Misbruk av betalingskort

av Øystein Haugen

Liten masteroppgave i rettsvitenskap

Ved Universitetet i Tromsø

Det juridiske fakultet

JUR – 3902

Høst 2012

Innhold

Innledning:

1 Innledning

1.1 Bakgrunn for oppgaven

I dagens samfunn er det nærmest blitt vanlig for alle, å basere store deler av sin private økonomi gjennom bruk av ulike former for plastkort.

Plastkort er gjerne også hovedkilden til kapital på ulike reiser. I manges tilfeller vil nok betalingskort være hovedverdikilden, og kanskje også den eneste verdi den enkelte tar med seg.

Finansnæringens Hovedorganisasjon (FNO) har nylig publisert statistikk som viser at "digitale ran" utgjorde 126 millioner kroner i 2011[1][2]. I norgeshistoriens mest omtalte bankkran, Nokas ranet, fikk ranerne med seg kun ca 57 millioner [3]. Omfanget av misbruk av nettbank og kortsvindel er således meget stort.

Kortholderne blir stadig yngre. Selv under arbeidet med oppgaven var det to oppslag i media om at stadig yngre kortholdere skulle slippes til. I disse dager fortelles det nå om at barn helt ned i 7 års alderen slippes til med bruk av bank kort [4][5].

Av nyere forskningstall fra Statens institutt for forbruksforskning (SIFO), [6] slås det fast at 6,8 % av den voksne norske befolkningen hevder å ha blitt utsatt for identitets tyveri.

I rapporten fra SIFO hevdes det at ca 240.000,- nordmenn, har blitt utsatt for misbruk eller forsøk på misbruk [7].

Med den nevnte stadig økende bruken av plastkort som betalingsmiddel, ønskes det å se nærmere på situasjonene rundt misbruk av betalingskort, hvor ansvaret ligger i ulike situasjoner, samt bakgrunn og benyttelsen av de ulike bestemmelsene.

---

[1] http://www.fno.no/Hoved/Aktuelt/Pressemeldinger/2012/Kortsvindelen-gar-ned/ lest den 22.11.2012

[2] http://www.norges-bank.no/pages/89034/Betalingssystemet2011.pdf pkt 1.5 Nettbank og kort lest den 22.11.2012

[3] http://no.wikipedia.org/wiki/NOKAS-ranet lest den 03.12.2012

[4] http://www.klikk.no/foreldre/article801468.ece lest den 02.12.2012

[5] Artikkel i NA24.no lest den 29.10.2012, publisert den 27.12.2012 klokken 12.01 under headingen "8-åringer får bankkort.

[6] http://www.sifo.no/page/preview/preview/10081/78015.html Oppdragsrapport nr 6 – 2011 Ragnhild Brusdal & Randi Lervik Identitetstyveri "Omfang Tillitt Beskyttelse mot risiko. sammendrag side 3.

[7] http://www.sifo.no/page/preview/preview/10081/78015.html sammendrag

1.2 Problembeskrivelse

I samfunnet i dag er det en voldsom økning i bruken av betalingskort.
I denne oppgaven skal jeg se nærmere på utfordringer knyttet til denne økningen, nemlig misbruk av betalingskort, hvordan dette skjer, ulike metoder, samt hvilke konsekvenser dette har for partene. Og ikke minst hvem skal bære kostnadene og ansvaret, dersom misbruk skulle oppstå. Videre er det interessant å se nærmere på grensedragningene rundt ansvaret og aktsomhetsnormen ved misbruk.

1.3 Historisk Perspektiv

En tidsmessig klargjøring om når penger og pengenes historie stammer i fra, lar seg vanskelig gjøre å stadfeste eksakt. Dette skyldes følgelig tidsperspektivet, samt usikkerheten rundt nedtegnelsene. Det som imidlertid er klart, er at penger som betalingsmiddel strekker seg over flere tusener av år.

På tross av hva man kanskje skulle tro, er ikke selve ordet penger knyttet til en eksakt type gjenstander. I dagens samfunn ser en gjerne på penger utelukkende som mynter eller pengesedler. Man må kunne anta ut ifra et historisk perspektiv, at fra det øyeblikket noe målbart kunne anses som verdifullt, kunne bruken av denne verdigjenstanden anses som en form for penger. Behovet for penger og bruken av penger, var da gjerne knyttet opp til ulike former for byttehandler. Eller som en ren utveksling av ulike varer og tjenester, som man verdimessig vektet opp i mot hverandre. Hva som kunne anes som verdier hadde følgelig sammenheng med i hvilken tidsepoke, samt i hvilket samfunn en tok utgangspunkt i.

Det antas at alt ble så meget bedre, da en kunne ta utgangspunkt i betalingsmidler med en ensartet verdi. Det hevdes at metall som verdi har vært benyttet i minst 4000 år, og som penger i form av mynter i kanskje 2700 år. [8]

Etter hvert som en innså behovet for andre verdier enn nevnte gjenstander, og bruken av disse som bytteobjekter, vokste det etter hvert frem et behov for et mer formalisert system, for økonomiske systemer [9]. Og da var det særskilt Babylonerne som dannet grunnlaget for dagens økonomiske systemer.

Når det gjelder selve lovfestingen av pengenes rolle i det økonomiske samfunnet, så må man se hen til lovene som ble utferdiget av Hammurabi, omtalt som Hammurabi lover eller ”codex Hammurabi”. Utarbeidelsen av dette lovverket stammer fra oldtidens Babyloniske rike ca 17 – 1800 f.kr. Det hevdes at bakgrunnen for lovverket var å få en nærmere beskrivelse, og ikke minst en formalisering rundt penger og verdier: Penger og lovverket rundt dette, ble ansett som sentralt for å få ethvert samfunn til å fungere. Dette synspunktet kan vel sies å ha vel så mye i seg den dag i dag.

[8] Store Norske Leksikon penger, lest 05.11.2012 http://snl.no/penger.
[9] Sheila c dow Journal of Post Keynesian Economics Issue: Volume 27, Number 3 / Spring 2005 side 385 – 391.

Når man etter hvert begynner å se nærmere på de moderne tider, er det fra gammelt av penger i mynt og etter hvert pengesedler som er hovedbetalingsmiddelet. Som betalingsmiddel ved kjøp av varer og tjenester, ved avtaleinngåelser og ulike kontraktsinngåelser.

Når det gjelder koblingen mellom penger og bankfunksjoner, så går dette langt tilbake i tid. Som nevnt over, var Babylonerne sentrale i utarbeidelsen av dagens økonomiske systemer. Ser man på innskudd og utlån som krav til at det er etablert en reel bankvirksomhet, så finner en de første tegnene på dette 1700 f.kr i Babylon, og da koblet til templene. [10]

Det har i de seneste ti år i takt med den teknologiske utviklingen, blitt en ganske formidabel økning i bruken av ulike plastkort. Bruken er da knyttet til betaling av varer, samt andre tjenester. Som nevnt over er ordet penger ikke direkte knyttet til det vi i dag ser på som penge. Alt som kan måles i en verdi, kan defineres som penger. Og i dag er det mer avstand mellom den håndfaste verdien, og pengebruken enn noen gang. Om det kan sies å være en fordel at pengene bare er en sum knyttet opp i mot en liten plastgjenstand, kan det vel i en del tilfeller stilles spørsmålstegn ved [11]

Gjennom økt kortbruk, har man følgelig en helt annen frihet og brukervennlighet. Totalt antall debet kort utstedt av Norske banker, har siden 2000 økt med over 50 %. Og utgjør nå nær 6,9 mill kort pr utgangen av 2011[12].

Transaksjonsmengden gjennom elektroniske kanaler utgjør ganske så store tall, med et gjennomsnittlig bruk på ca 14.000,- kroner pr bank axept kort pr år. I 2010 var antallet registrerte Bank Axept transaksjoner i overkant av en milliard. Fortsetter denne økningen, antas det at vi vil passere 1,3 milliarder transaksjoner med BankAxcept kort i 2012 [13].

Som nevnt går den teknologiske utviklingen voldsomt fremover. Det lanseres stadig nye teknologiske løsninger. Alle løsninger har samme mål, at alt skal gjøres så mye enklere for oss forbrukere.

Ett eksempel på en slik nyvinning er elektronisk kortterminal. Koblet mot mobilen blir den en tilkoblingsbar kortleser [14] Sikkerhetsaspektet er enda ikke særskilt trukket fram som et tema.

Et annet tilsvarende enkelhetsprodukt, er såkalte ”close range” betalingsløsninger (NFC ”near field communication”).

NFC vil høyst sannsynlig i en nær fremtid få betalingskort og penger til å fremstå som gammeldags og utrangert. Gjennom NFC teknologien kan mobilen benyttes som lommebok, der betaling skjer ved å holde mobiltelefonen eller tilsvarende teknologiske løsninger opp i mot en leser.

---

[10] http://historienet.no/handel-og-produksjon/bank-krakk-og-gradighet Lest den 02.11.2012.

[11] http://www.forskning.no/artikler/2011/mai/288038 Frihet i et kredittkort Asle Rønning, publisert onsdag 11. mai 2011 klokken 05. Lest 02.11.2012.

[12] http://www.fno.no/PageFiles/1533/Betalingsformidling%20(kortbruk%20giro%20sjekk).xlsx

[13] Kilde Norges Bank, samt publikasjon av bank statistikk av FNO http://www.fno.no/Hoved/Statistikk/Bank/ (27.10.2012)

[14] www.izettle.com, hentet fra nettstedet den 13.11.2012.

Dette kan jo for enhver høres som en enkel og kjekk løsning, men er man da sikker på at man ikke gjennom slike løsninger utsettes for uautoriserte misbruk? I en nettartikkel vises det til toppsjefene i de to selskapene Telenor og DNB, som sammen demonstrerer slike løsninger.[15] Begge hevder at vi her står ovenfor fremtidens løsninger. I starten så legges løsningene til bruk uten pin kode, og legger da virkelig til rette for kyndiges misbruk av løsningen. Toppsjefen i DNB, Rune Bjerke, hevder i samme artikkel at så lenge kundene ikke opptrer uaktsomt, vil brukerne holdes skadesløse. Uten at dette kan sies å ha noen hold rettslig, all den tid dette er såpass ny teknologi, samt enda ikke tatt i bruk av det store flertallet.

Finansavtaleloven gir i § 35 6 ledd en anledning til å avtale unntak for ansvarsreglene i 1-5 ledd for situasjoner ved bruk av "småpengeinstrumenter" jfr. finansavtalelovens § 12 bokstav r. Jeg forfølger ikke denne misbrukssituasjonen særskilt ytterligere. Det kan imidlertid antas at det for fremtiden nok vil bli en mer aktuell situasjon, da det kan trekkes visse analogier mellom småpengeinstrumenter og rene penger. Det spørs det om det vil bli behov for ytterligere reguleringsbehov på dette feltet.

En som har mye kompetanse på feltet, og gjerne omtales som "iphone- hackeren" Charlie Miller, har holdt en del foredrag og uttalt seg til dels negativt om sikkerhetsaspektet i denne nye teknologien.

I en artikkel fra august 2012 [16]skriver han sågar en bred artikkel om ulike aspekter med NFC, og dens sårbarhet for angrep og misbruk. Han omtaler bruken av NFC teknologi som en egnet inngangsvei for misbrukere til å tømme mobil og mobile enheter for ytterligere sensitive data.

Gjennom en rivende utvikling både i bruk av teknologiske betalingsløsninger og kort liknende produkter, så dukker følgelig spørsmålet opp om en gjennom dette også åpner opp for nye og økte misbruksløsninger. Historien slik en ser det i dag etter innføringen av betalingskort med magnetstripe, viser nettopp dette. Mer om dette nedenfor.

Gjennom at noe blir enklere dukker det gjerne også opp noen negative aspekter med dette, og det er noen av disse oppgaven skal synliggjøre.

Ser en gjennom den korte skisserte historien jfr. over om penger og dens verd, Så er misbruk og tyveri av andres verdier og eiendeler gått hånd i hånd med utviklingen. Gjerne slik at misbrukeren er vel så kreativ som de som arbeider med å forhindre og utelukke.

[15] http://www.dagensit.no/article2172880.ece?screenArea=readmore lest den 12.11.2012, Her betaler Bjerke og Baksaas med mobilen.
[16] Exploring The NFC Attack Surface Charlie Miller August 13. http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf Lest fra nettstedet 10.11.2012.

Kontanter som betalingsmiddel utgjør nå pr 2011, kun om lag 6 % av verdien av de ulike betalingsmidler som forbrukerne disponerer [17]. Aktualiteten av kort og kortmisbruk blir da meget sentral. Dette spesielt i Norge, der kontantmengden er lav sammenliknet med andre land[18].

1.4 Ulike typer Betalingskort

Som nevnt over så skiller man gjerne mellom to typer betalingskort, debet (kontokort) og kredittkort.

Debetkortet gir anledning til direkte trekk mot innestående saldo på kontoen. Identifikasjonen er her gjerne pin kode i sammenheng med magnetstripe eller id-chip.

Problemstillingene skjer følgelig når betalingskortet kommer på uvedkommendes hender. Hvis kortet er et debetkort, vil bruk av bankkortet stort sett fordre bruk av pin kode. Dette siden kortet etter all sannsynlighet er et BankAxcept kort, som er et betalingssystem som vi benytter i Norge. Debet kortet kan også være knyttet mot en av de internasjonale betalingssystemene, som American Express, Eurocard, MasterCard eller Visa.

De aller fleste brukersteder i Norge benytter BankAxcept, der pin-kode er obligatorisk ved kjøp og bruk. Dette gjør at Stjålne debetkort lettere lar seg benytte mot internasjonale betalingssystemer som ikke har like strenge krav om pin kode, eventuelt mot Internett der bruken av CVC kode er tilstrekkelig. CVC kode er et sikkerhetssystem som benyttes hos visa og Mastercard.

Kredittkort, eksempelvis Mastercard, Visa eller Eurocard, benyttes enten ved bruk av pin kode eller ved bruk av signatur. Når det gjelder bruk ved signatur, skal det i de fleste tilfellene kreve at brukeren legitimerer seg, selv om det må antas at det syndes mot dette i mange tilfeller.

1.5 Rettsutvikling kort

Som rettskildemessig utgangs punkt så vil misbrukssituasjoner og forholdet mellom kontohaver og bank / finansinstitusjon, være regulert i finansavtalelovens § 34 og § 35.

Finansavtalelovens § 2 slår fast at lovens bestemmelser ikke kan fravikes til ugunst for kontohaver i misbrukssituasjoner.

Etter den ordlyden og terminologien som benyttes i dag, regulerer § 34 og § 35 plikten og ansvarsfordelingen ved tilfeller av uautoriserte betalingstransaksjoner. De nåværende bestemmelsene er til dels nye. Hovedreguleringen av ansvar finner en i dag i lovens § 35, som tidligere blant annet var regulert av en opphevet § 34.

[17] http://www.norges-bank.no/pages/89034/Betalingssystemet2011.pdf pkt 1 Kunderettet Betalingsformidling. Lest den 22.11.2012.
[18] http://www.norges-bank.no/pages/89034/Betalingssystemet2011.pdf Pkt 1.2 kortbetalinger. lest den 22.11.2012.

Begge bestemmelsene er en gjennomføring av betalingstjeneste direktivet 07 / 64, gjennom artiklene 56 og artikkel 57. Selve innholdet og tanken bak endringen av den tidligere § 34 og utarbeidelsen av den nye § 35 er nærmere omhandlet i forarbeidene [19].

Forarbeidene til samme lov og bestemmelser har følgelig interesse. Forarbeidssituasjonen er stor og mangeartet, med forgreininger inn i flere ulike rapporter. Mer om dette nedenfor.

Bruken av begrepet "grov uaktsomhet" i § 35 leder hen til en utpensling av begrepet gjennom rettspraksis. Med bruken av et slikt juridisk sett allmenngyldig begrep, vil en følgelig finne fragmenter av interesse og juridisk vekt gjennom hele det rettslige universet.

Så selv om en ser på uaktsomhetsvurderingen i lys av en strafferettslig hjemmel, vil det åpenbart kunne være likheter og momenter som kan benyttes ved en vurdering knyttet opp i mot finansavtalelovens bestemmelser. Mer om dette under blant annet teori senere i oppgaven.

Gjennom dagens Finansklagenemnden har en etter hvert ganske omfangsrik praksis knyttet til selve problemet og ikke minst begrepsbruken, mens høyere rettspraksis er begrenset til noen få sentrale dommer.

1.6 Avgrensning og videre fremstilling

I oppgaven skal jeg redegjøre for misbruk av betalingskort.

Finansavtalelovens bestemmelser vil da være sentral for hele oppgaven.

Området har lite rettspraksis, men derav en meget omfattende nemndspraksis samt forarbeider. Siden mye av praksisen er knyttet til nemnden får praksis knyttet til denne en sentral plass i oppgaven. Tar et kritisk blikk på denne mot slutten, da det er aspekter med dette som det kan stilles spørsmålstegn ved.

Et moment som gjerne går igjen i praksis er om kontohaver kan sies å ha opptrådt grovt uaktsomt. Denne aktsomhetsnormen gis da en sentral posisjon gjennom hele oppgaven.

[19] Ot.prp. 94 2008/2009 pkt 15 side 117 felg.

Misbrukssituasjoner

2. Misbrukssituasjoner

Tyveri og misbruk av andres verdier, er trolig en like gammel tradisjon som verdier som betalingsmiddel. Så for å kunne danne seg en oversikt over reglene, er det da viktig å ha kunnskap om de mest sentrale metodene for misbruk som finnes i dag.

Misbruk av betalingskort er en form for organisert kriminalitet, der målet er å skaffe seg økonomisk vinning gjennom tapping av den svindledes kontoer.

Det finnes mange forskjellige metoder for å utføre slike handlinger. Metodene og fremgangsmåtene varierer mye, alt ettersom hvilke svindlere som står bak. Fra det enkleste som et simpelt lommetyveri, til mer avanserte databaserte metoder, der metodene og teknikkene bak både fordrer inngående teknologisk kunnskap samt midler for å fremskaffe teknologien. Bak de mer avanserte metodene, står gjerne større organisasjoner med et stort bak - apparat. Disse opererer gjerne over større flater, og til dels over landegrenser.

Lommetyveri / stjeling av kort er nok den mest vanlige varianten av misbruk blant småkriminelle. Med dagens bruk av pinkoder, samt gode varslingsrutiner ved tap av kort, antas det at kortet i seg selv blir mindre og mindre attraktivt med mindre man besitter kode eller teknisk informasjon / kompetanse. Rent juridisk kan den være vel så interessant med sine aspekter.

2.1 Phishing

Pishing brukes om tilfeller der noen tilegner seg urettmessig informasjon fra kortholder [20]. Det finnes flere former for dette. Nedenfor følger de mest aktuelle. Med dagens teknologiske samfunn med hyppig bruk av nettsider og elektronisk kommunikasjon, har misbruk ved elektronisk post (e-post) blitt en høyaktuell metode. Phishing foregår da ved at avsender av e-posten, fremstår som en troverdig avsender. Gjerne i form av logo / firmainformasjon som skal få mottaker av e-posten til å oppnå tillit. Både elektroniske adresser (url), design og utseende likner gjerne meget på de som skal kopieres. I e-posten eller til en av de sidene man blir linket videre til, oppfordres det da gjerne til å legge inn kortinformasjon eller lignende.

Lokkemidlet for å få e-post mottaker til å legge inn sin kortinformasjon, er gjerne at deres kortinformasjon er kommet på avveie, eller at deres koder er kommet uvedkommende for øye.

Sistnevnte er meget elegant, da den kan utformes slik at man både lokker ut pin-kode samt ber kontoinnehaver opprette et sikkert passord elektronisk til nettbank etc. Her er det da potensial for både kortinformasjon, pinkoden samt i verste konsekvens øvrig passordbruk fra kortholder.

Det siste er spesielt skummelt, da det må antas at bruken av standardiserte passord for privatpersoner øker. På grunn av den økte passord eksponeringen i samfunnet.

[20] Cleber K., Olivo , Altair O., Santin , Luiz S., Oliveira (July 2011). "Obtaining the Threat Model for E-mail Phishing" (PDF). Applied Soft Computing. Archived from the original on 2011-07-08. http://www.inf.ufpr.br/lesoliveira/download/ASOC2011.pdf

Med passordbruk i flere ulike sammenhenger, gjør man det lettere for seg selv å huske ved å benytte faste passord. Følgelig med den risiko at en gjør seg selv mye mer sårbar ved tap av passord.

2.2 Skimming

Ordet skimming brukes om en situasjon der målet er å kopiere kortinformasjon, gjerne fra magnetstripen i bankkortene.

Man kan si at det likner litt på pishing i å søke kortinformasjon, men at det her forgår uten kortholders aktive deltakelse og viten. Ved den mest omtalte og vanlige skimmingmetoden så foregår denne ved uttakssituasjoner i minibanker. Det festes da en form for kortleser utenpå minibanken, som leser av og kopierer kortinformasjonen. Disse innretningene kan være meget avanserte, og ikke minst utformet slik at de kan være meget vanskelig å oppdage. Målet for svindleren er følgelig at kortleseren skal se ut som en naturlig del av selve minibanken. Gjennom kopiering av magnetstripen, kan da svindlerne skaffe seg tilstrekkelig informasjon til å lage en kopi av kortet.

Som kjent vil en dersom en skal bruke et kopiert kort i andre situasjoner enn via eksempelvis internett, være nødt til å skaffe tilgang på pin-kode eller CVC kode. CVC kode er noe som Visa og Mastercard benytter for å trygge sikkerheten. CVC koden, som finnes på baksiden av kortet, skal sikre kortholder mot at det ikke er en skimming kopi av kortet som brukes ved eksempelvis nettbasert handel. Siden CVC koden står på baksiden av kortet, vil det være vanskeligere for svindlerne å kunne få tilgang på denne koden samtidig som en kopierer innholdet i kortets magnetstripe.

Når det gjelder CVC kode og sikkerheten i forhold til denne, er det utredet nærmere når svenskene jobbet med gjennomføringen av betalingstjeneste direktivet[21]. Her tolkes det dit hen at en CVC kode ikke kan anses for å være en personlig sikkerhetsanordning, sett opp i mot direktivets artikkel 61 se særskilt pkt 3.

For ytterligere å bedre sikkerheten, utsteder de norske bankene nå stort sett alle sine betalingskort med chip. Grunnen er at bruken av chip gjør at bankene sikrere kan lagre data på kortet. Chip muliggjør også at mye mer informasjon kan legges inn i selve kortet. Ved bruk av chip, kreves det stort sett bruk av pin-kode. Norge er et foregangsland på dette feltet, bankene kommer dog etter på verdensbasis. Vi må nok fremdeles forholde oss til bruken av magnetstripe enda noen år fremover, og da særskilt på utenlandsturer.

Pinkode står for Personal identifikation kode. Selve koden er en firesifret kode, som trengs i tillegg til informasjonen i selve kortet til å identifisere kortholderen. Bankene har opprettet en sikringsmekanisme, slik at all den datakommunikasjonen som foregår fra en minibank eller en bankterminal forgår som en sikker kommunikasjon. Dette ved at informasjonen som sendes mellom brukerstedet og banken blir kryptert, slik at det vanskelig kan gå an å plukke opp informasjonen som sendes. Og da er det særskilt pinkode sjekken som foregår mellom brukersted og bank som er sentral. Siden bankene har denne praksisen, så må svindlerne finne andre metoder for å skaffe seg pinkode informasjonen.

Dette kan skje ved ”kikke over skulderen” situasjoner. Sikkert virkningsfullt i enkelt situasjoner, men det må vel antas at dette neppe virker over særlig tid. Samt at oppdagelsesrisikoen, samt gjenkjennelsesrisikoen er vel stor.

[21] DS 2008: 86 side 38.

En mer vanlig metode for å skaffe seg pinkoden, er å montere en eller annen form for kamerainnretning over eller rundt minibanken. Innretningen har som formål å kopiere kode informasjonen. Alternativt finnes også ulike teleobjektiv løsninger.

Andre typiske skimming situasjoner er i butikker, taxier eller lignende. Dette er da situasjoner der det er enklere å montere og gjemme unna utstyret som trengs for å utføre svindelen. Både leser - apparater, samt utstyr til avlesning av koder.

2.3 Hacking

Vi er i dag vitne til en enorm utvikling på det teknologiske feltet. Mye av den teknologien som finnes i dag var bortimot uvirkelig for kun noen år tilbake.

Noe så enkelt som dagens mobiltelefoner, innehar i dag mer datakraft og muligheter enn stasjonære og bærbare pcèr for kun noen år tilbake. Gjennom en slik utvikling så sier det seg nesten selv at muligheten for misbruksløsninger knyttet til data blir større. Ulike metoder her er typisk Hacking og web-spoofing, mer om sistnevnte i eget kapittel nedenfor. Det skilles her mellom Hacking som mer aktive angrep på de ulike informasjonskildene, og web-spoofing som mer passive former for misbruk.

Når stort sett alle betalingstransaksjoner i dag er knyttet opp til datatrafikk over internettbaserte løsninger, vil man hele tiden være eksponert for at uvedkommende forsøker å fange opp informasjonen som sendes. Enten ved å bryte seg inn i de ulike finansinstitusjonenes systemer for å tilegne seg verdifull informasjon, eller fange opp informasjonen som sendes fra forbrukerne / kontohaverne.

Når det gjelder de som står bak Hacking, var det fra tidlig av knyttet opp i mot noen få spesielt datakyndige personer. Bakgrunnen for hackingen var ikke nødvendigvis knyttet direkte opp i mot å tilegne seg økonomisk gevinst. Disse var gjerne mer opptatt av å bevise sine kompetanse, samt evner i mer subbaserte grupperinger. Første gang begrepet ble direkte knyttet opp imot en gruppe, var tilbake på 1960 tallet mot en gruppe på Massachusetts Institute of Technology (MIT)[22]. Det som startet i det mer ufarlige, har nå etter hvert utviklet seg til å bli så mye mer.

Hacking er nå i dagen samfunn gjerne tatt over av profesjonelle aktører. Følgelig med minst samme faglige nivå.
Men, nå er målsettingen av utelukkende økonomisk karakter. [23]

Hvis man deler opp Hacking, kan man for enkelhets skyld dele misbrukssituasjoner i fem typer.

1) Misbruk ved inntreden i en annens datamaskin.
   Dette er gjerne forbundet med innbrudd i datatrafikk gjennom trådløse nettverk. Denne formen krever korte avstander. Dette skjer typisk enten i store byer med lett tilgang til nettverk, og ikke minst vanskeligheter i å identifisere angriper. Alternativt kan dette foregå ved at misbrukerne kjører rundt, eller setter seg selv i nærheten av den som det ønskes å kunne hente data fra. Slike typer angrep kan kreve relativt enkle midler, og til en viss grad begrenset kunnskap. Sett ovenfor at målgruppen er til dels lite datakyndige, er muligheten for gevinst ganske stor. Selv om de fleste av dagens nettbrukere har kryptert sine egne trådløse nettverk, hevder de med kunnskap på feltet at dette uten relativt mye vanskeligheter lar seg knekke. Så her er åpenbart risikoen stor.

[22] http://en.wikipedia.org/wiki/Hacker_(programmer_subculture) lest den 22.11.2012 på internett
[23] NOU 2008: 21 Nettbankbasert betalingsoverføring pkt 5.6.1.

2) En annen måte å hacke seg inn i brukerenes datamaskin er via dennes bruk av internett. Her kan det skje ved at brukeren ubevisst blir infisert av program som er laget av misbrukeren. Dette kan skje ved å oppsøke nettsider der slike programmer er representert. Tidligere har besøk på pornografiske nettsider, eller ulike spillsider på internett, vært forbundet med risiko for å bli utsatt for slike programmer. Dette har imidlertid endret seg noe, slik at man nå kan bli utsatt for slik programvare på mer legitime sider. Sågar statlige og kommunale sider [24]

3) En annen måte er at programmet legges inn av brukeren, som blir lurt til å tro at dette er et legitimt program. Dette er gjerne kamuflert som et vanlig program. Slike programmer kan til dels være betydelig mer avanserte. Programmene er gjerne laget med den misjon at de skal ligge i bakgrunnen på pcèn og overvåke. Meningen er at programmet skal oppdage og sende over sensitiv informasjon til tredje part, som da kan benytte eksempelvis passord, fødselsnummer og kontonummer til videre misbruk. I dag er muligheten for direkte misbruk av nettbank mindre, da det gjerne trengs en ekstern kodegenerator eks. Bankid til dette formål. Jo mer avanserte programmene er, jo mer risiko er forbundet med infisering av disse. De mer avanserte programmene kan utføre til dels mange oppgaver på den infiserte pcèn. Fra å ligge i bakgrunnen og overvåke, til mer aktive handlinger som å kopiere alt av bruk via skjerm. I takt med ny teknologi så ser en også her nye former. Her er det faktisk også risiko for kamera overvåkning. De fleste nyere bærbare datamaskiner er i dag utstyrt med kamera, som via riktig program kan sende bilder til misbruker.

4) En annen form for misbruk er angrep på en kundes bruk av pc, eller annen elektronisk innretning. Her er det kundens oppkobling mot internettet som er det sentrale, og ikke minst hva det er som går av data trafikk mellom kundens pc og den mottaker som er tilknyttet. Her er mulighetene for misbruk mange. Det som trolig er mest interessant er følgelig å fange opp data knyttet opp til bruken av nettbaserte betalingstjenester m.m. Med dagens innførte Bankid pålogging, så er direkte tilgang til innloggingen i nettbanken vanskeligere. Men, ved bruk av betalingskort og cvc kode vil tilstrekkelig informasjon for misbruk kunne la seg avdekke ved hacking. Denne formen for misbruk ved at misbrukeren stiller seg mellom kontohaver og bruker og finansinstitusjon, kalles gjerne ”man in the middle” situasjoner [25]. Som nevnt noe redusert risiko ved bruk av nye sikkerhetsløsninger, men åpenbart et problem som foreligger.

5) Den siste potensielle situasjonen for misbruk er der misbruker går direkte på finansinstitusjonene for å hente ut data av interesse. For å lykkes med dette i dag så stilles det til dels betydelige krav til kyndighet og kompetanse. Finansinstitusjonene blir utsatt for tusenvis av forsøk på inntreden i deres system hver dag, både eksternt, samt via infiserte brukere. Når vi i dag hører svært lite om problemer i media, skyldes nok dette at bankene i stor grad lykkes i sitt arbeide med å trygge sine systemer. Men utviklingen går stadig fremover, så dette vil i all anskuelig fremtid være en kilde til utrygghet for både brukere samt institusjoner.

[24] NOU 2008: 21 Pkt 5.6.2 under punkt 2.
[25] http://en.wikipedia.org/wiki/Man-in-the-middle_attack Lest den 22.11.2012.

2.4 Web – Spoofing

Web-spoofing er, som hacking, en internettbasert misbruksmetode. Hele hovedpoenget her er å skape en falsk virkelighet for brukeren, det vil si den som blir utsatt for misbruket [26].

Web-spoofing kan utføres på mange måter. En metode er via mail, der man gjennom en epost som ser legitim ut lures til en side kun opprettet for å hente ut informasjon fra brukeren. Dette er problemstilling som gjerne kobles opp i mot tyveri av identitet jfr. behandling nedenfor, samt pishing jfr. behandling ovenfor.

Falsk identitet gjør at misbrukeren fremstår som noe annet enn hva man egentlig er. Nøkkelen til suksess vil da være å få forbrukeren til å tro på dette. Misbrukerne skaper gjerne en nettside som i form og innhold enten ligner ekstremt på den som man skal etterligne, eller bruker mye arbeid på å få denne til å fremstå så profesjonell og tillitsvekkende som mulig. Ordet tillit er her det viktigste, da det antas at det er tilliten som får de fleste til å bli misbrukt. Linker til falske sider legges da slik at brukerne skal komme over disse, enten via populære nettsteder eller via mail. Det vil i de mest avanserte tilfellene være vanskelig for brukeren å se at en blir videresendt til andre sider enn de planlagte.

Misbrukerne legger gjerne mye arbeide i å kopiere adresser og layout, slik at dette ser nesten eksakt ut som den ekte. Et eksempel kan være www.creditagricoIe.no, her er bokstaven l byttet med bokstaven i i stor form. I en hastig hverdag vil dette raskt bli oppfattet som riktig. Annet eksempel kan være å bytte tallet 0 mot bokstaven o. Alt etter hvilken font og teksttype som benyttes, kan slike skifter bli til forveksling meget likt. Når en først er videresendt til den nye nettsiden, så er det bortimot umulig å avdekke svindelen. En er gjerne vant med at alt som er bak den opprinnelige nettsiden er programmert med en lang adresselinje som en gjerne ser bare et lite utdrag av. *http://www.nordea.no/Privat/Daglig+bruk/*Nett-+og+telefontjenester/Nettbank+Privat/872142.html?WT.svl=mega-menu_daglig-bruk_product_nettbank-privat Her har man et typisk eksempel der bruker søkt etter Nordea nettbank privat og blitt videresendt tilfølgende side. Kun det som er markert med kursiv var synlig i nettleseren. Og for den typiske bruker er det neppe verken vanlig, eller vil gi spesielt mye forståelig informasjon å se hele url-adressen heller. Nordea sin adresse er her kun brukt som en illustrasjon, og utmerker seg heller i positiv forstand i forhold til forståelig tekst i første del av adressen, contra negativt. Poenget er her at dagens adresser er så lange og så intrikate at det for den gjengse bruker er bortimot umulig å se om en blir sendt til feil sted eller ei.

[26] http://www.techterms.com/definition/spoofing lest den 23.11.2012

2.5 Tyveri av identiteten til kontohaveren

I samfunnet i dag ser man stadig oftere tilfeller og forekomster av situasjoner der noen misbruker en annens identitet.

Dette kan følgelig foretas på mange ulike måter. En metode som benyttes ofte i praksis, er bestilling av ulike betalingskort i kontohavers navn. Da vanlige debet kort gjerne fordrer bilder, vil det her være mest hensiktsmessig med en type kredittkort, da disse som oftest utstedes uten bilde. For å kunne utføre en slik svindel, må svindleren skaffe seg tilgang til den fornærmedes fødsel og personnummer. Svindleren benytter da personnummeret til å omadressere post til en annen adresse, for da å motta både kode og pinkode i to separate forsendelser.

Først og fremst må en her mane til alminnelig sunn fornuft. Det viktigste er at personlig informasjon aldri skal komme uvedkommende for øye. Dette er særskilt i tilfeller der dette etterspørres gjennom elektroniske kanaler. Banker og finans institusjoner vil stort sett aldri be om slike informasjoner, med mindre det er kontohaver som har initiert disse opplysningene. Ikke minst gjelder dette passord og pin-kode, som da aldri skal deles med andre uansett.

Relevante rettskilder

3 Relevante rettskilder

3.1 Lovgivningen

Hovedlovginingen om misbruk av betalingskort finner som utgangspunkt i finansavtalelovens kapittel 2 femte under ledd. Her reguleres tilfeller av andres uberettigede misbruk av betalingskort. Av dette kapittelet er det §§ 34 og 35 som er sentrale.

Loven har på dette feltet blitt endret i nyere tid, for å tilpasse terminologi og kundens plikter i forhold til inkorporasjon av betalingstjeneste direktivet. Mer om dette i eget punkt nedenfor.

Lov om finansavtaler har sitt utspring i kredittkjøpslovens (krkjl)[27]. Kredittkjøpsloven, tok over etter den tidligere lov om avbetaling av 1916. Det må kunne sies at kredittkjøpsloven og dagens finansavtalelov har en rimelig broket forhistorie. Med hyppige endringer, og tildels meget omfattende forarbeids mengde tilgjengelig.

Hovedformålet med disse bestemmelsene er å plassere ansvar og fordelig av tap, dersom noen urettmessig skulle tilegne seg en vinning gjennom bruk av et betalingsinstrument.

Her kan man innledningsvis påpeke at det klare utgangspunktet, er at kontohaver ikke kan holdes ansvarlig ved andres uautoriserte betalingstransaksjoner. Det vil si ved uberettigedes misbruk av kontoen jfr. finans avtalelovens § 35.

3.2 Forarbeider

Finansavtalelovens bestemmelser er i henhold til oppgaven av sentral betydning, og derav vil følgelig forarbeidene til denne også være det.

Det samme gjelder også betalingstjenestedirektivet, og dets forarbeider[28]. Direktivet og dets forhistorie vil etter forfatterens mening også favne under hva en kan anse som forarbeider.

Da betalingstjenestedirektivet er såpass sentralt, er dette tatt ut som et eget ledd i forhold til kapittelet relevante rettskilder.

De første forarbeidene til loven stammer tilbake til 1994 [29] Dette var da banklovkommisjonen som den gang, og faktisk også i dag, ble ledet av professor Erling Selvig.

Selvig er i dag over 81 år gammel, og i full sving med Banklovkommisjonens arbeider med å tilpasse tjeneste pensjoner til modernisert folketrygd. Så det er således ikke noe å si på kontinuiteten på banklovkommisjonens arbeider. Arbeidet ledet frem til lovs form [30]

[27] L21.06.1985 nr. 82 Lov om kredittkjøp m. m
[28] Ot.prp. nr 94 (2008-2009)
[29] NOU 1994: 19
[30] Ot.prp. nr 41 (1998-1999) Innst.o. NR 84 (1998-1999).

Norge har inkorporert betalingstjenestedirektivet. Bakgrunnen for direktivet er mangeartet men blant annet er det anført som viktig å opprette et slags indre marked for betalingstjenester. Hovedtanken her antas å være en samordning av de ulike lands rett.

3.3 Rettspraksis

Som nevnt tidligere i oppgaven er det relativt lite dommer i det ordinære rettsystemet knyttet til misbruk av betalingskort.

Tidligere praksis til den nå opphevede kredittkjøpslovens § 13, kan følgelig også ha interesse. Hvor mye vekt det skal legges på eldre dommer, må sees opp imot hvilke aspekter med dommen man trekker slutninger ut ifra.

Betalingskort og forholdene rundt dette har hatt en såpass stor utvikling siden kredittkjøpslovens virke, at praksis rundt denne bør benyttes med varsomhet. Det er imidlertid begrepsbruk som går igjen både i dagens lovgivning, og dagens praksis. Det er særskilt vurderinger rundt aktsomhetsnormen og begrepet grovt uaktsomt, der det gjerne hentes momenter fra eldre tids praksis.

3. 4 Nemndspraksis

Det har vokst frem en ikke ubetydelig nemnds praksis i Norge i dag. Mye av dette er knyttet til perioden etter innføringen av dagens regelverk, med base i betalingstjeneste direktivet.

Tidligere nemnds praksis vil følgelig også være av interesse, all den tid den tar for seg mer generelle situasjoner eller begreper som uaktsomhets betraktninger eller lignende.

Når en ser på rettens bruk av nemndspraksis i sine vurderinger, er det åpenbart at denne er av sentral betydning.

I nesten alle de nyere dommene knyttet til finansavtaleloven, er det knyttet argumentasjon opp i mot praksis i Bankklagenemnda, eller Finansklagenemnda som den kalles i dag.

Finansklagenemnda nyter åpenbart stor respekt. I dag er nemnden ledet av Cecilie Østensen, til daglig leder av Borgarting Lagmannsrett.

Ser en på noen av de nyere sakene i Finansklagenemnda, så vil selve saksforholdet og de typiske trekkene ved sakene, minne mye om de nevnte sakene i det ordinære rettsapparatet.

Dog er det aspekter ved nemndspraksis som bør trekkes frem spesielt. Behandler dette senere i oppgaven.

3.5 Betalingstjenestedirektivet

Norge har inkorporert betalingstjenestedirektivet. Bakgrunnen for direktivet er mangeartet. Som bakgrunn er det påpekt viktigheten av å opprette et slags indre marked for betalingstjenester "Single European Payments Area" i Europa[31].

Hovedtanken her antas å være en samordning av de ulike lands rett. Da det etter hvert har vist seg som en utfordring at betalingstjenester og regulering av disse tjenestene, har vært basert på det enkelte lands egne retningslinjer og regelverk.

Ved utarbeidelsen av direktivet hadde inntil 27 forskjellige land retningslinjer på dette feltet.[32]. Med den fremvoksende globaliseringen og stadig økende betalingstransaksjoner mellom de ulike landene, har det presset seg frem et behov for en mer ensartet regulering av dette feltet.

3.6 Juridisk teori

Hvis en ser på selve temaet for oppgaven "misbruk av betalingskort" er det meget begrenset av stoff som er skrevet direkte mot dette temaet. Så vidt forfatteren kan fastslå, så er dette den eneste oppgaven med dette som tema. Med forbehold om at det finnes oppgaver / tekster, med begrenset publisitet.

Hvis en ser på antall artikler eller korte notiser rundt problemstillingen, er dette til dels en meget betydelig mengde. Dog er den juridiske interessen i mange av disse av høyst moderat betydning. Da disse enten ikke går spesielt i dybden, eller i sin helhet ikke går inne på de juridiske aspekter av temaet. Mengden er gjerne nyhetsartikler eller lignende.

Hvis en trekker temaet litt utover og ser på juridisk teori om viktige aspekter med problemstillingene, så blir forholdet en helt annen.

Det temaet som i denne sammenhengen kanskje er det mest sentrale, er uaktsomhet.

Uaktsomhet er et begrep uten konkrete retningslinjer for hvorledes denne aktsomhets vurdering skal foretas i de ulike sakene. Vil juridisk teori om aktsomhet åpenbart ha sin verdi. Da disse i likhet med denne oppgaven, tar sikte på å utpensle noen generelle momenter som definerer aktsomhetsnormen på dette feltet.

3.7 Forskning om misbruk av betalingskort

Når det gjelder forskning om misbruk av betalingskort så er det stort sett begrenset til ren statistikk og tallmateriale. Statens institutt for forbruks forskning foretar årlig en undersøkelse på dette feltet. [33]

Denne gjennomføres årlig på et gitt representativt utvalg. I denne er det blant annet lagt inn spørsmål om bank og banktjenester. Og tanken er at det er et representativt utvalg av respondenter som svarer på undersøkelsen.

[31] Ot.Prp nr.94 (2008-2009) pkt 2.2 Betalingstjenestedirektivet.
[32] Reir. 2007/64/EF (Betalingstjenestedirektivet, innledning, underpunkt 2).
[33] http://www.sifo.no/page/Publikasjoner//10081/78015.html lest den 11.12.2012

Utvalget skal være på nærmere 50.000 personer mellom 18-80 år. Så det må antas at dette tross metodikk med bruk av elektroniske media innhenting (utfordring blant de eldre), vil gi en relativt god pekepinn blant de 1124 respondentene. [34]

Videre har både Finansnæringens Hovedorganisasjon (FNO), og statistisk Sentralbyrå tellinger om både kortbruk og kortmisbruk. Av disse er nok de mest oppdaterte og frekvensmessige hyppigste, fra FNO.

Når det gjelder forskning direkte mot misbruk, er dette av mer lukket publisitet, da både finansinstitusjoner samt statlige organer bruker en del midler på dette.

[34] Oppdragsrapport nr 6 – 2011 Ragnhild Brusdal & Randi Lervik Identitetstyveri "Omfang Tillitt Beskyttelse mot risiko. Pkt 1-2.

Finansavtalelovens regler om misbruk

4 Finansavtalelovens regler om misbruk

4.1 Kundens plikter i forhold til bruken av ulike betalingsinstrumenter

En oversikt over kundens plikter ved bruk av betalingsinstrumenter, finner en nå i FiL § 34 (1) som er en gjennomføring av direktivets artikkel 58 [35]

Her er det kundens plikter for å forhindre misbruk, og hva denne skal foreta seg ved eventuelle situasjoner, eksempelvis varslingsplikter som er påpekt.

En kan gjerne se fil § 34 første og annet ledd, som en form for skikk og bruk regel. Gjennom å påpeke at dette er forhold som det er viktig at kunden tenker over, og er seg bevisst. Hvor mye vekt domstolene har lagt på første ledd første punktum, kommer jeg tilbake til senere i oppgaven. Det kan imidlertid påpekes at de ensidig utferdigede standard vilkårene, nok rent praktisk viser seg å ha begrenset vekt

Første ledd slår fast at bruken av betalingsinstrument skal skje i samråd med de vilkårene som foreligger ved utstedelse. Første ledd viser da til de standardvilkår som utsendes fra finansinstitusjonene. Behandler senere i oppgaven anvendelsen, og den rettskildemessige betydningen av standardvilkårene.

Kontohaver skal beskytte sine personlige sikkerhetsanordninger så godt det lar seg gjøre. Og dersom misbruk oppstår, varsle om dette så snart det lar seg gjøre, jfr. bruken av begrepet ”uten ugrunnet opphold” jfr. 1 ledd annet punktum.

FIL § 34 er også knyttet til fil § 35 Fjerde ledd, Som er direkte knyttet til § 34 første ledd, første punktum, og påpeker at kunden ikke svarer for tap etter varsling om misbruk. Forsømmelse av underretning om misbruk kan etter § 35 tredje ledd medføre økt ansvar for tap. [36]

Fjerde ledd regulerer ansvaret for bankene i forhold til når og ikke minst hvor ofte disse kan skifte ut betalingsinstrumenter.

Jo hyppigere skifte og utsendelse, jo større er risikoen for at uvedkommende får tilgang på instrumentet. Jfr. ovenfor i forhold til identitetstyveri m.m.
Bankenes ansvar er da frem til utlevering til kunden. Bestemmelsen er en gjennomføring av direktivets artikkel 56.[37]

Her kommer det da inn et problem i forhold til post og postkasser. Etter hva forfatter har kunnet avdekke, så er det ikke noen kortutstedere som pr dags dato krever låsbare postkasser eller lignende.

[35] DIR 07/64 artikkel 56.
[36] DIR 07/64 artikkel 59.
[37] DIR 07/64 artikkel 56.

Videre så bør kontoinnehaver være påpasselig med destruering av personopplysninger og liknende før disse kastes i avfallet. Gjennom moderne avfallsorterings krav, vil følgelig papir avfallscontainer kunne være et yndet sted for slike opplysninger.

Mye av tanken bak arbeidet med loven, og de endringene denne medførte, var å gi en mer oversiktelig rettstilstand enn det var før. Veldig mye av regelverket på en del av områdene, var knyttet opp til finansinstitusjonene sine standard vilkår [3839].

Når det gjelder bruk og hvorledes kortene skal oppbevares, så sier standard vilkårene gjerne ikke spesielt detaljert om hvordan kortholder skal forholde seg. Standard vilkårene har gjerne generelle passuser, som at kortene skal oppbevares på betryggende måter eller lignende. Samt at kort og koder (Pinkoden) skal oppbevares adskilt.

Hva som ligger i betryggende måter, vil da være vanskelig å forholde seg til.

Forfatteren gjorde en undersøkelse i Trondheim by en formiddag, og spurte enkeltpersoner på gaten. Om hvorvidt de oppbevarte koder til sine bankkort i sitt eget hjem. Av de ca 50 stykker som svarte, så hevdet halvparten at de nok kunne ha koder en eller annen plass i hjemmet. Følgelig ingen kvalitativ eller kvantitativ representativ undersøkelse, men det viser til problemet rundt kort og pin koder samt betryggende oppbevaring. Og ikke minst hvor lite fokus det er på beskyttelse av sine egne personlige sikkerhetsanordninger.
Det kan således stilles spørsmålstegn ved mange av de sammenlikningene som gjøres i rettspraksis, om hva som kan forventes av en normalt aktsom person..

Standard vilkår er som kjent gjerne utferdiget med hovedvekt på den ene parten sine hensyn. Siden dette var et område som angikk så mange mennesker, var det et åpenbart behov for regulering av dette feltet. Og da ikke minst å sørge for regler på dette feltet, som ivaretok tanken om forbrukerbeskyttende lovgiving [40]

Mye av behovet for lovgivningen, var å tilpasse regelverket vårt til datidens internasjonale direktiver og lover og regler. Følgelig knyttet opp til EØS avtalen og EF lovgivningen.

I Nord-Troms herredsrett sin sak fra 1991 var det et spørsmål om det var kontohaver eller banken som skulle dekke tapet ved ikke autorisert uttak. [41] Saken var her at kontohaver hadde tapt sitt kort, som senere over en tidsperiode på opptil 2 måneder hadde blitt utsatt for urettmessig bruk av kortet over en tidsperiode fra mai 1987 til oktober 1988 på inntil kroner 93.400,- Det springende punktet i dommen er hvorvidt kontohaver hadde utvist grov uaktsomhet. Her henviser de både til Torvund [42] samt analogislutinger til datidens kredittkjøpslov § 13. Betraktninger om hvorvidt kontohaver har opptrådt grovt uaktsomt, er typisk noe som også går igjen i dagen praksis. I selve hendelsesforløpet går det frem at kontohaver hadde for vane (grunnet dårlig husk), å oppbevare sin pin kode på en lapp oppbevart sammen med lommeboken. Følgelig stikk i strid med bankens tilsendte kontoinstruks.

[38] NOU 1994: 19 side 12 pkt 1.2 sammendrag.
[39] NOU 1994: side 25-25 pkt 2.2 mandatet, samt pkt 2.3.
[40] NOU 1994: 19 Del 1 alminnelige motiver side 11, pkt 1.1 i. f.
[41] RG 1992 297 Nord-Troms herredsrett. Dom 19. september 1991 i sak nr. 1133/90
[42] Olav Torvund betalingsformidiling s 126.

Dette ble av retten konkludert med som en lite betryggende metode. Banken ble av retten idømt å dekke kontohavers tap i nærmere 3 måneder etter at kortet ble varslet tapt, det ble i denne saken knyttet ansvar opp i mot skadeerstatningslovens § 5-1 om at medvirkning fra skadelidte sin side, kan medføre lemping av ansvar. Banken ble bebreidet for ikke å iverksette sikringstiltak og nærmere undersøkelser, når kortet ble varslet tapt i mai 1987. Kontohaver sitt ansvar ble her lempet i perioden frem til 7. juli 1987, men det ble fra retten sin side påpekt at lempingen ikke kunne fortsette i det uendelige.

Det kan vel stilles bemerkninger til om ikke kontohaver her nok måtte bli ilagt ytterligere ansvar etter dagens regelverk og praksis, men det antas at prinsipper om lemping etter skadeerstatningslovens § 5-1 fremdeles kan være av interesse i dag.

Av Finansklagenemndens sin sak av 2010[43] Ser en et tilfelle der kortholder kan sies ikke å ha overholdt sin aktivitetsplikt etter § 34. Her hadde kontoen i over et år blitt gjenstand for misbruk av kontohavers sønn. Her hadde ikke kontohaver verken ved tilsendte kontoutskrifter, eller på annet grunnlag oppdaget misbruket av ca 240.000,- Kontohaver ble av nemnden funnet å kunne bli holdt ansvarlig for hele det oppståtte tapet, grunnet passivitet.

I Eidsivating lagmannsretts dom [44]fra 1993 etter datidens kredittkjøpslov § 13 var det også et spørsmål om hvorvidt kontohaver hadde opptrådt på en måte at denne kunne anses for å ha opptrådt grovt uaktsomt.

Den ankede part (banken) støttet sin argumentasjon på blant annet Torvund og Liv Synnøve Taraldsrud. [45] Retten mente at kontohaver hadde opptrådt på en slik måte at forholdet kunne anses som et avvik fra det forsvarlige (uaktsomhet). Mindretallet mente i tillegg, at det hadde forekommet et markert avvik fra det forsvarlige og derav kunne karakteriseres som grovt uaktsomt.

Kontohaver hadde lagt fra seg lommeboken på et utstillingsområde uten tilsyn, og derav fått frastjålet sitt betalingskort av typen Eurocard. Det er Interessant at retten viser til et 5 dagers kontrollkrav til kontohaver om hver femte dag å sjekke hvorvidt kortene fremdeles er i besittelse. Prinsippet er hentet i en uttalelse i datidens Bank klage nemnd. [46] Prinsippet er hjemlet i Kredittkjøpslovens § 13, og nærmer utdypet i forarbeidene [47] " at kontoinnehaveren har plikt til løpende å kontrollere at han har kontokortet i sin besittelse."

Av Agder Lagmannsretts dom av 2009 er det spørsmål om forståelsen av finansavtalelovens § 35 4 ledd annet punktum. [48]

[43] FINkn 2010 – 162. (15.10.2010)
[44] LE-1993-65 - RG-1994-676 (105-94)
[45] Olav Torvund i Lov og Rett 1986 347, Olav Torvund: Betalingsformidling i et rettslig perspektiv (1993) 269 og Liv Synnøve Taraldsrud: Betalingskort i forhold til kredittkjøpsloven og finansieringsvirksomhetsloven 31.

[46] BKN-1993-2
[47] Ot.prp.nr.34 (1980-1981), side 84 spalte 2
[48] RG-2009-746

For at Kontohaver skal holdes ansvarlig for inntil kroner 8000,- er det et krav om at kontohaver har fått faktisk kunnskap om den irregulære bruken. Selve bestemmelsen i § 35 4 ledd kom inn under behandlingen av lovforslaget, og var således ikke den del av den utredningen som kom fra banklovkommisjonen.

Det vises til forarbeidene[49] om hvordan bestemmelsen er tiltenkt en funksjon som en sikkerhetsventil, slik at det i tilfeller der kontohaver har eller burde ha fått kunnskap kan ilegge denne utvidet ansvar.

Finner ikke rettens argumentasjon spesielt overbevisende, i forhold til A sitt krav til kontroll av kontoer. Det hevdes fra rettens side at kontohaver burde ha oppdaget det misbruket som foregikk, på tross av at kontohaver hadde kortet i sin besittelse.

Selve misbruket ville kunne latt seg avdekke ved bruk av nettbank i den perioden.

Det kan spørres om retten i dette tilfellet, la vekt på den i dette tilfellet avdøde sin svekkede helse og alder i forhold til kravet til kontroll. Her kunne det kanskje vært på sin plass med en nærmere utredning i forhold til hvorledes kravet til kontroll er å anse, eksempelvis trukket inn lagmannsrettens dom av 1993 [50], i forhold til dennes påpekte 5 dagers kontroll?

Når det gjelder vekten av de tilsendte standardvilkårene er de til en viss grad henvist til i praksis [51] [52]. Det som imidlertid gjerne går igjen som i nevnte dom i Oslo byfogdembete, er at retten viser til standardvilkårene, da disse gjerne er trukket frem fra Bankenes side.

Retten nevner dette, men velger å støtte sin argumentasjon mer mot lovverket og retts og nemndspraksis. Dette er nok noe grunnet at det i de samme tilfellene er påstander om hvorvidt kontohaver har opptrådt grov uaktsomt. Så av dette samt nærmere behandling nedenfor i forhold til aktsomhetsnormen, kan det nok utledes at bankenes vilkår er sentrale dog med noe begrenset vekt rent praktisk.

[49] Ot.prp.nr 41 (1998-1999) s 44 -45.
[50] LE-1993-65 - RG-1994-676 (105-94)
[51] RT 2004 – 499 pkt 30.
[52] TOBYF – 2010 – 77875 Rettens vurdering pkt 1 – 2.

4.2 Finansinstitusjonenes ansvar for å motvirke misbruk

I Fil § 34 annet ledd reguleres bankenes ansvar.

Hovedpoenget her er at bankene skal sørge for personlige sikkerhetsanordninger, typisk at pin koder ikke kommer på avveie eller kommer på uvedkommendes hender. Følgelig er ansvaret begrenset til å gjøre dette tilgjengelig for kunde. Kundenes separate ansvar for å forhindre at uvedkommende får tilgang til sikkerhetsanordningene etter første ledd gjelder følgelig sidestilt. Herunder også bankenes ansvar for til stadighet å videreutvikle sine sikkerhetsrutiner i takt med misbrukeres stadig økende kunnskap og kreativitet. Som nevnt utvikles det stadig nye "smarte" løsninger for betaling. Ved svikt i sikkerhetsløsningene rundt disse, vil dette åpenbart kunne brukes mot bankene.

Bankene bruker enorme ressurser for å bedre sikkerheten i sine betalingsterminaler og minibanker. Det som gjerne brukes nå, er ulike former for elektroniske sensorer og følere. Disse monteres av bankene, med eneste oppgave å oppdage uvedkommendes forsøk på misbruk.

Finansinstitusjonene opererer gjerne med egne til dels store avdelinger, som kun har som oppgave å oppdage og forhindre kortsvindel. Disse avdelingene er gjerne satt opp med tidligere spesialister, fra eksempelvis Kripos eller Økokrim: De samme statlige organene som til daglig arbeider med organisert økonomisk kriminalitet. Etterforskning og påtale ligger således til disse organer.

En måte å avdekke slik organisert virksomhet, er ved å oppdage og kartlegge mistenkelige transaksjoner. Dette vil si transaksjoner som avviker fra det normale handlingsmønsteret til kontohaveren, og gjerne knyttet til transaksjoner over internett. Dette er en meget utfordrende og tidkrevende prosess, og ikke minst må en trå varsomt i forhold til hvor langt bankene kan gå i kartleggingen i forhold til personvernet. Bakgrunnen er å avdekke svindlernes tester. Da det har blitt avdekket og konstatert tilfeller der svindlerne ønsker å teste sine kopierte kort og koder i små skala, før de benytter dette til eksempelvis store kontantuttak eller varekjøp.

Noe å glede seg over, er at det kan se ut som om tross ekspansiv økning i kortbruk så reduseres svindel mengden. Fra 200 mill i 2010 til nærmere 130 mill i 2011. Tallene for 2012 er enda ikke klare, men på telefonkontakt med FNO så signaliseres det en videre bedring fra 2011 tallene.[53]

Problemet er om reglene slik de etter hvert har blitt, maner til ytterligere innsats på dette feltet. Noen tanker om det rent rettspolitiske mot slutten av avhandlingen.

[53] Kilde FNO 31.10.2012.

4.3 Tapsbegrensningsreglene

Finansavtalelovens § 35 gir en samlet oversikt over ansvaret for kontohaver ved misbrukssituasjoner, både i forhold til hvilke betalingsinstrumenter som er misbrukt, samt hvordan forholdet stiller seg ved ulike skyldgrader hos kontohaver

Tidligere skilte loven mellom misbruk av konto og misbruk av betalingsinstrument. Med betalingsinstrument henviser § 35 1 ledd til fil § 12 C

Med betalingsinstrument menes "personlig instrument eller sett av prosedyrer som er avtalt mellom kunden og institusjonen, og som kunden benytter for å iverksette en betalingsordre". Fra forarbeidene er bruken av ordlyden betalingsinstrument noe annerledes, som en oppramsing: sjekk, giro, betalingskort eller annet særskilt hjelpemiddel for uttak eller overføring av betalingsmidler[54]

Finansinstitusjonen bærer det fulle ansvaret ved tap. For kunden sin del vil dette som utgangspunkt tilsi at kontoen ikke kan belastes til kontohavers skade. Her må da finansinstitusjonen bære hele tapet dersom det skulle oppstå en misbruks situasjon. Fra denne hovedregelen gjøres unntak dersom kontoen er tappet ved bruk av personlig sikkerhetsanordning, og at dette kommer som følge av at kontohaver har opptrådt grovt uaktsom eller forsettlig. Kunden er ikke ansvarlig ved lavere grader av uaktsomhet [55] Dersom kunden har opptrådt forsettlig kan denne holdes ansvarlig for hele tapet. Det presiseres at kunden kun svarer for inntil kroner 12.000,-. Dersom transaksjonen har skjedd ved bruk av et elektronisk betalingsinstrument. Ikke elektroniske betalingsinstrumenter er typisk sjekk, papirgiro etc. Som nevnt senere i oppgaven, er det til dels betydelig praksis knyttet til akkurat denne delen av bestemmelsen. Da i utgangspunktet i de tilfeller der kontohaver hevdes å ha opptrådt grovt uaktsomt

Fil § 35 første ledd er en direkte inkorporasjon av Betalingsdirektivet DIR 07/64 art 60 (1). [56]

Går en videre til andre punktum så presiseres det hva en uautorisert betalingstransaksjon er. En autorisert betalingstransaksjon er i utgangspunktet en transaksjon som er foregått uten at kontohaver har samtykket. Dette ser vi av lovens disponeringsregler i § 24 2-4 ledd. For at denne bestemmelsen skal komme til anvendelse, må det ha forekommet en situasjon der andre har skaffet seg tilgang til kontoen og belastet denne.

Ved tilfeller der finansinstitusjonen selv har medvirket til feilaktig trekk fra konto eller lignende, faller slike tilfeller under finansavtalelovens § 32. Dette kan være ulike tilfeller av systemsvikt, enten selv eller av leverandører eller lignende [57].

[54] NOU 1994: 18 Finansavtaler og betalingsoppdrag. Del utredning 1 1994-12-15. Kap 2 innskuddskonto og betalingsoppdrag § 2-4 (c) definisjoner
[55] Innst O.nr 124 (2008-2009) side 8 -9.
[56] Rdir.2007/64/ef (betalingstjenestedirektivet - konsolidert) artikkel 60.
[57] NOU 2008: 21 Nettbankbasert Betalingsoverføring 2.6.1.

Andre ledd er også en inkorporasjon av betalingsdirektivets regler. [58]

Dette leddet regulerer egenandelsansvaret for kunden dersom det skulle oppstå misbruks situasjoner. Typisk tilfeller er hvor bankkort blir stjålet eller kopiert og deretter misbrukt. For at egenandelsansvaret skal være aktuelt etter 2 ledd så er det en forutsetning om at personlig sikkerhetsanordning er benyttet, herunder typisk pin kode i oppgavens sammenheng, Eventuelt tilfeller der noen på en lovstridig måte har tilegnet seg kunnskap om sikkerhetsanordningen og benyttet seg av denne.

Under arbeidet med finansavtaleloven var det mye diskusjon rundt ansvarsfordelingene mellom kunde og finansinstitusjon. Ikke minst om det skulle være egenandelsregler, og eventuelt hvorledes disse skulle utformes. Her er det følgelig til dels forskjellige syn som kom frem under prosessen alt etter hvilken del av partene som uttalte seg. [59]

Den delen av paragrafen som kanskje har mest omtale og mest praksis knyttet til seg er bestemmelsenes 3 ledd. Dette er en inkorporasjon av betalingsdirektivets art 61 som annet ledd. Tredje ledd gjør at kunden må svare for tap inntil kroner 12.000,- Dette ved uautoriserte betalingstransaksjoner der kunden kan hevdes å ha opptrådt grovt uaktsomt. Eksempelvis ved å unnlate å oppfylle sine plikter etter § 34 første ledd.
.

4.4 Bevisbyrdesituasjonen

Finansavtalelovens § 35 5 ledd omhandler bevisbyrdesituasjonen.

Bevisbyrdesituasjonen var mye diskutert i forarbeidene, samt har vært gjenstand for mye praksis både etter gammel og ny lovgivning [60]

Selv om det nå fremkommer eksplisitt av loven hvem som er pålagt bevisbyrden, kan man også i dag se noe forskjellig praktisering.

Bestemmelsen i § 35 5 ledd viser til at dersom et betalingsinstrument er benyttet, og at dette i følge kunden er en uautorisert betalingstransaksjon etter § 24 annet ledd, skal ikke bruken i seg selv være bevis for at kunden har medvirket, opptrådt forsettlig eller opptrådt på en grov uaktsom måte. Bevisbyrden er her da følgelig pålagt institusjonen.

Om en ser nærmere på praksis, så er dette ofte påpekt i saker i forhold til vurderingen av sannsynlighetsovervekt. Og det er nettopp dette sakene ofte dreier seg om. Hvor sannsynlig er følgende scenario, sett opp i mot de forhold som foreligger.

Bankene tar følgelig en nøye teknisk og spormessig undersøkelse, slik at mye av faktum for en sannsynlighetsvurdering ligger klart fra dennes side. Selve bestemmelsen er en gjennomføring av direktivets artikkel 59, med ny lovtekst med virkning fra 01.01.2009. [61]
Ser en på Moss Byrett sin dom av 2001 [62] vises det til at det ikke foreligger en særskilt bevisbyrderegel når det gjelder sannsynligheten av misbruket.

[58] DIR 07/64 art 61. nr1
[59] Ot.prp. nr 94 (2008-2009) side 133 pkt 15.6. Høringsinstansenes syn.
[60] Ot.prp. nr 94 (2008-2009) side 113- 114, 119.
[61] L19.06.2009 nr. 81 i kraft 01.11.2009
[62] RG 2001 1294

Dette er en sak etter gammel lovgivning, før selve bevisbyrderegelen kom inn i loven som følge av direktivet jfr. ovenfor. Her er det prosedert på en alminnelig regel om sannsynlighetsovervekt, noe annet enn etter ny lov. Og ikke minst i henhold til uttalelsene om dette i forarbeidene til datidens lov [63].

Retten går inn i forarbeidene og ikke minst innst. O der stortingskomiteen støtter departementets syn. Dommen er etter forfatterens mening en meget utfyllende og klar definisjon på hvorledes bevisbyrderegelen skal forstås, og vil av den grunn kunne være sentral også etter ny lovgivning. Kortholder ble her ikke anset for å ha muliggjort misbruket ved grov uaktsomhet.

Retten tar i dommen en inngående vurdering av både bevisfremlegg og vitneavhør. Trekker man en parallell mot nemndas summariske skriftlige behandling, kan en åpenbart syne noen problemstillinger. Og da særskilt i forhold til hva som kan anses å være bevist eller ei. Mer om denne problemstillingen, mot slutten av oppgaven.

Det som er verdt å merke seg er at det kan synes om de ulike innstansene har et noe annerledes forhold til bevisbyrdesituasjonen. Der retten i stor grad er tro mot lovgiver og forarbeider, mens det i nemnden vurderes litt annerledes i noen saker.

Det kan synes som om det oppstod et regimeskifte tilbake til 2001, som fortsatt virker å ha virkning. Her i en sak fra 2001 i datidens bankklagenemnd [64] Kortholder ble frastjålet sin lommebok med betalingskort. Spørsmålet var da hvorvidt det var sannsynliggjort at koden hadde blitt oppbevart sammen med kortet. Banken pekte på tidsaspektet siden kortet sist var i bruk, samt at pinkoden ble benyttet riktig på første forsøk. Nemnda hadde forut for dette vært tilbakeholdne med å behandle slike saker grunnet uklarhet rundt årsaksforholdene [65]. Tidligere hadde de kun behandlet saker der det var bevist hvorledes pinkoden hadde kommet misbrukeren til kjennskap.

Nemnden viser her til at det tidligere ikke har blitt sett på som hensiktmessig med en behandling i nemnden, grunnet den skriftelige behandlingsformen. Nemnden finner i denne saken grunnlag for å skifte retning, og heller ta saken under behandling. " I og med at denne type saker, som nevnt, antagelig ofte vil være like opplyst under behandlingen for Bankklagenemnda, som det er grunn til å tro at den vil bli under en eventuell domstolsbehandling".

Nemnden peker her på mye av den samme utfordringen som jeg kommer tilbake til i et eget kapittel nedenfor.

Nemnden har da vist og holdt seg til denne betraktningen også etter senere tids praksis eksempelvis i sak av 2011 [66], som typisk er avgitt i dissens, dog med at nemnden finner forholdet tilstrekkelig sannsynliggjort til å kunne realitetsbehandles..

[63] Ot.prp nr 41 (1998 – 1999) s 44., samt Innst. 0 nr 84 (1998 – 1999)
[64] BKN 2001 - 017.
[65] BKN 2001 – 017 Del 2 nemdas begrunnelse.
[66] 2001 – 555.

4.4 Aktsomhets normen

Når en ser nærmere på det antallet med dommer og rettspraksis som knytter seg til misbruk av betalingskort, så er det rimelig åpenbart at det springende punktet er rundt vurderingen av om kortholder har muliggjort misbruket på en måte som kan karakteriseres som grovt uaktsomt. Dette gjelder særskilt finansklagenemnden, som til stadighet har tilsig av saker knyttet mot finansavtalelovens § 35 3 ledd. 3 ledd hensetter til en konkret skjønnmessig totalvurdering, om hvorvidt kunden har opptrådt grovt uaktsomt i henhold til pliktene etter kontoavtalen, samt forhold rundt misbruket og beskyttelse av de personlige sikkerhetsanordningene.

Som nevnt tidligere er utgangspunktet at det er bankene eller finansinstitusjonene som er ansvarlige ved misbruk av betalingskort. Dette er synliggjort gjennom både forarbeider samt rettspraksis og til dels gjennom den store mengden nemndspraksis som foreligger. Det må i forhold til aktsomhetsnormen foretas en skjønnmessig totalvurdering i hvert enkelt tilfelle, om hvorvidt kontohaver har opptrådt grovt uaktsomt. Herunder spesielt om kontohaver har gjort det som forventes i forhold til å beskytte de sikkerhets foranstaltninger som foreligger i forhold til betalingskort, særskilt pinkoden.

Det er ofte i praksis henvist til forarbeidene både til innføring av betalingstjenestedirektivet, samt til tidligere arbeider. Det antas at bakgrunnen for dette er at det gjennom praksis som nevnt nedenfor, ikke lar seg gjøre å oppstille en konkret regel. Når en ser nærmere på forarbeidene, så kan det sies at disse vel så bra som i en del praksis gir viktige parametre for selve uaktsomhet vurderingen. Samt det forhold at forarbeidene er påberopt i et stort antall saker.

Da endringene knyttet til direktivet er av såpass nytt tidsperspektiv, så er det følgelig enda ikke så mye praksis knyttet til disse forarbeidene som de som er nevnt ovenfor. Dog er dette, i forhold til oppgaven, av meget sentral betydning da dette er en gjennomføring av de privatrettslige bestemmelsene i direktivet 2007/64 [67] Bakgrunnen for disse endringene var å gjennomføre direktivets bestemmelser til norsk rett.

Når det gjelder situasjoner med misbruk av konto og betalingsinstrument, er dette også drøftet under en annen utredning fra banklovkommisjonen [68], som i utgangspunktet var om nettbankbasert betalingsoverføring.

Begge disse forarbeidene vil da være høyst aktuelle rettskilder, der stoffet i dette tilfellet går over i hverandre. Ganske spesielt da de i tid ligger nær knyttet opp til hverandre. Utredningen fra banklovkommisjonen er også tatt inn i forarbeidene knyttet til direktivet [69]

[67] DIR 2007/64/EF
[68] NOU 2008:21 nettbank basert betalingsoverføring
[69] OT prp: NR 94 (2008-2009) pkt 15.4 side 125.

Gjennom denne sammenflettingen, vil følgelig begge settene med forarbeider være av interesse ved bruk av forarbeider som rettskilde. Nå er imidlertid forarbeidene knyttet til betalingstjenestedirektivet som til syvende og sist resulterte i utferdigelsen av de konkrete paragrafer. Dette vises følgelig av synene til departementet, som mener at en må se bort i fra Banklovkommisjonens forslag, da denne ikke tydelig nok tar inn en gjennomføring av betalingstjenestedirektivet[70] Dog nyter Banklovkommisjonen stor anseelse for kvaliteten av sitt arbeide, slik at der dennes arbeide går på generelle betraktninger kan dette være å anse som vektige argumenter ved juridiske vurderinger. Spørsmålet er om de omfattende tilpasningene og endringene de senere år, kan virke ekskluderende på forarbeider knyttet til de foranliggende lovreglene. Forfatteren kan ikke se at temaet er særskilt behandlet av øvrige, så dette får være opp til rettsapparatet, å eventuelt vekte betydning av dersom aktuelt.

Når det gjelder bruken av forarbeidene så er disse til dels ofte vist til i praksis, og da ofte i forhold til saker om misbruk av betalingskort. Det er åpenbart at forarbeidene står sterkt, dog er henvisningene gjerne knyttet til generelle retningslinjer.

I forhold til aktsomhetsnormen er det vanskelig å hente ut materiale av forarbeidene som direkte setter linjer for vurderingen. Det som imidlertid kan utledes er at normen i seg selv ikke kan sies å være konkret, og at uttalelse om dette prinsippet i forarbeidene [71]ofte er hevdet i praksis. Så gjennom dette må en søke å oppstille noen ytterligere momenter, hentet fra rettspraksis.

Som Borgarting Lagmannsretts dom av 2002 [72] Der pin koden var oppbevart sammen med kortene i pengeboken, vesken med innholdet ble stjålet og kortene ble misbrukt. Pinkoden var skjult i et fiktivt telefonnummer, og spørsmålet var om dette karakteriserte som grovt uaktsomt i henhold til finansavtalovens § 35 annet ledd bokstav a. I tilfelle kontohavers forhold tilfredstilte kravet til grov uaktsomhet, så fikk banken medhold i sitt krav om utvidet egenandel.

Selve rettens konklusjon og bemerkning er her noe vanskelig å få tak i, da denne ikke knytter argumentasjonen opp til noen konkrete rettskildefaktorer, annet enn at denne konkluderer med at det foreligger grov uaktsomhet fra kontohavers side og at dommen var enstemmig.

Fra den ankende parts side (banken) er det henvist til både generelle høyesterettsdommer om grov uaktsomhet [73] , samt til teorien her representert ved Peter Lødrup. [74] , samt forarbeidene til finansavtaleloven [75] Sistnevnte har en nærmere redegjørelse av pin kodens oppbevaring sammen med kortene, er et eksempel på situasjon som kan lede til at forholdet anses som å være grovt uaktsomt. I dette tilfellet var Pinkoden kamuflert på en etter (red.anm. noe enkel måte), slik at bevisbyrden i forhold til selve forholdet var noe lettere.

[70] Ot.prp. Nr: 94: (2008-2009) Pkt 15-7Side 134.
[71] NOU 1994:19 side 145
[72] RG-2002-1273 (198-2002)
[73] til Rt-1970-1235, Rt-1989-1318 og Rt-1995-486
[74] Peter Lødrup Lærebok i Erstatningsrett. 4 utg.
[75] Ot.prp. nr 41!1998 – 1999) side 45.

Saken, samt konklusjon minner mye om dom i Borgarting Lagmannsrett av 2003. [76] i saken ble kortholder frastjålet sin lommebok med tre kredittkort, sammen med sin 7. sans. I sistnevnte var kodene kamuflerte blant en rekke av tall, koblet til sine sønners fødselsdager og tall. Her også var det hvorvidt kontohaver hadde opptrådt grovt uaktsomt, som var det springende punktet. Dom ble avsagt i dissens der lagmannsretten sitt flertall konkluderte med at det forelå grov uaktsomhet. Sakens fakta var om nedtegning av koden samt oppbevaring av denne sammen med kortene, eller i hvert fall i umiddelbar nærhet, var å betrakte som grovt uaktsomt. Kodene var her nedtegnet i kamuflert form, dog oppbevart sammen med kortene i en avlåst leilighet der det ble foretatt innbrudd.

Det kan i så måte argumenteres for at kontohaver her er mindre å bebreide, enn for eksempel i Borgarting lagmannsretts dom nevnt over. Der både kort og kode nedtegninger var konstant oppbevart sammen i lommeboken, samt muligens dårlig påpasselighet med vesken i forkant av tyveriet.

Lagmannsretten konkluderte med at forholdet samlet sett kunne anses som grovt uaktsomt, og at kontohaver da etter § 35 annet ledd svarte for inntil kroner 8000 for andres urettmessige bruk av betalingskort.

Lagmannsretten har her i motsetning til dom i Borgarting lagmannsrett [77]jfr. over, tydeliggjort hvorledes denne har kommet frem til sin konklusjon. Når det gjelder selve uaktsomhetsvurderingen legger retten til grunn forarbeidene sine krav til at det må foreligge et markert avvik fra en forsvarlig handlemåte [78]. Med støtte i forarbeidene viser retten til at det må foretas en skjønnmessig totalvurdering, også sett i lys av den kontoavtale som er inngått.

Retten delte seg i et flertall og et mindretall. Mindretallet mente at det forelå uaktsomhet, men at denne ikke burde karakteriseres som grov. Bakgrunnen for at mindretallet tok dissens, kan tyde på at disse la avgjørende vekt på at innbruddet foregikk fra en forsvarlig låst leilighet i en noe tyveriutsatt by. Slik at koden og kamufleringen totalt sett ikke alene var tilstrekkelig til å kunne kalle dette uaktsomt. Det spilte nok også et forhold at kort og kode var oppbevart i en låst koffert, samt at korthaver var ute av leiligheten i en kort periode.

Høyesterettspraksis knyttet til finansavtaleloven § 35 er begrenset til å gjelde en sak. Dette er ankesaken over Borgarting Lagmannsretts dom nevnt over [79] [80]

Høyesterett kom til motsatt konklusjon i forhold til lagmannsretten, og anså ikke forholdet til å være grovt uaktsomt. Banken prosederte mye av sine argumenter opp i mot at deres avtalevilkår klart bestemte at koden ikke under noen omstendighet skulle noteres ned. Noe som banken i ettertid hadde fjernet fra sine standardvilkår, til at koden burde huskes. HR la åpenbart lite vekt på bankens utferdigede standard vilkår, og gikk videre til å vurdere selve uaktsomhetsvurderingen. Der uaktsomhetsvurdering ble knyttet til hvordan koden ble oppbevart og kamuflert.

[76] LB-2002-1943
[77] RG-2002-1273 (198-2002)
[78] NOU 1994:19 side 145.
[79] Borgarting Lagmannsrett LB 2002 – 1943, RT 2004-499.
[80] Rt-2004-499

Denne dommen trekkes frem i et kapittel nedenfor, da denne viser med tydelighet både rettskildemessig forskjellig bruk mellom de ulike domstolene, tvisteorganer, samt viser tydelig utfordringer med forskjellene på saksforløp.

Av finKN sin sak av 2011 [81] ble kortholders betalingskort misbrukt ved tre tilfeller i utlandet. Kortet ble hevdet å ikke ha vært på avveie, men det ble blant annet forsøkt anført at kort og kode kunne ha blitt kopiert. I denne saken ble kortets chip benyttet ved bruken, noe som FinKn konkluderte er et bevis for at riktig kort ble benyttet. Sett opp i mot riktig kode på første forsøk, er dette sterke indisier på at det her høyst sannsynlig stammet fra kortholders egne bruk av kortet. Kortholder ble her dømt til å holdes ansvarlig for hele beløpet. I denne saken ville også et mindretall, henvise videre til det ordinære rettsapparatet for ytterligere opplysning og nærmere utredning. (Ytterligere et eksempel i forhold til bevisbyrde situasjonen nevnt ovenfor).

Nemnden og domstolene har da funnet det nærliggende at koder eller forsøk på kamuflerte koder har vært oppbevart i sammenheng med kortene. De faller da gjerne ned på at kontohaver har opptrådt grovt uaktsomt. Sånn sett stikk i strid med de uttalelsene om bevisbyrde som fremgår av forarbeidene, samt finansavtalelovens § 35 femte ledd.

Høyesterett sin vurdering nevnt over gir etter forfatterens mening den beste presiseringen, i forhold til å definere normen som en vid total vurdering.

Ser en på domspraksis, så har partene tildeles brukt gamle anerkjente lærebøker og forfattere når de skulle søke støtte for sine aktsomhetsvurderinger. Når er ser på de ulike forfatterne som har skrevet om dette temaet, samt hvordan de har angrepet dette, så er det vanskelig å finne store avvik opp igjennom tidene.

Eksempelvis i lagmannsrettens dom av 2002 [82]. Her blir to av de sentrale forfatterne trukket frem henholdsvis Peter Lødrup og Nils Nygaard [83] Her er det den ankende part som trekker inn teorien, og henviser til alminnelig strafferettslig og erstatningsrettslig litteratur. Retten viser ikke direkte til dette i sin konklusjon, så det er usikkert på hvorvidt de la avgjørende vekt på dette. Ganske likt er det i Borgarting Lagmannsrett sin dom av 2002 [84] Her ble det også fra bankens side anført de samme forfatterne. Her ble imidlertid banken gitt medhold i sin vurdering om det forelå grov uaktsomhet, dog uten at retten anførte dette til prinsipper knyttet mot de nevnte forfatterne.

Slik en kan se det så er teorien i mange saker trukket frem som argumentasjon fra partene i forhold til uaktsomhetsvurderinger, dog er det vanskelig å finne eksempler på at retten har benyttet disse aktivt i sin argumentasjon. Juridisk teori sin rettslige vekt i disse sakene er således noe usikkert. På den annen side så kan det anføres at betraktninger rundt uaktsomhets vurderinger nok trolig sitter såpass i ryggmargen til jurister. Det kan både i erstatningsrettslige samt strafferettslige sammenhenger, sees som alminnelig kunnskap og således mindre sentralt å trekke frem eksplisitt.

[81] FinKN -2011-224.
[82] LB 2002 - 01943
[83] Peter Lødrup Lærebok i Erstatningsrett 4 utg. side 123, og Nils Nygard Skade og Ansvar side 212.
[84] RG 2002 1273.

En kan se en forskjellig bruk av rettskilder avhengig av i hvilket domsorgan saken er behandlet. Det kan fra forfatterens side se ut som om det er stor grad av variasjon om hvorledes dommerne, eller nemnden angriper uaktsomhetsvurderingen.

Av mange av nemndens saker, samt saker behandlet av underrettene kan det se ut som om de meget lett faller ned på at kontohaver har opptrådt grovt uaktsomt dersom misbruket av kortene har kommet uten at dette har medført for mye prøving og feiling hos misbruker.

Dette vil si at det vanskelig kan la seg gjøre å definere en konkret grense for normen, og at det nok blir for enkelt slik enkelte domsavgjørelser samt nemndsavgjørelser faller ned på i forhold til misbruk ved bruk av pin kodene.

Dette er åpenbart reelle faktorer i vurderingen, men som enkeltfaktorer i en totalvurdering. Det er vanskelig å oppstille en generell aktsomhetsnorm om hvorledes kontohaver skal oppbevare samt skjule sine sikkerhetsanordninger.

Som nevnt i HR sin dom over [85], der HR fant at forholdet og kontohavers opptreden åpenbart var å bebreide, men ikke i tilstrekkelig grad til at dette kunne karakteriseres som grovt uaktsomt.

Av dette kan det trolig utledes at dersom en oppbevarer koder sammen eller i nærheten av betalingskortene, er det lite som skal til for at forholdet anses som grovt uaktsomt. Særskilt dersom koden eksponeres i ren form, eller en relativt enkel kamuflert form.

[85] RT 2004 s 449.

Rettspolitiske problemstillinger på området

5. Rettspolitiske problemstillinger på området

5.1 Nemnden et rettsikkerhetsproblem?

Det er helt åpenbart at gjennom sin kvalitet og ikke minst ved involvering av profilerte og meget kompetente personer, eksempelvis tidligere ved Viggo Hagstøm, og i dag nestleder Trygve Bergsåker, har Finansklagenemnda fungert som den klart mest sentrale formen for tvisteløsning på dette feltet. Mange av sakene har stoppet etter nemndsbehandling, og har av den grunn ikke belastet det ordinære rettssystemet nevneverdig. Til dette kan det imidlertid settes noen betraktninger om dette er fullt ut ønskelig fra samfunnet sin side, da med henblikk på rettssikkerheten.

Av flere av nemndsakene fremgår det at medlemmer av nemnden (ofte mindretallet), påpeker at nemnden ikke kan ta stilling til saken grunnet for liten opplysning. Det er i sakene gjerne forbrukersiden som tar dissens. Viser i så måte til regimeskiftet av 2001 som nevnt i kapittelet over om bevisbyrdesituasjonen.

Den summariske behandlingen vil alltid være en svakhet med slike nemnder, og det er også gjerne dens styrke som da er rask og kostnadseffektiv saksbehandling. Når nemnden likevel fatter beslutning i slike saker, til dels på en meget overbevisende måte, må det antas at det ved flere av disse sakene nok kunne ha vært fordelaktig med en ytterligere bevisføring.

Ytterligere saksgang er følgelig opp til partene. Antagelsen er at nemnda nyter så stor respekt fra partene sin side, at de anser dette for et signal om hvorledes retning saken står.

Verdt å merke seg at nemnden i flere av sakene faktisk går i mot både rettspraksis og klare føringer tatt ut ifra forarbeidene [86]

Av FinKN sak av juni 2011 [87] fremgår argumentasjonen som ganske interessant sett opp imot både ordinære domstolers rettspraksis, samt klare uttalelser i forarbeidene fra departementets side. Her er det som ofte i slike saker, spørsmål om oppbevaring av kode sammen med et frastjålet kort. Kortet ble frastjålet fra kortholders hjem. Kortet ble senere misbrukt, og banken holder da kortholder ansvarlig for inntil kroner 12.000,- av tapet som fremkom. Det ble sannsynliggjort at pinkoden ikke ble avdekket sist kortet var i bruk 4 dager før misbruket.

Det springende punktet er da om det er sannsynliggjort at koden i ren form eller i kamuflert form, er oppbevart sammen med kortet. Også i denne saken delte nemnda seg i et flertall og et mindretall, der flertallet mente at saken er tiltrekkelig opplyst til å kunne realitetsbehandles. Det fremgår ikke av faktum at koden er bevist oppbevart sammen med kort eller i nærheten av kortet, dette anses uansett av nemnda som overveiende sannsynlig.

[86] FinKN 2011-276
[87] FinKN 2011-276

Mindretallet viser til uttalelser i tidligere sak [88], som igjen viser til uttalelser i forarbeidene om bevisbyrderegel.[89] I forarbeidene er forholdene rundt en generell bevisbyrderegel i slike tilfeller nøye vurdert. Lovgiver falt ned på ikke å lovfeste en generell bevisbyrderegel på dette feltet. Og uttaler videre:

"Det bør også understrekes at selv uten en lovfestet bevisbyrderegel vil en nemnd eller en domstol ikke kunne legge til grunn at kunden har opptrådt grovt uaktsomt uten at det foreligger særskilte holdepunkter for dette. At Pinkoden er brukt uten at kunden har noen forklaring på hvordan koden er blitt kjent for uvedkommende, kan ikke være tilstrekkelig til å legge til grunn at kunden har opptrådt grovt uaktsomt og på dette grunnlag ilegge ansvar. Koden kan f. eks ha blitt kjent for uvedkommende ved at misbrukeren, uten at kunden har merket det, har iakttatt kundens inntasting av kode i forbindelse med bruk av kortet. "

I forbindelse med aktuelle sak finner imidlertid flertallet stikk i strid med ovennevnte uttalelse i forarbeidene, at det totalt sett er mest sannsynlig at koden er ervervet gjennom oppbevaring sammen med det tapte betalingskortet.

Nemnda tar igjen en avgjørelse i dissens i en sak om misbruk av betalingskort, med et saksforhold som tyder på et noe uklart forhold rent faktummessig. Uenigheten skyldes både om saken er tilstrekkelig opplyst, samt det rettslige grunnlaget for avgjørelsen.

Nemnden bruker åpenbart den mest sentrale retningsskiftende avgjørelsen som nevnt over [90]. Dette kan anføres som en svekkelse av hvorledes nemnda sine avgjørelser vil kunne stå seg i en behandling for de ordinære domstolene. Etter hva forfatteren kan se ligger det en noe usikker rettstilstand, der nemnden har en noe annen bevisbyrde regel enn hva en kan se av rettspraksis.

Dette kan synliggjøres ytterligere i en tidligere sak.

Denne saken har gått igjennom hele rettsapparatet, og sluppet helt opp til HR og nevnt under rettspraksis ovenfor. Denne saken vil nok kunne være et god eksempel på tilfeller der nemnda og det ordinære rettssystemet betrakter sakene ulikt.

Ikke minst de rent juridiske vurderingene, som avviker på sentrale punkter. Dommen er noen år gammel, men er knyttet til de samme bestemmelsene, så det antas at de samme vurderingene er like aktuelle i dag. Det er lite i høyere rettsinstanser, som det kan utledes noe annet ut av. Denne saken viser at det er forskjeller mellom nemnda og det ordinære rettssystemet i hvorledes faktorene vektes og ikke minst hva det legges avgjørende vekt på. Ikke minst er det verdt å merke seg på hvorledes nemnden er tro mot sine egne avgjørelser, mens retten bruker flere rettskildefaktorer i sin argumentasjon.

Av nemnda sin sak av 2001 [91], er det som tidligere nevnt en sak om misbruk av betalingskort. Nedenfor følger en sammenlikning fra nemnden opp til HR, for å se om det er noen generelle betraktninger som kan trekkes ut.

[88] BKN 2001-38
[89] Ot.prp. nr 41(1998-1999) side 44 pkt 8.7.4. Departementets vurdering.
[90] BKN 2001 - 017.
[91] BKN 2001-38.

Saken er en kunde som ble frastjålet en lommebok fra en låst koffert i en låst leilighet i Spania. Nemndas mindretall hevder også her at saken er for lite opplyst til at denne bør realitetsbehandles i nemnda, og heller behandles i det ordinære rettsystemet. De viser også her på samme måte som nevnt over i [92], at det vil være vanskelig for en domstol eller nemnd å legge til grunn at kunden har opptrådt grovt uaktsomt dersom det ikke foreligger helt særskilte holdepunkter for dette.

Flertallet mente saken burde behandles, samt konkluderte med at koden etter all sannsynlighet ble oppbevart sammen med bankkortet i lommeboken, og ikke nødvendigvis ble lest ut av den syvende sansen som kortholder stadig hadde i sin besittelse? (annet fremgår av faktum som fremkommer av den ordinære rettspraksis).

Nemnden finner ikke å kunne klarlegge hvorledes koden kunne komme i misbrukeren sin besittelse, men velger da likevel å konstatere at det foreligger grov uaktsomhet.

Saken ble deretter påanket til Oslo Tingsrett som avsa dom av 2002 [93], etter at kontohaver hadde blitt dømt i forliksrådet, som også tolket forholdet til å anses som grovt uaktsomt. Retten påpeker som ganske selvsagt at selve kjernespørsmålet er om "saksøker ved grov uaktsomhet har muliggjort misbruket".

Tingsretten går her mer tilbake til kjernen i uaktsomhetsvurderingen, og trekker inn blant annet skadeerstatningsteorien [94]. Retten viser til en rekke tilsvarende saker i forhold til datidens bankklagenemnd, som henviser til at det skal benyttes en streng aktsomhetsnorm i slike tilfeller.

Det vil si kontohavers plikt til å hindre andre i å misbruke ens betalingskort. Tingretten trekker sammenlikninger opp i mot flere saker i nemnda, som har ganske sammenfattende hendelsesforløp. Som vist over, er mange av disse sakene avsagt i dissens, der dissensen i mange tilfeller dreier seg om hvorvidt saken er tilstrekkelig opplyst til at realitetsbehandling er egnet i nemnden.

Det som imidlertid skaper problemer, og som retten så riktig påpeker, er at det etter hva forfatteren kan se ikke finnes noen klare bestemmelser som klart trekker en grense mellom simpel og grov uaktsomhet.

Det kan synes som om retten her ved å vise til andre saker med forsøk på å kamuflere kodene, har tatt en selvstendig vurdering av "kvaliteten" i selve kamufleringen og benyttet dette som en vektig faktor i selve uaktsomhetsvurderingen.

Forhold om selve innbruddet oppbevaring i låst koffert m. m kan ikke sees vurdert av retten. Retten konkluderte noe overraskende ut i fra sin egen argumentasjon med grov uaktsomhet.

Det forhold at den syvende sans nå plutselig i forhold til behandlingen i klagenemnden, ikke var i kortholders besittelse, er overhodet ikke omtalt. Her er etter forfatters mening et typisk eksempel som støtter opp i mot mange av de avgjørelser som er avgjort under dissens nevnt over. Det vil si ved anførsler fra mindretallet hvorvidt sakene er tilstrekkelig opplyste, og derav egnet for realitetsavgjørelse.

[92] FinKN 2011-276
[93] TOSLO -2001-11895.
[94] Nils Nygaard Skade og ansvar side 209.

Slike eksempler kan således tas til argument for at nemndens praksis bør benyttes med varsomhet, da en ikke nødvendigvis har tilstrekkelig oversikt over hele faktumbildet.

Saken ble videre anket til Lagmannsretten som tok denne inn i 2002 [95] Saksforholdet stod følgelig likt i forhold til tingrettens behandling. Lagmannsretten går her videre i forhold til dybden av argumentasjonen i forhold til tingsrettens dom. Lagmannsretten viser til utgangspunktet i forarbeidene om at nedtegning av koden i seg selv ikke kan karakteriseres som grovt uaktsomt [96], går dernest videre på en generell vurdering av aktsomhetskravet sett i lys av alminnelig erstatningsrett.

Retten viser videre til at for å hevde et forhold til å kunne anses som grovt uaktsomt, så tilsier dette et markert avvik fra vanlig forsvarlig handlemåte. Selve vurderingen måtte sees i lys av både oppbevaringen av betalingskortet, samt oppbevaring av koden og evt. kvaliteten av kamufleringen. Her går da retten etter forfatters mening mer i dybden, og det anses som en bedre utredning rent juridisk.

I selve domsslutningen delte retten seg. Flertallet gikk inn for at kortholder hadde muliggjort misbruket, på en måte som kunne karakteriseres som grovt uaktsomt. De la særskilt vekt på at den syvende sansen med kodene var oppbevart sammen med lommeboken i den låste kofferten.

Mindretallet konkluderte motsatt, og la sin betraktning på hva som ville være en normal forsvarlig handlemåte i denne situasjonen. Blant annet det forhold at byen der misbruket hadde funnet sted, var preget av til dels høy kriminalitet. Og at det for folk flest ville betraktes som en fornuftig handling å unnlate å ta med seg kortene ut i bybildet.

At kortene samt den syvende sansen, til slutt ble lagt sammen i samme låste koffert, er følgelig å bebreide kortholder. Men, sett opp i mot forholdene samt det relativt korte fraværet, anså de dette som en handlemåte som ikke kan karakteriseres som et markert avvik fra forsvarlig handlemåte.

Etter forfatterens mening har mindretallets konklusjon mye for seg, i forhold til både forarbeider samt øvrig praksis. Problemet er her følgelig som nevnt over, at det ikke finnes klarlagte retningslinjer å legge avgjørelsen opp i mot.

Saken ble sluppet inn for Høyesterett som avsa dom i 2004 [97]. Høyesterett kom her til en avgjørelse som i konklusjon strider mot tingretten og lagmannsretten sine avgjørelser.

HR tar en generell betraktning til innholdet og kravet til om forholdet kan anses ”grovt uaktsomt”, med hentydning til en generell dom om uaktsomhet. Det må « foreligge en kvalifisert klanderverdig opptreden, som foranlediger sterke bebreidelser for mangel på aktsomhet »

Selve vekten av denne uaktsomhetstolkning i dommen reduseres ved at HR selv refererer til at denne behandler Grov Uaktsomhet i forhold til en straffebestemmelse. HR viser videre til et par andre dommer der markert avvik fra forsvarlig handlemåte etc., er behandlet.

Det som HR i likhet med de nevnte dommer jfr. ovenfor sitter igjen med, er en skjønnmessig totalvurdering av om selve forholdet kan være å anse som grovt uaktsomt.

[95] LB 2002-1943.
[96] Ot.prp. nr 41 (1998-1999) side 44.
[97] RT-2004-499

HR går videre inn i selve vurderingen av kvaliteten av kamufleringen av kodene, samt en vurdering av selve forholdet rundt tyveriet og situasjonen. Totalt sett antas det at kodene ble oppbevart sammen med kortene i en kort periode, i en situasjon som for de fleste personer kunne anses som en trygg situasjon. Dette ble nok ilagt avgjørende vekt.

Når det skal forsøkes å trekke noen generelle betydninger av dommen, så er det et par momenter som peker seg ut.

For det første så legger HR i denne saken relativt liten vekt på de ensidig utferdigede standard vilkårene til banken, og mye mer vekt på generelle vurderinger.

Dette kan tyde på at disse vil bli ilagt liten betydning også i lignende saker. Videre er det verdt å merke seg at det forholdet at kodene er nedskrevet, ikke i seg selv er noe som automatisk vil anses som grovt uaktsomt.

At kodene er nedtegnet kommenterer HR på følgende måte:

” for mange kortinnehavere ville det også være meget vanskelig å praktisere en ordning hvor man var helt avskåret fra å notere ned tallkoden ”.

Men, at dette ved den totale aktsomhetsvurderingen vil være av vesentlig betydning hvordan koden var nedtegnet og forsøkt skjult.

I motsetning til flertallet i underrettsdommene, så går HR nøyere inn på forholdene rundt selve oppbevaringen, og vurderte dette opp i mot hva en forsvarlig handlemåte totalt sett ville være for en normalt aktsom person.

Det vil si oppbevaring i en tyveriutsatt by, og at koden ble først riktig på 4 forsøket.
HR anfører videre at det for en normal person antagelig ville være utfordrende å finne de riktige kodene basert på de forsøk som bankenes sikringssystem legger som tilgjengelige.

Med en kamuflering, som åpenbart kunne ha være bedre, karakteriserer HR ved flertallet dette som uaktsomt, men ikke som en handlemåte som kan karakteriseres som grovt uaktsomt.

Mindretallet la forøvrig til grunn samme argumentasjonsmetoden, og hadde i utgangspunktet samme rettslige vurderings kriterier. Disse vektet kvaliteten av kamufleringen, samt det at koder og kort ble oppbevart i nærhet, til at det totalt sett og i lys av situasjonen kunne dekkes som grovt uaktsomt.

5.2 Rettskildebildet i Endring

Rettskildebildet som vi kjenner det fra vår tradisjonelle metode, er under stadig utfordring. Og da særskilt med bakgrunn i innføringen av EMK i norsk rett, samt tilsluttingen til EØS avtalen. Mange kompetente jurister har stilt spørsmålstegn på hvorledes den nye situasjonen til syvende og sist skal løse seg [98] .

Rettskildebildet vil i saker som oppgaven her tar for seg, utvides med muligheten til å dra inn nye rettskilder i mange av de sakene som føres for norske rettssystemer og saler. For de partene som da fører saker med benyttelse av utenlandske rettskilder, får sakene en meget utvidet kompleksitet samt en fordyrende prosess for alle involverte parter.

For aktørene vil materialet følgelig være vanskelig tilgjengelig, og fellesnevneren vil i så måte være fordyrende. Om dette er ønskelig i aktuelle saker, kan det følgelig stilles spørsmålstegn ved, da det i prosesser om misbruk av bankkort gjerne kjennetegnes med en finansielt sterk part med bortimot ubegrensede prosessmidler. Dette i mot en part som tar prosesskostnader som et vektig vurderingstema underveis [99].

Her kan man undertiden håpe på en mer ensartet juridisk tenkning, og kanskje så langt som et juridisk samarbeide på tvers av landegrensene. Dette i saker som omhandler bestemmelser som springer ut av direktiver eller lignende.

Professor Kai Kruger har i et par tekster ganske tidlig sett nærmere på problemstillingen rundt ovennevnte, samt norske juristers ensartede juridiske metoder.

Hvordan kan dette medføre problemstillinger sett opp i mot den stadig økende internasjonaliseringen? Artiklene er noen år gamle, men kan sies å være mer aktuelle enn noen gang.[100] [101]

Mye av reglene i eksempelvis finansavtalelovens § 34 og 35 er, som nevnt knyttet nært opp til innføringen av betalingstjenestedirektivet i norsk rett. Hovedtanken her antas å være en samordning av de ulike lands rett. Da det etter hvert har vist seg som en utfordring at betalingstjenester og regulering av disse tjenestene, har vært basert på det enkelte lands egne retningslinjer og regelverk.

[98] Se for eksempel Gunnar Nerdrum, Menneskerettighetene ved en skilleveg? Lov og Rett 1997 s. 102-111, Kai Krüger, Finanger-dommen og den nye rettskildefaktor: Frykten, Jussens Venner 2001 s. 89-104, Morten Eriksen, Parallell bruk av administrativ tilleggsskatt og straff etter ligningsloven, Tidsskrift for strafferett 2001 s. 167-210 og Tolle Stabell, Rettsliggjøring - domstolenes skjønnsmessige overprøvingen Festskrift til Carsten Smith, Oslo 2002 s. 811-832.

[99] Hans Peter Graver Internasjonale Konvensjoner som rettskilde (Publ: Lov og Rett s 468).

[100] Kai Krüger Vil Norsk Juridisk Metode overleve i et integrert Europa? Publ: Juristkontakt 2/96 s 2 (JK-1996-2-2).

[101] Kai Krüger Komparativ Rettsmetode – observasjoner vedrørende metoder for rettsanvendelsen i Europa. Publ: Jussens venner 1996 s 281 – (JV-1996.281).

Ved utarbeidelsen av direktivet hadde inntil 27 forskjellige land retningslinjer på dette feltet.[102]. Med den fremvoksende globaliseringen, og stadig økende betalingstransaksjoner mellom de ulike landene, har det presset seg frem et behov for en mer ensartet regulering av dette feltet. I så måte så vil andre lands praksis i forhold til lignende situasjoner åpenbart kunne benyttes som rettskilder. Spesielt vil dette være i perioder etter at det annet land har tatt inn bestemmelser som bygger på betalingstjenestedirektivet. Dog må man ta hensyn til de underliggende forskjeller, som ligger i det å benytte annet lands rettsregler. Dette med bakgrunn i de øvrige rettskildefaktorene som også kan hensyntas ved vurderingen, kan være forskjellige fra land til land.

Dette kan man blant annet se i forhold til lov forarbeidene [103] .

Da man vurderte løsninger knyttet til fastsettelsen av bevisbyrderegler, var det mye uenighet i forhold til dette. Sett opp imot andre lands løsninger, herunder i dette tilfellet våre naboland Sverige og Danmark. I Sverige ville de legge bevisbyrden for at kundens personlige sikkerhetsanordninger ikke har blitt beskyttet, på kontohaver. Dette møtte motstand i den norske arbeidsgruppen, all den tid slike bevisbyrderegler ikke var vanlige i norsk rett. Denne ville heller legge bevisbyrdereglene basert på ulovfestede prinsipper, som ville gi større rom for en konkret bevismessig totalvurdering i hvert enkelt tilfelle.

Det må sies å kunne være en utfordring for alle lands jurister at man gjennom studier, og etter hvert praktisering, tilegner seg et for vår del fornorsket syn på retten.

Gjennom studiet, samt senere ved praktiseringen, så tilegner juristene seg en ganske ensartet måte å angripe rettskildene, samt vekte disse opp i mot hverandre. Noe av dette skyldes følgelig Høyesteretts benyttelse av metoden. Mye skyldes også den tradisjonelle oppfatningen som gjerne hevdes å ha sitt utspring i Torstein Eckhoff sin lærebok i rettskildelære. Som det må antas at veldig mange av dagens norske jurister har hatt ett eller annet forhold til gjennom studietiden eller senere. [104]

Annen lands rett vil etter hvert spille en mer sentral rolle i vårt rettsystem, og utfordringene er åpenbare. Som i dette tilfellet der et felles direktiv flettes inn i 27 lands rettsystemer som gjeldende rett.

Når man da skal trekke komperasjoner og trekke inn den utenlandske rettspraksisen som relevant, er det særs viktig å ha forskjellene for øye. I norsk rett har man en syntetisk lovgivermetode som gir en stor grad av fleksibilitet, dette vil i så måte anses som vanskelig å forholde seg til for en jurist fra det britiske systemet med stor grad av case law systemer.

[102] Reir. 2007/64/EF (Betalingstjenestedirektivet, innledning, underpunkt 2).
[103] Ot.prp. nr 94 (2008-2009) pkt 15.2.
[104] Se f. eks Stuer Lauridsen (1992) og Strömholm (1996). I sistnevnte boken omtales Eckhoff på s 314-315.
Strömholm, Stig 1996 Rätt, rättskällor och rättstillämping, 5 uppl Stockholm: Norstedts juridik 1996
Stuer Lauridsen, Preben 1992 Om ret og retsvidenskab, København: Gyldendal 1992

6. Avsluttende bemerkninger

Bestemmelsene om misbruk av betalingskort går meget langt i å beskytte kontohaver. Reglene går langt i å holde bankene ansvarlige. Dette er rettslig sett ufordrende. I ytterste konsekvens holder det for kontohaver å benekte sin uaktsomhet, i situasjoner der bankene beviselig har slått fast at riktig pinkode er benyttet av uvedkommende. Spørsmålet er her om regelverket slik det nå har blitt utformet, legger det riktige presset på bankene til stadig å utvikle nye tekniske løsninger? Selv om nemnden som påpekt i oppgaven går lengre i å ansvarliggjøre kontohaver, spørs det om ikke dette er riktige vei å gå.

7. Kildeliste

Lover

L21.06.1985 nr. 82 Lov om kredittkjøp m. m

L19.06.2009 nr. 81 i kraft 01.11.2009 endringslov til Finansavtaleloven

L 25.06.1999 nr 46 Lov om finansavtaler

Rettsavgjørelser

RG 2002 1273.

LB-2002-1943

LB 2002 – 01943

RG 2001 1294

RG 1992 297

LE-1993-65

RG-2009-746

RT 2004 – 499

LE-1993-65

RG-1994-676

Rt-1970-1235

Rt-1989-1318

Rt-1995-486

TOSLO -2001-11895

TOBYF – 2010 – 77875

Nemndsavgjørelser

BKN 1993-2

FinKN 2010–162.

FinKN 2011-276

BKN 2001-017.

BKN 2001-38.

BKN 2001-38

FinKN 2011-224.

FinKN 2011–555

Forarbeider

DIR 2007/64/EF Betalingstjenestedirektivet.

NOU 2008:21 nettbank basert betalingsoverføring

NOU 1994:19

Ot.prp. nr 94 (2008-2009)

Ot.prp. nr 41 (1998-1999)

Innst.o. NR 84 (1998-1999).

NOU 1994: 18 Finansavtaler og betalingsoppdrag. Del utredning 1 1994-12-15

Innst O.nr 124 (2008-2009)

Ot.prp.nr.34 (1980-1981)

DS 2008: 86 side 38. http://www.regeringen.se/sb/d/9989/a/118124

Forskningsartikler

http://www.sifo.no/page/Publikasjoner//10081/78015.html lest den 11.12.2012
Oppdragsrapport nr 6 – 2011 Ragnhild Brusdal & Randi Lervik Identitetstyveri ”Omfang Tillitt Beskyttelse mot risiko. Pkt 1-2.

http://www.forskning.no/artikler/2011/mai/288038 Frihet i et kredittkort Asle Rønning, publisert onsdag 11. mai 2011 klokken 05. Lest 02.11.2012.

Kilde Norges Bank, samt publikasjon av bank statistikk av FNO
http://www.fno.no/Hoved/Statistikk/Bank/ (27.10.2012)

Exploring The NFC Attack Surface Charlie Miller August 13. http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf Lest fra nettstedet 10.11.2012.

Cleber K., Olivo , Altair O., Santin , Luiz S., Oliveira (July 2011). "Obtaining the Threat Model for E-mail Phishing" (PDF). Applied Soft Computing. Archived from the original on 2011-07-08.
http://www.inf.ufpr.br/lesoliveira/download/ASOC2011.pdf
Lest den 10.11.2012.

Nettartikler

http://www.fno.no/Hoved/Aktuelt/Pressemeldinger/2012/Kortsvindelen-gar-ned/ lest den 22.11.2012

http://www.norges-bank.no/pages/89034/Betalingssystemet2011.pdf pkt 1.5 Nettbank og kort lest den 22.11.2012

http://no.wikipedia.org/wiki/NOKAS-ranet lest den 03.12.2012

http://www.klikk.no/foreldre/article801468.ece lest den 02.12.2012

http://en.wikipedia.org/wiki/Hacker_(programmer_subculture) lest den 22.11.2012 t

http://en.wikipedia.org/wiki/Man-in-the-middle_attack Lest den 22.11.2012.

http://www.techterms.com/definition/spoofing lest den 23.11.2012

http://www.na24.no/article3501653.ece lest den 29.10.2012, ”8-åringer får bankkort.

http://snl.no/penger. Store Norske Leksikon penger, lest 05.11.2012

http://historienet.no/handel-og-produksjon/bank-krakk-og-gradighet Lest den 02.11.2012.

http://no.wikipedia.org/wiki/Norske_mynter, (26.10.2012),

www.norges-bank.no, Norges banks sin historie.

www.izettle.com, hentet fra nettstedet den 13.11.2012.

http://www.dagensit.no/article2172880.ece?screenArea=readmore lest den 12.11.2012,

http://www.norges-bank.no/pages/89034/Betalingssystemet2011.pdf pkt 1 Kunderettet Betalingsformidling. Lest den 22.11.2012.

http://www.norges-bank.no/pages/89034/Betalingssystemet2011.pdf Pkt 1.2 kortbetalinger. lest den 22.11.2012.

Juridisk Litteratur

Peter Lødrup Lærebok i Erstatningsrett. 4 utg.

Nils Nygard Skade og Ansvar

Gunnar Nerdrum, Menneskerettighetene ved en skilleveg? Lov og Rett 1997

Kai Krüger, Finanger-dommen og den nye rettskildefaktor: Frykten, Jussens Venner 2001 s. 89-104.

Morten Eriksen, Parallell bruk av administrativ tilleggsskatt og straff etter ligningsloven, Tidsskrift for strafferett 2001 s. 167-210

Tolle Stabell, Rettsliggjøring - domstolenes skjønnsmessige overprøvingen Festskrift til Carsten Smith, Oslo 2002 s. 811-832.

Hans Peter Graver Internasjonale Konvensjoner som rettskilde (Publ: Lov og Rett s 468).

Kai Krüger Vil Norsk Juridisk Metode overleve i et integrert Europa? Publ: Juristkontakt 2/96 s 2 (JK-1996-2-2).

Kai Krüger Komparativ Rettsmetode – observasjoner vedrørende metoder for rettsanvendelsen i Europa. Publ: Jussens venner 1996 s 281 – (JV-1996.281).

Strömholm, Stig 1996 Rätt, rättskällor och rättstillämping, 5 uppl Stockholm: Norstedts juridik 1996

Stuer Lauridsen, Preben 1992 Om ret og retsvidenskab, København: Gyldendal 1992

Olav Torvund i Lov og Rett 1986 347, Olav Torvund: Betalingsformidling i et rettslig perspektiv (1993) 269

Liv Synnøve Taraldsrud: Betalingskort i forhold til kredittkjøpsloven og finansieringsvirksomhetsloven. Utg. 145 av stensilserie UIO 1993 66 sider.

Sheila c dow Journal of Post Keynesian Economics Issue: Volume 27, Number 3 / Spring 2005 side 385 – 391