Institutionen för ekonomi

Examensarbete i Handelsrätt

VT 2004

Kontokort som grund för datarelaterat bedrägeri.

Författare:
Hanna Jeppsson
Jesper Persson

Handledare:
Jan Silvander

Abstract

Syftet med denna uppsats är att granska de förutsättningar som skall vara uppfyllda när det gäller att kunna bedöma en gärning som datarelaterat bedrägeri eller förberedelse till annan brottslig gärning. Utöver detta kommer vi att undersöka vilka förutsättningar som skall vara uppfyllda för att kunna bedöma om en gärning skall kunna klassas både som bedrägeri och annat förmögenhetsbrott. Kombinationer som kommer att behandlas är bedrägeri ställt i relation till stöld och dataintrång. Utöver detta kommer vi även att undersöka om datarelaterat bedrägeri kan betraktas som grovt brott. Vi har använt rättsdogmatisk metod, det vill säga, studerat material i form av litteratur, offentliga tryck, lagförslag, författningar och lagar samt rättsfall och därigenom kommit fram till att alla former av olovlig påverkan av en upptagning eller automatisk process inte kan betraktas som datarelaterat bedrägeri. Som exempel på detta kan nämnas de fall då gärningsmannen olovligen utnyttjar ett kontokort som denne erhållit via ett traditionellt bedrägeri. För att kunna jämföra de olika brotten bedrägeri och stöld måste man granska de olika gärningsmomenten i den totala kedjan. Förfarandet datarelaterat brott kan vara förbrott och/eller ett renodlat brott. Förfarandet då gärningsmannen kommer i besittning av en textbärare och dess bakomliggande värde genom vilseledande kan delas in i två steg. Gärningsmannen skaffar sig först ett verktyg genom bedrägeri av traditionellt slag. Denne kommer sedan i besittning av textbärarens bakomliggande värde genom att utnyttja kortet. Gärningsmannen har då för avsikt att ta de bakomliggande medlen i sin besittning. Detta kan inte betraktas som datarelaterat bedrägeri. Steg ett kan betraktas som förberedelse till stöld i de fall gärningsmannen uppfyller kraven som föreligger i 9:11 BrB. Då gärningsmannen genom traditionellt bedrägeri kommer i besittning av kontokort och internkod respektive att han fått den i sin lovliga besittning via ett vilseledande är gärningsmannens förfarande exakt detsamma som den drabbade skulle ha gjort i liknade fall.

Förord

Inledningsvis skulle vi vilja tacka alla de som gjort detta arbete möjligt att genomföra.

Ett stort tack till vår handledare Jan Silvander, som har varit mycket förstående, hjälpsam och inspirerande under arbetets gång.

Ett varmt tack till våra underbara familjer och sambos som stått ut med oss, utan deras uppmuntran och stöd hade detta arbete inte kunnat genomföras.

Slutligen vill vi tacka alla som varit mer eller mindre involverade i detta projekt, då speciellt Staffan, vår vän. Detta arbete är tillägnat honom.

Lund, Maj 2004

Hanna Jeppsson Jesper Persson

Innehållsförteckning

Förkortningar

ABL	Aktiebolagslagen (1975:1385)
ADB	Automatisk databehandling
AMOB	Arbetsgruppen mot organiserad brottslighet
BrB	Brottsbalken
DS	Departementsserien
IT	Internet
KkrL	Konsumentkreditlagen
NJA	Nytt Juridiskt Arkiv
PIN-kod	Personal Identification Number
Prop.	Proposition
SOU	Statens offentliga utredningar
TF	Tryckfrihetsförordningen

1. Inledning

I detta kapitel presenteras val av ämne, problemformulering, syfte, metod, avgränsningar samt arbetets disposition.

1.1 Presentation av ämnet

Bedrägeri som brott har lång en historisk bakgrund. Gärningen innebär att en gärningsman vilseleder annan till handling eller underlåtelse att göra någonting som resulterar i vinning för gärningsmannen och skada för den drabbade.

Dagens lagstiftning vad gäller bedrägeri har sin grund i 1942 års strafflagsrevision (NJA II 1942 s.383) (SoU 1940:20 s.129 ff. och prop. 1942:4 s.96 f). Förändringar av lagtexten skedde 1962, dock utan att lagrummets tillämpningsgränser förändrades. (Holmqvist, Leijonhufvud, Träskman, Wennberg, 2002 s.9:3).

I samband med att kontokort av olika typ introducerades i samhället förändrades hanteringen av penningmedel från att ha varit ett fysiskt betalningsmedel till att bli ett elektroniskt sådant. Den tidigare lagstiftningen om bedrägeri och dess dåvarande utformning kunde inte fullt ut tillämpas i de fall där gärningsmannen med hjälp av ett kontokort försöker tillägna sig elektroniska betalningsmedel och tillgängligheten förutsätter att gärningsmannen använder sig av mekaniska objekt. Den ursprungliga betydelsen av bedrägeri har sin grund i att gärningen avsåg ett fysiskt objekt och att gärningsmannen vilseledde den drabbade genom psykiska medel. Frågan aktualiseras i de fall då gärningsmannen tillskansar sig medel från ett konto kopplat till kontokort och då förfarandet sker via bankomat eller annan typ av automat. Eftersom gärningsmannen använt sig av en bankomat för att fullborda sin gärning, och bankomaten i sig är att betrakta som en mekanisk enhet vilken inte kan vilseledas, var det svårt att rubricera gärningen som bedrägeri enligt den ursprungliga lagstiftningen med utgångspunkt i utnyttjandet av en mekanisk enhet. Detta tolkningsproblem

resulterade i att regeringen utsåg en kommitté som fick till uppgift att lägga fram förslag till ny lagstiftning om datarelaterade olovliga förfaranden som skedde med hjälp av bland annat kontokort. Kommitténs arbete resulterade i betänkandet SoU 1983:50, ”Förmögenhetsbrotten utom gäldenärsbrotten”. Utredningens förslag till lagstiftning låg sedan till grund för regeringens proposition 1985/86:65 som i sin tur resulterade i lag 1986:123.
Det tidigare lagrummet beträffande bedrägeri 9:1 BrB delades då upp i två stycken. Stycke ett behandlar traditionellt bedrägeri medan stycke två behandlar datarelaterat bedrägeri.

Vårt arbete kommer främst att behandla bedrägeri i den meningen som framgår av 9:1 andra stycket BrB, det vill säga, då gärningen kan betraktas som datarelaterat bedrägeri.

För att en gärning ska kunna rubriceras som datarelaterat bedrägeri kan tre förfaringssätt föreligga, nämligen:

- Lämna oriktig eller ofullständig uppgift.
- Ändra i program eller upptagning.
- På annat sätt olovligen påverka resultatet av automatisk informationsbehandling eller annan liknande automatiserad process. Förfarandet skall i likhet med traditionellt bedrägeri resultera i vinning för gärningsmannen och skada för den drabbade.

Vårt arbete kommer i huvudsak att inrikta sig på de fall där gärningsmannen olovligen utnyttjar annans kontokort för att på så sätt kunna tillägna sig de penningmedel som finns på det bakomliggande kontot.

Ett kontokort kan även betraktas som en textbärare. Ett sådant kort kan vara ett betalkort och då finns ett inbyggt värde, exempelvis Cash-kort, betalningsmedel för färd eller vissa telefonkort. Den andra typen av textbärare kännetecknas av att de har ett bakomliggande värde, exempelvis bankomatkortet som inte i sig har något värde. Det är endast det bakomliggande värdet som är av betydelse. Detta kort kan sägas vara nyckeln till ett bakomliggande konto och det

tillgodohavande i form av penningmedel som finns på detta. Det är denna typ av kontokort som i huvudsak kommer att behandlas i vårt arbete.

1.2 Problemformulering

Den fråga som ligger till grund för vår analys är: Kan man i alla lägen betrakta olovlig påverkan av en upptagning eller automatisk process som datarelaterat bedrägeri? En följdfråga blir då: Kan ett olovligt förfarande med hjälp av kontokort alltid betraktas som datarelaterat bedrägeri enligt 9:1 stycke två BrB? En tredje fråga är: Kan denna typ av gärning också betraktas som annan typ av brottslig gärning? Ett svar på de ställda frågorna är att förfarandet i vissa fall kan betraktas som stöld även om gärningsmannen i ett inledande skede får den drabbade att överlämna både kontokort och PIN-kod genom vilseledande. En annan möjligt brottsbeskrivning är om förfarandet kan betraktas som dataintrång enligt 4:9c BrB. En annan frågeställning som kan aktualiseras är om datarelaterat bedrägeri alltid omfattas av 9:3 BrB, det vill säga att det klassas som grovt brott?

1.3 Syfte

Syftet med detta arbete är att granska de förutsättningar som skall vara uppfyllda när det gäller att kunna bedöma en gärning som datarelaterat bedrägeri eller förberedelse till annan brottslig gärning. Utöver detta kommer vi att undersöka vilka förutsättningar som skall vara uppfyllda för att kunna bedöma om en gärning skall kunna klassas både som datarelaterat bedrägeri och annat förmögenhetsbrott. De kombinationer som vi kommer att behandla är bedrägeri ställt i relation till stöld och dataintrång. Vidare kommer vi även att undersöka om datarelaterat bedrägeri kan betraktas som grovt brott.

1.4 Metod

För att kunna besvara de frågor som ställdes i vår problemformulering har vi använt oss av rättsdogmatisk metod, det vill säga vi har ingående studerat och tagit del av allmän litteratur inom området för vårt arbete, offentliga utredningar, lagförslag, författningar och lagar samt rättsfall.

1.5 Avgränsningar

Vi kommer endast att behandla datarelaterat bedrägeri och dess koppling till andra brott enligt Brottsbalken. Undersökningen kommer att fokuseras på svensk lagstiftning. Närliggande områden såsom dataintrång kommer endast att behandlas översiktligt. Anledningen till detta är dels det begränsade utrymme som ställs till vårt förfogande och framförallt den tid som finns till vårt förfogande.

1.6 Disposition

I kapitel två presenteras bakgrunden till olika typer av kontokort. Därefter beskrivs hur en betalning med kontokort fungerar och slutligen beskrivs kontokortmarknaden och dess aktörer.

I kapitel tre kommer begreppen ekonomisk brottslighet, bedrägeri, datarelaterat bedrägeri, datarelaterad brottslighet, stöld samt egenmäktigt förfarande definieras, samt en beskrivning kommer att ges varför dessa är av stor vikt för arbetets fortskridande och förståelse.

I kapitel fyra, analysen, presenteras gärningar riktade mot textbärare med inbyggt eller bakomliggande värde. Därefter behandlas huvudgärningar som bedöms som stöld och datarelaterat bedrägeri. Därefter jämförs gärningarna stöld och bedrägeri och slutligen analyseras huvudgärningar som bedöms som datorintrång.

I kapitel fem framställs våra slutsatser.

Kapitel sex återger litteraturförteckningen, det vill säga, de källor som använts under arbetets gång.

2. Bakgrund till kontokort

I detta kapitel presenteras först hur en betalning med kontokort går till, därefter berättas om kontokortsmarknaden och slutligen återges kontokortsmarknadens aktörer, såsom kortutgivare, kortinnehavare, säljföretag och inlösare av kontokortstransaktioner.

2.1 Inledning

För att skapa ökad förståelse för detta arbete och dess problemformulering anser vi det vara viktigt att ge en översiktlig bild av dels hur en betalning med kontokort går till och dels kontokortsmarknaden och dess aktörer.

Det viktigaste i ett kortsystem är att kortets äkthet kan kontrolleras. Kortets magnetremsa är ett av dessa elektroniska kännetecken, dock kan denna manipuleras. Om någon skulle kopiera information från ett spärrat kort, kan detta vara mycket svårt att upptäcka. Ett kontokort kan betraktas som ett legitimationsmedel eller en behörighetshandling som visar att kontoinnehavaren har en kredit eller ett tillgodohavande hos kortutgivaren. Ett kontokort används vanligen i förening med PIN-kod. (SOU 1995:69 s.77)

Kontokortet ger innehavaren rätt att disponera över kontot som finns hos ett kontoförande institut. Man kan se kontokortet som en nyckel till betalsystemet. En transaktion godkänns genom signering eller att kortinnehavaren knappar in sin PIN-kod som klartecken. Kontokorten delas i bankkort/debetkort, betalkort och kreditkort beroende på de betalningsfunktioner som är knutna till kortet. Debetkort/bankkort eller uttagskort är kopplade till ett tillgångskonto och betal- och kreditkort till ett skuldkonto. Kontokort kan vara öppna eller slutna. De öppna kontokorten är generellt användbara medan de slutna endast kan användas på vissa inköpsställen.

Betalningsförmedling med kontokort bygger på ett avtalsförhållande mellan tre aktörer; kortutgivaren, kortinnehavaren samt säljföretaget. Då det finns flera kortutgivare i kortsystemet finns ytterligare en aktör: kallad inlösaren. (SOU 1995:69 s.103 f.)

2.2 Betalning med kontokort

Det mest grundläggande i ett kortsystem är att man kan kontrollera kortets äkthet, det vill säga att det kommer från en behörig tillverkare. I ett manuellt system är man hänvisade till kortets synbara utseende, alltså logotypen utformning, hologram och utstansad text. Ett elektroniskt kännetecken på kortet är magnetremsan. Innehållet på magnetremsan kan manipuleras. Vid kopiering av information från ett spärrat kort finns mycket små möjligheter att avslöja detta, både för kortläsaren och för system i övrigt. Kortet märks också med senaste giltighetsdatum vid utfärdandet. Kontokortet i sig betraktas som en behörighetshandling eller ett legitimationsbevis, vilket visar att kontohavaren har ett tillgodohavande eller en kredit hos kortutgivaren. (SOU 1995:69 s.77)

Kontokort används numera mestadels i förening med Personal Identification Number (PIN-kod). Vanligtvis består koden av fyra siffror och denna är mycket personlig. I vissa fall väljer kunden själv sin egen kod, i andra fall tilldelas denne en slumpmässigt utvald kod. Kontrollen av att rätt kod knappats in sker, vanligtvis genom att ett anpassningsvärde skapas på elektronisk väg, efter att kortterminalen läst in kontokortets nummer och PIN-koden. På basis av kortnumret och PIN-koden räknas sedan anpassningsvärdet, med hjälp av algoritm fram, detta gör att koden inte behöver lagras. Istället måste algoritmen, det vill säga, sambandet mellan koden och kortens anpassningsvärde hemlighållas. Alternativ till PIN-koden kan vara biometriska metoder som röstidentifiering, fingeravtryck eller ögonkaraktär. Dock har ingen av dessa metoder visat sig ha tillräckligt hög säkerhet. (SOU 1995:69 s.77)

Normalt kan en kontokortsinnehavare inte göras ansvarig för en transaktion med kontokort om det kan konstateras att transaktionen inte godkänts av någon som

var behörig enligt kontokortsavtalet. Emellertid kan kontohavaren enligt avtalet åläggas ansvar även i dessa situationer. Enligt KkrL 34 § kan en kontohavare göras ansvarig för obehöriga transaktioner om han:

- förfarit svikligt gentemot den betaltjänstansvarige
- frivilligt lämnat ut det legitimationsmedel som hör till kontot utan att utlämnandet ingick i användningen av betaltjänsten
- Inte spärrat kontot snarast efter upptäckten eller efter han fått skälig anledning att misstänka att han förlorat kontrollen över legitimationsmedlet
- På annat sätt genom grov oaktsamhet medverkat till att utnyttjandet kunde ske. (SOU 1995:69 s.27)

2.3 Kontokortsmarknaden

Ett kontokort är ett bevis på att den som står angiven som innehavare på kortet har rätt att disponera över sitt konto hos ett visst kontoförande institut. Utöver att ha kontobevisfunktion fungerar kortet som en typ av legitimation vid disposition av kontot för betalning. Kontokortet kan ses som en nyckel till betalsystemet. I regel krävs dock ytterligare legitimationsmedel i form av ID, pass, körkort eller PIN-kod. Kortinnehavaren godkänner vanligen en transaktion genom signering av köpnota eller genom särskild kod som klartecken efter godkänd behörighetskontroll. Kontokort är ett samlingsnamn innefattande kredit-, betal-, och debetkort. Man delar in kontokorten i bankkort/debetkort, betalkort och kreditkort detta beroende på vilka betalningsfunktioner som är knutna till kortet. Debetkort/bankkort eller uttagskort är kopplade till ett tillgångskonto och betal- och kreditkort till ett skuldkonto. (Konsumentverket, 2001 s.25)

Ett kontokort kan vara öppet eller slutet. De öppna kontokorten är generellt användbara. Kontokort som endast kan användas för inköp i en viss butikskedja eller liknade, exempelvis ICA-kort kallas slutna kontokort.

En kontokortsbetalning innebär att en betalning sker från kontoinnehavarens konto till mottagarens konto. Alltså behöver ingen av parterna besöka en bank som direkt följd av en betalning. (Konsumentverket, 2001 s.26)

Kontroll och överföring av information till bank eller transaktionsinsamlare sker numera i huvudsak elektroniskt via en terminal som är uppkopplad mot en centraldator. (Konsumentverket, 2001 s.26)

2.4 Aktörer på kontokortsmarknaden

Den enklaste situationen av betalningsförmedling med hjälp av kontokort bygger på ett avtalsförhållande mellan tre aktörer; kortutgivaren, kortinnehavaren samt säljföretaget. I det fall det ingår flera kortutgivare i kortsystemet finns ytterligare en aktör kallad inlösaren, denne har avtalsrelationer med säljföretaget och kortutgivarna. Andra aktörer kallade servicebyråer utför praktiskt arbete som insamlande av köpnotor och själva databearbetningen. (SOU 1995:69 s.106)

2.4.1. Kortutgivare

Oftast är kortutgivaren en bank eller ett kreditmarknadsbolag. Dessa bestämmer vilka villkor som skall ligga till grund för kortet och kontots utnyttjande, samt kortets utformande och utseende. Kortutgivaren för register över kortinnehavarna samt fakturerar och aviserar kortinnehavarna för gjorda inköp. Kortutgivaren skall även se till att de bestämmelser och lagar som finns avseende kortutgivning följs. (SOU 1995:69 s.106)

2.4.2 Kortinnehavare

Vanligtvis är kortinnehavaren en fysisk person som ingått avtal med en kortutgivare om att använda ett kontokort för betalningsändamål. (SOU 1995:69 s.107)

2.4.3 Säljföretag

Ett säljföretag består av näringsidkare som tillhandahåller tjänster eller varor och som slutit avtal med viss kortutgivare eller inlösare om att acceptera kontokort vid betalning. Som kund kan man oftast räkna med att kunna betala med sitt kontokort på de flesta köpställe. (SOU 1995:69 s.107)

2.4.4 Inlösare av kontokortstransaktioner

Uppgiften för en inlösare är att ge säljföretag betalt för kontokortstransaktionerna. (SOU 1995:69 s.108)

2.5 Sammanfattning

I detta kapitel har vi behandlat hur en betalning med kontokort går till. Vidare har berättats om vikten av kortets äkthet och hur svårt det kan vara att upptäcka om någon skulle kopiera information från ett spärrat kort. Som nämnts kan ett kontokort betraktas som ett legitimationsmedel eller en behörighetshandling som visar att kontoinnehavaren har en kredit eller ett tillgodohavande hos kortutgivaren och används vanligen i förening med PIN-kod. Kontokortet kan ses som en nyckel till betalsystemet.

Transaktioner godkänns genom signering eller att kortinnehavaren knappar in sin PIN-kod som klartecken. En kontokortsinnehavare kan normalt inte göras ansvarig för en transaktion med kontokort om transaktionen inte godkänts av någon som var behörig enligt kontokortsavtalet. Kontohavaren kan i vissa fall åläggas ansvar även i dessa situationer, nämligen om han: förfarit svikligt gentemot den betaltjänstansvarige, frivilligt lämnat ut det legitimationsmedel som hör till kontot, kontot inte spärrats snarast efter upptäckten eller efter han fått skälig anledning att misstänka att han förlorat kontrollen över legitimationsmedlet eller om han på annat sätt genom grov oaktsamhet medverkat till att utnyttjandet kunde ske.

Beroende på de betalningsfunktioner som finns knutna kontokorten delas i de in i bankkort/debetkort, betalkort och kreditkort. Debetkort/bankkort eller uttagskort är kopplade till ett tillgångskonto och betal- och kreditkort till ett skuldkonto. Kontokorten är öppna eller slutna. De öppna kontokorten är generellt användbara, dock kan de slutna endast användas på vissa inköpsställen.

Ett avtalsförhållande mellan tre aktörer; kortutgivaren, kortinnehavaren samt säljföretaget är grunden till betalningsförmedling.

3. Definitioner av begrepp

Detta kapitel behandlar olika begrepp såsom ekonomisk brottslighet, bedrägeri, datarelaterat bedrägeri, datarelaterade brott, skimming, stöld och egenmäktigt förfarande samt dess definitioner.

3.1 Inledning

När det gäller straffrättslig lagstiftning styrs lagrummets tillämpningsgränser av, den i 1 kapitlet BrB noterade, legalitetsprincipen. Detta pekar på vikten av att strikt hålla sig till lagrummens tillämpningsramar. Av den anledning kommer vi att närmare analysera vissa begrepp som är av största vikt i detta arbetes analys. I vårt arbete kommer att undersökas om datarelaterat bedrägeri och dess koppling till förmögenhetsbrottsliga gärningar kan innehållas i begreppet ekonomisk brottslighet. Utöver detta kommer andra väsentliga begrepp att ingående förklaras, detta för att skapa förståelse för arbetets analys. Begrepp som kommer att behandlas är förutom ekonomisk brottslighet, bedrägeri, datarelaterat bedrägeri, datarelaterad brottslighet, skimming, stöld samt egenmäktigt förfarande.

Innebörden av begreppet ekonomisk brottslighet är inte helt klarlagt, dock har myndigheter, kommittéer och i doktrin har man försökt definiera begreppet som har viss karaktär av ett kriminologiskt samlingsbegrepp. (BRÅ 1999:7)

Brottsrekvisiten för bedrägeri är en gärning där gärningsmannen genom vilseledande förmår någon till underlåtenhet eller handling och där denna underlåtenhet eller handling innebär vinning för gärningsmannen och skada för den vilseledda, det vill säga förmögenhetsöverföring. (Holmqvist et al. 2002 s.9:3)

Datarelaterat bedrägeri innebär enligt 9:1 andra stycket BrB att gärningsmannen skall påverka resultatet av en automatisk informationsbehandling och detta skall som effekt innebära vinning för

gärningsmannen och skada för den drabbade, det vill säga innebära en förmögenhetsöverföring. (Holmqvist et al. 2002 s.9:3)

I svensk lagstiftning finns det endast två lagrum som direkt kan tillämpas när det gäller datarelaterade gärningar och datarelaterad brottslighet. Dessa är lagrummen 4:9 c BrB och 9:1 andra stycket BrB.

Skimming är en falsk kortläsare som kopierar magnetremsan på bankomatkort och som placeras på bankomater. Sedan placeras små kameralinser ovanför nummerplattan för att gärningsmannen skall få tillgång till PIN-koden.

Stöldparagrafen förutsätter att fyra rekvisit skall vara uppfyllda nämligen; olovligt tagande, ett stöldobjekt som tillhör annan, tillägnelseuppsåt och att tillgreppet innebär skada. (Holmqvist et al. 2002 s.9:4)

Egenmäktigt förfarande delas in i tre gärningar nämligen; att tillgripa något, rubba någon annans besittning, eller att med våld eller hot om våld hindra annan i utövning av rätt att kvarhålla eller taga något. (Holmqvist et al. 2002 s.8:59)

Därefter görs en delanalys där en diskussion avseende förfaranden med kontokort framförs och slutligen sammanfattas kapitlet.

3.2 Begreppet ekonomisk brottslighet

Innehållet i begreppet ekonomisk brottslighet är ännu inte helt klarlagt. Ett antal mer eller mindre klarläggande definitioner har presenterats. Nedan kommer ett antal definitioner av begreppet närmare beskrivas.

I Sverige uppmärksammades vissa former av olovliga förfaranden som kunde betraktas som ekonomisk brottslighet redan i början av 1970-talet. Myndigheter, kommittéer och i doktrin har man försökt definiera begreppet. Begreppet har viss karaktär av ett kriminologiskt samlingsbegrepp. Man kan även se det som

en närmare definition av den lagstiftning som numera framgår av 10:38 ABL. En definition av begreppet är att gärningen sker inom ramen för en i övrigt lagligt bedriven näringsverksamhet, detta till skillnad mot begreppet organiserad brottslighet där verksamheten och själva affärsidén i sig är brottslig. (BRÅ 1999:7)

Redan 1939 introducerade Sutherland begreppet ”white collar crime”. Edlerhertz, (1970) ansåg att med ekonomisk brottslighet avsågs en illegal handling eller en serie illegala handlingar som begås utan fysiska medel och med hemlighållande eller svek i syfte att erhålla pengar eller egendom, för att undvika kostnader eller förlust av egendom eller att erhålla affärsmässiga eller personliga fördelar (Lindgren, 2000). Även andra författare har försökt sig på att definiera begreppet ekonomisk brottslighet exempelvis Clinard, Mashall och Quinney, (1973) samt Tiedeman, (1976) som menade att ekonomisk brottslighet kännetecknas dels av att den är lagstridig och dels av att den hotar eller stör samhällets ekonomiska intressen. Coleman, 1994, ansåg att ekonomisk brottslighet begås av fysiska personer eller grupper av sådana i utövandet av ett annars respekterat och legitimt yrke eller finansiell verksamhet. (Silvander, 2004 s.185 f.).

Den första breda kartläggningen och även den första större utredningen gällande ekonomisk brottslighet i Sverige gjordes av Rikspolisstyrelsens arbetsgrupp mot organiserad brottslighet (AMOB, 1977).

Under mitten av 1980-talet fram till mitten av 1990-talet dominerade Justitieutskottets beskrivning (JuU 1980/81:21) där ekonomisk brottslighet är kriminalitet som har ekonomisk vinning som direkt motiv. Brottsligheten ska vara av kontinuerlig karaktär, utövas på ett systematiskt sätt och bedrivas inom ramen för en näringsverksamhet som i sig inte är kriminaliserad, förfarandet skall utgöra grund för ett brottsligt förfarande i det enskilda fallet. Denna definition anser vi vara den mest klarläggande därför kan denna ligga till grund för vår bedömning. (BRÅ 1999:7)

Idag finns det få skrivna översikter gällande ekonomisk brottslighet, exempelvis; Eko-kommissionens huvudbetänkande (SOU 1984:15), Ekonomisk brottslighet i Sverige, Riksdagens revisorers rapport om den ekonomiska brottsligheten om rättssäkerheten (Riksdagens revisorer, 1994), Internationella ekobrott (DS 1997:51 s.59 f.). (BRÅ 1999:7)

3.3 Begreppet traditionellt bedrägeri

Bedrägeri kännetecknas som tidigare nämnts i traditionell mening av ett vilseledande. Eftersom man inte kan vilseleda en mekanisk enhet så kommer vi främst behandla datarelaterat bedrägeri. Vi anser det vara betydelsefullt att ingående beskriva båda dessa brott eftersom detta är vad arbetet i huvudsak behandlar. Inledningsvis beröres 9:1 BrB stycke ett samt två eftersom vi ska analysera huruvida man i alla lägen kan säga att en olovlig påverkan av en upptagning eller automatisk process ska kunna betraktas som datarelaterat bedrägeri? I detta fall främst gällande kontokort.

Första stycket i 9:1 BrB behandlar bedrägeri, där brottsrekvisiten gäller gärning där gärningsmannen genom vilseledande förmår någon till handling eller underlåtenhet, där denna handling eller underlåtenhet innebär skada för den vilseledda och vinning för gärningsmannen, det vill säga förmögenhetsöverföring. Vinning för annan än gärningsmannen kan enligt 23:7 BrB vara tillräcklig. (Holmqvist et al. 2002 s.9:3)

Att någon framkallar en oriktig föreställning hos annan är ett huvudfall av vilseledande. Att endast dra nytta av någon annans villfarelse utan att påverka denne i vilseledande riktning är inte straffbelagt som bedrägeri. Vilseledande kan också ske med hjälp av förfalskning. (Holmqvist et al. 2002 s.9:4)

Enligt Holmqvist et al. (2002) föreligger som tidigare nämnts inte bedrägeri när gärningsmannen lurar någon att överlämna ett pass eller kontokort, eftersom dessa objekt saknar förmögenhetsvärde i sig. Emellertid kan bedrägeribrott begås då kontokortet används. Det är detta som utgör grunden för vårt arbete.

För brottet bedrägeri finns olika straffgrader. För mindre allvarliga bedrägerier döms gärningsmannen enligt 9:2 BrB bedrägligt beteende. För grövre brott, stadgas straff enligt 9:3 i BrB. (Holmqvist et al. 2002 s.9:40)

3.4 Begreppet datarelaterat bedrägeri

9:1 andra stycket BrB avser datorrelaterat bedrägeri och denna brottsbeskrivning tillkom år 1986. Gärningsmannen skall påverka resultatet av en automatisk informationsbehandling och detta skall som effekt innebära vinning för gärningsmannen och skada för den drabbade, det vill säga det skall uppkomma förmögenhetsöverföring. Andra stycket i 9:1 BrB är en utvidgning av ett traditionellt bedrägeri. Vad som skiljer ett datarelaterat bedrägeri från ett traditionellt är att det i det förra ställs inga krav ställs på att en fysisk person skall ha blivit vilseledd att göra en viss disposition. Gärningen har, som tidigare nämnts, som grund att gärningsmannen lämnar oriktig eller ofullständig uppgift som i sin tur skall ligga till grund för en automatisk informationsbehandling. Gärningsmannen kan även ändra i upptagning eller program eller på annat sätt olovligen påverkar resultaten av en informationsbehandling eller liknande. Dessa bestämmelser omfattar även olovliga förfaranden med bankomater. (Holmqvist et al. 2002 s.9:3)

Rekvisitet *”på annat sätt olovligen påverkar resultatet av en automatisk informations behandling eller någon annan liknande automatisk process”*. Kan appliceras på ett förfarande så gärningsmannen olovligen använder annans bankomatkort för att tillägna sig pengar från dennes konto, detta förutsätter att gärningsmannen har kunskap om den personliga koden. Vid bedömningen bör då hänsyn tagas till om gärningsmannen haft någon form av förtroendeställning enligt 10:5 BrB. Det avgörande för om bedrägeri föreligger eller ej, är om gärningsmannen på något sätt olovligen ingripit i den automatiska informationsbehandlingen och därigenom påverkat det slutgiltiga resultatet och förmögenhetsöverföring har skett till följd av detta. Att förmögenhetsöverföring är en följd av förfarandet krävs för att bedrägeribrottet skall anses fullbordat.

Förfarandet skall **innebära** förmögenhetsöverföring. Departementschefen anförde att utanför lagrummet tillämpningsområde faller exempelvis att någon genom att manipulera ett datorstyrt lås, olovligen bereder sig tillträde till ett låst utrymme och där tillgriper pengar eller annan egendom. Visserligen innefattar gärningen manipulation med en datorstyrd informationsbehandling men det innebär inte en förmögenhetsöverföring och faller därmed inte inom ramen för bedrägeri. (Holmqvist et al. 2002 s.9:15)

För ansvar enligt andra stycket, krävs inte ett vilseledande utan det är tillräckligt att resultatet av informationsbehandlingen påverkas så att det innebär vinning för gärningsmannen och skada för någon annan. Andra stycket behandlar endast automatisk informationsbehandling och liknande automatisk process. Även om ingen fysisk person har blivit vilseledd anses olovlig påverkan av resultatet av handlingen föreligga. Bestämmelsen är inte begränsad till olovlig påverkan av datorer utan även bankomater och varuautomater ryms inom denna bestämmelse. Inom ramen för datorrelaterat bedrägeri avses endast pengar. (Holmqvist et al. 2002 s.9:3)

3.4.1 Analys av övriga begrepp i 9:1 stycke 2 BrB

Det är av största vikt att bestämma gränserna för de begrepp som ligger till grund för lagrummet gällande den gärning som klassas som datarelaterar bedrägeri. Följande begrepp kommer därför att nedan kortfattat beskrivas. Dessa begrepp är: uppgift, upptagning, automatisk informationsbehandling samt automatisk process. Med hjälp av dessa begrepp är det sedan möjligt att analysera om man kan betrakta all olovlig påverkan av en automatisk process som datarelaterat bedrägeri. (Silvander, 2004 s.87 f.)

3.4.2 Begreppet uppgift

En handling består av uppgifter vars text är visuellt läsbar för fysisk person. (Silvander, 2004 s.104)

3.4.3 Begreppet upptagning

I samband med att bestämmelserna om allmänna handlingars offentlighet ändrades infördes begreppet upptagning i svensk lagstiftning. Orsaken till ändringen var att en text som bearbetades och lagrades med hjälp av dator inte utan vidare kunde falla inom ramen för det tidigare begreppet handling (Prop 1973:33 s. 75 och 1975/76: 160 s. 40). Det framgår av lagändringen i TF 2:4 att begreppen handling och upptagning är att betrakta som synonyma. Skillnaden mellan en upptagning och en traditionell handling är att en upptagning består av data och en text som är avsedd för att maskinbearbetas, dessutom kan texten i de flesta fall inte läsas av en fysisk person. Anledningen till att en fysisk person inte kan läsa texten i en upptagning har sin grund i att teckenrepresentationen skiljer sig från en den som används i en handling. Det finns emellertid även grundläggande likheter mellan upptagning och traditionell handling. De båda kan innehålla samma information och handlingstyperna kan därför utnyttjas för informationsöverföring. (Silvander, 2004 s.114 f.). I prop 1973: 33 skriver departementschefen följande:

"...med en upptagning avses själva informationsinnehållet, dvs. den uppgift som har fixerats på det tekniska mediet"
(Prop 1973: 33 s. 75)

3.4.4 Begreppet automatisk informationsbehandling

Begreppet informationsbehandling definieras bäst med utgångspunkt i de olika sätt på vilka bearbetning av information kan ske, nämligen helautomatisk, halvautomatisk eller helt manuell bearbetning. I vårt arbete är det den helautomatiska informationsbehandlingen via en dator eller annan mekanisk enhet som är föremål för vårt intresse. Helautomatisk informationsbehandling sker med hjälp av ett helautomatiskt förfarande. (Silvander, 2004 s.123). Departementschefen fastslog i prop. 1973:33:

> *”Med ADB-teknik kan man utföra alla tänkbara åtgärder för hantering av uppgifter. En nödvändig förutsättning för att datamaskinen skall kunna användas är att den försetts med noggranna instruktioner, s.k. program, som anger vilka åtgärder som skall vidtas”. (Prop 1973:33 s. 15)*

3.4.5 Begreppet automatisk process

Med automatisk process menas att via någon form av påverkan, via kontokort eller nyckel, kommer en mekanisk enhet att påverkas. När det gäller bankomat och kontokort öppnar den automatiska processorn upp kontot och lämnar ut pengarna. (Silvander, 2004 s.123)

3.5 Datarelaterad brottslighet

I svensk lagstiftning finns det endast två lagrum som direkt kan tillämpas när det gäller datarelaterade gärningar. Dessa är 4:9 c BrB och 9:1 andra stycket BrB.

Datorn kan även vara mål för gärningen. Gärningsmannens uppsåt kan då vara att förstöra dator eller datoranläggningen. Gärningen kan då betraktas som skadegörelse och bedömas enligt 12 kapitlet i BrB. En dator kan vara föremål för stöld och man kan även använda den som verktyg för att förstöra information genom att göra intrång i en upptagning. Datatekniken kan emellertid vara ett verktyg för att begå datarelaterade brott. Datorn kan därför ha beröring med ett datarelaterat brott utan för den sakens skull vara mål eller medel för gärningsmannen. (BRÅ 2000:2)

Dataintrång bedöms enligt 4:9 c BrB. Gärningen består då i att gärningsmannen olovligen skaffar sig tillgång till lagrade eller överförda data. Gärningsmannen kan i sådant fall utplåna eller på annat vis förstöra lagrade data. Detta förfarande kan delas in i två typer: det interna och det externa. När en tjänsteman överskrider sina befogenheter genom att olovligen skaffa sig tillgång till lagrade data är detta exempel på ett internt dataintrång. Gärningsmannen kan även göra

intrång i en upptagning med uppsåt att undersöka vad som finns lagrat. En sådan gärningsman kan då betraktas som hacker. Om däremot gärningsmannen gör dataintrång med syftet att kopiera, ändra eller förstöra lagrad information kan denne betraktas som cracker. (BRÅ 2000:2)

3.6 Skimming

Som tidigare nämnts måste gärningsmannen skaffa sig tillgång till både det aktuella kortet och tillhörande PIN-kod. Detta kan göras på olika sätt. Ett sätt är att gärningsmannen genom ett vilseledande får den drabbade att självmant överlämna kortet och koden till gärningsmannen varefter denna utnyttjar det överlämnade. En annan typ av förfarande som gärningsmannen kan utnyttja sig av för att ta reda på, dels kortets internkod och dels PIN-koden, är att använda sig av skimming. Skimming kan utnyttjas som förberedelse till en gärning som innebär att gärningsmannen skaffar sig ett verksamt verktyg för att nå sitt syfte. Detta syfte är att tillägna sig de bakomliggande medel som finns på kontot och som är kopplat till verktyget. Skimming i sig är inte att betrakta som kortbedrägeri utan används endast för att skaffa sig ett verktyg.

Skimming är en falsk kortläsare som kopierar magnetremsan på bankomatkort och som placeras på bankomater. Kortets magnetremsa, eller internkod, spelas av i skimmern. Utöver ovannämnda så måste även gärningsmannen få tillgång till den aktuella PIN-koden. Små kameralinser placeras ovanför nummerplattan för att på så sätt få tillgång till PIN-koden. Man hoppas helt kunna komma ifrån detta problem senast år 2005 när alla kontokort i Europa ska bli försedda med ett mikrochips som ersätter magnetremsan.

3.7 Begreppet stöld

I detta arbete skall vi även analysera om andra gärningar också kan omfattas eller tillsammans med bedrägeri kan utgöra gärningsmoment för gärningsmannen i det fall han vill få tag i ett bakomliggande värde med hjälp av en textbärare. Kan gärningens slutmoment betraktas som stöld?

För att detta skall vara möjligt är det nödvändigt att närmare granska de förutsättningar som då skall gälla.

Stöldparagrafen enligt 8:1 BrB indelas huvudsakligen i två objektiva rekvisit:

- Olovligt tagande
- Stöldobjektet skall tillhöra annan

En fråga som kan ställas är: Kan dessa nämnda objektiva rekvisit appliceras på en gärning då gärningsmannen tillägnar sig ett kontokort?

3.7.1 Olovligt tagande

Olovligt tagande är en olovlig besittningsrubbning. Begreppet besittning nämns inte uttryckligen i lagtexten utan endast indirekt. Besittningsbegreppet är av intresse beroende på att det inte blir aktuellt med olovligt tagande i besittning, då gärningsmannen redan har saken i sin besittning. I de fall någon försätter sig i besittning av en sak som någon annan har i sin besittning, föreligger tillgrepp. Tillgrepp kan också föreligga om någon tar en sak i besittning som inte varit i någons besittning, dock måste man i detta fall vara uppmärksam att kravet på tagandet ska vara olovligt för att det ska bli aktuellt med tillgreppsbrott. Något annat som gör tagandet olovligt är att annans besittning blir kränkt av gärningen.

Besittningsbegreppet och besittningsskyddet har konstruerats primärt utifrån ett ägarperspektiv även om annan person än ägaren kan vara besittare till saken. Detta anses vara det grundläggande för arbetets diskussion.

Även då sambesittning av viss egendom föreligger och någon av sambesittarna olovligen tar från någon annan sambesittare gör han sig skyldig till olovligt tagande eller till stöld.

Den egendom som skall vara föremål för stöld förutsätts har fysisk substans. Detta medför att exempelvis en fordringsrätt inte kan bli utsatt för en stöld. En kontohavare har medelbar besittning till sitt tillgodohavande på sitt konto. (Holmqvist et al. 2002 s.8:4 f.).

3.7.2 Stöldobjektet skall tillhöra annan

I lagrummet 8:1 BrB beskrivs att objektet för stölden skall tillhöra annan. Tidigare beskrevs stöldobjektet som annans sak, vilket förändrades i lagutskottets yttrande (NJA II 1942 s.343) Anledningen till ändringen var att ordet sak inte tydligt omfattade allt som var avsett, exempelvis pengar. Objektet för stöld kan endast vara ett konkret föremål alltså ha fysisk substans. Stöldobjektet begränsas av att gärningen skall vara ett tagande, i lagtexten beskrivet som tillgrepp. (Holmqvist et al. 2002 s.8:17 f.).

3.7.3 Tillägnelseuppsåt

Stöldbrottets fullbordande sker när tagande med tillägnelseuppsåt föreligger. Fullbordande sker enligt lagtexten tidigt, i regel redan vid det olovliga tagandet, under förutsättning att detta sker under tillägnelseuppsåt och att det innebär skada. Redan när gärningsmannen har uppsåt att tillägna sig saken är gärningen fullbordad. Det är svårt för utomstående att vid det tillfället bestämma vad gärningsmannen haft i åtanke. När gärningsmannen haft direkt uppsåt att tillägna annan saken förekommer stöldansvar. Begreppet tillägnelseuppsåt härstammar från straffrättskommitténs förslag (NJA II 1942 s. 338) till brottsbeskrivning för stöldbrottet. (Holmqvist et al. 2002 s.8:20 f.).

3.7.4 Tillgreppet skall innebära skada

Då stöldansvar föreligger skall tillgreppet innebära skada. Skada är i detta fall ekonomisk skada. Tillgrepp av saker som har marknadsvärde innebär då därför alltid skada. Uppsåtet att tillägna sig eller tillgripa innebär att gärningsmannen

skall föra in föremålet i sin förmögehetssfär. Handlingar som exempelvis resecheckar och postväxlar representerar ett förmögenhetsvärde även om det saknar marknadsvärde. Enligt Holmqvist et al (2002) anses bankomatkort och kontokort inte vara stöldobjekt eftersom dessa inte har något förmögenhetsvärde, utan det endast har ett bakomliggande värde i form av ett tillgodohavande på ett konto. (Holmqvist et al. 2002 s.8:23 f.). Vi anser dock att detta indirekt kan innebära skada i och med att kontokortet har ett bakomliggande värde.

3.8 Egenmäktigt förfarande

Egenmäktigt förfarande bestraffas enligt 8:8 BrB. Gärningen kan indelas i tre objektiva rekvisit nämligen; att tillgripa något, annorledes rubba någon annans besittning, eller att med våld eller hot om våld hindra annan i utövning av rätt att kvarhålla eller taga något. Detta arbete behandlar de båda första fallen som enligt lag kräver att gärningen är olovlig, dock krävs det inte att gärningen innebär vinning eller skada. Den första gärningstypen omfattar det fall då gärningsmannen olovligen tager och brukar eller eljest tillgriper något. Bestämmelsen om ansvar för egenmäktigt förfarande skyddar en persons besittning, oberoende av dennes rätt till objektet. Den andra gärningstypen är olovlig besittningsrubbning utan tillägnande (NJA II. 1942 s. 364). (Holmqvist et al. 2002 s.8:59).

Egenmäktigt förfarande föreligger då gärningsmannen olovligen tar eller tillgriper fysiskt objekt enbart för att bruka detta. Gärningsmannen får inte tillägna sig värdet av det tillgripna objektet. Däremot kan gärningsmannen utnyttja det tillgripna som verktyg för att exempelvis komma åt ett bakomliggande värde.

3.9 Delanalys

Kan stöld eller egenmäktigt förfarande kombineras med en gärning som är att betrakta som datarelaterat bedrägeri? Frågeställningen har sin grund i det förhållandet att gärningsmannen utnyttjar kortet exakt likadant som den drabbade skulle ha gjort i samma situation.

Enligt vår åsikt är det inte möjligt att i alla tänkbara fall då gärningsmannen olovligen utnyttjar ett kontokort betrakta detta som datarelaterat bedrägeri. I det fall gärningsmannen genom skimming eller genom traditionellt bedrägeri kommer i besittning av kontokort och internkod eller i det fall gärningsmannen fått kontokortet i sin lovliga besittning via ett vilseledande kan man inte utan vidare betrakta förfarandet som ett datarelaterat bedrägeri. Gärningsmannen hanterar ju kortet på samma sätt som den drabbade skulle ha gjort i liknade fall. Vi anser därför att man inte kan betrakta förfarandet som bedrägeri eller påverkan av en upptagning. I så fall skulle förfarandet innebära att den drabbade också olovligen påverkade en upptagning. Kontokortet utnyttjas enbart som ett verksamt verktyg, för att komma åt de bakomliggande medlen.

I skimmingfallet har gärningsmannen fått reda på PIN-koden och internkoden och han tillverkar ett kort och utnyttjar detta exakt likadant som den drabbade skulle ha gjort.

När det gäller traditionellt bedrägeri har gärningsmannen utnyttjat kortet precis som den drabbade skulle ha gjort. Alltså kan man betrakta detta som att gärningsmannen utnyttjar kortet som ett verksamt verktyg för att komma åt de bakomliggande pengarna. Detta förfaringssätt kan jämföras med de fall då gärningsmannen använder sig av en nyckel till ett låst utrymme. Nyckeln utgörs av en textbärare. Gärningsmannen är i detta fall helt ointresserad av kortet som sådant, eftersom detta i sig inte har något värde. Det som är av värde för gärningsmannen är det bakomliggande medlen respektive det som finns i det låsta utrymmet. Detta gör det möjligt att jämföra dessa två gärningstyperna. I båda fallen kan man betrakta gärningen som stöld.

4. Analys

I detta kapitel analyseras det insamlade materialet i form litteratur, offentliga tryck, lagförslag, författningar och lagar samt rättsfall.

4.1 Inledning

I detta kapitel presenteras de brottsliga gärningar som föregå huvudbrottets fullbordande. Därefter beskrivs textbärare, samt gärningar riktade mot textbärare med inbyggt och bakomliggande värde. Slutligen skildras huvudgärningar som bedöms som stöld, datarelaterat bedrägeri, dataintrång samt företagsspionerі.

4.2 Allmänt om textbärare

Man kan anse att det finns tre olika kategorier av textbärare nämligen; 1. textbärare med inbyggt värde. 2. textbärare med bakomliggande värde. 3. textbärare fungerande som bärare av en lagrad upptagning. Detta arbete handlar främst om textbärare med bakomliggande värde dock kommer textbärare med inbyggt värde kommer att behandlas. Alla tre typerna av textbärare har som regel fysisk substans och är individualiserade.

Textbäraren är oftast ett nödvändigt verktyg eller arbetsredskap för att gärningsmannen ska kunna utnyttja en automatisk processor eller en dator. Exempelvis är det en textbärare som aktiverar en automatisk processor. En textbärare kan också användas som nyckel till ett låst utrymme eller kan användas som betalningsmedel. De textbärare som har inbyggt värde har ett begränsat förmögenhetsvärde. (Silvander, 2004 s.150)

4.2.1 Gärning riktad mot textbärare med inbyggt värde

Textbärare med inbyggt värde kännetecknas av att värdet står i relation till den lagrade upptagningen. Det är den lagrade upptagningen som utgör textbärarens värde eftersom textbäraren som sådan inte har något värde av betydelse i sig. Textbärare i form av Cash-kort kan utnyttjas som betalningsmedel vid ekonomiska transaktioner. En textbärare i denna form kan bli föremål för ett tillgreppsbrott och därmed bedömas enligt 8 kapitlet BrB.

Ofta överstiger dock textbärarens inbyggda värde inte 800 kr, vilket är den nuvarande nedre gränsen för stöld. Av den anledningen bedöms denna typ av gärning sannolikt som snatteri enligt 8:2 BrB. Ett krav för att kunna bedöma förfarandet som stöld eller snatteri är att gärningsmannen fått tillgång till det inbyggda värdet. Så inte alltid är fallet. En orsak till detta kan vara att gärningsmannen inte får tillgång till den personliga koden som textbäraren kan vara sammankopplad med. Det inbyggda värdet är då låst. Då gärningsmannen inte har tillgång till koden är det inte heller sannolikt att gärningen kan bedömas som snatteri. Det är svårt att döma förfarandet som försök till snatteri eftersom sådant brott inte finns enligt 9:11 BrB. En möjlighet är att gärningsmannen istället döms för egenmäktigt förfarande enligt 8:8 BrB.

Då textbärarens värde i de flesta fall understiger 800 kr, är det tveksamt om gärningen kan bedömas som bedrägeri enligt 9:1 BrB. Det är mest troligt att gärningen rubriceras som bedrägligt beteende enligt 9:2 BrB. Samma bedömning gäller då gärningsmannen har tillgång till den personliga kod som är kopplad till textbäraren. Har gärningsmannen inte tillgång till koden anser vi det vara osannolikt att han döms till bedrägligt beteende. Det uppkommer ingen direkt vinning för gärningsmannen även om den drabbade lider skada. Inte heller någon möjlighet finns att brottet kommer att rubriceras som försök till bedrägligt beteende eftersom det inte finns något som klassas som försöksbrott till bedrägligt beteende enligt 9:11 BrB.

Vi anser att i de fall, då gärningsmannen inte kan tillgodogöra sig det inbyggda värdet i brist på den personliga koden, kommer den drabbade trots detta att lida skada eftersom han inte kan komma åt det inbyggda värdet av den anledningen bör gärningen därför bedömas som oredligt förfarande enligt 9:8 BrB.

En textbärare kan också bli utsatt för en gärning som behandlas i 10 kapitlet BrB, det vill säga förskingring och annan trolöshet. Gärningsbedömningen är beroende av om gärningsmannen har tillgång till den personliga koden eller ej.

Har gärningsmannen tillgång till den personliga koden kan det inbyggda värdet förändras negativt för den drabbade då textbäraren utnyttjas. Vinning uppkommer för gärningsmannen och skada för den drabbade. I grunden kan en sådan gärning bedömas som förskingring enligt 10:1 BrB. Eftersom värdet vanligtvis är lågt bedöms gärningen troligen som undandräkt i enlighet med 10:2 BrB. Om det inbyggda värdet kan sägas vara låst det vill säga att gärningsmannen inte har tillgång till koden uppkommer ingen vinning för honom. Därför kan förfarandet inte dömas som förskingring och inte heller som undandräkt. Istället kan gärningen dömas som olovligt förfogande enligt 10:4 BrB eller olovligt brukande enligt 10:7 BrB. (Silvander, 2004 s.151 f.)

4.2.2 Textbärare med bakomliggande värde

En textbärare med bakomliggande värde har ett värde som är fristående från textbäraren, det vill säga, värdet är inte integrerat med denna. Värdet kan flyttas mellan olika textbärare utan att upptagningen eller textbäraren för den skull förändras. Man måste undersöka om tillgång till det bakomliggande värdet förutsätter presentation av en personlig kod eller ej för att kunna bedöma gärningen. Ytterligare ett gärningsmoment uppkommer om en personlig kod måste presenteras nämligen ett osant intygande. Gärningsmannen har ju felaktigt utgett sig att vara behörig att utnyttja det bakomliggande värdet. Gärningsförfarandet kan i många fall uppdelas i två moment: ett som avser det bakomliggande värdet och ett som avser textbäraren som sådan. I den del av gärningen som riktas mot textbäraren kan man utgå ifrån att textbäraren i sig har

ett lågt ekonomiskt värde eller inget värde alls. Gärningsmannen använder textbäraren som ett verktyg för att han på så sätt skall kunna tillägna sig eller göra intrång i det bakomliggande objektet. Vi anser detta vara förberedelse till huvudbrottet. Detta kan som tidigare nämnts jämställas med när någon, med hjälp av en nyckel i form av en textbärare, skaffar sig tillgång till ett låst utrymme. (Silvander, 2004 s.156 f.)

Frågan som vi har ställt oss är hur skall en gärning bedömas då gärningsmannen tillgriper en textbärare i form av ett kontokort, utnyttjar den personliga koden och på så sätt kommer i besittning av de medlen finns på det anslutna kontot? Vi anser att gärningen har vissa likheter med en gärning som kan bedömas som stöld. Gärningsmannen har genom att tillgripa ett verktyg, det vill säga, textbäraren och även skaffat sig tillgång till PIN-koden. Detta gör att gärningsmannen kan tillägna sig det bakomliggande värdet. (Silvander, 2004)

I de fall gärningsmannen endast tillgriper textbäraren utan att få tillgång till PIN-koden anser vi det vara svårt att bedöma förfarandet som förberedelse till stöld. Gärningsmannen kommer inte att få tillgång till det bakomliggande värdet. (Silvander, 2004 s.156 f.)

Textbäraren kan också bli föremål för en disposition som har sin grund i ett vilseledande och gärningen bedöms i sådant fall enligt 9 kapitlet BrB. Brottsrubriceringen beror på om vilseledandet innebär förmögenhetsöverföring eller ej och om den personliga koden kommit till gärningsmannens förfogande eller ej. Uppkommer en förmögenhetsöverföring vilket förutsätter att gärningsmannen har tillgång till den personliga koden, kan gärningen bedömas som bedrägeri enligt 9:1 första stycket BrB eller som bedrägligt beteende enligt 9:2 BrB. Storleken på det bakomliggande värdet bestämmer vilket lagrum som gäller. Gärningen kan också bedömas som förberedelse till bedrägeri enligt 9:11 BrB, beroende på om gärningen då den fullbordas kan bedömas som bedrägeri enligt 9:1 BrB.
Om det bakomliggande värdet är låst för gärningsmannen det vill säga då om den personliga koden inte omfattas av vilseledandet, kan gärningsmannen inte

skaffa sig vinning även om den drabbade lider skada. Gärningen kan då dömas som oredligt förfarande med stöd av 9:8 BrB. (Silvander, 2004 s.156 f.)

4.3 Huvudgärning bedöms som datarelaterat bedrägeri

Vi anser att även om ett kontokort har erhållits via ett bedrägligt förfarande och det sedermera används för att gärningsmannen skall kunna komma i besittning av de bakomliggande medlen är förfarandet inte att betrakta som ett renodlat datarelaterat bedrägeri. Anledningen till detta är att gärningsmannen har vilselett den drabbade att självmant överlämna såväl kontokort som PIN-kod till gärningsmannen. Detta bidrar till att gärningsmannen har fått ett verksamt medel för att komma åt det bakomliggande kontot, det är inte kontokortet som sådant som är av intresse för gärningsmannen utan det bakomliggande värdet.
Bedrägeri förutsätter att gärningsmannen genom vilseledande förmår någon till underlåtenhet eller till en handling som innebär förmögenhetsöverföring. Alltså skall vilseledande vara orsak till motparten eller offrets beteende. När det gäller datarelaterat bedrägeri finns det som tidigare nämnts olika rekvisit som skall vara uppfyllda för att detta brott skall föreligga. I detta fall har gärningsmannens förfarande en särpräglad form. Gärningsmannen skall olovligen ha påverkat en automatisk process, påverkat en upptagning eller påverkat resultatet av en informationsbehandling. För att betrakta ett datarelaterat bedrägeri som grovt brott skall enligt 9:3 andra stycket BrB ske med hjälp av falsk urkund eller felaktig bokföring. Förfalskning förutsätter att det är visuellt läsbart, det är tveksamt om man då kan betrakta en gärning som datarelaterat grovt brott, där man förfalskar urkund. Enligt nuvarande lagstiftning så kan man säga att det är endast 11:5 BrB databaserad bokföring som kan aktualiseras.

4.4 Jämförelse mellan bedrägeri och stöld

Efter att ha jämfört de olika rekvisiten som skall vara uppfyllda för att bedrägeri respektive stöld skall föreligga kan man inte utan vidare jämföra gärningarna bedrägeri och stöld. Istället måste man se på om olika gärningsmoment i gärningskedjan. Bedrägeri är vilseledande och stöld är olovligt tagande.

Gärningsmannens handlande skiljer sig i de olika fallen. Kan man koppla samman de olika fallen? För att kunna besvara denna fråga måste hela händelseförloppet, från förberedelse av brottet till fullbordandet, granskas.

Förfarandet då gärningsmannen kommer i besittning av en textbärare, som i sin tur ger möjlighet att komma åt dennes bakomliggande värde, genom vilseledande kan delas in i tre steg: I det första steget skaffar gärningsmannen ett verktyg och här föreligger bedrägeri av traditionellt slag. Det andra steget utmärks av att gärningsmannen nyttjar textbäraren. Det andra steget kan betraktas som egenmäktigt förfarande enligt 8:8 BrB. Det tredje steget är när gärningsmannen kommer i besittning av textbärarens bakomliggande värde. Detta kan jämföras med när någon skaffar sig olovlig besittning till exempelvis en nyckel till ett utrymme, där saker av värde finns. Dessa har gärningsmannen för avsikt att ta i sin besittning. Även om gärningsmannen olovligen påverkar dörrlåset kan man inte betrakta detta som att han begår ett datarelaterat bedrägeri.

Steg ett och två kan betraktas som förberedelse till stöld om han i dessa fall uppfyller kraven som föreligger i 9:11 BrB, som hänvisar till 23 kapitlet i BrB.

4.5 Huvudgärning bedöms som dataintrång

Vad som straffbeläggs enligt 4:9c BrB avser när någon olovligen bereder sig tillgång till en upptagning. Gärningen behöver inte ske i något speciellt syfte och detta behöver inte heller medföra någon effekt, utan det är själva intrånget i en upptagning som straffbeläggs. Även en gärning som består i att någon olovligen utplånar eller ändrar eller i register för in sådan upptagning straffas enligt 4:9c BrB. Bestämmelsen förutsätter att gärningsmannen handlat med uppsåt. (Holmqvist et al. 2002 s.4:47) Det moment som avser den lagrade upptagningen hos en textbärare, oavsett om värdet är inbyggt eller bakomliggande, kan bedömas som ett dataintrång enligt 4:9 c BrB. Dataintrång kan enligt 23:1, 23:2 BrB också straffas som förberedelse och försöksbrott. Man kan även dömas till medhjälp till dataintrång enligt 23:4 BrB. Intrångets kvalitativa och kvantitativa omfattning

utgör bedömningen för brottets svårighetsgrad. Den ekonomiska skadan vägs också in i bedömningen.

4.6 Sammanfattning

I detta kapitel har analyserats textbärare i allmänhet, gärningar riktade mot textbärare med inbyggt värde eller bakomliggande värde. Vi har analyserat de fall då en huvudgärning kan bedömas som renodlat datarelaterat bedrägeri eller förfarandet kan betraktas som ett traditionellt bedrägeri och då gärningen även kan bedömas som stöld. Slutligen har vi även översiktligt belyst de fall då en gärning kan bedömas som dataintrång.

5. Slutdiskussion

I detta kapitel presenteras den slutsats som vi har kommit fram till. Därefter ges förslag till fortsatt forskning.

5.1 Inledning

De frågor som vi presenterade i problemformuleringen kommer nedan att besvaras. Följande frågor ställdes: Kan man i alla lägen betrakta olovlig påverkan av en upptagning eller automatisk process som datarelaterat bedrägeri? Kan ett olovligt förfarande med hjälp av kontokort alltid betraktas som datarelaterat bedrägeri enligt 9:1 stycke två BrB? Kan denna typ av gärning också betraktas som annan typ av brottslig gärning? Kan datarelaterat bedrägeri alltid omfattas av 9:3 BrB, det vill säga att det klassas som grovt brott?

5.2 Slutsats

Vi har i vårt arbete funnit att alla former av olovlig påverkan av en upptagning eller automatisk process inte kan betraktas som datarelaterat bedrägeri. Som exempel på denna åsikt kan nämnas de fall då gärningsmannen olovligen utnyttjar ett kontokort som denne erhållit via ett traditionellt bedrägeri. Då gärningsmannen genom skimming eller genom traditionellt bedrägeri kommer i besittning av kontokort och internkod respektive att han fått den i sin lovliga besittning via ett vilseledande är gärningsmannens förfarande exakt detsamma som den drabbade skulle ha gjort i liknade fall. Detta kan därför inte betraktas som bedrägeri eller påverkan av en upptagning, om så var fallet skulle den drabbade också olovligen påverka en upptagning. Kontokortet utnyttjas av gärningsmannen endast för att komma åt de bakomliggande medlen, alltså enbart som ett verksamt verktyg.

Gärningsmannen har i skimmingfallet fått kännedom om PIN-koden och internkoden. Han tillverkar ett identiskt kort och utnyttjar detta på samma sätt som den drabbade skulle ha gjort.

När gärningsmannen erhållit ett kontokort genom ett traditionellt bedrägeri utnyttjar denne kortet precis på samma sätt som den drabbade skulle ha gjort. Gärningsmannen utnyttjar kortet som ett verksamt verktyg för att komma åt de bakomliggande pengarna. Som tidigare nämnts kan detta förfaringssätt jämföras med de fall då gärningsmannen använder sig av en nyckel till ett låst utrymme i form av en textbärare. Gärningsmannen är i detta fall ointresserad av kortet som sådant, eftersom detta i sig inte har något värde. Det som är av värde för gärningsmannen är det bakomliggande medlen respektive det som finns i det låsta utrymmet. Detta gör det möjligt att jämföra dessa två gärningstyperna. I båda fallen kan man betrakta gärningen som stöld.

Mycket talar för att man i sådana fall kan betrakta slutförfarandet som stöld även om gärningsmannen i ett inledande skede får den drabbade att överlämna både kontokort och PIN-kod genom vilseledande.

Gärningarna bedrägeri och stöld kan inte utan vidare jämföras. Detta eftersom de båda brotten har olika brottsrekvisit. Istället får man granska de olika gärningsmomenten i den totala gärningskedjan. Bedrägeri är vilseledande och stöld är olovligt tagande. Det kan konstateras att gärningsmannens handlande skiljer sig i de olika fallen.

Förfarandet då gärningsmannen kommer i besittning av en textbärare, som i sin tur ger möjlighet att komma åt dennes bakomliggande värde, genom vilseledande kan delas in i två steg: Först skaffar gärningsmannen ett verktyg genom ett bedrägeri av traditionellt slag. Genom att utnyttja kortet kommer sedan gärningsmannen i besittning av textbärarens bakomliggande värde. Som nämnts under arbetets gång kan detta jämföras med när någon skaffar sig olovlig besittning till exempelvis en nyckel till ett utrymme, där saker av värde finns. Dessa har gärningsmannen för avsikt att ta i sin besittning. Även om

gärningsmannen olovligen påverkar dörrlåset kan man inte betrakta detta som att han begår ett datarelaterat bedrägeri.

Steg ett kan betraktas som förberedelse till stöld i de fall gärningsmannen uppfyller kraven som föreligger i 9:11 BrB, som hänvisar till 23 kapitlet i BrB.

Datarelaterat bedrägeri som grovt brott skall enligt 9:3 andra stycket BrB ske med hjälp av falsk urkund eller felaktig bokföring. Förfalskning förutsätter att det är visuellt läsbart, det är tveksamt om man då kan betrakta en gärning som datarelaterat grovt brott, där man förfalskar urkund. Nuvarande lagstiftning pekar på att det är endast 11:5 BrB databaserad bokföring som kan aktualiseras.

5.3 Förslag till fortsatt forskning

Det skulle vara av intresse att studera hur internationell lagstiftning inom detta område ser ut. Vidare kan man mer ingående undersöka huvudgärningar som betraktas som dataintrång och företagsspionage.

6. Litteraturförteckning

6.1 Allmän litteratur

Bernitz, U., & Heuman, L., & Leijonhufvud, M., & Seipel, P., & Warnling-Nerep, W., & Victorin, A., & Vogel, H. (1998). *Finna rätt- juristens källmaterial och arbetsmetoder* (5: e uppl.). Stockholm: Norstedts Juridik AB.

BRÅ 1999:7. *Forskning om ekonomisk brottslighet.* Stockholm: BRÅ.

BRÅ 2000:2. *IT-relaterad brottslighet.*

Holmqvist, L., & Leijonhufvud, M., & Träskman, P., & Wennberg, S. (2002). *Brottsbalken – En kommentar, Del 1 (1-12 kap)* (3: e uppl.). Stockholm: Norstedts Juridik.

Konsumentverket. Rapport nr 13/2001. (2001). *Betaltjänster, Förslag om rätt för alla att ha inlåningskontoförenat med tillgång till betaltjänster.*

Lindgren, S-Å. (2000). *Ekonomisk brottslighet ett samhällsproblem med förhinder.*

Riksdagens revisorer. (1994). Rapport 1993/94. *Den ekonomiska brottsligheten om rättssäkerheten.*

Silvander, J. (2004). Dator och datarelaterade brott. Lunds universitet, Juridiska fakulteten.

Silvander, J. (1998). *Dator- Datarelaterade förmögenhetsbrott utom borgenärsbrotten.* Lunds universitet: Juridiska fakulteten.

Strömholm, S. (1981). *Rätt, Rättskällor och rättstillämpning.* Stockholm: PA Norstedts & Söners förlag.

6.2 Offentliga utredningar

DsJu 1997:51. *Internationella ekobrott.*

SOU 1983:50. *Förmögenhetsbrotten utom gäldenärsbrotten.*

SOU 1984:15. *Ekonomisk brottslighet i Sverige.*

SOU 1995: 69. *Betaltjänster.*

6.3 Lagförslag

Prop. 1973:33. Ändringar i tryckfrihetsförordningen m.m.

Prop. 1975/76:160. Nya grundlagsbestämmelser angående allmänna handlingars offentlighet.

Prop. 1985/86:65. Förslag till ändring i brottsbalken m.m. (Vissa frågor om datorrelaterade brott och ocker)

6.4 Rättsfall

NJA II 1942 s. 338, 343, 364 och 383