informasjonssamfunnet*, Universitetsforlaget, 2022, s. 243 flg.

⁴¹ E-post fra Statens kartverk 2.2.2023 punkt 1. EU-domstolen har tolket Europaparlaments- og rådsforordning [\(EU\) nr. 910/2014](#) av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked slik at man skal se bort fra transkriberingsproblemer, se sak [C-362/21](#) «'Ekofrukt' EOOD», konklusjonens avsnitt 4.

⁴² Slik Europaparlaments- og rådsforordning [\(EU\) nr. 910/2014](#) av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked artikkel 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

kan bygge på pass,⁴³ men det er ikke veldig lenge siden pass ble utstedt på grunnlag av førerkort⁴⁴ eller dåpsattest⁴⁵, og er pass først utstedt, vil det gamle kunne danne grunnlag for et nytt pass og altså en elektronisk signatur.

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,⁴⁶ 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.⁴⁷

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 punkt 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 punkt 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.

ISO/IEC DIS 29115 (2011). Information technology – Security techniques – Entity authentication assurance framework.

⁴³ [Bits AS: Regler om BankID](#), Fastsett av Finans Norge Servicekontor etter behandling i Bransjestyre betalingsformidling og infrastruktur 28.11.2013. Sist endret av Bits AS 23.05.2023, punkt 10.3.

⁴⁴ Den nå opphevede forskrift [9. desember 1999 nr. 1263](#) om pass (passforskriften) [§ 7](#).

⁴⁵ Jeg bygger her på egen erfaring.

⁴⁶ [Bits AS: Regler om BankID](#) artikkel 10.2.

⁴⁷ [Kundeavtale for Buypass ID – smartkort, mobil og ID-nøkkel](#) (versjon 8.1) artikkel 8.2 godtar «elektronisk fremmøte».

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

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.⁴⁸

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.⁴⁹ 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.⁵⁰ 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.⁵¹ 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

⁴⁸ Se om begrepet i [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, s. 11 flg.

⁴⁹ Om virkningen av tinglysing for andre enn avtalepartene (en «tredjeperson»), se nedenfor i punkt 7.

⁵⁰ Se ovenfor i punkt 2.3.

⁵¹ Kommunal- og distriktsdepartementet. [Nasjonal strategi for eID i offentlig sektor](#), 2023, punkt 3.1.

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.⁵²

Det er i dag ingen mekanismer som sikrer bevis i slike situasjoner som i eksempelet.⁵³ 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,⁵⁴ men slike meldinger vil typisk sønne 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.⁵⁵ Hvitvaskingsreglene krever at mellommenn, som eiendomsめklere om det brukes, skal klargjøre partenes identitet, men ikke at disposisjonsviljen skal undersøkes.⁵⁶ 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.⁵⁷ I vårt eksempel ville dette altså si den senile eller døde moren. Hun – eller arvingen hennes – kunne⁵⁸ føre bevis for at det ikke var hun som tastet brukerkodene mv., eller at brukerkodene mv. har kommet på avveier uten hennes medvirkning. Bevisbyrderreglene er nå kraftig modifisert, iallfall på finansavtalelovens område.⁵⁹ Det synes uansett mer formålstjenlig å sørge for bevis enn å bruke bevisbyrderregler.

⁵² Muligheten er nevnt for BankID, men ikke prioritert, i Thea Melsbø Aarseth mfl., *Trygge forbrukere: Sluttrapport analysefasen*, BITS, 2023, upublisert. Se om denne muligheten også Olav Torvund, *Formueretten i informasjonssamfunnet*, Universitetsforlaget, 2022, s. 208 flg. I Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked avsnitt 37 i [fortalen](#) synes man mest opptatt av slike begrensninger i utsteders interesse. I Henrik Udsen, *Den digitale signatur: ansvarsspørsmål*, Thomson, 2002, s. 68 fremholdes det at begrensninger bør kunne gjøres gjeldende på tross av at den som signerte elektronisk, ønsket å binde seg.

⁵³ 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.

⁵⁴ Se [Statens Kartverk: Melding fra kartverket](#).

⁵⁵ Statens kartverk: [Avtale om tilgang og bruk av system for elektronisk tinglysing](#) (versjon 4 2017).

⁵⁶ 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).

⁵⁷ [HR-2017-639-U](#).

⁵⁸ En arving som eventuelt har misbrukt den elektroniske signaturen, er neppe interessert i å gjøre dette.

⁵⁹ Finansavtaleloven [§ 3-7](#).

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

Arbeidsgruppen som utredet rettslige spørsmål om elektronisk tinglysing, foreslo at dette bevisvakuumet kunne avhjelpes ved et krav om vitner.⁶⁰ 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.⁶¹ 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.⁶²

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.⁶³ 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.

⁶⁰ [2010-utredningen punkt 8.3.](#)

⁶¹ Se tinglysingsforskriften [§ 3](#).

⁶² Kommunal- og moderniseringsdepartementet: [Høringsnotat – forslag til endringer i tinglysingsforskriften m.m. \(elektronisk tinglysing\)](#) 22.6.2015 punkt 3.3.3.

⁶³ [HR-2020-2021-A avsnitt 104.](#)

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.⁶⁴ 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.⁶⁵ Slik toleransefullmakt, kombinasjonsfullmakt eller hva en vil kalle det, er vel kjent i norsk rett.⁶⁶ 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.⁶⁷ 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

⁶⁴ Se slik uttrykkelig [UNCITRAL Model Law](#) artikkel 8(2), jf. veiledningen avsnitt 129 og 141.

⁶⁵ Se f.eks. Mads Bryde Andersen, [Grundlæggende aftaleret](#), Gjellerup, 2021, s. 52 flg.

⁶⁶ Se f.eks. Geir Woxholth, *Avtalerett*, Gyldendal, 2021, s. 241 flg., Johan Giertsen, *Avtaler*, Universitetsforlaget, 2021, s. 369 flg., Birger Stuevold Lassen, [Kontraktsrettslig representasjon: en lærebok med et avsnitt om kommisjon](#), Universitetsforlaget, 1992, s. 32–39.

⁶⁷ Se ovenfor i punkt 2.3 om hemmelighold av brukerkoder mv.

kunne påberopes overfor den som stoler på signaturen. Dette likner mer på en skriftlig fullmakt enn en oppdragsfullmakt.⁶⁸

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.⁶⁹ 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.

⁶⁸ Geir Woxholth, *Avtalerett*, Gyldendal, 2021, s. 253.

⁶⁹ Denne muligheten er drøftet i denne antologien av Line Utne Norland og Marte Eidsand Kjørven, «Elektroniske signaturer og avtalebinding», som ikke anbefaler den.

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,⁷⁰ 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.⁷¹

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.⁷² På denne måten holdes kontrakts- og erstatningskrav klarere fra hverandre. Dette fører nok til at fullmaktssynspunktet er mer naturlig i disse landene enn erstatningssynspunktet,⁷³ 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.⁷⁴ 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.⁷⁵ 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.⁷⁶ 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

⁷⁰ Lov [18. mai 1979 nr. 18](#) om foreldelse av fordringer (foreldelsesloven) § 9.

⁷¹ [HR-2012-672-A](#).

⁷² [Svensk skadeståndslag \(1972:207\) 2 kap. 2 §](#) og [finsk skadeståndslag 412/74 5 kap. 1 §](#). Det er unntak for grov uaktsomhet.

⁷³ Marianne M. Rødvei Aagaard, «[Kreditgivares ersättningsanspråk efter obehörig användning av bank-id. Kommentar till Høyesteretts avgörande HR-2020-2021-A](#)», Svensk Juristtidning, 2021, s. 235, s. 238 flg.

⁷⁴ Se nærmere i punkt 2.3 ovenfor.

⁷⁵ [HR-2015-537-A](#) Bori, [HR-2017-1834-A](#) Branncelle, [HR-2020-312-A](#) Solem og [HR-2021-2201-A](#).

⁷⁶ Disse sakene dreier seg også om andre spørsmål, som ikke skal drøftes her.

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».⁷⁷ 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 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 aktsomhetsstandard.⁷⁸ Det er i grunnen merkelig at regelen om hemmelighold ikke er generelt lovfestet eller skrevet inn i eIDAS-forordningen.⁷⁹

I [HR-2021-2201-A avsnitt 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

⁷⁷ [HR-2015-537-A Bori avsnitt 26](#) og [HR-2021-2201-A avsnitt 66](#).

⁷⁸ 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*, Universitetsforlaget, 2007, s. 499. I denne retningen [HR-2020-2021-A premiss 54](#).

⁷⁹ Se ovenfor i punkt 2.3 om plikt til hemmelighold av brukerkoder mv.

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

temmelig grovt, og berører ofte grunnleggende forhold som rett til hjem og eiendom.⁸⁰ At slike forhold er grunnleggende, følger allerede av at de er beskyttet som menneskerettigheter.⁸¹

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. Ansaret kan være basert på en fullmaktskonstruksjon eller på erstatningsansvar 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.

⁸⁰ 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.

⁸¹ [European Convention on Human Rights](#) 1950 artikkel 8 om beskyttelse av hjem og familieliv og dens protokoll 1 artikkel 1 om beskyttelse av eiendom.

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. 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 forretningssted⁸² og for forbrukerkredittavtaler,⁸³ uavhengig av om avtalen er gjort utenom fast forretningssted. De førstnevnte reglene gjelder imidlertid ikke for lån med pant i fast eiendom,⁸⁴ og lån med pant i fast eiendom kan unntas fra de sistnevnte i nasjonal rett.⁸⁵ Norge har bare unntatt boliglån.⁸⁶

Man kan diskutere om denne adgangen til å gå fra låneavtaler er for vid eller for snever. Likevel er det slik at uansett om tinglysing 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 tinglysing ikke spille noen rolle i seg selv. Tinglysing av pant sikrer bare krav som kan gjøres gjeldende etter låneavtalen.⁸⁷

Rask etablering av pantelån representerer ikke en økt risiko for låntakeren.⁸⁸

⁸² Europaparlaments- og rådsdirektiv [2002/65/EF](#) av 23. september 2002 om fjernsal av finansielle tenester til forbrukere, og om endring av rådsdirektiv 90/619/EØF og av direktiv 97/7/EF og 98/27/EF artikkel 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.

⁸³ Europaparlaments- og rådsdirektiv [2008/48/EF](#) av 23. april 2008 om forbrukerkredittavtaler og om oppheving av rådsdirektiv 87/102/EØF (forbrukerkredittdirektivet) artikkel 14.

⁸⁴ Se Europaparlaments- og rådsdirektiv [2008/48/EF](#) av 23. april 2008 om forbrukerkredittavtaler og om oppheving av rådsdirektiv 87/102/EØF (forbrukerkredittdirektivet) artikkel 2 nr. 2 bokstav 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.

⁸⁵ Europaparlaments- og rådsdirektiv [2002/65/EF](#) av 23. september 2002 om fjernsal av finansielle tenester til forbrukere artikkel 6(3).

⁸⁶ Finansavtaleloven [§ 3-41](#).

⁸⁷ Se slik forutsetningsvis lov [26. juni 1992 nr. 86](#) om tvangsfullbyrdelse [§ 11-2](#).

⁸⁸ [2010-utredningen kapittel 10](#) 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](#).

5 Risiko for tap av prioritet

I tinglysing gjelder prinsippet om først tinglyst, best i rett.⁸⁹ 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.⁹⁰ 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.⁹¹ 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.⁹²

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 avtaleerhververen ha tinglyst ikke bare rett før utleggstakeren, men dagen før.⁹³ Og ved konkursbeslag er det konkursåpningstidspunktet, og ikke tinglysingen av det, som teller;⁹⁴ tinglysingen av det

⁸⁹ Se tingl. [§ 20](#).

⁹⁰ Se nærmere tinglysingsforskriften [§ 11](#).

⁹¹ Tinglysingsforskriften [§ 11](#).

⁹² De som bruker elektronisk tinglysing, har også den fordel at de ikke trenger å bruke formularene for skjøter etc. som gjelder for papirdokumenter, se tinglysingsforskriften [§ 2](#). Det er ikke godt å si om en privatperson taper tid på å finne frem til og fylle ut et slikt formular.

⁹³ 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](#).

⁹⁴ 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

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

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.⁹⁵

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.⁹⁶ 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.⁹⁷

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.⁹⁸ 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,

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](#).

⁹⁵ [2010-utredningen](#) godtar også dette, se [s. 39](#).

⁹⁶ [HR-2014-1465-U avsnitt 23](#).

⁹⁷ Se tingl. [§ 35](#).

⁹⁸ 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 [Lantmäteriet: Lagfartskapning](#). 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).

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.⁹⁹ De garanterer selvsagt heller ikke mot misbruk av signaturene. Deres erstatningsansvar er uansett svært begrenset, selv når de tillates brukt i elektronisk tinglysing.¹⁰⁰ 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

⁹⁹ Se ovenfor i punkt 3.3.

¹⁰⁰ Se f.eks. SpareBank 1 avtalevilkår artikkel 14 om uaktsomhetsansvar (riktignok med omvendt bevisbyrde) begrenset til kr 100 000 i disse tilfellene. I Buypass' kundeavtale artikkel 3.2 er ansvarsgrensen enda lavere – kr 5000 pr. transaksjon.

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. Skadeserstatningsloven¹⁰¹ [§ 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 konkret syndebukk ved et samvirke av tilkortkommenheter.¹⁰² 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.¹⁰³ 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.¹⁰⁴ 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 nevnt¹⁰⁵ 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,

¹⁰¹ Lov [13. juni 1969 nr. 26](#) om skadeserstatning (skadeserstatningsloven).

¹⁰² Viggo Hagstrøm og Are Stenvik, *Erstatningsrett*, Universitetsforlaget, 2019, s. 241 flg.

¹⁰³ Se Viggo Hagstrøm og Are Stenvik, *Erstatningsrett*, Universitetsforlaget, 2019, s. 253 flg.

¹⁰⁴ [Prop. 53 L \(2013–2014\) kapittel 14](#).

¹⁰⁵ Ovenfor i punkt 3.4.

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 tinglysning 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 punkt 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.¹⁰⁶ 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

¹⁰⁶ 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.

historiske eieren ikke lett kan beskytte seg mot, som grov tvang.¹⁰⁷ 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 antydning 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.¹⁰⁸ 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

¹⁰⁷Thor Falkanger og Aage Thor Falkanger, *Tingsrett*, Universitetsforlaget, 2022, s. 692.

¹⁰⁸ Se ovenfor i punkt 3.5.

tinglysningslovens 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,¹⁰⁹ 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 hans 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.¹¹⁰ 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.¹¹¹

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

¹⁰⁹ Olav Torvund, *Formueretten i informasjonssamfunnet*, Universitetsforlaget, 2022, s. 89.

¹¹⁰ Se i denne retning fra andre områder f.eks. Erik Røsæg i [Förhandlingarna vid det 34:e nordiska juristmötet i Stockholm 21–23 augusti 1996: 2](#), 1997, s. 713–742, 735 og Jan Kleineman, «[Robotrådgivning – finns det?](#)», i Torsten Iversen mfl., red., *Festskrift til Bent Iversen*, Adlibris, 2019, s. 151–165.

¹¹¹ Olav Torvund, *Formueretten i informasjonssamfunnet*, Universitetsforlaget, 2022, s. 247.

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. Ansvar 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.