

Obehörig användning av e-legitimation och avtalsbundenhet i finsk rätt

Av professor JOHAN BÄRLUND

Artikeln belyser hur man i finsk rätt förhåller sig till en obehörig användning av bland annat bankkoderna som e-legitimation med utgångspunkt i den finska högsta domstolens avgörande HD 2016:73. I Finland är användningen av bankkoder omfattande och sedan 2013 har även överlåtelser av fastigheter kunnat ske på elektronisk väg. I finsk rätt är det inte ovanligt att den rätta innehavaren av e-legitimationen blir avtalsrättsligt bunden av missbrukarens rättshandling.

1 Inledning

Enligt regeringsprogrammet för Sanna Marins regering (2019–2023) ska Finland vara känt som ett föregångsland i fråga om de möjligheter som digitaliseringen och den tekniska utvecklingen ger inom många av samhällets sektorer.¹ Ett viktigt mål för regeringen har bland annat varit att ett enhetligt system för elektronisk identifiering skapas för finska medborgare och över huvud taget för alla som bor i Finland.² Med avstamp i dessa målsättningar lämnades i september 2022 en proposition till riksdagen med förslag till lagstiftning om digital identitet. Denna lagstiftning ska utgöras dels av en lag om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata, dels av en lag om e-legitimation.³ E-legitimationen kommer enligt propositionen att ha formen av en app i en smarttelefon, men mitt intryck är att också surfplattor eller andra slags mobila apparater, t.ex. en smartklocka, ska kunna fungera som underlag för e-legitimationen.

Den finska propositionen grundar sig delvis på den utveckling av digitala identitetslösningar som skett under de senaste åren inom EU. Nyligen har Europeiska unionens råd antagit en allmän riktlinje om förslaget till lagstiftning om en ram för en europeisk digital identitet (e-legitimation).⁴ Enligt ett pressmeddelande från Rådet är målet med den nya europeiska lagstiftningen ”att ge människor och företag i EU allmän tillgång till säker och tillförlitlig elektronisk identifiering och

¹ Regeringsprogrammet för statsminister Sanna Marins regering 10.12.2019: Ett inkluderande och kunnigt Finland — ett socialt, ekonomiskt och ekologiskt hållbart samhälle, Statsrådets publikationer 2019:32, s. 111.

² Regeringsprogrammet 10.12.2019 s. 117.

³ Regeringens proposition (RP) 133/2022 till riksdagen med förslag till lagstiftning om digital identitet.

⁴ 2021/0136 (COD), <https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/sv/pdf>, besökt 27.2.2023. Europeiska kommissionen har i juni 2021 avlatit förslaget COM (2021)281 till ändring av Europaparlamentets och rådets förordning (EU) nr 910/2014.

autentisering med hjälp av en personlig e-plånbok i mobiltelefonen”.⁵ Denna utveckling inom EU kommer alltså högst sannolikt att leda till en ökad användning av e-legitimationen inte bara i Finland utan inom hela EU. När man har utarbetat det finska förslaget om e-legitimation har man försökt beakta utvecklingen inom EU, även om den finska lösningen ännu inte kommer att utgöra en sådan e-plånbok som man håller på att utveckla inom EU.⁶

Hittills har e-legitimationen i Finland reglerats i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, AutentiseringsL), som lägger grunden för den finska delen av den sam-europeiska identifieringen (eIDAS), vilken skapar förutsättningarna för en säker användning av den offentliga förvaltningens e-tjänster i Europa över landsgränserna. Inga av de finländska identifieringsverktygen har än så länge lämnats in för godkännande i EU. I den process som gäller för ett godkännande ser man till att identifieringsverktyget uppfyller informationssäkerhetskraven och att det även är betrott i andra länder. Av de nordiska ländernas lösningar har danska, norska och svenska identifikationsverktyg redan godkänts. Finländare kan alltså med finländska identifieringsverktyg än så länge inte uträtta ärenden i andra EU- och EES-länder. De föreslagna lösningarna i propositionen från september 2022 är ett led i den utveckling genom vilken Finland ska uppnå sådana gränsöverskridande lösningar för att uträtta ärenden som det europeiska eIDAS-ändringsförslaget förutsätter. I Finland är tanken nu att de nya reglerna ska göra det möjligt att en eller flera lösningar enligt förslaget kan anmälas enligt förfarandet i eIDAS-förordningen. Detta skapar möjligheter för tillgängligheten av myndigheternas tjänster i andra medlemsstater för både finska medborgare och finska näringsidkare i och med att de kan identifiera sig där förutsatt att dessa utländska tjänster är tillgängliga för användare över gränserna. Det är ju inte tillfredsställande att finländarna för närvarande inte har någon tillgång till sådana identifieringsverktyg som ger rätt till elektronisk identifiering över nationsgränserna inom EU.⁷

I Finland finns det för närvarande tre kategorier av tjänster för stark autentisering på nätet: mobilcertifikat, nätbankskoder och certifikatkort. Med mobilcertifikaten och nätbankskoderna kan man skapa avancerade elektroniska signaturer, medan man med certifikatkorten kan skapa kvalificerade elektroniska signaturer i enlighet med den nivåindelning som följer av eIDAS-förordningen.⁸

⁵ <https://www.consilium.europa.eu/sv/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/>, besökt 22.2.2023.

⁶ RP 133/2022 s. 36.

⁷ RP 133/2022 s. 37.

⁸ Se närmare om de olika elektroniska signaturerna i Rautanen, Eino & Skult, Staffan, Giltigheten av elektroniska underskrifter i kommersiella avtal, JFT 2020 s. 649–675 och särskilt s. 657–661.

Teleföretagens mobilcertifikat finns i mobiltelefonernas SIM-kort. När användaren har tagit i bruk mobilcertifikatet, kan användaren identifiera sig med mobiltelefonen och en personlig pinkod. I dagens läge erbjuder endast tre teleoperatörer i Finland ett mobilcertifikat. I början av 2022 när Ryssland inledde sitt krig mot Ukraina, ökade antalet mobilcertifikat i Finland, eftersom många användare av nätbankskoderna ville ha ett alternativ till identifieringen.⁹

Det vanligaste identifikationsverktyg i Finland som bygger på stark autentisering utgörs av bankernas nätbankskoder, som i stor utsträckning kan användas även för inloggning i myndigheternas tjänster.¹⁰ En webbank kan nå antingen med en webbläsare eller genom bankernas särskilda appar. Inloggningen med ett användar-ID kan ske på olika sätt, t.ex. genom användningen av en ID-app, med hjälp av en kodkalkylator eller än så länge genom användningen av kodkort eller lösenord, vilka i en nära framtid kommer att försvinna som inloggningsmetod och vilka ytterligare kan kräva att inloggningen bestyrks med ett sms. De finska bankerna har alla utvecklat sina egna system med bankkoder, vilket gör att Finland avviker från de övriga nordiska länderna där man alltså skapat ett enhetligt identifieringssystem för bankerna.

Den tredje gruppen identifikationsverktyg utgörs av de certifikat som utställs av Myndigheten för digitalisering och befolkningsdata i Finland. Dessa certifikat är medborgarcertifikaten, som finns i de finska identitetskorten, eller de två andra formerna av certifikat, dvs. organisationscertifikaten och certifikaten för social- och hälsovården. Dessa certifikat är alltid anslutna till ett fysiskt kort, vilka kräver både personlig pinkod och kortläsare för att fungera. Till följd av detta tekniska tilläggskrav har intresset för medborgarcertifikatet blivit relativt lamt. Inom kort kommer certifikaten att ersättas av en digital identitetshandling som Myndigheten för digitalisering och befolkningsdata som bäst utvecklar med stöd av den nya lagstiftningen om e-legitimation. Denna nya digitala lösning för identifiering är tänkt att vara kompatibel med den kommande europeiska e-plånboken.¹¹

De tekniska lösningarna för e-legitimationen kommer alltså att konvergera till följd av den europeiska utvecklingen, även om Finland idag ligger något efter i utvecklingen i jämförelse med de övriga stora nordiska länderna. Det oaktat har dessvärre de juridiska problem som sammanhängt med missbruk av dagens lösningar för e-legitimation varit likartade i Finland som i de övriga nordiska länderna. Ett av syftena med reformen av bestämmelserna om e-legitimation är därför att minska missbruket av e-legitimationer. Också i Finland har antalet missbruksfall kraftigt ökat under de senaste åren. I juni 2021 gick

⁹ <https://etn.fi/index.php/13-news/13314-mobiilivarmenteen-kaeyttoe-kolminkertaistunut>, besökt 10.1.2023.

¹⁰ Situationen när alltså i stort sett densamma som i de övriga nordiska länderna, även om man i Finland inte känner till något enhetligt system såsom BankID i Sverige och Norge samt NemID i Danmark.

¹¹ <https://dvv.fi/sv/fornyelse-av-den-digitala-identiteten>, besökt 11.1.2023.

polisen ut med en allmän varning om att brottslingar försöker komma åt nätbankskoderna på olika sätt i syfte att sko sig ekonomiskt på brotts-offren. Att det är ett vanligt fenomen visar den enkät från våren 2020 enligt vilken över en tiondedel av de finska konsumenterna hade råkat ut för bedrägeriförsök på nätet. Enligt färsk statistik från den finska banknämnden har antalet bedrägerier på nätet ökat så markant att banknämnden 2022 fick ca 450 anmälningar jämfört med ca 200 anmälningar år 2021.¹² Missbruk av e-legitimation är alltså inte ett alldeles obetydligt fenomen i det finska samhället.

Följande steg i den tekniska utvecklingen är säkerligen att de biometrisk identifieringsmedlen ökar. Identifiering med hjälp av fingeravtryck eller avläsning av ansikte eller ögats iris kommer att minska risken för missbruk bland annat genom att överlåtbarheten av dessa är mer begränsad än till exempel personliga pinkoder eller andra lösenord.

Syftet med denna artikel är att analysera det finska rättsläget kring missbruket av en annans e-legitimation, till exempel genom att någon annans identifikationsverktyg obehörigt används för handel och transaktioner på nätet.¹³ Fokus i artikeln ligger på frågan om vilket slags ansvar det blir fråga om för den person vars identifikationsverktyg har missbrukats. I vilken mån blir missbruksoffret till exempel avtalsrättsligt bunden av de rättshandlingar som missbrukaren vidtar eller i vilken mån är det fråga om ett utomkontraktuellt ansvar? I min artikel koncentrerar jag mig uttryckligen på rättsläget i Finland och gör endast sporadiska hänvisningar till rättsläget i de övriga nordiska länderna.

2 De grundläggande reglerna för hur en användare ska förfara med sina identifieringsverktyg

2.1 De aktuella lagrummen

Den gällande lagstiftningen om e-legitimation i Finland är inte enhetlig. Förutom reglerna i AutentiseringsL finns det regler av betydelse för detta sammanhang även i betaltjänstlagen (290/2010; BetaltjänstL) och i 7 kap. i konsumentskyddslagen (38/1978, KSL). BetaltjänstL blir aktuell när missbruket av e-legitimationen består av att missbrukaren kommer över ett bankkonto och i 7 kap. i KSL finns regler om sådant missbruk som utgörs av att ett kreditkort eller någon annan identifikator som möjliggör användning av kredit används på ett obehörigt sätt. Slutligen ska även nämnas lagen om tjänster inom elektronisk kommunikation (917/2014) där det finns en bestämmelse om obehörig användning av kommunikationstjänster. En missbrukare

¹² <https://www.fine.fi/ajankohtaista/2023/kotivakuutusasiat-ja-huijaukset-nakyivat-finessa-eniten-viime-vuonna.html>, besökt 30.1.2023.

¹³ I de nordiska framställningar som finns om e-legitimation saknas i regel det finska perspektivet, se Kjørven, Marte Eidsand, Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe *European Business Law Review* 2020 s. 77–109 samt Aagaard, Marianne M. Rødvei, Kreditgivares ersättningsanspråk efter obehörig användning av bank-id, *SvJT* 2021 s. 235–250.

kan bland annat obehörigt logga sig in på offrets bredband och dra ekonomisk nytta av detta. Men då det här egentligen inte är fråga om användning av e-legitimation går jag inte närmare in på detta lagrum i det följande.

I de uppräknade lagarna finns bestämmelser som reglerar ansvarsfördelningen mellan offret för ett missbruk och den institution som erbjuder användningen av e-legitimationen, oftast en bank. Det blir aktuellt att närmare fastställa ansvarsfördelningen när en utomstående missbrukar de identifieringsverktyg som hör ihop med e-legitimationen. Självfallet gör sig missbrukaren i regel skyldig till brott, särskilt identitetsstöld enligt 38 kap. 9a § och de olika formerna av bedrägeri enligt 36 kap. 1–3 § i den finska strafflagen (39/1889). I denna artikel förbigås ändå frågan om missbrukarens ansvar eftersom tyngdpunkten här ligger på det ansvar som drabbar den vars identifieringsverktyg missbrukas.

Lagrummen i AutentiseringsL, BetaltjänstL och KSL är alla skrivna så att de innehåller en närmare definition av tre ansvarssituationer för innehavaren av ett identifieringsverktyg vid obehörig användning av verktyget. Som huvudregel kan man därför ange att den rätta innehavaren av identifieringsverktyget inte har något generellt ansvar för en obehörig användning av verktyget, med undantag för de tre situationer som anges i 27.1 § i AutentiseringsL, 62.1 § i BetaltjänstL och 7:40.1 i KSL. Förhållandet mellan huvudregel och undantag i AutentiseringsL beskrivs även av Olli Norros på detta sätt.¹⁴ Också Tuire Saaripuu anger i sin doktorsavhandling från 2019 att det uttryckligen är fråga om en begränsning av innehavarens ansvar.¹⁵ En sådan uppfattning av den rätta innehavarens ansvar borde leda till en restriktiv tolkning av undantagen.

Förutom dessa regler om ansvaret vid användningen av identifieringsverktyg innehåller AutentiseringsL också bestämmelser i 40 § om ansvaret för obehörig användning av framställningsdata för en underteckning eller elektronisk stämpel. En sådan innehavare av signaturframställningsdata som har ställningen av en konsument berörs av motsvarande regler som i 27 §. Samma regel ingick redan i 17 § i lagen om elektroniska signaturer (14/2003), eller med andra ord föregångaren till AutentiseringsL. I det följande kommer jag bara att behandla missbruk av identifieringsverktyg även om reglerna även kunde tillämpas på obehörig användning av framställningsdata för en elektronisk signatur.

Vilka är då de tre situationer som räknas upp i lagrummen och i vilka innehavaren av ett identifieringsverktyg alltså ansvarar för den obehöriga användningen av verktyget?

¹⁴ Norros, Olli, *Selvitys tunnistamiseen liittyvistä vahingonkorvauskysymyksistä, Viestintäviraston julkaisuja 003/2016 J*, s. 30.

¹⁵ Saaripuu, Tuire, *Vahingonkorvausvastuun määräytyminen luonnollisen henkilön sähköisen identiteetin tunnistus- ja allekirjoituspalveluissa*, Helsingfors 2019, s. 317.

2.2 Frivillig överlåtelse av identifieringsverktyget

Såsom i de övriga nordiska länderna gäller i finsk rätt som huvudregel att innehavaren av ett identifieringsverktyg inte får överlåta verktyget att användas av någon annan. Detta följer dels av 23.2 § i AutentiseringsL, dels av de avtalsvillkor som kreditinstituten använder sig av när det gäller till exempel bankkoder samt bank- och kreditkort. En finsk bank skriver i sina avtalsvillkor: ”Man får inte använda sin närståendes nättjänstkoder ens med hens tillstånd, och man får aldrig ge sin egen kod till någon annan, inte ens till en familjemedlem.”¹⁶ Ändå är det uppenbart att överlåtelser sker i praktiken mellan närstående, till exempel när ett äldre barn hjälper sina åldrande föräldrar att sköta bankärendena eller när den ena maken sköter bägge makarnas bankärenden.

Först och främst har innehavaren alltså ett ansvar om innehavaren har överlåtit identifieringsverktyget till någon annan. Detta följer av 27.1 § 1 punkten i AutentiseringsL, av 62.1 § 1 punkten i BetaltjänstL och av 7:40.1 1 punkten i KSL. Lagrummen skiljer sig åt på så sätt att överlåtelseförbudet i AutentiseringsL är absolut, medan förbuden i BetaltjänstL och KSL gäller överlåtelse till obehöriga användare. Eftersom möjligheten att överlåta bankkoder och bank- och kreditkort ändå begränsas med stöd av avtalsvillkor, kommer situationerna att vara desamma enligt de tre lagarna. Med tanke på syftet med denna artikel har dessa skillnader på detaljnivå inte heller någon betydelse.

Eftersom AutentiseringsL i 23.2 § innehåller förbudet för innehavaren att överlåta identifieringsverktyget till någon annan, vilket även är innehållet i avtalsvillkoren, ter det sig naturligt att innehavaren vid en överlåtelse svarar fullt ut för de rättshandlingar som en mottagare av identifieringsverktyget företagit oavsett överlåtarens och mottagarens subjektiva uppfattning om överlåtelens rättsverkningar. Eftersom syftet med identifieringsverktygen är att fastställa identiteten hos den personen som använder sig av dem, har man i propositionen till lagrummet angett att innehavaren måste ”förstå att verktygen inte får överlåtas åt någon annan”.¹⁷ Även om det är allmänt känt — och detta medges i propositionen — att det inte är ovanligt att identifieringsverktygen överlåts att användas av andra inom familjen, så är överlåtelserna alltså strängt sanktionerad.¹⁸ Överlåtelserna av besittningen till identifieringsverktyget ska vara frivillig, även om det saknar betydelse i vilket syfte

¹⁶ Den finska OP-banken (<https://www.op.fi/ingangssidan> > Privatkunder > Pengar > Sköter du bankärenden åt en närstående till dig), besökt 22.2.2023.

¹⁷ Regeringens proposition 36/2009 till Riksdagen med förslag till lag om stark autentisering och elektroniska signaturer samt till vissa lagar som har samband med den, s. 63.

¹⁸ RP 36/2009 s. 63.

överlåtelsen har skett.¹⁹ Även praxis från den finska banknämnden bekräftar denna linje.²⁰

Om det identifieringsverktyg som överlåts finns till exempel i en mobiltelefon i form av en webb-banks app, tar överlåtaren en risk för att verktyget används på ett obehörigt sätt, även om överlåtaren av mobiltelefonen och därmed identifieringsverktyget, bara avser att mottagaren ska förvara mobiltelefonen för innehavarens räkning en kortare tid. Innehavaren kan följaktligen bli ansvarig, om risken realiserar.²¹ Det är viktigt att märka att det är fråga om en sådan överlåtelse som avses i bestämmelsen endast då innehavaren av ett identifieringsverktyg avsiktligt överlåter besittningen av själva verktyget till någon annan. I propositionen till bestämmelsen anges att lagrummet således inte ska gälla till exempel i en sådan situation där innehavaren av identifieringsverktyget låter någon förvara en väska som innehåller identifieringsverktyget, om inte innehavaren av identifieringsverktyget kan anses ha handlat klandervärt eller med andra ord vårdslöst i denna situation.²² Då kan ansvar nämligen inträda med stöd av 27.1 § 2 punkten i AutentiseringsL, som jag behandlar i följande avsnitt. Gränsdragningen mellan den aktiva överlåtelsen enligt 1 punkten och vårdslösheten enligt 2 punkten kan onekligen bli besvärlig ibland.

Ansvar vid brott mot överlåtelseförbudet i 27.1 § 1 punkten i AutentiseringsL motsvaras som sagt av ett liknande ansvar i 62.1 § 1 punkten i BetaltjänstL och 7:40.1 1 punkten i KSL. I den finska banknämndens praxis finns det fall där nämnden har dragit slutsatsen att nätbankskoderna på frivillig väg har överlåtit till en obehörig användare, varför den rätta innehavaren av identifieringsverktyget ansvarar för missbruket.²³

2.3 Användningen sker till följd av innehavarens vårdslöshet

Den andra situationen då innehavaren får ett ansvar utgörs enligt 27.1 § 2 punkten i AutentiseringsL av de fall då identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt på grund av innehavarens vårdslöshet, som inte är lindrig. Enligt 23 § 1 andra meningen i AutentiseringsL har innehavaren en allmän skyldighet att ”förvara identifieringsverktyget omsorgsfullt”. Ansvar för innehavarens vårdslöshet inträder likväl först när oaktsamheten är mer allvarlig än lindrig vårdslöshet. Inte heller

¹⁹ Regeringens proposition 197/2001 till Riksdagen med förslag till lagar om elektroniska signaturer och om ändring av 2 § lagen om kommunikationsförvaltningen, s. 35.

²⁰ Den finska banknämnden (PKL) 69/11. Fallen finns samlade på webbadressen <https://www.fine.fi/sv/kontakta-oss/ratkaisutietokanta.html>, besökt 23.2.2023. Fallen finns tyvärr bara på finska.

²¹ RP 36/2009 s. 67.

²² RP 36/2009 s. 67.

²³ Se FINE-012916 och FINE-036135. Från hösten 2017 har banknämndens fall ny numrering och förkortningen FINE.

gränsdragningen mellan lindrig vårdslöshet och vårdslöshet som är grövre än lindrig är lätt att göra.

Innehavarens ansvar enligt i 62 § i BetaltjänstL och 7 kap. 40 § i KSL ser aningen annorlunda ut, eftersom innehavaren av ett betalningsinstrument påförs ett ansvar redan vid lindrig vårdslöshet, men där ansvaret är begränsat till ett belopp av 50 euro, om inte vårdslösheten är grov eller innehavaren har handlat avsiktligt. Även i KSL finns samma regel för innehavaren av ett kreditkort eller av någon annan identifikator som berättigar till användningen av en kredit. I de två sistnämnda lagrummen innebär ansvaret uttryckligen ett betalningsansvar, medan ansvaret för en obehörig användning av ett identifieringsverktyg enligt AutentiseringsL ju kan omfatta annan bundenhet än en betalningsskyldighet. Därför kommer jag inte att fästa närmare uppmärksamhet vid dessa skillnader i detaljerna mellan å ena sidan AutentiseringsL och å andra sidan BetaltjänstL och KSL.

I den finska banknämnden handlar den största delen av missbruksfallen om gränsdragningen dels mellan avsaknaden av vårdslöshet och vårdslöst beteende hos innehavaren av identifieringsverktyget enligt BetaltjänstL:s reglering om innehavarens ansvar, dels mellan vårdslöst och grovt vårdslöst beteende. I de fall då innehavaren har ansetts ha varit vårdslös vid denna gränsdragning, men inte grovt vårdslös, har bestämmelsen om taket för innehavarens ansvar på 50 euro utgjort en klar begränsning av innehavarens ansvar.²⁴ Om innehavaren däremot har ansetts ha förfarit grovt vårdslöst i samband med den utomstående missbruk, har innehavaren ansvarat för hela beloppet. Största delen av dessa fall i banknämnden har gällt nätfiske (eng. phishing) där innehavaren alltför lättvindigt har avslöjat sitt användar-ID och bankkoderna för missbrukaren.²⁵

Också i det finska HD-fallet 2018:71 var det fråga om gränsdragningen mellan vanlig vårdslöshet och grov vårdslöshet. En advokat hade förvarat sitt kombinerade bank- och kreditkort i sin plånbok. Pinkoden till kortet fanns i ett kuvert med bankens logga i en skrivbordslåda på advokatens kontor. Advokaten hade avlägsnat sig från kontoret i ca tio minuters tid utan att låsa ytterdörren, medan plånboken låg på hans skrivbord. En okänd inkräktare hade under tiden kommit in på kontoret och tagit plånboken och kuvertet med pinkoden och strax därefter tagit ut pengar med advokatens kort i en bankautomat i närheten. Avgörandet var inte enhälligt. Majoriteten 3–2 i HD ansåg inte att advokatens beteende hade utvisat så klandervärd likgiltighet mot säkerhetsföreskrifterna och den ökade risken för missbruk av kortet att hans vårdslöshet skulle anses som grov. Advokatens ansvar för den obehöriga användningen av betalkortet begränsades därför till 150 euro

²⁴ Fram till 13.1.2018 var denna självrisk 150 euro. Färska fall från banknämnden där innehavaren har ansetts ha ett ansvar på 50 euro för missbruket är FINE-049807 och FINE 050512.

²⁵ Färska fall från banknämnden är FINE-049778 och FINE-052589.

som då var det belopp som utgjorde taket för innehavarens ansvar enligt 62.2 § i BetaltjänstL. Minoriteten ansåg däremot att det förelåg grov vårdslöshet, varför advokatens skulle anses ansvarig till fullt belopp gentemot banken för de uttagna pengarna.

Dessvärre torde en av de vanligaste situationerna av missbruk bestå av en obehörig användning av olika konton som innehavaren använder sig av. Genom nätfiske försöker förövare komma åt offrets bankkonto, e-postkonto eller konton på sociala medier i syfte att komma över offrets pengar, känsliga information eller identitet på sociala media. Ett annat syfte med nätfisket kan vara att i offrets namn uppta kredit eller ingå avtal om köp av varor eller tjänster. I den rättsliga bedömningen blir frågan ofta just att ta ställning till offrets agerande och eventuella vårdslöshet.

2.4 Underlåtelse att anmäla förlusten

För det tredje kan innehavaren av ett identifieringsverktyg enligt 27.1 § 3 punkten i AutentiseringsL bli ansvarig för en obehörig användning av verktyget, om innehavaren efter en upptäckt av förlusten eller av den obehöriga användningen har försummat att utan obefogat dröjsmål anmäla förlusten. Genom att göra anmälan på ett effektivt sätt, begränsar innehavaren av identifieringsverktyget alltså sitt ansvar som följer av lagen. Samma regel finns i 62.1 § 3 punkten i BetaltjänstL och 7:40.1 3 punkten i KSL.

I den finska banknämnden har några fall behandlats där nämnden har ansett att innehavaren har försummat sin skyldighet enligt 62.1 § 3 punkten i BetaltjänstL att utan obefogat dröjsmål göra anmälan och detta har ansetts utvisa grov vårdslöshet.²⁶ Den grova vårdslösheten leder ju i sin tur till att taket för innehavarens ansvar på 50 euro inte tillämpas. I ett fall har banknämnden pekat på att förseningen med anmälan inte ska beaktas, om inte förlusterna har ökat på grund av den. I fallet hade ändå innehavaren förfarit vårdslöst i och med att missbrukaren hade kommit över identifieringsverktygen i samband med ett inbrott. Nämnden ansåg att delarna nämligen inte i tillräcklig mån hade hållits åtskilda från varandra.²⁷

2.5 I vissa fall bortfaller innehavarens ansvar

Enligt 27.2 § i AutentiseringsL bortfaller innehavarens ansvar för en obehörig användning enligt 1 mom. 1) efter att anmälan har gjorts om förlusten, 2) om anmälan om förlusten inte har kunnat göras till följd av en försummelse av leverantören av identifieringstjänster eller 3) om en tjänsteleverantör har försummat att iaktta begränsningar för användningen av identifieringsverktyget. Dessa regler är i huvuddrag desamma även i 62.3 § i BetaltjänstL och 7:40.3 i KSL.

²⁶ FINE-041305.

²⁷ FINE-023164.

I den finska banknämnden har nämnden i ett fall ansett att banken försummat sina förpliktelser att kräva stark autentisering av innehavaren av identifieringsverktyget, varför innehavarens ansvar för missbruket föll bort. Banken uppmanades stå för förlusten.²⁸

Efter denna genomgång av bestämmelserna om fördelningen av ansvaret mellan innehavaren av identifieringsverktyget och upplåtaren av det, ska jag skifta fokus och närmare behandla vad ansvaret består av för innehavaren som blir bunden av en obehörig användning av identifieringsverktyget. Det intressanta är att någon mer detaljerad analys av innehållet i ansvaret inte kan hittas i finsk rätt, utan det gäller att ta fasta på några sporadiska uttalanden i lagförarbeten, praxis och doktrin.

3 Vad består innehavarens ansvar av?

I propositionen till AutentiseringsL konstateras lakoniskt att den rätta innehavaren av identifieringsverktyget ansvarar för den obehöriga användningen i de situationer som jag redogjort för ovan, men vad detta ansvar utgörs av anges inte närmare. I samband med regeln om ansvar för en obehörig användning av signaturframställningsdata framgår ändå att den obehöriga användningen leder till att en obehörig person ingår rättshandlingar och att detta kan leda till skador.²⁹ Vad kan ansvaret för den obehöriga användningen alltså bestå av? Först och främst ska frågan analyseras om ansvaret kan utgöras av avtalsbundenhet. En annan möjlighet är att ansvaret består i att den rätta innehavaren blir skadeståndsskyldig till följd av en bristande avtalsbundenhet. Slutligen kunde rättsinstitutet återbäring av obehörig vinst aktualiseras i vissa situationer om denna rätta innehavaren har upplevt en obefogad ökning av sin egendomsmassa till följd av den obehöriga användningen av ett identifieringsverktyg.

Avtalsbundenhet för den rätta innehavaren av identifieringsverktyget är en påföljd vid obehörig användning av e-legitimation som skymtar fram i många av lagförarbetena till de regler som jag nämnt ovan. BetaltjänstL gäller betalningstransaktioner och då kommer en obehörig användning av offrets e-legitimation att innebära förlust av pengar. I motiven till en ändring av 62 § i BetaltjänstL anges att en betaltjänstanvändare som överlåtit betalningsinstrumentet till någon annan ”då ska anses vara ansvarig för den persons handlingar till vilken betalningsinstrumentet har överlåtitits...”.³⁰ Detta ska rimligtvis innebära att en rättshandling som missbrukaren har vidtagit blir bindande för offret i förhållande till en godtroende utomstående betalningsmottagare. En annan situation beskrivs i en av propositionerna till en ändring av kommunikationsmarknadslagen, som jag ju i övrigt inte behandlar i denna artikel, eller med andra ord när en konsument

²⁸ FINE-045341.

²⁹ RP 197/2001 s. 35.

³⁰ Regeringens proposition 132/2017 till riksdagen med förslag till lag om ändring av betaltjänstlagen och till vissa lagar som har samband med den, s. 46.

modem kapas och ett långt och dyrt utlandssamtal rings från konsumentens dator utan konsumentens medgivande. Om konsumenten kan anses ha varit förfarit mer klandervärdt än lindrigt vårdslöst, svarar konsumenten för samtalet. Om konsumenten anses ha förfarit omsorgsfullt eller endast lindrigt vårdslöst utblir ansvaret däremot.³¹ Innehållet i ansvaret utgörs av en skyldighet att betala för samtalet enligt de avtalsvillkor som gäller för abonnenten, vilket tyder på att avtalsbundenhet uppstår i denna situation.

Ett av de få HD-fall som berör missbruk av e-legitimation och som uttryckligen gäller 27 § i AutentiseringsL är HD 2016:73, som dessvärre bara finns på finska. I fallet hade en konsument B, som bodde tillsammans med sin make C, förvarat sitt användar-ID och sina bankkoder hemma i en och samma låda där även maken förvarade sina identifieringsverktyg. Maken C hade utan B:s lov använt B:s identifieringsverktyg för att ingå ett avtal om en snabbkredit på 100 euro med A Ab, som hade betalat in summan på C:s konto. HD angav att B inte hade överlåtit identifieringsverktygen till C, men nog förfarit mer än lindrigt vårdslöst genom att förvara användar-ID och bankkoderna på ett och samma ställe så att C lätt hade tillgång till dem. I punkt 28 i domen tar HD närmare ställning till ansvarets innehåll och konstaterar (i min översättning): "... Ansvaret för innehavaren av identifikationsverktyget är sålunda detsamma som i ett kreditavtal som hen själv ingått." HD konkluderar med att B är tvungen att återbetala krediten till A Ab.³² Det är intressant att HD betonar att man varken i lagrummet eller i förarbetena till lagrummet närmare har tagit ställning till vad ansvaret utgörs av, vilket domstolen alltså nu utvecklar i fallet: Ansvaret är detsamma som om innehavaren av identifieringsverktyget själv hade ingått avtalet.³³ Här är det alltså fråga om att avtalsbundenhet och följaktligen att ett avtalsrättsligt ansvar har inträtt.³⁴

Avtalsbundenheten till följd av vårdslöshet är onekligen ett dramatiskt avsteg från den allmänna principen om att partsviljan är ett grundläggande element i avtalsbundenheten. Såsom Kurt Grönfors träffande har argumenterat för har partsviljan ändå fått en nedtonad roll i avtals-

³¹ Regeringens proposition 231/2005 till Riksdagen med förslag till lag om ändring av kommunikationsmarknadslagen och lagen om behandling om vissa marknadsrättsliga ärenden, s. 32.

³² HD 2016:73 punkt 29. HD anger i punkt 26 att varken själva lagtexten eller lagförarbetena anger vad ansvaret utgörs av och inte heller den bakomliggande EU-förordningen (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG innehåller någon närmare anvisning om ansvarets innehåll.

³³ Saaripuu 2019 s. 384 använder sig snarare av terminologin att innehavaren blir bunden till de obehöriga rättshandlingarna. Det är ändå fråga om samma sak. Likväl analyserar Saaripuu inte närmare ansvarets innehåll.

³⁴ Se även Norros 2016 s. 30 som anger att den skada som den riktiga innehavaren av identifieringsverktyget kan drabbas av till följd av den obehöriga användningen kan vara betydande.

läran under senare delen av 1900-talet, varför en avtalsverkan kan inträda också med stöd av andra avtalsgrundande rättsfakta.³⁵ Visserligen ter det sig för en godtroende utomstående som om det existerade en partsvilja, men den är uttryckt av en obehörig person i en situation där den rätte innehavaren av identifieringsverktyget har förfarit klandervärt på något sätt. Denna rätta innehavares ansvar förutsätter ju vårdslöshet från hens sida. Avtalsbundenheten uppstår utan att den bundnes partsvilja existerar, vilket kan anses utgöra ett betydande avsteg från principen om avtalsfrihet.³⁶ Avsteget i vårt fall har ändå tagits av lagstiftaren på grunder som säkert kan anses vara väl avvägda med tanke på den tekniska utveckling som lett till utvecklingen av elektroniska identiteter.

En nedtoning av partsviljan återspeglar sig i hur vi uppfattar avtalsfriheten, som ju har ansetts vara en av de bärande avtalsrättsliga principerna.³⁷ I detta sammanhang kommer ju lagstiftarens lösning att föreskriva avtalsbundenhet vid avsaknad av den rätta innehavarens vilja en klar inskränkning av principen. Med en positivistisk syn på vårt avtalsrättsliga system kan ändå slutsatsen dras att detta ibland är fallet: Avtalsprincipen är inte obegränsad bland annat till följd av att lagstiftaren infört begränsningar.³⁸ Också Kurt Grönfors konstaterar att avtalsfriheten ”inte längre” är någon ”grundbult” i vår nordiska rätt.³⁹ I och med att lagstiftaren tagit ställning i frågan behöver vi inte gå in på frågan i vilken mån de grundläggande fri- och rättigheterna ska påverka situationen. I finsk rätt har man ju kraftigt betonat att man vid lagtolkning ska eftersträva en ”grundlagsenlig lagtolkning eller en lagtolkning som ställer sig positiv till de grundläggande fri- och rättigheterna.”⁴⁰ Det är ändå bra att märka att den aktuella problematiken innehåller en motsättning mellan avtalsfrihet och avtalsbundenheten i och med att en ökad avtalsbundenhet för den rätta innehavaren samtidigt utgör en inskränkning av avtalsfriheten.

I de situationer då den rätta innehavaren av identifieringsverktyget helt saknar vårdslöshet eller har förfarit på ett sätt som utvisar bara ringa vårdslöshet när identifieringsverktyget har försvunnit, kommit i

³⁵ Grönfors, Kurt, *Avtalsgrundande rättsfakta*, Göteborg 1993, s. 127–129.

³⁶ Päläs, Jenna & Salminen, Mirva, *Alustan asiakkaan vastuusta ja vastuuttamisesta yksilöturvallisuuden tuottamisessa — sopimusoikeudellinen näkökulma kyberturvallisuuteen jakamistaloudessa*. I *verket: Päläs, Jenna & Määttä, Kalle (red.) Jakamistalousjuridiikan käsikirja*, Helsingfors 2019, s. 319–380, s. 363.

³⁷ Pöyhönen, Juha, *Sopimusoikeuden järjestelmä ja sopimusten sovittelu*, Vammala 1988, s. 27, 177 och 266.

³⁸ Meri, Otto, *Lain ja hyvän tavan vastaiset sopimukset — Sopimusoikeudellinen tutkimus kiellonvastaisista oikeustoimista ja niiden oikeusvaikutuksista*, Keuruu 2023, s. 45 och 84. Meri hör till de forskare i Finland som anser att principen om avtalsfriheten är den ledande principen i avtalsrätten. Jfr med Pöyhönen 1988 s. 191 som anser att skälighetsprincipen är viktigare än principen om avtalsfrihet.

³⁹ Grönfors 1993 s. 29.

⁴⁰ Grundlagsutskottets betänkande 25/1994 om regeringens proposition med förslag till ändring av grundlagarnas stadganden om de grundläggande fri- och rättigheterna, s. 4.

någon annans besittning obehörigt eller använts obehörigt, utblir ansvaret enligt 27 § i AutentiseringsL. Detta betyder att rättshandlingen mellan å ena sidan den rätta innehavaren av identifieringsverktyget och å andra sidan den utomstående saknar bindande verkan och kan uppfattas som ogiltig.

I den finska banknämnden har den 9 mars 2020 ett fall avgjorts som påminner om fallet i Högsta domstolen. I banknämndsfallet var det också fråga om att en samboende make utan den andra makens vetskap hade utnyttjat dennes användar-ID och bankkoder i syfte att ingå avtal om ett lån i en annan bank än den bank i vilken den rätta innehavaren av identifieringsverktygen var kund. Till skillnad från HD-fallet hade den rätta innehavaren förvarat sitt användar-ID och bankkoder på olika ställen i bostaden. Banknämnden ansåg att det inte förelåg sådan vårdslöshet hos innehavaren av identifieringsverktygen som skulle ha varit grövre än lindrig vårdslöshet. Därför blev slutsatsen att innehavaren inte ansvarade för lånet, varför innehavarens bank var skyldig att betala tillbaka de fyra rater som banken från innehavarens konto tagit ut som amortering för lånet.⁴¹ Den obehöriga användningen av identifieringsverktygen hade alltså inte lett till avtalsbundenhet till följd av att den rätta innehavaren inte hade utvisat vårdslöshet som var grövre än lindrig vårdslöshet.

Om man alltså tolkar lagstiftarens reglering ordagrant, kommer innehavaren eller abonnenten inte heller att ha något skadeståndsansvar för det negativa avtalsintresset i de situationer då innehavaren eller abonnenten förfarit endast lindrigt vårdslöst, trots att ersättning för det negativa avtalsintresset kan aktualiseras uttryckligen som en påföljd vid ogiltiga avtal.⁴² Den rätta innehavaren ska ju inte ha något ansvar alls, varför även skadeståndspåföljden utesluts.

Frågan om bundenhet är även intressant i ljuset av de liknande bestämmelserna i 62 § i BetaltjänstL och i 7 kap. 40 § i KSL där ju ansvaret inträder redan vid lindrig vårdslöshet, men där ansvaret är begränsat till ett belopp av 50 euro, om inte vårdslösheten är grov eller innehavaren handlat avsiktligt. Ska man anse att det föreligger avtalsbundenhet också i det fall att bara självriskan utgör det beloppsmässiga ansvaret? I praktiken blir slutresultatet att betalningsrörelsen eller kreditgivaren blir tvungen att kompensera konsumenten för den förlust som konsumenten drabbats av till den del förlusten överstiger 50 euro, medan den utomstående ofta kan hålla fast vid det avtal som ingåtts förutsatt att den utomstående avtalsparten inte kan klandras för sitt förfarande. I de fall då betalningsmottagaren eller kreditgivaren medverkat till den obehöriga användningen av identifieringsverktygen

⁴¹ FINE-020522.

⁴² Se Hemmo, Mika, *Sopimusoiikeus II*, Helsingfors 2003 s. 261. Jfr med Taxell, Lars-Erik, *Avtal och rättsskydd*, Åbo 1972, s. 147, som betonar utgångspunkten att bristande avtalsbundenhet inte leder till ersättningsskyldighet, eftersom parterna själva bär risken för att ett bindande avtal inte uppstår.

kan dessa självfallet inte åberopa avtalsbundenhet. I många missbruksfall är nämligen betalningsmottagaren medskyldig till missbruket.⁴³

Uppfattningen att en obehörig användning av e-legitimationen under vissa omständigheter kan leda till avtalsbundenhet har inte varit helt oemotsagd i finsk doktrin. I sin doktorsavhandling från 2013 förespråkar Ilja Ponka att en klar och entydig lösning vore att alla rättshandlingar som företas av en annan än den rätta innehavaren av identifieringsverktyget uppfattas som obehöriga och att dessa som en utgångspunkt inte blir bindande.⁴⁴ Därför beskriver författaren rättsförhållandet mellan den rätta innehavaren av identifieringsverktyget och den utomstående tredjemannen som förlitat sig på den orättmätiga användningen av identifieringsverktyget som ett utomobligatoriskt förhållande.⁴⁵ Detta inskränker även möjligheten att befullmäktiga en annan att handla utgående från fullmaktsgivarens identifieringsverktyg. Ponka anger att det därför alltid saknas en grund för exempelvis en frivillig överlåtelse av identifieringsverktyget. En sådan lösning skulle ha preventiva verkningar och öka säkerheten vid användningen av digitala identifieringsmetoder.⁴⁶ Det finns anledning att betona att Ponkas åsikt ligger i tiden före HD-fallet 2016:73, som ju klart tar ställning till avtalsbundenhet som en möjlig rättslig påföljd vid obehörig användning av ett identifieringsverktyg.

I HD-fallet 2016:73 ansåg Högsta domstolen alltså att den rätta innehavaren av identifieringsverktyget till följd av sin vårdslöshet, som inte ansågs utgöra enbart lindrig vårdslöshet, var bunden till krediten på 100 euro. Summan var onekligen liten. I banknämnds-fallet från den 9 mars 2020 var lånebeloppet som störst 13 682 euro eller med andra ord klart större än i HD-fallet. Ska avtalsbundenheten bedömas på samma sätt om kreditbeloppet hade varit ytterligare mångdubbelt större? Eller hur ska man förhålla sig till rättshandlingar där det ekonomiska värdet är avsevärt mycket större, såsom till exempel vid fastighetsköp? Dessa två situationer tarvar en egen analys.

I den mån bankerna i dagens läge stöder sig på stark autentisering vid beviljande av banklån, kan en obehörig användning av till exempel de identifieringsverktyg som bankerna erbjuder även innebära att avtal om krediter till större än tre och fyrsiffriga belopp ingås obehörigen. I 7a kap. i KSL, som generellt gäller bostadskrediter, finns inga normer som utesluter tillämpningen av lagen om stark autentisering och betrodda elektroniska tjänster, varför kreditens belopp inte ska ha någon betydelse för hur frågan om avtalsbundenheten löses i Finland.

⁴³ Ett gott exempel är FINE-017936. Kundens kreditkort hade på ett obehörigt sätt debiterats upprepade gånger på en nattklubb i S:t Petersburg efter att kunden där använt kortet för en enda betalning på 23,43 euro.

⁴⁴ Ponka, Ilja, Sähköinen tunnustaminen ja allekirjoitus Suomen velvoiteoikeudessa, Helsingfors 2013, s. 287–288.

⁴⁵ Ponka 2013 s. 418–419.

⁴⁶ Ponka 2013 s. 287–288.

Däremot har avtalsbundenheten berörts i samband med införande av reglerna om elektroniska fastighetsköp i 2 kap. i jordabalken (540/1995, JB). Huvudregeln för bundenheten vid ett fastighetsköp anges i 2:1.3 i JB enligt vilket ett fastighetsköp ”som inte slutits i överensstämmelse med denna paragraf” inte är bindande. Enligt 2:1.2 i JB ska ”säljaren och köparen eller deras ombud ... godkänna likalydande elektroniska köpebrev på det sätt som föreskrivs i 9a kap.” i JB. Det är alltså uttryckligen säljarens och köparens godkännande som behövs för att fastighetsköpet ska vara giltigt. Vid missbruk av någon annans e-legitimation är det ju någon annan än parterna som har godkänt köpet. Reglerna i 9a kap. i JB är utformade så att staten har ett primärt skadeståndsansvar för alla de fall då fastighetsköpet inte blir bindande, till exempel vid identitetsmissbruk. Enligt 9a:3.2 i JB har staten ett primärt skadeståndsansvar för en skada som bland annat ”orsakats av att ärendehanteringssystemet orättmätigt har använts av någon annan än den som identifierats som användare”. Med tanke på att jordabalkens reglering om elektroniska fastighetsköp är *lex specialis* i förhållande till den mer generella regleringen om den rätta innehavarens ansvar enligt 27 § i AutentiseringsL har vi alltså här ett undantag till avtalsbundenheten. I motiveringen till 9a:3.2 i JB anges:

Staten ska således ersätta köparens skada, om ett köp som slutits i fastighetsöverlåtelssystemet *visar sig vara utan verkan* därför att köpebrevet orättmätigt har godkänts av en person i egenskap av säljare som är någon annan än fastighetsägaren.⁴⁷

Om fastighetsköpet alltså inte blir bindande till exempel till följd av att säljaren överlåtit identifieringsverktyget till någon annan eller förvarat det på ett vårdslöst sätt så att någon annan kommit över det, kommer köparens skada att bestå i att köpet inte blir bindande och de följdverkningar som uppstår av detta. Att lagstiftaren utgått ifrån att fastighetsköpet blir ogiltigt vid den rätta innehavarens överlåtelse eller vårdslösa förvaring av identifieringsverktygen, framgår av ett resonemang i propositionen som gäller statens regressrätt vid utbetalat skadestånd. I propositionen anges nämligen att staten har regressrätt ”i en situation där t.ex. fastighetens ägare har överlåtit identifieringsverktyget i någon annans besittning eller förvarat det oaktsamt”.⁴⁸ Denna rätta innehavares ansvar kommer i detta fall inte att bestå av avtalsbundenhet, utan av en skadeståndsskyldighet gentemot staten som haft det primära skadeståndsansvaret. På statens regressrätt ska enligt 9a:3.3 i JB bestämmelserna i 13:6–8 i JB tillämpas.⁴⁹

⁴⁷ Regeringens proposition 146/2010 till Riksdagen med förslag till lagstiftning om fastighetsköp, pantsättning och inskrivningsförfarande på elektronisk väg, s. 35.

⁴⁸ RP 146/2010 s. 15.

⁴⁹ I Norros, Olli, *Obligationsrätt*, Helsingfors 2018, s. 429 nämns 13:7 i JB som en särskild regel om regressrätt. Norros betonar på s. 426–427 att de olika lagrummen om regressrätt ”har varierande grund”, men liknande drag utan att ändå utgöra en ”normativt enhetlig typ av fordringsrätt”.

När de elektroniska fastighetsköpen infördes genom lagändringen 96/2011 hade ju 27 § i AutentiseringsL varit i kraft sedan den 1 september 2009. Även om den rätta innehavarens ansvar kan utgöras av avtalsbundenhet enligt HD-fallet 2016:73, ändrade fallet ändå inte rättsläget för identitetsmissbruk vid elektroniska fastighetsköp. Den rätta innehavaren av identifieringsverktygen kan inte bli avtalsrättsligt bunden till rättshandlingen, men kan däremot få ett skadeståndsansvar för sin vårdslöshet gentemot staten.

Regressrätten enligt 9a:3.2 i JB kan förstås riktas mot missbrukaren av identifieringsverktyget, men såsom det anges i propositionen till 9a:3 i JB kan skadeståndsansvaret ”också rikta sig till den person i vars namn rättshandlingen utförts orättmätigt.” I propositionen förklaras vidare att i så fall ska personens ansvar ”basera sig på lag eller avtalsbestämmelser”.⁵⁰ Den lag som blir tillämpligt på den rätta innehavarens ansvar vid missbruk av identifieringsverktyget är utan tvivel 27 § i AutentiseringsL, varför de ansvarsbegränsningar som i lagen gäller för den rätta innehavaren även gäller den rätta innehavarens ansvar vid statens regressrätt. För att den rätta innehavaren således ska bli skadeståndsansvarig ska vårdslösheten vara grövre än lindrig vårdslöshet för att statens regressrätt ska ha framgång.

Slutligen är det värt att kort nämna att den rätta innehavare av ett identifieringsverktyg som blivit avtalsrättsligt bunden till en rättshandling som ingåtts av en missbrukare, i vissa fall kan ty sig till den frånträdesrätt eller ångerrätt som finns vid olika former av konsumentavtal som ingåtts på distans. Ångerrätten blir användbar i de fall då missbrukaren har ingått avtal om varor och tjänster med en utomstående godtroende näringsidkare som ännu inte levererat varorna och tjänsterna. När konsumenten frånträder ett avtal, blir näringsidkaren skyldig att återbetala priset för nyttigheten. Bestämmelser om konsumentens ångerrätt finns i 6:14 i KSL i fråga om bland annat distansförsäljning av varor och tjänster, i 6a:12 i KSL i fråga om distansförsäljning av finansiella tjänster och finansiella instrument, i 7:20 i KSL i fråga om konsumentkrediter, i 7a:17 i KSL i fråga om konsumentkrediter som har samband med bostadsegendom, i 10:9 i KSL i fråga om tidsdelat boende och långfristiga semesterprodukter samt i 15 § i lagen om kombinerade resetjänster (901/2017). Om missbrukaren har lyckats få varan eller tjänsten utlevererad till sig, förlorar frånträdesrätten i regel sin funktion.

I min framställning ovan har avtalsbundenheten stått i förgrunden i de fall då den rätta innehavaren har ansetts ha ett eget ansvar för missbrukssituationerna. De ansvarsregler som finns i finsk rätt läser jag ändå så att de är uttömmande i fråga om innehavarens ansvar och att skadeståndspåföljden även faller bort om den rätta innehavaren undgår avtalsbundenhet. Bestämmelsernas syfte är ju att uttömmande reglera ansvaret hos den vars identifieringsverktyg har missbrukats. Det

⁵⁰ RP 146/2010 s. 35.

blir alltså inte aktuellt att analysera om den rätta innehavaren av identifieringsverktyget kan bli skadeståndsskyldig med stöd av allmänna kontraktuella eller utomkontraktuella regler i de situationer när ansvar inte föreligger enligt de lagrum som jag behandlat här. Inte ens i fråga om de elektroniska fastighetsköpen där ett regresskrav kan riktas mot den rätta innehavaren åsidosätts de ansvarsbegränsande reglerna. Därför blir det inte aktuellt i finsk rätt att diskutera i vilken mån den allmänna bestämmelsen om ren förmögenhetsskada i 5:1 i skadeståndslagen (412/1974) kan tillämpas på den rätta innehavarens ansvar.

Däremot har 5:1 i skadeståndslagen tillämpats i några fall där det har blivit aktuellt att pröva en banks ansvar gentemot en annan banks kund, vars identitet använts när missbrukaren har lyckats få identifieringsverktyg med bankkundens identitet. Rättsförhållandet har ju här varit utomkontraktuellt. I två fall har banken ansetts vårdslös och ren förmögenhetsskada har kunnat utdömas med stöd av motiveringen att det funnits synnerligen vägande skäl i fallen.⁵¹ Enligt den finska skadeståndslagen kan ju ersättning för ren förmögenhetsskada utgå, om orsaken till skadan varit en straffbar handling, myndighetsutövning eller om det i andra fall finns synnerligen vägande skäl.

Till skillnad från svensk rätt har det i finsk rätt inte funnits behov av att gentemot den rätta innehavaren av identifieringsverktyget tillgripa rättsinstitutet återbäring av obehörig vinst i samband med missbruk av e-legitimation. Däremot kan naturligtvis den som mottagit en obefogad prestation genom missbruket bli förpliktad att återbära den obefogade prestationen.

4 Slutsatser

Finsk rätt har sina särdrag i fråga om hur reglerna om ansvaret för den rätta innehavaren av identifieringsverktyg löses i situationer när verktygen missbrukas av någon annan. Ansvarsreglerna motsvarar i stora drag reglerna i de övriga nordiska länderna, men vid en skärskådning av detaljerna i regelverket blir det uppenbart att det finns klara skillnader mellan de nordiska länderna. I artikeln har jag behandlat i huvudsak tre lagrum enligt vilka den rätta innehavarens ansvar begränsas. Dessa lagrum är 27 § i AutentiseringsL, 62 § i BetaltjänstL och 7:40 i KSL. I det förstnämnda lagrummet inträder innehavarens ansvar först när vårdslösheten är grövre än lindrig vårdslöshet, medan ansvaret enligt de två senare lagrummen omfattar även lindrig vårdslöshet. Likväl innehåller de två sistnämnda lagrummen ett tak på 50 euro för innehavaren så länge det inte är fråga om uppsåt eller grov vårdslöshet. I motsats till dansk, norsk och svensk rätt finns det i finsk rätt inget annat tak för innehavarens penningmässiga ansvar.

⁵¹ PKL 32/15 och PKL 117/15.

Innehållet i innehavarens ansvar kan vara antingen att innehavaren blir avtalsrättsligt bunden till den rättshandling som missbrukaren vidtagit eller att innehavaren i övrigt får stå för den förlust som missbrukaren har gett upphov till. Den rättspraxis som finns är sparsam och utgörs främst av fall från banknämnden. Det enda HD-fallet av större betydelse har gällt frågan om avtalsbundenhet vid upptagande av kredit vid ett missbruk av den rätta innehavarens identifieringsverktyg.

I sig skulle det finnas fog för de nordiska länderna att driva utvecklingen av ansvaret kring missbruken av e-legitimation mot en större enhetlighet. Detta skulle kräva aktiva åtgärder dels av lagstiftarna, dels av de rättskipande instanserna. Nu ter det sig som om skillnaderna mellan de nordiska är slumpartade och i stor utsträckning beror på bristande koordination mellan länderna. Detta är förstås inget unikt för missbruksfallen, utan en vanlig tendens i nordisk rätt.