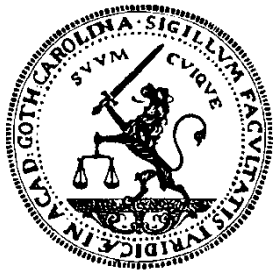

JURIDISKA FAKULTETEN
vid Lunds universitet

Ellen Johansson Wintzell

Social manipulation i en straffrättslig kontext

- beaktas mänskliga sårbarhetsfaktorer i den straffrättsliga bedömningen?

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Sverker Jönsson

Termin för examen: Period 1 VT2020

Innehållsförteckning

Summary

By utilizing general social psychological human vulnerability factors, an offender can manipulate an individual to disclose confidential information. The utilization of human contact and trust for the purpose of obtaining information can be done with the help of information technology or through traditional humanistic interaction. This type of exploitation is referred to as *social engineering*. The perpetrator uses behavioral psychological tools in order to create an illusion of emotions, which the perpetrator subsequently uses to exert influence over an individual.

Provided that the criminal prerequisite of the Trade Secrets Act (2018:558) is fulfilled, the information may constitute a company secret and thus obtain legal protection. The assessment of the prerequisite regarding the type of information covered by the legislation is fairly generous. The legal source material does not give any indication that the legislature intended that the legal practitioner should adhere to the procedure itself when the accused exploited human weaknesses. Whether the method used by the perpetrator when he or she has obtained access to the company secret is illegal has no significance in the assessment of criminal liability. The approaches listed by the legislation indicate that the prerequisite's structure has something of a technical character as they give the impression of focusing primarily on the facts rather than emotional factors.

Companies often have a certain self-interest in maintaining the confidentiality of intern information. In order to strengthen the protection of trade secrets, extrajudicial protection can be obtained through systematic information security work. The company's work on information security establishes a certain measure of knowledge regarding the ability to identify security risks. With these risks in mind, the company should consider taking appropriate and effective security measures. The concept of information security is closely related to technology and computer science. This may be one of the reasons

why companies often prioritize information security work of technical protection measures. This, in order to counteract external IT-related threats. However, regardless of the technical level of protection in the company, *the endpoint of the security problem* remains - the employee. As long as human labor exists, human vulnerability factors are considered to be a permanent risk factor.

The problem can mainly be portrayed based on two aspects. First, the difficulty consists in the ability to identify and detect social engineering, which is a common occurrence. Clearing the company´s confidential information can have significant adverse effects, which can hamper the promotion process. Secondly, the legal implication of social engineering in existing research has only been emphasized but does not appear to have been studied in either Sweden or internationally. This is why the aim of the thesis is to, with the support of the legal dogmatic method and the legal analytical method, investigate whether criminal law correlates with social engineering. The Trade Secrets Act is used as an illustrative example in order to showcase the extent of the exploitation of human weaknesses in the criminal law assessment. The study of legal sources gives an indication that neither the origin nor the effects of social engineering are explicitly taken into account in the criminal law assessment.

Although the field of social engineering research is fairly broad, research to date has not addressed the phenomenon in a jurisprudence context. Social engineering, according to my research, has only been recognized in the context of sociological, behavioral- and computer science. In order to raise awareness, to be able to identify and elucidate a generally widespread and fairly disguised method of attack, the present thesis is intended to constitute an approach to illustrate this problem.

Sammanfattning

Genom att utnyttja generella socialpsykologiska mänskliga sårbarhetsfaktorer kan en gärningsperson manipulera en individ att lämna ifrån sig konfidentiell information. Utnyttjandet av mänsklig kontakt och förtroende i syfte att erhålla information kan företas med hjälp av informationsteknik eller genom en mer traditionell och humanistisk interaktion. Denna typ av utnyttjande benämns som *social manipulation*. Gärningspersonen använder beteendepsykologiska verktyg i syfte att skapa en illusion av känslor, vilket gärningspersonen sedermera utnyttjar för att utöva inflytande över denne.

Under förutsättning att de straffrättsliga rekvisiten i lag (2018:558) om företagshemligheter är uppfyllda kan informationen utgöra en företagshemlighet och således erhålla rättsligt skydd. Bedömningen av rekvisiten avseende vilken typ av information som omfattas av lagstiftningens skydd är tämligen generös. Rättskällematerialet ger ingen indikation på att lagstiftaren avsett att rättstillämparen, vid den straffrättsliga bedömningen, ska fästa avseende vid det tillvägagångssätt som den tilltalade använde sig av. Huruvida den metod som gärningspersonen använt sig av, då denne berett sig tillgång till företagshemligheten, är rättsstridig har ingen betydelse vid bedömning av straffansvar. De angreppssätt som lagstiftningen föreskriver tyder på att rekvisitens struktur har något av en teknisk karaktär, eftersom de ger intryck av att primärt fokusera på de faktiska omständigheterna istället för på emotionella faktorer.

Företag har ofta ett visst egenintresse av att vidmakthålla konfidentialiteten i intern information. I syfte att förstärka skyddet för företagshemligheter kan utomrättsligt skydd uppbäras genom företagandet av systematiskt informationssäkerhetsarbete. Verksamhetens arbete med informationssäkerhet uppställer emellertid ett visst mått av kunskap avseende förmåga att identifiera säkerhetsrisker och utifrån dessa vidta lämpliga och effektiva säkerhetsåtgärder. Informationssäkerhetsbegreppet står i nära förbindelse med teknik-

och datavetenskap. Detta kan vara en anledning till att verksamheter ofta koncentrerar informationssäkerhetsarbetet till att utarbeta tekniska skyddsåtgärder i syfte att motverka externa IT-relaterade hot. Oberoende av verksamhetens tekniska skyddsnivå kvarstår emellertid *säkerhetsproblemets slutpunkt* – arbetstagarna. Så länge som mänsklig arbetskraft existerar befaras mänskliga sårbarhetsfaktorer utgöra en beständig riskfaktor.

Problematiken kan i huvudsak porträtteras på två sätt. För det första utgörs svårigheten av att överhuvudtaget förmå identifiera och upptäcka social manipulation som är en vanlig förekommande företeelse. Röjandet av verksamhetens konfidentiella information kan få omfattande skadeverkningar, vilket kan hämma det konkurrensfrämjande arbetet. För det andra har den rättsliga implikationen av social manipulation i den befintliga forskningen endast poängterats, men förefaller inte ha studerats i vare sig Sverige eller utomlands. Uppsatsens syftar således till att, med stöd av den rättsdogmatiska och den rättsanalytiska metoden, undersöka om straffrätten korrelerar med social manipulation. Genom att använda lagen om företagshemligheter som ett illustrerande exempel granskas i vilken mån som straffrätten beaktar utnyttjandet av mänskliga svagheter i den straffrättsliga bedömningen. Studiet av rättskällorna ger en antydan om att vare sig upphovet till eller effekterna av social manipulation uttryckligen beaktas vid den straffrättsliga bedömningen.

Trots att forskningsfältet avseende social manipulation är tämligen brett har forskningen hittills inte behandlat företeelsen i den rättsvetenskapliga kontexten. Social manipulation har, enligt min undersökning, uteslutande studerats i en sociologisk, beteende- och datavetenskaplig kontext. Behovet av att belysa social manipulation i den rättsvetenskapliga kontexten torde således vara stort. I syfte att öka medvetenheten, förmå identifiera och belysa en allmänt utbredd och tämligen förtäckt angreppsmetod har förevarande uppsats för avsikt att utgöra en ansats till att åskådliggöra denna problematik.

Förord

Denna rättsvetenskapliga uppsats utgör examensarbetet för termin nio på juristprogrammet vid Lunds universitet.

Jag vill tacka min handledare Sverker Jönsson, som med stort engagemang handlett mig i mitt uppsatsskrivande och bidragit med värdefulla synpunkter. Jag vill även rikta ett stort tack till alla Er som på ett eller annat sätt funnits där för mig under studietiden.

Lund, 25 maj 2020
Ellen Johansson Wintzell

Förkortningar

Bet.	Betänkande
Brå	Brottsförebyggande rådet
Di	Dagens industri
Europeiska kommissionen	EU-kommissionen
EU	Europeiska unionen
EY	Ernst & Young
Företagshemlighetsdirektivet	Europaparlamentets och rådet direktiv (EU) 2016/943 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs.
FHL	Lag (1990:409) om skydd för företagshemligheter
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
Ibid.	Ibidem (används då hänvisning upprepas i efterföljande fotnot)
IT	informationsteknik
JT	Juridisk tidskrift
LFH	Lag (2018:558) om företagshemligheter
MSB	Myndigheten för samhällsskydd och beredskap
NAFTA	North American Free Trade Agreement
NE	Nationalencyklopedin

OSL	Offentlighets- och sekretesslag (2009:400)
PM	Promemoria
prop.	proposition
RF	Regeringsformen (1974:152)
SCB	Statistiska centralbyrån
SiS	Svenska institutet för standarder
Skr.	skrivelse
SvJT	Svensk juristtidning
TF	Tryckfrihetsförordning (1949:105)
TfR	Tidsskrift for Rettsvitenskap
TRIPS-avtalet	Agreement on Trade-Related Aspects of Intellectual Property Rights
USMCA	United States – Mexico – Canada Agreement
YGL	Yttrandefrihetsgrundlag (1991:1469)

1 Inledning

1.1 Bakgrund

Sedan tidigt 1900-tal har den svenska lagstiftning avseende otillbörlig konkurrens och skydd mot företagshemligheter debatterats av och an. Trots ett flertal utdragna lagstiftningsprocesser under mitten av 1900-talet resulterade överläggandet i en lagstiftning som, ur ett internationellt hänseende, var unik till sin karaktär. Skyddet för företagshemligheter fick sedermera ett internationellt uppsving då företagshemlighetsdirektivet trädde ikraft 2016. Från ett svenskt perspektiv resulterade direktivet i en reviderad lagstiftning – lag (2018:558) om företagshemligheter (LFH). LFH skyddar obehöriga angrepp som företas på information rörande affärs- eller driftförhållanden i en näringsidkares rörelse eller i en forskningsinstitutions verksamhet.[1] För att informationen ska erhålla rättsligt skydd uppställs bland annat ett aktivitetskrav, vilket innebär att informationsinnehavaren ska ha vidtagit rimliga åtgärder för att hemlighålla företagshemligheten.[2]

Den som uppsåtligen och olovligen bereder sig tillgång till en företagshemlighet kan dömas för *företagsspionerі*.[3] På motsvarande sätt kan den som uppsåtligen anskaffar en företagshemlighet, med vetskap om att den som tillhandahållit hemligheten eller någon före denne i sin tur har berett sig tillgång till hemligheten genom företagsspionerі, kan dömas för *olovlig befattning med företagshemlighet*.[4] I förarbetena anges uttryckligen att det inte har någon betydelse vilket underliggande syfte som den tilltalade hade vid tillfället för anskaffandet av företagshemligheten. Det avgörande för frågan avseende straffansvar är istället huruvida den tilltalade olovligen har berett sig tillgång till företagshemligheten. Vid bedömning av straffansvar är det även irrelevant huruvida den metod som angriparen använt sig är rättsstridig.[5]

[1] 2 § 1 st. p. 1 LFH.
[2] 2 § 1 st. p. 3 LFH.
[3] 26 § LFH.
[4] 27 § LFH.
[5] Se närmre kap. 3.2.1.1.

En metod som frekvent förekommer vid anskaffanden av information är social manipulation. Social manipulation utgör ett samlingsbegrepp för ett flertal manipulativa metoder. Samtliga metoder innebär ett utnyttjande av socialpsykologiska mänskliga sårbarhetsfaktorer i syfte att manipulera människor.[6] Social manipulation kan å ena sidan företas i välvillig bemärkelse – exempelvis då föräldrar manipulerar sina barn i syfte att barnen ska göra det som föräldrarna anser är bäst för dem. Å andra sidan kan metoden användas i mer eller mindre moraliska sammanhang eller i rent utav illegala kontexter. Social manipulation kan i viss mån beskrivas som en teknikneutral angreppsmetod då den kan företas oberoende av teknik. I syfte att få kännedom om företagshemlig information kan exempelvis en gärningsperson gradvis utveckla en förtroenderelation med en arbetstagare inom en viss verksamhet. Gärningspersonen kan söka kontakt med arbetstagaren på dennes fritid – som en nyinflyttad granne eller som en förälder på barnens fotbollsträning. Upprättandet av en stark förtroenderelation kan således förankras i arbetstagarens lediga tid och behöva pågå under en längre tidsperiod för att gärningspersonen ska få insikt om verksamhetens information och arbetstagarens kunskap.[7] Social manipulation kan även företas gentemot äldre och funktionshindrade genom att gärningspersonen utger sig för att komma från en tillförlitlig institution.[8] Angreppsmetoden har sitt ursprung i sociologiska, beteendevetenskapliga och datavetenskapliga kontexter, men har sedan den 1 januari 2019 tilldelats en brottskod av Brå.[9]

Intresset av att skydda informationstillgångar påträffas även i den utomrättsliga sfären. Informationssäkerhet utgör ett område vars arbete bland annat innebär ett identifierande av säkerhetsrisker i syfte att förmå vidta relevanta säkerhetsåtgärder i såväl privata som offentliga verksamheter.

[6] Se närmre kap. 4.3–4.4.
[7] Jfr *Industrispionage – ett svårarbetat fält.* (2019). Copenhagen: Saga, s. 21–22 – Social manipulation kan t.ex. företas i samband med industrispionage och metoden nämns således ofta i dessa sammanhang.
[8] Jfr Polisen (2020). *Kraftfullare informationsåtgärder krävs för att minska bedrägeribrott mot äldre*, <https://polisen.se/aktuellt/nyheter/2020/februari/kraftfullare-informationsatgarder-kravs-for-att-minska-bedrageribrott-mot-aldre/>, (hämtad 2020-05-11).
[9] Se närmre kap. 4.3.

Informationssäkerhetsbegreppet står i nära förbindelse med teknik- och datavetenskap. Denna förbindelse medför att det systematiska informationssäkerhetsarbetet ofta koncentreras till att verksamheterna väljer att prioritera utarbetandet av tekniska skyddsåtgärder i syfte att motverka externa IT-relaterade hot. Intet att förglömma är de interna hoten, vilka främst utgörs av verksamhetens egna arbetstagare. *Säkerhetsproblemets slutpunkt* är en benämning på den inverkan som arbetstagare har gentemot verksamhetens integritet. Oberoende av omfattningen på det tekniska skyddet som etableras i verksamheten utgör social manipulering ett kryphål för potentiella gärningspersoner.[10] Om verksamheterna tar hjälp av befintliga modeller, utbildar och medvetandegör sina arbetstagare om förefintliga säkerhetsrisker avseende social manipulation, finns det en möjlighet att angreppsmetoden enklare kan identifieras och således förhindras.

Behovet av att ytterligare synliggöra social manipulation torde vara stort, inte minst med avseende på metodens vidsträckta tillämpningsområde. Det presumerade mörkertalet avseende angreppsmetodens frekvens tyder på att metoden är svår att identifiera och upptäcka. Likaså torde majoriteten av alla företag, oberoende av verksamhetsform, storlek eller primära syfte, ha ett egenintresse av att verksamhetens information skyddas från obehöriga angrepp. Utnyttjandet av mänskliga sårbarhetsfaktorer bedöms även i en framtida kontext ha en övergripande påverkan inom socialpsykologin, datavetenskapen och rättsvetenskapen. Allteftersom tekniken utvecklas finjusteras de tekniska möjligheterna avseende efterliknandet av mänskligt beteende. Förbättrandet av tekniska skyddsåtgärder kan emellertid ge upphov till ett kringgående av denna sortens teknik. Detta kan resultera i ett uppsving av den typ av social manipulation som i huvudsak företas genom en traditionell och humanistisk interaktion med offret.

I den forskning som hittills presenterats behandlas social manipulation fristående från den rättsvetenskapliga disciplinen. Behovet av att belysa social

[10] Se närmre kap. 4.2.2.

manipulation grundar sig bland annat i att lagstiftningen måste kunna hålla ett något så när jämnt tempo med utvecklingen av nya bedrägerimetoder. Ökad kunskap avseende vilka mänskliga svagheter som ny teknik potentiellt kan komma att utnyttja kan bidra till att öka lagstiftarens medvetenhet om hur skyddslagstiftningen ska konstrueras för att dess funktion ska optimeras. Det finns således ett behov av att belysa social manipulation i den rättsvetenskapliga kontexten. Genom att använda LFH som ett illustrerande exempel avser förevarande uppsats utgöra en ansats till att åskådliggöra denna problematik.

1.2 Syfte och frågeställningar

Uppsatsens syfte är att undersöka om straffrätten korrelerar med social manipulation. I syfte att förmå genomföra undersökningen fordras svar på den övergripande frågeställningen – i vilken mån beaktar straffrätten mänskliga sårbarhetsfaktorer som utnyttjas vid social manipulation?

För att finna ett svar uppsatsens frågeställning krävs det inledningsvis att ett antal delfrågor löpande besvaras:

- Hur är det straffrättsliga skyddet för företagshemligheter utformat?
- Hur diskuteras skyddet för informationstillgångar i utomrättsliga sammanhang?
- Vad innebär social manipulation och i vilka sammanhang tar det sig uttryck?

Undersökningens syfte och frågeställning är avsiktligen generellt utformade. Ändamålet är att uppsatsen ska konkretisera och medvetandegöra en beteendevetenskaplig infallsvinkel som ännu inte, enligt min uppfattning, i tillräckligt stor utsträckning uppmärksammats och koordinerats i en rättslig kontext. LFH utgör i förevarande uppsats ett illustrativt exempel på en lagstiftning som, enligt min mening, bör granskas utifrån ett beteendevetenskapligt perspektiv. Det torde finnas ytterligare lagstiftning som bör genomgå

en liknande granskning. LFH är emellertid metodiskt utvald till att tjäna som belysande exempel. Anledningen till detta är då den rättsliga regleringen inbegriper ett sådant skyddsvärt intresse, vilket ofta utgör föremål förutom-rättsliga diskussioner avseende såväl tekniska som icke-tekniska angrepp som utförs genom social manipulation. Valet av lagstiftning kan även motiveras utifrån den problematik som för närvarande är relativt dold. Problematiken inbegriper bland annat utnyttjanden av arbetstagare i syfte att få åtkomst till information. För den händelse att angreppet, för gärningspersonens del, når framgång kan förödande konsekvenser uppstå för såväl den enskilda verksamheten, dess kunder och samhället i stort.

1.3 Metod och material

1.3.1 Introduktion

För att förmå analysera huruvida lagstiftaren har beaktat social manipulation i konstruerandet av den svenska skyddslagstiftningen rörande företagshemligheter fordras inledningsvis kunskap om lagstiftningens karaktär och struktur. Denna kunskap erhålls fördelaktigast genom studiet av rättskällorna.[11] Den rättsdogmatiska metoden är i detta avseendet lämplig att tillämpa. Metodvalet motiveras av att svar på uppsatsens frågeställning till övervägande del söks hos de allmänt accepterade rättskällorna – lagstiftning, rättspraxis, förarbeten och doktrin.[12]

1.3.2 Den rättsdogmatiska metoden och gällande rätt

Svaret på frågeställningen ska till viss del presumeras återspegla innehållet i *gällande rätt*.[13] *Gällande rätt* är ett väl vedertaget uttryck som har tilldelats ett antal olika definitioner. En av dessa definitioner har utarbetats av Ross[14]

[11] Kleineman, Jan, *Rättsdogmatisk metod*, Korling, Fredric & Zamboni, Mauro (red.) (2013). Juridisk metodlära. 1. uppl. Lund: Studentlitteratur, s. 23.
[12] Sandgren, Claes (2018). *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*. Fjärde upplagan Stockholm: Norstedts Juridik, s. 49.
[13] Kleineman 2013, s. 26.
[14] Alf Ross var en dansk jurist och filosof och verksam som professor vid Köpenhamns universitet mellan åren 1938–1969.

och går under beteckningen prognosteorin. Prognosteorin innebär att en regel som i doktrin påstås utgöra *gällande rätt* är en slags förutsägelse om att regeln kommer att tillämpas i framtida rättsliga avgöranden.[15] Även Kelsen och Merkl[16] har arbetat fram en definition, vari *gällande rätt* utgörs av en bestämd regel som tillkommit i enlighet med den procedur som överensstämmer med en tillämpbar rättsregel av högre dignitet. Reglerna av högre dignitet fastslår vem som har behörighet att instifta regler och hur en sådan procedur ska ske.[17] Peczenik[18] har delvis kritiserat dessa definitionerna och menar att det endast finns två olika definitioner att tillgå.[19] Begreppet kan dels avse en regel som kännetecknas av rättslig giltighet under premissen att regeln infriar ett antal kriterier, dels avse en regel som bör följas ur juridiskt hänseende.[20] Peczenik förtydligar att det som vanligtvis åsyftas vid beskrivandet av *gällande rätt* är när en rättsregel tillhör den gällande rättsordningen.[21] Denna beskrivning harmonierar med hur begreppet tolkas och används i detta uppsatsarbetet. Med *gällande rätt* avses i förevarande uppsats följaktligen de rättsregler som för närvarande är i kraft och tillämpas inom det svenska rättssystemet.

Den rättsdogmatiska metoden har inte uteslutande tillämpats okritiskt. Begreppet *rättsdogmatik* har bland annat kritiserats för att tolkas som *dogmatisk*.[22] Sandgren[23] framhåller att ett dogmatiskt förhållningssätt karaktäriseras av en ovilja till vidsynthet och modernisering.[24] Kleineman[25] framhåller å andra sidan att detta är en feltolkning som måste ignoreras då den rättsdogmatiska metoden inte nödvändigtvis inbegriper en dogmatisk inställning. Trots att den rättsdogmatiska metoden vanligtvis associeras till att,

[15] Peczenik, Aleksander, *Rättsordningens struktur*, SvJT 1974 s. 369.
[16] Hans Kelsen var en österrikisk rättsfilosof och var verksam som professor på universiteten i bl.a. Wien, Genéve och Kalifornien. Adolf Merkl var en österrikisk professor och student till Kelsen.
[17] Peczenik 1974, s. 370.
[18] Aleksander Peczenik var under senare hälften av 1900-talet verksam professor i allmän rättslära vid Lunds universitet.
[19] Peczenik 1974, s. 371.
[20] Peczenik, Aleksander, *Rätt och moral*, SvJT 1982 s. 609.
[21] Peczenik 1974, s. 371.
[22] Med *dogmatisk* avses överdrivandet av praktiserandet av dogmer genom att t.ex. inneha en strikt hållning gentemot en specifik doktrin eller princip.
[23] Claes Sandgren är verksam professor i civilrätt vid Stockholms universitet.
[24] Sandberg, Claes, *Är rättsdogmatiken dogmatisk?,* TfR 2005 s. 648.
[25] Jan Kleineman är verksam professor i civilrätt vid Stockholms universitet.

utifrån rättskällorna, klargöra innehållet i *gällande rätt* innebär det emellertid inte nödvändigtvis att betraktaren besitter en dogmatisk inställning till innehållet i de rättskällor som denne studerat. Jareborg[26] påpekar å andra sidan att begreppets innebörd inte behöver stipuleras som en problematisk företeelse. Istället finner Jareborg ett värde i att, vid rättsdogmatisk argumentation, tillåta ett perspektivvidgande genom att inte uteslutande begränsa argumentationen till *gällande rätt*.[27]

1.3.3 Det kritiska tänkandet

När *gällande rätt* ska utredas och preciseras kan dess innehåll upplevas som diffust eller bristfälligt. Schelin[28] menar att kritiskt tänkande, vid sådant precisions- och utfyllnadsarbete, är essentiellt för att *gällande rätt* ska kunna tolkas och tillämpas. Förmågan att ifrågasätta fakta och ge uttryck för ett analytiskt ställningstagande är särskilt betydelsefullt för juristers vidkommande. Jurister besitter en enorm samhällsmakt och får av rättssäkerhetsskäl inte riskeras att hämmas i det analytiska arbetet eller desorienteras från sin yrkesetik.[29] Sandgren framhåller emellertid att värderingar som utvecklats från icke rättskällematerial kan framkalla viss tvivelaktighet avseende huruvida värderingen bör tillåtas ingå i den rättsdogmatiska argumentationen eller inte.[30]

Svensson[31] har redogjort för hur den svenska rätten under lång tid haft för vana att särskilja beskrivande fakta från värderingar.[32] När författarna till den juridiska litteraturen inte, i tillräckligt stor utsträckning, klargör vilket material som ett specifikt argumenten härstammar från kan värnandet om rätten som en fristående disciplin försvåras. Svensson indikerar faran med att enbart låta rätten bestå av allmänna tolkningar, eftersom den auktoritativa styrkan i vissa argument då kan riskeras att urholkas. Ur ett bredare perspektiv

[26] Nils Jareborg är verksam professor emeritus i straffrätt vid Uppsala universitet.
[27] Jareborg, Nils, *Rättsdogmatik som vetenskap*, SvJT 2004 s. 4.
[28] Johan Schelin är verksam professor i civilrätt vid Stockholms universitet.
[29] Schelin, Johan (2018). *Kritiska perspektiv på rätten*. [Stockholm]: Poseidon Förlag, s. 13–15.
[30] Sandgren 2005, s. 652–653.
[31] Eva-Maria Svensson är verksam professor i rättsvetenskap vid Göteborgs universitet.
[32] Schelin 2018, s. 107.

kan grundläggande rättsprinciper, bland andra förutsebarheten, undermineras. Om tolkning av rätten sker under öppna former där tydliga åtskillnader görs mellan argument och antaganden samt ett rutinmässigt företagande av transparenta källhänvisningar kan riskerna reduceras. Åtskillnaden kan förklaras med hjälp av uttrycken *de lege lata* – hur rätten är, samt *de lege ferenda* – hur rätten borde vara. Ambitionen har sedan länge varit att eftersträva en välavgränsad distinktion mellan de två sätten att argumentera, vilket inte har varit helt okomplicerat.[33] Svensson proponerar emellertid för en återanvändning av uttrycket *de lege interpretata* – rätten som den uttolkas eller har uttolkats. På så vis fordras att doktrinen alltid inbegripa en noggrann redogörelse över vilken metod samt vilket material som ligger till grund för en viss tolkning.[34]

I den mån som rätten framställs och tolkas är kravet på att framhålla argumentens härkomst centralt. Vid bedrivandet av kritisk granskning, menar Svensson, att framförandet av fri argumentation är större för rättsvetenskapliga forskare än för juristers vidkommande. Anledningen till att forskare tillåts bedriva en fri, transparent och kritisk forskning kan vara den högt värderande demokratiska digniteten. Prioriterandet av att förhindra förekomsten av maktmissbruk utgör däri kärnan för ett välfungerande och demokratiskt rättssamhälle.[35] Fahlbeck[36] har emellertid ställt sig frågande till om det i en vetenskaplig avhandling överhuvudtaget är möjligt att ”forska” om den lagstiftning som bör gälla samt vilka villkor som uppställs för att en juridisk text ska godtas som vetenskaplig.[37] Fahlbeck ställer sig nekande till om forskning kan ske de lege ferenda. Fahlbeck menar att förslagen som presenteras i sådana typer av avhandlingar mer är att likna vid slutsatser som dras från premisserna i det material som den rättsvetenskapliga forskaren granskats.[38]

---

[33] Svensson, Eva-Marie (2014). *De lege interpretata – om behovet av metodologisk reflektion*, Juridisk publikation, jubileumsnummer, s. 225–226.
[34] Svensson 2014, s. 212–214.
[35] Ibid. s. 214–215.
[36] Reinholt Fahlbeck är verksam professor emeritus i arbetsrätt vid Lunds universitet.
[37] Fahlbeck, Reinhold (2016/17). *Kan forskning ske de lege ferenda? Några ord om vetenskap och den lag som bör införas*, JT Nr 2 2016/17, s. 529.
[38] Ibid. s. 531–532.

1.3.4 Rättskällornas auktoritativa styrka

Genom praktiserandet av den rättsdogmatiska metoden studeras rättskällorna, vilka är de källor som utgör grunden för att kunna utreda och precisera innehållet i *gällande rätt*. Fastställandet av *gällande rätt* sker i huvudsak genom att företa en deskriptiv och systematisk behandling av rättskällorna.[39] Praktiserandet av rättskällorna kommer framför allt till uttryck i uppsatsens tredje kapitel, vars innehåll till övervägande del utgår från rättskällematerial. Det är således av vikt att uppmärksamma distinktionen mellan de olika rättskällornas auktoritativa styrka. På så vis kan de auktoritativa rättskällorna – lagstiftning, förarbeten och rättspraxis – effektivt rättfärdigas, samtidigt som fakta från doktrin underbyggs. De auktoritativa rättskällorna innehar formell auktoritet och ger uttryck åt auktoritativa argument, medan doktrinen enbart kan övertyga genom en hög grad av styrka i de argument som framförs.[40] I syfte att förmå garantera en likvärdig och förutsebar rättstillämpning krävs det att en något så när strikt hållning företas gentemot de auktoritativa rättskällorna.[41] Med anledning av att rättspraxis tillhör de auktoritativa rättskällorna kan det tyckas förefalla naturligt att även låta denna rättskälla inbegripas i förevarande uppsats. Av ett flertal anledningar har jag emellertid valt att inte, i nämnvärd omfattning, inkludera rättspraxis.[42] Studiet av *gällande rätt* utgår istället primärt från förarbeten och doktrin.

Trots att doktrinen inte innehar en formell auktoritativ ställning inom rättskälleläran bör dess betydelse inte underskattas. Doktrinens styrka utgörs av dess inre tyngd, vilket innebär att doktrinen tillåts framföra en fri argumentation där normsystemets brister nästintill obehindrat kan kritiseras. Kleineman hävdar dessutom att det inte enbart är doktrinens inre tyngd som gör att den upphöjs som rättskälla, utan även dess starka och logiska struktur.[43] Lehreberg[44] menar att doktrinens praktiska funktionalitet i veten-

[39] Sandgren 2018, s. 49.
[40] Lehrberg, Bert (2019). *Praktisk juridisk metod*. Elfte upplagan Uppsala: Iusté, s. 203.
[41] Ibid. s. 99–100.
[42] Se närmre kap. 1.5.
[43] Kleineman 2013, s. 33.
[44] Bert Lehrberg är verksam professor i civilrätt vid Uppsala universitet.

skapliga diskussioner kan medföra att den tillskrivs en viss auktoritativ tyngd i rättskälleläran.[45] Genom tillämpandet av den rättsdogmatiska metoden kan doktrinen således förena deskription av *gällande rätt* med ett kritiskt förhållningssätt.[46] Denna konstellation utgör en bland flera faktorer som, enligt Kleineman, bidrar till att doktrinen intar en unik ställning i rättskälleläran. Med hjälp av den rättsdogmatiska metoden kan alltså doktrinen, i större utsträckning än övriga rättskällor, tillåtas framföra kritik mot det rådande rättsläget och resonera kring alternativa lösningar.[47]

En traditionell juridisk handbok och lagkommentar som repetitivt används i förevarande uppsatsarbete är 2019 års upplaga av Fahlbecks bok – *Lagen om företagshemligheter: en kommentar och rättsöversikter*. Frånsett bokens lagkommentarer impliceras en djupgående redogörelse hur det rättsliga skyddet för företagshemligheter utvecklats sedan början av 1900-talet fram tills modern tid. Den moderna litteraturen i form av handböcker och lagkommentarer har av Lehrberg kritiserats för dess avsaknad av detaljerade och varierande källhänvisningar. Lehrberg menar att detta har åsamkat negativ inverkan på litteraturens auktoritativa tyngd.[48] Fahlbecks bok bedömer jag emellertid som transparent då det till brödtexten tillfogas detaljerade fotnoter. Fahlbeck bidrar med omfattande kunskap om hur enskilda lagar förhåller sig till varandra i det svenska rättssystemet, vilket medför att skyddet för företagshemligheter studeras på en övergripande och detaljerad nivå.

Kompletterande litteratur har använts i syfte att redogöra för företagshemligheter utifrån ett information- och säkerhetsperspektiv.[49] Denna typ av

[45] Lehrberg 2019, s. 203.
[46] Kleineman 2013, s. 35–36.
[47] Ibid. s. 33.
[48] Lehrberg 2019, s. 205–206.
[49] Se bl.a. Helgesson, Christina (2000). *Affärshemligheter i samtid och framtid*. Diss. Stockholm: Univ.; Sandgren, Claes & Andersson, Anderz (red.) (1995). *Kunskapsföretaget i ett rättsligt perspektiv: [bolagsrätt, arbetsrätt, familjerätt, immaterialrätt, avtalsrätt, köprätt, skadeståndsrätt, skatterätt]*. 1. uppl. Stockholm: Fritze.; Svensson, Tommy (2011). *Lönsam säkerhetsjuridik: om konsten att skydda sig själv och sina tillgångar*. 5. omarb. utg. Hässelby: M I J media.

litteratur har avgränsats till forskare vars expertis på området är uttalad och uppvisar såväl trovärdighet som transparens i valet av källmaterial.

1.3.5 Den rättsanalytiska metoden och dess korrelation till rättsdogmatiken

Den juridiska litteraturen förefaller för närvarande vidmakthålla distinktionen mellan den rättsdogmatiska och den rättsanalytiska metoden, trots att en sådan distinktion i praktiken inte alltid verkar upprätthållas.[50] Rättsdogmatiken och den rättsanalytiska metoden har emellertid ett flertal gemensamma drag. Sandgren menar att tillämpandet av den rättsdogmatiska metoden inbegriper en relativt fri argumentation.[51] I jämförelse med den rättsdogmatiska metoden beskrivs den rättsanalytiska metoden förhålla sig neutral gentemot de allmänt accepterade rättskällorna. Ett neutralt förhållningssätt kan medföra en ökad självständighet i förhållande till det material som studeras, eftersom den rättsanalytiska metoden inte fordrar en lika strikt hållning gentemot rättskällorna som den rättsdogmatiska metoden gör.[52] I syfte att upprätta en fullgod analys fordras en metod där fri argumentation tillåts att beaktas, utan att arbetet för den skull hamnar utanför det vetenskapliga området.

Schelin beskriver det *kritiska tänkandet* som en självständig reflektion över fakta och värderingar, medan det vid framställningen av *akademisk kritik* fordras ett mer vetenskapligt tillvägagångssätt.[53] Denna framställning kan förefalla förhållandevis abstrakt, men gör sig verklig i förhållande till varför förevarande uppsats tillämpar en rättsdogmatisk metod med inslag av såväl intern som extern kritik.[54] Genom att förena kritiskt tänkande med ett disciplinöverskridande förhållningssätt och ett de lege ferenda perspektiv anläggs en

[50] Jfr Sandgren, Claes (2007). Juridikavhandlingar vid Stockholms universitet 1957–2006, *ingår i Juridiska fakulteten 1907–2007. En minnesskrift (2007)*, s. 454–467.
[51] Sandgren 2005, s. 655–656.
[52] Sandgren 2018, s. 50.
[53] Schelin 2018, s. 16.
[54] Med *intern kritik* avses kritik som utvecklats på grundval av rättssystemet. Med *extern kritik* åsyftas sådan kritik som huvudsakligen härrör från vetenskaper bortom rättsvetenskapen. Schelin beskriver intern kritik som nära besläktad med frågan om de lege lata och den externa kritiken som nära besläktad med frågan om de lege ferenda.

bred grund som främjar den avslutande analysen. Med utgångspunkt i den rättsdogmatiska metoden kan således olika element inkorporeras i uppsatsens arbete, samtidig som den fakta och de värderingar som inhämtas från utomrättsliga källor tvingas genomgå en kritisk granskning.

Den rättsanalytiska metoden ska i förevarande uppsats tjäna som komplement till den rättsdogmatiska metoden och bidra till utformandet av en transparent och fri analys. Den rättsanalytiska metoden gör det möjligt att i större utsträckning tillämpa argument som härrör från andra vetenskapsdiscipliner. Detta är av betydelse då förevarande uppsats inte uteslutande beaktar den kunskap som finns att tillgå inom rättskälleläran. Bortsett från att fastställa *gällande rätt* möjliggör den rättsanalytiska metoden företagandet av fri argumentation, vars material består av kunskap och värderingar som inte ursprungligen härstammar från *gällande rätt*.[55] Genom att kombinera den rättsdogmatiska och rättsanalytiska metoden är min förhoppning att tillämpningen av argument från den rättsvetenskapliga, den beteendevetenskapliga samt den datavetenskapliga disciplinen ska uppfattas som berättigande och bidra till en utförlig analys.

1.4 Forskningsläget

Skyddet för företagshemligheter har behandlats i såväl litteratur som i juridiska avhandlingar.[56] Ett flertal vetenskapliga undersökningar utgörs av studentuppsatser, vars forskningsområde inbegriper såväl arbetsrättsliga som immaterialrättsliga spörsmål. På motsvarande sätt har social manipulation varit föremål för ett flertal undersökningar – i huvudsak inom beteendevetenskapen och datavetenskapen.

I det följande har jag valt att inledningsvis uppmärksamma en äldre studie. Trots att studien har några år på nacken inbegriper den forskningsfrågor som

[55] Sandgren, 2018, s. 50–51.
[56] Se bl.a. Fahlbeck, Reinhold (2019). *Lagen om företagshemligheter: en kommentar och rättsöversikter*. Fjärde upplagan Stockholm: Norstedts Juridik.; Domeij, Bengt (2016). *Från anställd till konkurrent: lojalitetsplikt, företagshemligheter och konkurrensklausuler*. 1. uppl. Stockholm: Wolters Kluwer.

torde vara av relevans även idag. Studien uppvisar en hög kvalitet, eftersom valet av metod och det sammanhang, vari studien presenteras, inger tillförlitlighet.

1.4.1 Nationell fältstudie

I samband med utformningen av 1983 års betänkande om skydd för företagshemligheter företog 1983 års utredning en relativt omfattande fältundersökning. Avsikten med undersökningen var att, med hjälp av insamlade uppgifter från ett flertal svenska företag, kartlägga förekomsten av företagsspioneri och andra angrepp på företagshemligheter. Fältundersökningens resultat avsågs vara till stor hjälp, eftersom det vid denna tidpunkten inte existerade någon beaktansvärd rättspraxis på området. I syfte att åstadkomma en modern och ändamålsenlig lagstiftning ansågs det således nödvändigt att utarbeta ett underlag, vars material kunde bidra till att öka förståelsen för den rådande situationen.[57]

Fältundersökningens intention var att klarlägga det svenska läget avseende förekomsten av angrepp på företagshemligheter under slutet av 1900-talet. Valet av metod och den tolkning som gjorts avseende statistiken uppvisar ett tillförlitligt resultat över hur ett flertal företag, vid denna tidpunkten, uppfattade potentiella angrepp och effektiviteten av vidtagna skyddsåtgärder. Likaså indikerar utfallet att även om statistiken uppvisar förhållandevis låga siffror avseende antalet angripna företag uppskattas mörkertalet vara stort. Utredningen kunde bland annat konstatera att arbetstagarna utgjorde den största riskfaktorn vid röjande av företagshemligheter till konkurrenter.[58] Dessa konstateranden väcker fundering kring om resultatet sedermera de facto har beaktats i lagstiftningsarbetet. I vilken mån tar egentligen lagstiftaren hänsyn till den säkerhetsrisk som arbetstagare otvivelaktigt utgör avseende verksamhetens förmåga att hemlighålla information och delta i den fria konkurrensen?

[57] SOU 1983:52, *Företagshemligheter*, s. 161.
[58] Ibid. s. 191.

Fältundersökningen bestod utav två moment – en inledande enkätundersökning samt en efterföljande intervjustudie.[59]

1.4.1.1 Enkätundersökning

Med hjälp av svensk standard för näringsgrensindelning (SNI)[60] valdes 1 500 svenska företag ut. Företagen skulle via en utskickad enkät självständigt besvara fyra tämligen tvetydiga och extensiva ja eller nej-frågor.[61] Ungefär 87 procent av företagen inkom med ett svar, vilket ansågs vara en hög svarsprocent.[62]

På frågan om det inom företaget fanns kommersiell eller teknisk kunskap som hemlighölls för arbetstagare eller utomstående svarade 42 procent jakande. I branscher som inriktade sig på forskningsverksamhet påträffades de högsta procenttalen. De lägre procenttalen återfanns bland verksamheter inom tillverkningsindustrin och detaljhandeln. Med hjälp av enkätsvaren framgick det även att antalet företagshemligheter i ett företag har ett starkt samband till företagets storlek och då även indirekt antalet arbetstagare. Vidare ansåg 66 procent av de 573 företag som uppgav att de innehade en företagshemlighet att hemligheten omgavs av ett fullgott skydd. På frågan om företaget utsatts för företagsspionerі eller annat otillbörligt angrepp ansåg sig 13 procent av dessa 573 företag ha blivit utsatta. I likhet med svaret på frågan – om det i företaget fanns kunskap som hemlighölls från arbetstagare eller utomstående – återfanns även här de högsta procenttalen i de större företagen med över 500 arbetstagare. Det höga procenttalet återfanns i tillverkningsindustrin och i företag med över 500 arbetstagare.[63]

Utredningen konstaterande självmant att undersökningen i vissa avseenden hade brister. Dessa bestod bland annat av det vaga formulerandet av enkätfrågorna samt utredningens helhetsintryck av att vissa företag besvarat

[59] SOU 1983:52, s. 161.
[60] SNI används för att klassificera verksamheter utifrån vilken rörelse de bedriver.
[61] SOU 1983:52, s. 421.
[62] 87 procent av företagen motsvarar 1 359 företag.
[63] SOU 1983:52, s. 161–164.

frågorna förhållandevis ogenomtänkt. Trots detta bedömde utredningen att enkätundersökningen ingav validitet. Anledningen till studiens tilltro uppgavs vara på grund av det regelrätta och statistiska tillvägagångssättet vid urvalet av de studiedeltagande verksamheterna samt den höga svarsprocenten. Enligt utredningen var det dessa faktorer som bidrog till att resultatet kunde anses återspegla förekomsten av företagsspionerі inom utvalda delar av svenskt näringsliv. Baserat på fältundersökningens resultat från enkätundersökningen noterade utredningen således att även om förekomsten av företagsspionerі är förhållandevis låg bör införandet av ett rättsligt skydd inte bortprioriteras.[64]

1.4.1.2 Intervjuserie

Bland de företag som besvarade enkäten valdes 34 företag ut för att medverka i en efterföljande intervjustudie. Syftet med intervjun var bland annat att få en inblick i vilka företagshemligheter som fanns inom företagen, vilka typer av skyddsåtgärder som företogs mot dessa samt dess effektivitet, angrepp som företagshemligheten utsatts för, vilken angreppsmetod som använts samt vilka skyddsåtgärder som företaget vidtagit efter att ett angrepp skett. Premissen för att ingå i urvalet var att företaget hade, eller i vart fall bort ha, en företagshemlighet. Utredningen strävade även efter att de utvalda företagen, i görligaste mån, skulle återspegla det svenska näringslivet med en jämn fördelning över hela landet.[65]

Det resultat som intervjusvaren sammantaget ingav var att företagshemligheter av kommersiell karaktär återfanns i praktiskt taget samtliga företag – 25 av 34 företag. Majoriteten av företagens förebyggande skyddsåtgärder var generellt inriktade mot företagets egna arbetstagare. Bland de vanligaste förekommande skyddsåtgärderna påträffades bland annat försvårande åtkomst genom inlåsning eller att en anställd, som efter uppsägning skulle påbörja en ny tjänst hos en konkurrent, fick sluta befinna sig på arbets-

[64] Ibid. s. 161–164.
[65] Ibid. s. 425.

platsen under uppsägningstiden. Av intervjusvaren framgick det emellertid att skyddsåtgärderna, oberoende av dess omfattning, bedömdes vara ineffektiva gentemot företagets egna arbetstagare. De skyddsåtgärder som riktades mot utomstående bedömdes emellertid inneha en hög grad av effektivitet. Företagen själva påstod att det var svårare för utomstående att inträda i företaget än vad det var för en anställd att överlämna företagets interna hemligheter till en utomstående. Skyddsåtgärderna genomfördes som regel vid tillfälliga besök, exempelvis i form av inpasseringskontroller eller genom att införa särskilda bevakningsrutiner som förlades utanför ordinarie kontorstid.[66]

På frågan om företagen utsatts för angrepp på en företagshemlighet var svaret till viss del tvetydigt. Inte ett enda företag uppgav sig ha utstått ett utomstående angrepp där den tillfogade skadan varit särskilt stor. Resultatet påvisade att företagsspionerі förekommit vid 20 tillfällen och att angreppen primärt genomförts genom avlyssning, fotografering och tillgrepp. Regeringen bedömde att den låga siffran grundade sig på att företagens svårigheter avseende bevissäkring samt brist på vetskap om att ett angrepp mot företagshemligheten de facto hade inträffat.[67]

1.4.1.3 Slutsatser

Från undersökningsmaterialet kunde utredningen bland annat konstatera att angrepp på företagshemligheter i hög grad utförs av företagets egna arbetstagare. Bland de vanligaste förekommande angreppen är de fall där en anställd på ett konkurrerande företag uppsöker en anställd inom ett annat företag i syfte att angripa företagshemligheten.[68] Angreppet kan ske genom att en anställd utlämnar hemlig dokumentation eller avger muntlig information till konkurrenten. Trots företagandet av tekniska och icke-tekniska skyddsåtgärder i syfte att förhindra sådana angrepp, är det till syvende och sist företagets egna arbetstagare som utgör den största riskfaktorn för att företags-

[66] SOU 1983:52, s. 182–186.
[67] Ibid. s. 191–192.
[68] Ibid. s. 191–192.

hemligheter angrips.[69] Detta är en bidragande faktor till att det i praktiken blir svårt att påträffa ett heltäckande skydd mot angrepp på företagshemligheter.[70] Från undersökningsmaterialet kunde utredningen även konstatera att flertalet av de företag vars företagshemligheter utsatts för angrepp i efterhand hade vidtagit skyddsåtgärder, men att dessa inte varit särskild omfattande.[71]

1.4.2 Studierna av social manipulation

Det finns en rikhaltig samling av vetenskapliga arbeten som behandlar olika problemställningar avseende bedrägerimetoden social manipulation. Omfattningen på dessa arbeten varierar och inbegriper såväl studentuppsatser som doktorsavhandlingar. Oberoende av det vetenskapliga arbetets karaktär och metod är strukturen allt som oftast densamma – innebörden av social manipulation förklaras, bedrägerimetodens angrepp identifieras och potentiella förebyggande skyddsåtgärder presenteras. Ett flertal studier framställer social manipulation som en organisatorisk företeelse, vilket i förhållande till förevarande uppsatsarbete kan betraktas utgöra en fördel.[72] I förevarande uppsats avser *organisatorisk företeelse* sådan social manipulation som gärningspersonen företar gentemot en anställd inom en verksamhet i syfte att få denne att utlämna uppgifter av såväl informell som av organisatorisk karaktär. De analyser som framförts i denna typ av vetenskapliga arbeten är, trots varierande vetenskapsnivå, ändock omfattande då problemställningarna ofta bereder utrymme för en detaljerad diskussion.

Denna typ av forskningsarbeten har utan tvekan bidragit till att jag kunnat skapa mig en överblick över ämnet och utifrån denna vidta lämpliga av-

[69] SOU 1983:52, s. 312–313.
[70] Ibid. s. 193.
[71] Ibid. s. 199–200.
[72] Tidigare forskning utgörs av bl.a. Applegate, D. Scott. (2009). *Social Engineering: Hacking the Wetware!* Information Security Journal: A Global Perspective, 40-46.; Pieters, W., Montoya, L., Bullee, J. H., Junger, M., & Hartel, P. (2015), *The persuasion and security awareness experiment: reducing the success of social engineering attacks*, Journal of Experimental Criminology, 11(1), 97. doi:10.1007/s11292-014-9222-7.; Nohlberg, Marcus (2008). *Securing information assets: understanding, measuring and protecting against social engineering attacks*. Diss. (sammanfattning) Stockholm: Stockholms universitet, 2009, <http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-8379>, (hämtad 2020-04-12).

gränsningar. Inte desto mindre har den stora mängden material på området medfört att det varit av särskild vikt att kontinuerligt upprätthålla ett källkritiskt tänkande. Till följd av att social manipulation, inte i ringa omfattning, har behandlats i ett flertal sammanhang har det således varit relevant att avgränsa dess forskningsmaterial. Inhämtning av kunskap rörande social manipulation har således i huvudsak koncentrerats till tre forskare – Mitnick[73], Nohlberg[74] och Hadnagy.[75] Urvalet är primärt baserat på att forskarna förefaller inverka på forskningsfältets utveckling och att vetenskapliga arbeten och publikationer refererar till dessa.

Det forskningsmaterial som granskats behandlar inte det samband som kan råda mellan beteendevetenskapen och rättsreglernas utformning. Avsaknaden av en sådan diskussion innebär emellertid inte att det råder brist på intressanta och essentiella förbindelser mellan de två vetenskapsdisciplinerna. Tvärtom kan det snarare indikera att uppsatsämnet befinner sig inom ett tämligen outforskat område som är i behov av närmre efterforskning. I en av sina avhandlingar har Nohlberg kortfattat belyst samt bekräftat att de juridiska konsekvenserna av social manipulation onekligen är ett intressant område att undersöka. Nohlberg har emellertid valt att uteslutande fokusera på det sociala området och har således avgränsat bort det juridiska perspektivet.[76]

Social manipulation kan i större publika sammanhang företas genom att statliga myndigheter eller politiska partier nyttjar sociala medier för att sprida politisk propaganda.[77] Forskning som genomförts på området påvisar att den kommunikation som bedrivs på sociala medier företrädesvis pådrivs genom

[73] Kevin Mitnick kom under slutet av 1900-talet över företagshemlig information, vilket han dömdes för. Numera är han verksam som it-säkerhetskonsult och utger bl.a. böcker och arrangerar föreläsningar som behandlar säkerhetsrisker och säkerhetsåtgärder i syfte att öka informationssäkerheten i företag.
[74] Marcus Nohlberg forskar bl.a. inom ämnesområdet informationssäkerhet. Nohlberg är verksam som lektor i datavetenskap vid institutionen för informationsteknik vid Högskolan i Skövde.
[75] Christopher Hadnagy forskar inom säkerhetsområdet med inriktning på att förstå hur en gärningsperson, genom att tillämpa bedrägerimetoden social manipulation, utnyttjar mänsklig kontakt och förtroende i syfte att erhålla information.
[76] Nohlberg 2008, s. 12 och 74.
[77] Mittuniversitetets forskningscenter (2018). DEMICOM, *Hur används sociala medier inför ett val*, <https://www.miun.se/Forskning/forskningscentra/demicom/nyheter/2018-4/hur-anvands-sociala-medier-infor-ett-val/>, (hämtad 2020-04-07).

allmänhetens förtjänst och inte via politikerna själva. Detta kan förorsaka att redan befintlig desinformation förstärks eller att ny desinformation bildas.[78] I en rapport från 2019 presenterar forskare från universitetet i Oxford statistik som bland annat påvisar att det i de sammanlagt studerade 70 länderna påträffats bevisning avseende organiserad manipulation som förekommer i sociala medier. Jämfört med 2017 är det en ökning med 28 länder, närmre bestämt en ökning med 150 procent under en tidsperiod på två år. I rapporten konstaterar forskarna att den vanligaste förekommande kommunikationsmetoden utgörs av konstruerandet av desinformation genom manipulering via olika informationskanaler.[79]

Förekomsten av social manipulation i privata sammanhang kan bland annat illustreras genom en doktorsavhandling i samhällsvetenskap från 2007. I avhandlingen applicerar Arvidson[80] ett samhälleligt perspektiv på straffrättens bedrägeribegrepp. Detta sker i syfte att framföra argument som stödjer tesen – att bedrägeri utgör en social företeelse. Avhandlingen fokuserar särskilt på den sociala interaktionen mellan bedragaren och den bedragne i en pågående bedrägerisituation.[81] Den interaktion som uppstår är emellertid asymmetrisk, eftersom den bottnar i ett förtroendeberoende som bedragaren missbrukar gentemot den som bedras.[82] Arvidson menar att bedrägeri som företeelse är i behov av att synliggöras för att öka den allmänna kunskapen om hur interaktionsformen framträder i vår samtid. Då bedrägerier är en vanlig förekommande samhällsföreteelse är det således nödvändigt att bortse från det traditionella tänket avseende att bedrägerier enbart är en företeelse som figurerar i den juridiska kontexten som en enskild brottstyp. Arvidson be-

[78] Falasca, Kajsa, Mikolaj, Dymek, & Grandien, Christina (2019). *Social media election campaigning: who is working for whom? A conceptual exploration of digital political labour*, Contemporary Social Science, 14:1, DOI:10.1080/21582041.2017.1400089, s. 98. – Desinformation innebär ett avsiktligt spridande av falsk eller vilseledande information.
[79] Bradshaw, S., Howard, N. P. (2019). *The Global Disinformation Order*, Global Inventory of Organised, Social Media Manipulation, University of Oxford, Oxford Internet Institute, Computational Propaganda Research Project, s. 2.
[80] Markus Arvidson är verksam universitetslektor vid Karlstads universitet, vars huvudsakliga forskningsområde utgörs av att studera bedrägerier som ett socialt fenomen.
[81] Arvidson, Markus (2007). *Den fabricerande människan*, doktorsavhandling Karlstad universitet, 2007:20, s. 16.
[82] Ibid. s. 77.

lyser gränsdragningsproblematiken som råder mellan den legala och illegala formen av bedrägeri. Denna typ av kategorisering ger upphov till att enbart formella infallsvinklar konkretiseras. Detta kan vara problematiskt då den juridiska definitionen av bedrägeribegreppet är dynamiskt på så vis att begreppet ständigt kan bli föremål för en reformering.[83] Genom att introducera sociologin erhålls ytterligare en utgångspunkt som kan bidra till att underlätta den innehållsmässiga bedömningen av bedrägerier, så att bedömningen inte alltid enbart blir avhängig den juridiska definitionen. Arvidson konstaterar således att diskussionen behöver utvidgas till att även inbegripa bedrägerier i en samhällelig kontext.[84]

Sociologin kan alltså medverka till att åskådliggöra rättstillämpningens samhälleliga effekter. Strömholm[85] tar frågan ett steg längre och ställer sig undrande till om lagstiftningens utformning hade påverkats av att, i större utsträckning än vad som i nuläget sker, influeras av den samhällsvetenskapliga forskningen. Strömholm bemöter denna problemformulering med antagandet om att inverkan från sociologin troligtvis skulle kunna påverka lagstiftningens utformning i en lukrativ bemärkelse. Om det finns ett ökat intresse av att lagstiftningen har verkningar som social funktion, vars riktlinjer ingjuter en ökad tydlighet för dess adressater, kan de kommunikationsproblem som föreligger mellan rättstillämpande myndigheter och medborgarna reduceras. Invändningen mot en sådan allmänt lättillgänglig lagstiftning som detta skulle kunna innebära kan emellertid vara till nackdel då det i praktiken kan medföra att fackterminologin försvagas. Detta kan i sin tur motarbeta den precision som är avsedd att råda inom de rättstillämpande myndigheterna.[86]

Inom den psykologiska vetenskapen innebär *manipulation* att någon, med hjälp av dold vetskap om en individs identitet, ambitioner och anspråk, på-

[83] Ibid. s. 138.
[84] Ibid. s. 141–142.
[85] Stig Strömholm är professor emeritus i civilrätt med internationell privaträtt vid Uppsala universitet.
[86] Strömholm, Stig, *Något om sociologins betydelse för juridiken*, SvJT 1970 s. 97–125.

verkar dennes åsikter, beslut eller beteende.[87] Wahlgren[88] har särskilt uppmärksammat manipulationsmetodens generella kännetecken. I dessa inryms även sådan manipulation som företas i goda syften. Wahlgren menar att det är manipulationens generella metoder som gör den intressant att studera ur ett lagstiftningsperspektiv. Då ringa uppmärksamhet riktas mot den manipulation som förekommer i lagstiftningen förblir kunskaperna om de underliggande manipulationsmetoder förhållandevis låga. Wahlgren anser således att vetskapen om metoden behöver öka för att manipulativa handlingar ska kunna identifieras och sedermera regleras i lag. [89] Till skillnad från förevarande uppsatsarbete, applicerar Wahlgren ett lagstiftningsperspektiv på det som Wahlgren benämner som *juridisk manipulation*.[90] Trots detta angreppssätt betonar Wahlgren vikten av att kunskap bör sökas inom socialpsykologin i syfte att öka rättsväsendets medvetenhet om mänskliga beteenden och attityder.[91]

1.5 Avgränsningar

Vid en första anblick kan bestämmelserna i LFH förefalla tämligen avgränsade och originella. Den position och funktion som LFH intar i det svenska rättssystemet medför emellertid att lagstiftningen anknyter till ett flertal andra rättsområden. Lagstiftningens skärningspunkt medför att bestämmelserna kan få direkta konsekvenser gentemot angränsande rättsområden. Anledningen till detta är då ett flertal av reglerna i LFH även regleras i annan lagstiftning.[92] LFH tangerar bland annat till konkurrensrätten, immaterialrätten, arbetsrätten, straffrätten, skadeståndsrätten samt tryck- och yttrandefriheten. I ett flertal situationer har LFH företräde. Som exempel kan nämnas det kon-

[87] *Nationalencyklopedin,* manipulation, <http://www.ne.se/uppslagsverk/encyklopedi/lång/manipulation>, (hämtad 2020-04-14).
[88] Peter Wahlgren är verksam professor vid Stockholms universitet och forskar bl.a. inom juridisk metod, lagstiftningslära och säkerhet.
[89] Wahlgren, Peter (2014). *Manipulation – ny strategi för skattelagstiftaren?,* Ingår i: Skattelagstiftning: att lagstifta om skatt / [ed] Anders Hultqvist, Peter Melz, Robert Påhlsson, Stockholm: Norstedts Juridik AB, 2014, s. 33–34.
[90] Med *juridisk manipulation* avser Wahlgren manipulativa inslag i det svenska rättsväsendet, bl.a. i form av dolda påverkansmedel som kan nyttjas i syfte att få medborgarna att handla på ett visst önskvärt sätt.
[91] Wahlgren 2014, s. 39.
[92] Helgesson 2000, s. 385.

kurrerande straffansvar som föreligger avseende det straffmaximum som påbjuds i såväl LFH som i brottsbalken (1962:700) (BrB). Trots att straffbestämmelserna till viss del överlappar varandra har lagstiftaren uttryckligen framhållit att LFH som huvudregel har företräde framför BrB. Undantaget är om BrB, för samma gärning, föreskriver strängare straff än LFH.[93] Förevarande uppsatsarbete avser inte behandla vare sig angränsande rättsområden till LFH eller den rådande regelkonkurrensen mellan straffbestämmelserna i LFH och BrB.

Genom åren har bestämmelserna i LFH varit föremål för åtskilliga rättsliga prövningar, vilket har resulterat i en omfattande flora av rättspraxis.[94] Efter att ha granskat ett fyrtiotal rättsfall är det påfallande att huvudfrågan i majoriteten av rättsfallen bringar klarhet i huruvida arbetstagaren har haft lovlig tillgång till den omtvistade informationen.[95] Rättspraxis tydliggör även begreppsförklaringar och juridiska tolkningsfrågor. Granskningen har emellertid inte resulterat i att jag påträffat något rättsfall där social manipulation preciseras eller placeras in i en rättslig kontext. Mot bakgrund av denna avsaknad av rättspraxis har jag således valt att inte inbegripa detaljerad redogörelse över enskilda rättsfall.

Social manipulation förekommer inom ett flertal olika vetenskapsdiscipliner.[96] Uppsatsen belyser huvudsakligen sådan social manipulation där gärningspersonen har en uppsåtlig intention att genomföra det manipulativa angreppet. Social manipulation inbegriper dels en slags traditionell och humanistisk interaktion där interaktionen sker öppet och direkt mellan gärningspersonen och offret, dels social manipulation vars interaktion fordrar tekniska

[93] SOU 2017:45, *Ny lag om företagshemligheter*, s. 67.
[94] Se bl.a. Bengtsson, Henrik, Kahn, Johan (2002). Ny juridik 4:02, *Företagshemligheter i domstolarnas praxis*, <http://kahnpedersen.se/wp-content/uploads/2017/06/Johan-Kahn-Foretagshemligheter-i-domstolarnas-praxis-–-del-I-Ny-Juridik-nr-4-2002-s.-7.pdfs.>, (hämtad 2020-04-06).; Bengtsson, Henrik, Kahn, Johan (2018). Ny juridik 3:05, *Företagshemligheter i domstolarnas praxis – del 2*, <https://www.delphi.se/uploads/2018/07/05foretagshemligheteridomstolarnaspraxisdel2henrik-bengtsson.pdf>, (hämtad 2020-04-06).
[95] Se bl.a. Svea hovrätt, dom den 20 oktober 2003, mål nr B 5221-03; NJA 2001 s. 362.
[96] Se närmre kap. 4.

hjälpmedel. Kravet på att interaktionen företas med hjälp av tekniska hjälpmedel angränsar i viss mån till datavetenskap och IT-rätt, vilket förevarande uppsat inte avser att behandla.

I den mån som social manipulation diskuteras med utgångspunkt i en traditionell och humanistisk interaktion mellan gärningspersonen och offret omnämns ett antal emotionella triggers. Kemiska ämnen som hjärnan producerar och utsöndrar – bland annat hormoner dopamin och oxytocin – gränsar till läkarvetenskapen, vilket utgör ett område som förvarande uppsats inte har för avsikt att redogöra för.

1.6 Disposition

I uppsatsens inledande kapitel (kapitel 2) ges en historisk översikt över framväxten av den nu gällande nationella lagstiftningen. Syftet är att i kronologisk ordning synliggöra ett antal utvalda händelser som har haft betydelse för LFH:s tillkomst. På motsvarande sätt åskådliggörs några av de internationella regelverk som haft inverkan på upprättandet av Europaparlamentets och rådet direktiv 2016/943 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (företagshemlighetsdirektivet). I detta kapitel belyses även direktivets påverkan på reformerandet av den svenska skyddslagstiftningen.
För enkelhetens skull bör uppsatsens fortsatta framställning förstås utifrån en indelning i två block. I det första blocket (kapitel 3) ges en redogörelse över LFH. I detta kapitel studeras primärt rättskällorna i syfte att erhålla kunskap avseende i vilken mån som LFH erbjuder ett rättsligt skydd för företagshemligheter samt hur den straffrättsliga bedömningen går till. I det andra blocket (kapitel 4) anläggs ett utomrättsligt perspektiv, vilket sker genom att introducera relevanta utomrättsliga vetenskaper. Dessa perspektiv utgörs i huvudsak av den beteendevetenskapliga inriktningen – socialpsykologi, men även delar inom datavetenskapen berörs. I syfte att enklare förmå placera in social manipulation i ett utomrättsligt sammanhang ges inledningsvis en begreppsförklaring av informationssäkerhet.

I uppsatsens avslutande kapitel (kapitel 5) genomförs uppsatsarbetets analys. Analysen består inledningsvis av en redogörelse över arbetets resultat. Avslutningsvis företas en diskussion där syftet är att resonera kring resultaten utifrån det syfte och den frågeställning som presenterades i uppsatsens inledande kapitel.[97]

[97] Se närmre kap. 1.2.

2 Historisk översikt

2.1 Introduktion

Den 1 juni 2018 trädde LFH i kraft, vilket innebar att lagen om skydd för företagshemligheter (1990:409) (FHL) upphävdes. 2018 års lagstiftningsreform tillkom på grundval av att svensk lagstiftning skulle anpassas till företagshemlighetsdirektivet som antogs 2016 och sedermera implementerades i svenska lagstiftning 2018.[98] Bestämmelser om illojal konkurrens och företagshemligheter har emellertid, såväl nationellt som internationellt, diskuterats långt innan LFH trädde i kraft. Genom att studera regleringens bakomliggande syften är ambitionen att öka förståelsen för skyddsintressets omfattning och betydelse.

2.2 Nationell inblick

I början av 1900-talet existerade det ingen svensk skyddslagstiftning för företagshemligheter. Drygt tjugo år senare tillkom lagen med vissa bestämmelser mot illojal konkurrens (1919:446). Lagens tillkomst innebar att svensk lagstiftning för första gången erhöll rättsregler om skydd för, det som vid denna tidpunkten, rubricerades som yrkeshemligheter. Bestämmelserna i 1919 års lagstiftning överfördes sedermera i oförändrat skick till lagen med vissa bestämmelser mot illojal konkurrens (1931:152) (IKL). När skyddet för yrkeshemligheter sedermera skulle genomgå en utvidgning, beslutade utredningen att införa begreppet otillbörlig konkurrens. Otillbörlig konkurrens kännetecknades av ohederliga, omoraliska och klandervärda konkurrenshandlingar.[99] Utredningens lagförslag om otillbörlig konkurrens förverkligades 1970. En utvidgning av skyddet för yrkeshemligheter realiserade emellertid inte och således fortsatte IKL att gälla som skyddslagstiftning. Drygt nio år senare tillsattes en ny utredning i syfte att reformera skyddet för, det som nu börjat benämnas som, företagshemligheter.[100] Utredningen konstaterade att skyddet

[98] Jfr 1 § 2 st. LFH.
[99] SOU 1966:71, *Otillbörlig konkurrens*, s. 317.
[100] Fahlbeck 2019, s. 23.

för företagshemligheter i IKL var otidsenligt, bland annat eftersom flertalet av bestämmelserna hade tillkommit 60 år tidigare. Till skillnad från det föregående utredningsarbetet framhölls härvid att särskilt ohederliga angrepp på företagshemlighet utgjorde en metod inom gruppen av otillbörliga konkurrenshandlingar.[101]

Under 1980-talet, uppmärksammades ett flertal händelser där omständigheterna indikerade att det rörde sig om dåvarande Sovjetunionens försök av att bedriva industrispionage gentemot svensk industri.[102] Händelserna utgjorde ett starkt intryck och den svenska regeringens ambitioner att modernisera skyddet för företagshemligheter ökade.[103] Efter att utredningen remissbehandlats och en lagrådsremiss upprättats, presenterade regeringen ett lagförslag om skydd för företagshemligheter.[104] Med anledning av att förslaget tangerade yttrandefrihetens spelrum blev förslaget kontroversiellt, vilket resulterade i en utdragen debatt. Under dessa förhållanden var det oundvikligt att inte låta lagförslaget analyseras ytterligare.[105] De synpunkter och förslag på ändringar som utarbetades redovisades sedan i lagutskottets betänkande, vilket överlämnades till riksdagen 1989.[106] Riksdagens mottagande av det nya lagförslaget återföljdes av ytterligare en fördröjning då det vid omröstningen inte uppnådde den majoritet som krävdes för ett omedelbart antagande.[107] Lagförslaget vilandeförklarades under en tidsperiod på 12 månader.[108] Ett år senare när förslaget återigen, i nästintill oförändrat skick, lades fram i riksdagen var ett antagande för handen och den 1 juli 1990 trädde FHL i kraft.[109]

Skyddslagstiftningen i FHL kom att betraktas som originellt då övriga medlemsstater i Europeiska unionen (EU) saknade ett motsvarande skydd. Vid

[101] SOU 1983:52, s. 17.
[102] Nordblom, Charlie (1984). *Industrispionage*. Stockholm: Timbro, s. 197–199.
[103] Fahlbeck 2019, s. 27.
[104] Prop. 1987/88:155, *Om skydd för företagshemligheter.*
[105] Lagutskottets kansli utarbetade en PM med beteckningen 1988/89:KU2y, *Skydd för företagshemligheter*, vari lagförslaget analyserades.
[106] Bet. 1988/89:LU30, *Skydd för företagshemligheter*.
[107] Fahlbeck 2019, s. 24.
[108] Tidigare 2 kap. 12 § 3 st. RF, numera 2 kap. 22 § RF.
[109] Protokoll 1989/90:131, *Riksdagens protokoll*.

denna tidpunkt förelåg det ingen antydan om att EU hade för avsikt att harmonisera skyddet för företagshemligheter. Diskussionen om att införa ett övergripande EU-rättsligt skydd för företagshemligheter påbörjades först senare då det första direktivförslaget lades fram i november 2013.[110] Med anledning av att området inte var harmoniserat fick FHL begränsande gränsöverskridande tillämplighet. I praktiken kunde en sådan inskränkning i skyddets tillämpbarhet medföra att företag riskerade att erhålla ett sämre skydd om angreppet mot företagshemligheten vidtogs utanför Sveriges gränser.[111]

I jämförelse med annan angränsande nationell lagstiftning ansågs den struktur som omgav FHL unik till sin karaktär. Lagstiftningens säregna struktur gav upphov till viss svårighet då användningsområdet för FHL kunde förefalla olika beroende på utgångspunkten i det enskilda fallet.[112] Trots att FHL vid en första anblick uppfattades som tämligen avskild gentemot övriga rättsområden befann sig lagstiftningen i själva verket i mitten av en skärningspunkt.[113] Skyddet för företagshemligheter tangerade inte enbart till konkurrensrätten, arbetsrätten och immaterialrättens område, utan även till den grundlagsreglerade tryck- och yttrandefriheten. 1983 års utredning framhöll i sitt betänkande betydelsen av att granska hur en presumtiv avvägning skulle te sig gentemot andra regelverk.[114] I syfte att skapa en balans mellan lagstiftningens olika skyddsintressen ansåg regeringen att det var av vikt att företa en intern avvägning. Regeringen framhöll risken med ett alltför snävt rättsligt skydd för företagshemligheter då detta skulle kunna få en negativ inverkan på den effektiva och sunda konkurrensen. Vidare framhöll att företagens vilja att investera ökar då det råder ett fritt kunskapsutbyte. Regeringens menade att investeringsviljan är signifikant för företagens tillväxt på såväl den nationella som internationella marknaden. Även arbetstagarna har ett egenintresse av att tillägna sig kunskap för att ha möjlighet och

[110] Domeij 2016, s. 77.
[111] Fahlbeck 2019, s. 39–41.
[112] Wainikka, Christina (2010). *Företagshemligheter: en introduktion*. 1. uppl. Lund: Studentlitteratur, s. 13.
[113] Se närmre kap. 1.5.
[114] SOU 1983:52, s. 75–76.

tillåtelse att nyttja kunskapen i den befintliga som i eventuella framtida anställningar.[115]

Genom ikraftträdandet av FHL skapades således ett modernt och effektivt skydd för företagshemligheter som i princip varit obefintligt i IKL. Av betydelse var särskilt de effektiva straffbestämmelser som introducerades i och med FHL. Lagstiftningens primära syfte var att skydda såväl materiella som immateriella tillgångar mot den gärningsperson som olovligen utnyttjade dessa.[116] Flertalet av de illegala metoder som redan kriminaliserats i BrB omfattade emellertid inte alla förfaranden som inrymdes i *företagsspionerі*. Som exempel nämner regeringen särskilt fotografering och kopiering av företagshemlighet.[117] Regeringen refererar även till den fältundersökning som utredningen företog i samband med framställningen av 1983 års betänkande.[118] Undersökningens resultat gjorde det möjligt att konstatera att de företag som påstod sig ha blivit utsatta för företagsspionerі var betydande till antalet. I enlighet med utredningens remissvar tillkom emellertid en uppskattning om att mörkertalet var så pass stort att endast ett fåtal angrepp på företagshemligheter de facto klaras upp. Oavsett vilken metod som angriparen har vidtagit för att tillgripa företagshemligheten ligger det klandervärda i själva förvärvandet av denna. En individ som inte har haft tillåtelse att bereda sig tillgång till en företagshemlighet skulle således, på denna grund, kunna straffas. Införandet av en särskild straffbestämmelse om företagsspionerі skulle emellertid inbegripa redan straffbelagda handlingar såsom bedrägeri och stöld. Trots detta ansåg regeringen att det var motiverat att införa en separat lag i syfte att få fler situationer att omfattas av olovligt beredande av tillgång till företagshemlighet.[119]

[115] Prop. 1987/88:155, s. 8–9.
[116] Ibid. s. 8–9.
[117] Ibid. s. 14.
[118] Se närmre kap. 1.4.1.
[119] Prop. 1987/88:155, s. 13–15.

2.3 Internationell utblick

Frihandelsavtalet med benämningen *North American Free Trade Agreement* (NAFTA) är bindande för parterna Kanada, USA och Mexico. Avtalet trädde ikraft 1994 och skildras som dåtidens mest omfattande frihandelsavtal som framförhandlats.[120] Avtalet syftar till att förenkla den gränsöverskridande handeln genom att undanröja handelshinder och på så vis öka den ekonomiska samordningen mellan länderna. Målsättningen är även att främja rättvis konkurrens, stärka immaterialrättsskyddet samt öka möjligheterna till investering.[121] I jämförelse med världshandelsorganisationen, *World Trade Organization* (WTO), som också syftar till att främja internationell handel, beskrivs NAFTA som mer vidsträckt till sitt innehåll.[122]

I sammanhanget är det relevant att uppmärksamma det sentida framtagna nordamerikanska frihandelsavtalet som ska komma att ersätta NAFTA och således tillämpas mellan NAFTA:s nuvarande parter.[123] Det omförhandlade frihandelsavtalet, som benämns United States – Mexico – Canada Agreement (USMCA), antogs den 30 november 2018 på initiativ av USA.[124] Avtalet syftar huvudsakligen till att modernisera NAFTA och minska amerikansk import.[125] Den exakta tidpunkten då USMCA beräknas trädda i kraft är i skrivande stund oklart.[126] För att avtalet ska bli tillämpbart krävs det att

[120] Kommerskollegium (2017). Omförhandling av NAFTA och svenska företag i Mexico, <https://www.kommers.se/Documents/dokumentarkiv/publikationer/2017/publ-omforhandling-av-nafta.pdf>, (hämtad 2020-01-28), s. 1.
[121] Ibid. s. 15.
[122] *Nationalencyklopedin, NAFTA,* <http://www.ne.se/uppslagsverk/encyklopedi/lång/nafta>, (hämtad 2020-01-29).
[123] Kommerskollegium (2019a) National Board of Trade Sweden, *Handelsrelationen mellan USA, Kanada och Mexico – En jämförande analys mellan USMCA och Nafta, CPTPP respektive EU:s frihandelsavtal*, <https://www.kommers.se/Documents/dokumentarkiv/publikationer/2019/Publ_Analys-av-USMCA.pdf>, (hämtad 2020-01-29), s. 1.
[124] Office of the United States Trade Representative (2018). *United States – Mexico – Canada Agreement*, <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>, (hämtad 2020-01-29).
[125] NE*, NAFTA*.
[126] Investopedia (2020). *USMCA*, <https://www.investopedia.com/usmca-4582387>, (hämtad 2020-01-29).

samtliga parter till NAFTA ratificerar avtalet, vilket hittills endast har fullgjorts av USA och Mexico.[127]

Företagshemlighetsdirektivet baseras till övervägande del på den internationella överenskommelsen *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS-avtalet). Innehållet i TRIPS-avtalet bygger i stor utsträckning på NAFTA.[128] TRIPS-avtalet trädde i kraft den 1 januari 1995 och har sedan dess utgjort bindande bestämmelser för alla de länder som är medlemmar i WTO. Majoriteten av bestämmelserna i TRIPS-avtalet härstammar från äldre, multilaterala immaterialrättstraktat och inbegriper bland annat bestämmelser rörande patent, upphovsrätt, varumärken och företagshemligheter. TRIPS-avtalets bestämmelser utgör minimiregler för medlemsstaternas immaterialrättsliga skyddslagstiftning. Medlemsstaterna har emellertid tillåtelse att i nationell lagstiftning befästa skyddet ytterligare genom att erbjuda ett mer generöst skydd än vad TRIPS-avtalet föreskriver.[129]

2.4 Förslag till EU-direktiv

I november 2013 presenterade Europeiska kommissionen (EU-kommissionen) ett första förslag gällande harmonisering av ett rättsligt skydd för företagshemligheter. Förslaget motiverades främst utifrån en önskan om att förbättra förutsättningarna för att bedriva innovativ affärsverksamhet. Detta skulle bland annat ske genom att skapa en bättre utgångspunkt för företagens forsknings- och utvecklingsarbeten.[130]

---

[127] Dagens industri (2019). *Mexico godkänner ”nya Nafta”*, <https://www.di.se/live/mexiko-godkanner-handelsavtalet-usmca/>, (hämtad 2020-01-29).; The Wall Street Journal (2020). Canada Begins USMCA Ratification Process That Won´t Necessarily Be Smooth Sailing, <https://www.wsj.com/articles/canada-begins-nafta-ratification-process-that-wont-necessarily-be-smooth-sailing-11580152748>, (hämtad 2020-01-30).
[128] Fahlbeck 2019, s. 37.
[129] Kommerskollegium (2019b) National Board of Trade Sweden, *TRIPS-avtalet i WTO,* <https://www.kommers.se/verksamhetsomraden/Handelsfragor/Immaterialratt/Utanfor-EU/TRIPS-avtalet-i-WTO/>, (hämtad 2020-01-27).
[130] Domeij 2016, s. 79.

EU-kommissionens direktivförslag baserades ursprungligen på resultaten av två studier gjorda av två globala advokatbyråer – Hogan Lovells rapport från 2012[131] och Baker & McKenzies rapport från 2013.[132] Till grund låg även en konferens som anordnades av EU-kommissionen i juni 2012 samt en internetbaserad opinionsundersökning som pågick mellan åren 2012–2013. Rapporternas utfall vittnar om en omfattande diskrepans beträffande medlemsstaternas olika nivåer av rättsliga skydd för företagshemligheter. Skillnaderna avsåg huvudsakligen avsaknaden av enhetliga begreppsdefinitioner och svårigheten med att förstå i vilket eller vilka regelsystem som företagshemligheter ska inplaceras.[133]

Av direktivförslaget framgick det att trots att den kunskap som utvecklats till följd av skapandeprocessen i en verksamhet är ekonomiskt värdefull, omfattas den allt som oftast inte av något immaterialrättsligt skydd. I syfte att säkra kunskapstillgångar tillägnar sig företagen konfidentiell information, vilket innebär att företagshemligheter skyddas. Genom att erbjuda ett rättsligt skydd för företagshemligheter menade EU-kommissionen att företagen skulle kunna fortsätta att investera och konkurrera avseende innovation, utan att kunskapen utnyttjades i rättsstridiga syften. EU-kommissionen påpekade även hur kunskaps- och informationsutveckling, bland annat på grund av den ökade globaliseringen, har en betydande inverkan på EU:s ekonomi. De skillnader som föreligger mellan medlemsstaternas rättsliga skydd för företagshemligheter medför minskade möjligheter avseende att förhindra angrepp mot företagens utvecklade kunskaper. Detta är missgynnande för det gränsöverskridande forsknings- och utvecklingsarbetet, eftersom det motarbetar företagens incitament att konkurrera.[134]

[131] Hogan Lovells (2012) International, Study on Trade Secrets and Parasitic Copying (Look-alikes), MARKT/2010/20/D: Report on Trade Secrets for the European Commission.
[132] Baker & McKenzie (2013). Study on Trade Secrets and Confidential Business Information in the Internal Market, MARKT/2011/128/D.
[133] SOU 2017:45, s. 79.
[134] Europeiska kommissionen (2013). *COM (2013) 813 final*,<https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52013PC0813&from=EN >, (hämtad 2020-01-30), s. 2–3.

2.4.1 Syfte och disposition

Den 14 april 2016 röstade Europaparlamentet igenom direktivförslaget med överhängande majoritet.[135] Direktivet antogs sedermera den 8 juni 2016 med krav på införlivande i medlemsstaternas nationella lagstiftningar senast den 9 juni 2018.[136] Företagshemlighetsdirektivets primära syfte är att, i likhet med EU-kommissionens direktivförslag, förbättra möjligheterna för innovation och överföringen av kunskap på EU:s inre marknad och stärka konkurrenskraften mellan företag.[137] En harmoniserad EU-rättslig reglering på området ökar företagens incitament att bedriva ett innovativt och gränsöverskridande arbete, vilket gynnar den dynamiska utvecklingskurvan för ekonomisk tillväxt och sysselsättning på EU:s inre marknad.[138] Före 2016 existerade det inga övergripande EU-rättsliga bestämmelser om skydd för företagshemligheter.[139] En betydelsefull konsekvens av denna tidens obefintliga harmonisering var att information som omfattades av en medlemsstats skyddslagstiftningen kunde vara exkluderad från den motsvarande lagstiftningen i en annan medlemsstat. Utfallet resulterade i en påtaglig skillnad i utformningen av medlemsstaternas nationella straffbarhetsbestämmelser.[140]

Av företagshemlighetsdirektivet framgår det att TRIPS-avtalet erbjuder ett visst skydd mot att företagshemligheter olovligen anskaffas, utnyttjas eller röjs.[141] I TRIPS-avtalet framgår skyddet för företagshemligheter i artikel 39.2. Skyddet beskrivs som det första explicita internationella erkännandet av företagens tillgångar och dess ofrånkomliga behövlighet av ett rättsligt skydd.[142] I direktivet framhålls att bestämmelserna i TRIPS-avtalet utgör internationella fastställda normer och att dessa är bindande för samtliga medlemsstater.[143] I ett av direktivets inledande skäl framgår det emellertid att

[135] Domeij 2016, s. 80.
[136] Företagshemlighetsdirektivet, artikel 19.1.
[137] Prop. 2017/18:200, *En ny lag om företagshemligheter*, s. 21.
[138] Företagshemlighetsdirektivet, skäl 3 och 4.
[139] Prop. 2017/18:200, s. 21.
[140] Wainikka 2010, s. 14.
[141] Företagshemlighetsdirektivet, skäl 4.
[142] Domeij 2016, s. 78.
[143] Rådets beslut 94/800/EG av den 22 december 1994 om ingående, på Europeiska gemenskapens vägnar – vad beträffar frågor som omfattas av dess behörighet – av de avtal som är resultatet av de multilaterala förhandlingarna i Uruguayrundan (1986–1994).

TRIPS-avtalets existens inte är tillräckligt för att ett enhetlig skydd ska anses föreligga. I direktivets inledande skäl uppmärksammas ett antal illegala metoder som företas i syfte att angripa företagshemligheter i innovativa verksamheter. Som exempel nämns underlåtenhet att beakta konfidentiell information, stöld och företagsspionerі. Vikten av att vidta internationella insatser mot denna sortens vilseledande metoder betonas särskilt.[144]

Enhetliga begreppsdefinitioner går att finna i företagshemlighetsdirektivet artikel 2. Som exempel kan nämnas definitionen av begreppet *företagshemlighet*. Företagshemligheter avgränsas här till konfidentiell information som har ett kommersiellt värde. Informationsinnehavaren ska även ha vidtagit rimliga åtgärder för att bibehålla konfidentialiteten. Begreppet omfattar inte sådan kunskap som arbetstagare får genom utövandet av ordinär yrkesutövning, information som är välkänd eller lättillgänglig inom grupper som har för vana att arbeta med en viss typ av uppgifter samt sådan information som bedöms som obetydlig.[145] Andra begrepp som bedömts som nödvändiga att förse med en enhetlig definition är *innehavare* av en företagshemlighet, *intrångsgörare* samt *intrångsgörande varor*.[146] Identifikationen av de omständigheter som rättsligt utgör legal respektive illegal anskaffning, utnyttjande och röjande av företagshemlighet återfinns direktivets tredje och fjärde artikel.

2.4.2 Harmonisering i svensk rätt

Tiden efter företagshemlighetsdirektivets antagande förelåg det från svenskt hål, ytterst små förväntningar avseende direktivets inverkan på den befintliga svenska lagstiftningen. Konsekvenserna av direktivets ikraftträdande bedömdes med andra ord inte medföra någon större märkbar effekt på bestämmelserna i FHL. Denna uppfattningen kan ha grundats på att FHL redan ansågs inneha ett starkt skydd för företagshemligheter.[147]

[144] Företagshemlighetsdirektivet, skäl 4, 6 och 14–15.
[145] Ibid.
[146] Jfr företagshemlighetsdirektivet artikel 2.2–2.4.
[147] Fahlbeck 2019, s. 39.

Genom studiet av förarbeten ges intrycket av att FHL varit en förebild i arbetet med att framställa LFH.[148] De resonemang som presenterades av 2016 års utredning menade att införandet av LFH huvudsakligen syftade till att befästa det redan befintliga regelverket i FHL. Detta skulle ske genom att fortsätta tillämpa den terminologi och systematik som omgav FHL.[149] Utredningen anförde att det visserligen fordrades ett antal lagändringar i syfte att inkorporera direktivets bestämmelser, men att de övriga effekterna av direktivets ikraftträdande inte skulle vara särskilt omfattande.[150] Utredningen fick delvis medhåll från regeringen. Regeringen tillade emellertid att de föreslagna ändringarna var omfattande och att dessa inte på ett effektivt sätt skulle kunna inkorporeras i FHL. Regeringen fann det således lämpligare att anta en helt ny lag. Den nya lagstiftningen skulle syfta till att förstärka skyddet, vilket var nödvändigt för att understödja företagens gränsöverskridande verksamhet och därigenom gynna företagens konkurrenskraft.[151]

Utredningens bedömning avseende reformbehovets omfattning kom alltså i efterhand att förefalla som tämligen felaktigt. Flertalet av de nyheter som infördes i LFH utgör närmre bestämt ett intyg på att reformbehovets omfattning var något större än vad utredningen väntat sig.[152] Genom införandet av 2018 års LFH ansågs emellertid Sverige delvis ha implementerat företagshemlighetsdirektivet.[153]

[148] Prop. 2017/18:200, s. 130.
[149] Ibid. s. 23–24.
[150] SOU 2017:45, s. 381.
[151] Prop. 2017/18:200, s. 21.
[152] Fahlbeck 2019, s. 40–41.
[153] Se 1 § 2 st. LFH.

3 Lag om företagshemligheter

3.1 Introduktion

I syfte att få förståelse för vilket skydd som LFH faktiskt erbjuder och när ett sådant skydd inträder är det nödvändigt att inledningsvis precisera två centrala begrepp som lagen uppställer – *företagshemlighet* och *information*. Dessa begrepp står i och för sig i allra högsta grad i nära förbindelse med varandra, men ett särskiljande av dem är likväl väsentligt för att kärnan i skyddet ska konkretiseras. Särskiljandet är även av vikt för att klargöra den gränsdragningsproblematik som råder avseende huruvida viss typ av information i det enskilda fallet utgör en företagshemlighet i lagens mening.[154]

3.1.1 Företagshemligheter

Termen *företagshemlighet* utgör ett samlingsbegrepp för det objekt som LFH avser att skydda.[155] Andra motsvarande begrepp, som exempelvis *yrkeshemlighet* eller *affärshemlighet*, kan emellertid förekomma i den juridiska litteraturen.[156] Begreppet företagshemlighet är ursprungligen inspirerat av företagshemlighetsdirektivet där skyddsobjektet betecknas *trade secrets*.[157] Direktivets skyddsobjekt grundar sig i sin tur på den definition som anges i TRIPS-avtalet.[158] Fahlbeck menar att beteckningen *företagshemlighet* är vilseledande, eftersom hemligheter i såväl näringsverksamhet som icke-kommersiella forskningsinstitutioner omfattas av skyddet. Som alternativ föreslås begreppen *affärshemlighet* eller *näringshemlighet*. Fahlbeck framhåller emellertid att det kan vara besvärligt att ersätta ett allmänt vedertaget begrepp.[159]

[154] Prop. 1987/88:155, s. 34; Wainikka 2010, s. 20.
[155] Fahlbeck 2019, s. 394.
[156] Ibid. s. 385–387; Helgesson 2000, s. 28.
[157] Företagshemlighetsdirektivet, skäl 1.
[158] Fahlbeck 2019, s. 396–397.
[159] Ibid. s. 394.

Det nära sambandet som råder mellan begreppen *företagshemlighet* och *information* går att finna i inledningen till 2 § LFH där det uttryckligen görs gällande att begreppet *företagshemlighet* i själva verket avser *information*. I samma paragraf uppräknas sedermera fyra punkter som alla utgör fundamentala komponenter för att en viss typ av information ska anses utgöra en företagshemlighet i lagens mening.[160] Lagstiftaren har haft för avsikt att tilldela begreppet *information* en vidsträckt innebörd. Informationen kan således inrymma olika typer av uppgifter oberoende av dess karaktär. Vidare uppställs det inget krav på att informationen på förhand ska uppnå en bestämd nivå av trovärdighet eller klargörande.[161]

Begreppet *information* beskrivs utgöra en objektiv samlingsbeteckning för vitt skilda typer av uppgifter och kunskaper och något krav avseende informationens originalitet förekommer inte.[162] Såväl Fahlbeck som Wainikka[163] har delat in information efter dess karaktär – kommersiell, administrativ och teknisk information, varav samtliga informationstyper kan utgöra en företagshemlighet.[164] Indelningen får särskilt betydelse vid fastställandet av om en viss typ av information kan omfattas av det rättsliga skyddet. Det avgörande blir i sådana fall huruvida informationen kan sammankopplas till en näringsidkares affärs- eller driftförhållanden eller en forskningsinstitutions verksamhet. Gränsdragningen mellan de olika informationstyperna kan emellertid tyckas diffus.[165] Till begreppet *information* hör även ”negativ” information, vilket avser information där kunskapen består i att något exempelvis *inte* föreligger eller *inte* fungerar.[166]

I syfte att informationsinnehavaren ska förmå företa lämpliga säkerhetsåtgärder gentemot verksamhetens företagshemligheter kan även en intern klassificering av information förekomma. Klassificeringen kan företas utifrån

[160] Fahlbeck 2019, s. 387–388 och 394; 2 § 2 st. p. 1–4 LFH.
[161] Aspegren 2018, kommentar till 2 § JUNO.
[162] Fahlbeck 2019, s. 383–384.
[163] Christina Wainikka (tidigare Helgesson) är disputerad jurist och är för närvarande bl.a. policyexpert för immaterialrätt på Svenskt Näringsliv.
[164] Fahlbeck 2019, s. 384; Helgesson 2000, s. 91–93.
[165] Wainikka 2010, s. 33.
[166] Fahlbeck 2019, s. 383.

graden av konfidentialitet för den information som informationsinnehavaren avser skyddsvärd.[167]

Synonymt med *information* är begreppet *kunskap*. I sitt betänkande välkomnade 1983 års utredning kunskapsbegreppet och tillade att *kunskap*, i större utsträckning än begreppen *information* och *uppgift*, inbegriper immateriell kunskap.[168] Sandgren har beskrivit begreppsskillnaden genom att framställa *kunskap* som nära förbunden till människan, medan *information* avser sådant kunnande som kan avskiljas från människan.[169] Regeringen anförde i den efterföljande propositionen att kunskapsbegreppet kan försvåra förståelsen av lagstiftningens skyddsobjekt. Med anledning av att skyddsobjektet även fortsättningsvis avsågs inneha en vidsträckt innebörd, ansåg regeringen att det vore lämpligare att använda begreppet *information*.[170]

För den ifrågavarande informationen föreskrivs inget formkrav. Informationen kan exempelvis bestå av väl vedertagen dokumentation eller av en arbetstagares kunskaper som denne erhållits under anställningens gång.[171] Ett rättsligt begrepp som har en vidsträckt innebörd och saknar formkrav kan emellertid orsaka svårigheter vid rättstillämpningen. I detta avseendet åsyftas primärt den gränsdragningsproblematik som kan uppstå när en viss typ av information, som informationsinnehavaren anser utgör en företagshemlighet, inte har dokumenterats. I samband med att problematiken diskuteras framhåller ofta lagstiftaren en önskan om att värna om balansen mellan å ena sidan den rättsliga möjligheten för företag och forskningsinstitutioner att vidta skyddsåtgärder för sina företagshemligheter. Å andra sidan ska de arbetstagare som avslutar sin anställning för att påbörja en ny tjänst hos en konkurrerande verksamhet ha utrymme att vidta ett sådant skifte, utan att alltför stora hinder uppställs. I dessa situationer kan arbetstagaren, vid avsaknad av dokumentation av den information som arbetsgivaren avser att skydda, hävda

[167] Fahlbeck 2019, s. 385.
[168] SOU 1983:52, s. 371.
[169] Sandgren 1995, s. 23–24.
[170] Prop. 1987/88:155, s. 12.
[171] Ibid. s. 34.

att informationen är av personlig art.[172] Denna typ av information korrelerar normalt sett inte med sådant som uppbär företagets originalitet. Informationen är bunden till individen då den inte genom direktiv från arbetsgivaren kan överföras till någon annan.[173] Motivet bakom ett sådant påstående kan grunda sig i att arbetstagarens subjektiva yrkesförmåga och erfarenheter inte utgör företagshemligheter i lagens mening.[174] Gränsdragningen underlättas inte heller av det faktum att flertalet företagshemligheter i allmänhet består av arbetstagares kunskaper och innovationer.[175]

Bedömningen av huruvida en viss typ av information utgör en företagshemlighet fastställs inte utifrån informationens art eller egenskap. Trots att domstolarna frekvent använder en terminologi som kan insinuera att det förekommer information som *till sin art* utgör en företagshemlighet, måste bedömningen snarare utgå från de unika omständigheterna i det enskilda fallet. Bedömningen ska således primärt koncentreras till om informationsinnehavaren påstår att informationen utgör en företagshemlighet.[176] Det utslagsgivande i bedömningen är om informationsinnehavaren, som åberopar att informationen utgör en företagshemlighet, de facto har någon form av kontroll över den aktuella informationen.[177]

3.1.2 Affärs- eller driftförhållanden i en näringsidkares rörelse

Kravet på att informationen ska röra affärs- eller driftförhållanden i en näringsidkares rörelse har varit lagstadgat sedan tillkomsten av 1990 års FHL. Begreppet *affärs- eller driftförhållanden* förekommer även i sekretessbestämmelserna i offentlighets- och sekretesslagen (2009:400) (OSL) där termen är väletablerad.[178] För att denna typen av information ska omfattas av

[172] Wainikka 2010, s. 33.
[173] Aspegren 2018, kommentar till 2 § JUNO.
[174] Wainikka 2010, s. 33.
[175] Fahlbeck 2019, s. 383.
[176] Ibid. s. 388.
[177] Wainikka, 2010, s. 20.
[178] Jfr 36 kap. 2 § OSL; Prop. 2017/18:200, s. 100.

lagstiftningens skydd fordras ett samband mellan informationen och företagets sätt att bedriva verksamheten.[179] I närmre bemärkelse avses med begreppet affärs- eller driftförhållanden förvärv, överlåtelse, upplåtelser eller användning av egendom och tjänster.[180] Utöver kommersiella uppgifter avseende enskilda handelstransaktioner inrymmer begreppet även planläggning och analysering av den rådande marknaden i syfte att prissätta företagets varor eller tjänster samt utforma reklam.[181] Begreppet *näringsidkare* har en vidsträckt innebörd. Begreppet inbegriper såväl fysiska som juridiska personer som i sitt yrke bedriver en verksamhet som är av ekonomisk art.[182] Det uppställs inget krav på att verksamheten ska ha som målsättning att generera vinst eller utövas under privat eller offentlig ledning.[183] En gräns dras emellertid gentemot sådana delar i en offentlig näringsverksamhet där arbetet genomförs som ett led i offentlig förvaltning och där ingåendet av privaträttsliga avtal är obefintligt eller förekommer sällan. På motsvarande sätt som begreppet *affärs- eller driftförhållanden* är begreppet *näringsidkare* en term som repetitivt tillämpas inom andra rättsområden. Oberoende av företagets storlek föreligger ett krav på att verksamheten ska bedrivas yrkesmässigt.[184]

3.1.3 Icke-kommersiella forskningsinstitutioner

Sedan ikraftträdandet av LFH har skyddet för företagshemligheter utvidgats till att även omfatta information som förefinns hos icke-kommersiella forskningsinstitutioner.[185] Denna utvidgning var i princip en direkt inkorporering av de inledande skälen som föreskrivs i företagshemlighetsdirektivet.[186] Med forskningsinstitutioner åsyftas sådana verksamheter där forskning bedrivs under institutionaliserade former.[187] De forskningsinstitutioner som har information som omfattas av det rättsliga skyddet i LFH bedöms ofta vara näringsidkare i lagens mening.[188] Med *icke-kommersiella*

[179] Wainikka 2010, s. 36.
[180] Prop. 2017/18:200, s. 100.
[181] Aspegren 2018, kommentar till 2 § JUNO.
[182] Wainikka 2010, s. 39.
[183] Domeij 2016, s. 93.
[184] Fahlbeck 2019, s. 398–399.
[185] Prop. 2017/18:200, s. 130.
[186] Jfr företagshemlighetsdirektivet, skäl 1; Fahlbeck 2019, s. 406.
[187] Aspegren 2018, kommentar till 2 § JUNO.
[188] Prop. 2017/18:200, s. 137.

forskningsinstitutioner avses sådana institutioner, vars resultat inte har för avsikt att kommersialiseras. I begreppet inryms även sådana forskningsinstitutioner som, trots avsaknaden av strävan att kommersialisera sin upptäckt, likväl utgör ett kommersiellt värde. På motsvarande sätt som för företag kan forskningsinstitutioner sträva efter att hemlighålla vidtagna kunskapsinvesteringar samt ha en avsikt att överföra institutionens kunskap till andra institutioner eller företag.[189] I begreppet *forskningsinstitution* inryms såväl statliga universitet som statligt- och privatägda forskningsinstitutioner. Gränsen för vad som inom en forskningsinstitution får betraktas som en företagshemlighet dras vid de forskningsbedrivande myndigheter där resultatet av forskningen utgör publik information.[190] Till följd av att skyddsområdet utvidgades till att även omfatta konfidentiell information som finns hos forskningsinstitutioner, vidgades tillika det straffbara området.[191]

3.1.4 Hemlighållandet av information och aktivitetskrav

Den information som innehavaren avser hemlighålla får inte vara *allmänt känd* eller *lättillgänglig*.[192] Endast en begränsad grupp av individer får ha vetskap om informationen, vilket medför ett absolut förbud mot att utnyttja eller sprida informationen.[193] Information som bedöms vara *allmänt känd* kan emellertid omfattas av lagstiftningens skydd, såvida den upptagas i någon form av sammanställning.[194] Under sådana förhållanden är det sammanställningen som betraktas som det skyddsvärda objektet. I jämförelse med det obefintliga kravet på informationens originalitet för att kunna bedömas som information i rättslig mening, uppställs härvid ett krav på att sammanställningen ska uppnå en viss nivå av originalitet.[195] Den sammanställda informationen får därutöver inte var *lättillgänglig*. Trots att begreppet är

[189] Ibid. s. 27–28.
[190] Aspegren 2018, kommentar till 2 § JUNO.
[191] Prop. 2017/18:200, s. 121.
[192] 2 § 2 st. p. 2 LFH.
[193] Aspegren 2018, kommentar till 2 § JUNO.
[194] Fahlbeck 2019, s. 418.
[195] Se närmre kap. 3.1.1.

tämligen svårdefinierat, fastslår Fahlbeck att det inte ska fordras en särskilt komplicerad metod för att informationen ska förmås uppfattas.[196]

Det uppställs inte något krav på att innehavaren ska framhålla några särskilda skäl för att hemlighållandet av informationen ska ges rättsligt skydd.[197] Det som fordras är emellertid att informationsinnehavaren har vidtagit *rimliga åtgärder* för att ett hemlighållande ska vara för handen.[198] Hemlighetsrekvisitet består utav tre komponenter – tidsfaktor, personkrets och aktivitet. Under förutsättning att samtliga rekvisit i 2 § LFH är infriade föreligger ingen tidsbegränsning i det skydd som omger företagshemligheten. Utgångspunkten är att det är informationsinnehavaren som avgör vilken information som ska hemlighållas.[199] Informationsinnehavaren måste ha vidtagit någon form av aktivitet, vilket grundar sig i att innehavaren måste ha en inneboende vilja av att ett hemlighållande ska råda. Aktivitetskravet uppställer inget krav på att den vidtagna åtgärden måste uppnå en viss skyddsnivå. Kravet på aktivitet kan exempelvis anses uppfyllt om informationsinnehavaren utarbetar och tillkännager instruktioner, i vilka det tydliggörs hur hanteringen av konfidentiella uppgifter ska ske på arbetsplatsen.[200] Storleken på den personkrets som informationsinnehavaren väljer att utlämna informationen till, tillåts variera beroende på verksamheten utformning.[201]

Fahlbeck ställer sig frågande till om det enbart är det faktum att informationsinnehavaren hemlighåller viss information som medför att det föreligger en presumtion att informationen ska betraktas som en företagshemlighet i lagens mening. Fahlbeck besvarar frågan nekande och menar att en sådan presumtion sannolikt skulle resultera i att hemlighetsrekvisitet tilldelades en företrädesrätt gentemot bestämmelsens övriga rekvisit, vilket verken förarbetena eller lagstiftningens intresseavvägningar propagerar för.[202] Bedömningen

[196] Fahlbeck 2019, s. 419.
[197] Ibid. s. 383–384.
[198] 2 § 2 st. p. 3 LFH.
[199] Fahlbeck 2019, s. 420–421.
[200] Aspegren 2018, kommentar till 2 § JUNO.
[201] Fahlbeck 2019, s. 422–424.
[202] Ibid. s. 420–421.

avseende huruvida informationsinnehavaren vidtagit rimliga åtgärder ska alltid göras med utgångspunkt i informationens karaktär och omständigheterna i det enskilda fallet.[203]

Den information som informationsinnehavaren väljer att hemlighålla grundar sig som regel på dennes intresse av att inte gå miste om informationens kommersiella värde. Om emellertid innehavaren skulle förlora ett sådant värde kan verksamheten anse sig lida ekonomisk eller icke-ekonomisk skada.[204] Informationen som röjs måste, för att åtnjuta rättsligt skydd, ha betydelse för företagets förmåga att konkurrera på marknaden. Denna situationen föreligger i de fall där ett röjande av informationen får negativ inverkan på verksamhetens konkurrensförmåga.[205] Oberoende av i vilken utsträckning som informationsinnehavaren använder den hemliga informationen, kan informationen skyddas om lagstiftningens övriga rekvisit är uppfyllda.[206] Skadan behöver inte nödvändigtvis uppstå då informationen röjs. Det är snarare röjandets karaktär som är av väsentlig betydelse för att skadan ska förorsakas. Detta är särskilt relevant för de forskningsinstitutioner som inte, i samma utsträckning som företag, bedriver marknadskonkurrerande verksamhet.[207]

3.1.5 Behöriga och obehöriga angrepp

Information som rör *misstanke om brott* eller *annat allvarligt missförhållande* kan inte åtnjuta skydd som företagshemlighet.[208] Ett sådant avslöjande medför inte att det föreligger någon *skada* i rättslig bemärkelse.[209] Ett annat begrepp som i sammanhanget bör uppmärksammas är *obehöriga angrepp*, vilket utgör ett ofrånkomligt krav om det rättsliga skyddet ska inträda.[210] Bestämmelsen om *obehöriga angrepp* grundar sig på den intresseavvägning som, i varje enskilt fall, ska företas då skyddet för företags-

[203] Prop. 2017/18:200, s. 64.
[204] Fahlbeck 2019, s. 444.
[205] Se 2 § 2 st. p. 4 LFH; Prop. 2017/18:200, s. 139.
[206] Fahlbeck 2019, s. 448–449.
[207] Prop. 2017/18:200, s. 139.
[208] Se 2 § 3 st. LFH.
[209] Aspegren 2018, kommentar till 2 § JUNO.
[210] 4 § 1 st. LFH.

hemligheter bedöms vara tillämpligt.[211] Fahlbeck hänvisar i denna del till Lagrådets yttrande, av vilket det framgår att lagstiftningens bestämmelser i viss mån kan överlappa varandra.[212] Lagrådets förslag om att en utav de två bestämmelserna avseende *brott eller andra allvarliga missförhållanden* skulle uteslutas i LFH var emellertid inte ett förslag som infriades.[213] Bestämmelsen i 4 § LFH utgör emellertid ett tillägg till 2 § LFH och paragraferna ska således studeras gemensamt.[214] Fahlbeck understryker att 4 § LFH innehar status som generalklausul. Detta innebär att den intresseavvägning som rättstillämparen ska företa i varje enskilt fall kan resultera i en rik flora av rättspraxis avseende situationer där röjandet är behörigt.[215]

Ett annat begrepp som i sammanhanget är av vikt att definiera är *angrepp* på företagshemlighet.[216] Termen *angrepp* utgör ett samlingsbegrepp för de i lagstiftningen uppräknade handlingarna som en gärningsperson kan företa mot innehavaren av företagshemlighet, utan att denne avgett sitt samtycke.[217] Ett angrepp kan ske genom att någon *bereder sig tillgång till*, *tillägnar sig* eller *på annat sätt anskaffar, utnyttjar eller röjer* en företagshemlighet.[218] Med begreppet *bereda sig tillgång till* avses samtliga tillvägagångssätt som enligt 26 § LFH är straffbara som företagsspionerі. Detta innebär att anskaffandet måste bestå av att gärningspersonen anskaffar information som denne inte redan förfogar över. Inkluderat i begreppet är även ett aktivitetskrav som åvilar gärningspersonen. Aktivitetskravet innebär att gärningspersonen inte, på ett otillåtet tillvägagångssätt, kan anses bereda sig tillgång till information som kommer till dennes kännedom av en ren tillfällighet.[219]

En relativt nytillkommen angreppsform som infördes i samband med antagandet av 2018 års LFH och som fick särskild uppmärksamhet var uttrycket

[211] Aspegren, Jacob, lag om företagshemligheter (2018:558), kommentar till 4 § JUNO.
[212] Prop. 2017/18:200, s. 240.
[213] Fahlbeck 2019, s. 458.
[214] Ibid. s. 533.
[215] Ibid. s. 516.
[216] Jfr 3 § 1 st. LFH.
[217] Fahlbeck 2019, s. 474.
[218] 3 § 2 st. p. 1–3 LFH.
[219] Aspegren, Jacob, lag om företagshemligheter (2018:558), kommentar till 3 § JUNO.

tillägnar sig. Begreppet *tillägnande* är, i jämförelse med begreppet *bereda sig tillgång till*, vidsträckt till sin innebörd. Begreppet *tillägnar sig* inrymmer även de situationer då gärningspersonen, med något som denne redan innehar, gör till sitt eget. Den vanligaste formen av tillägnande är olovlig kopiering.[220] I jämförelse med 1990 års FHL var den första tillämpbara angreppsformen sådana omständigheter som omfattades av begreppet *utnyttjande*.[221] Termen *utnyttjar* finns emellertid fortfarande kvar i LFH.[222] Begreppet *utnyttjar* innebär att gärningspersonen i den egna verksamheten praktiskt använder sig av informationen. Det föreligger inget krav på att verksamheten ska gå med vinst, men det krävs att utnyttjandet är kommersiellt.[223] I samband med införandet av begreppet *tillägnande* förstärktes skyddet för företagshemligheter avsevärt. Med anledning av att *tillägnande* befinner sig före *utnyttjande* i händelsekedjan uppkom en ökad möjlighet att tidigarelägga olika skyddsåtgärder.[224]

I de fall där gärningspersonen avslöjar företagshemligheten för någon annan föreligger ett *röjande* enligt LFH.[225] Röjandet innefattar inget krav på motprestation eller bedömning av vilken metod som gärningspersonen vidtog för att avslöja informationen.[226] En tredje möjlighet för gärningspersonen är att *på annat sätt anskaffa* företagshemligheten.[227] Som exempel nämner förarbetena sådana anskaffanden som kan anses strida mot god sed inom näringslivet samt anskaffanden som sker genom köp, byte eller gåva och där informationsinnehavaren inte avgett sitt samtycke.[228] Med anledning av att företagshemligheten kan komma någon till del på andra sätt än genom att någon *bereder sig tillgång till* eller *tillägnar sig* företagshemligheten, utgör uttrycket – *på något annat sätt anskaffar* företagshemligheten – en general-

[220] Fahlbeck 2019, s. 479.
[221] Ibid. s. 40.
[222] 3 § 1 st. p. 2 LFH.
[223] Fahlbeck 2019, s. 489.
[224] Ibid. s. 495.
[225] 3 § 1 st. p. 3. LFH.
[226] Ibid. s. 502.
[227] 3 § 2 st. p. 1 LFH.
[228] Prop. 2017/18:200, s. 143–144.

klausul.[229] Begreppet *anskaffar* är teknikneutralt, vilket innebär att angreppet kan riktas mot såväl lagrad som icke lagrad information samt verkställas genom företagandet av digitala intrång hos informationsinnehavaren.[230]

3.2 Straffansvar

I likhet med den numera tillämpliga LFH var straffansvaret för såväl *företagsspioneri* som *olovlig befattning med företagshemlighet* föreskrivet i 1990 års FHL.[231] Med anledning av LFH:s ikraftträdande utvidgades begreppet *anskaffande.* På motsvarande sätt utvidgades lagens tillämpningsområde till att även omfatta icke-kommersiella forskningsinstitutioner, vilket har medfört att det straffbara området har expanderat.[232] De två straffansvarsbestämmelserna är av särskilt vikt att uppmärksamma, eftersom dessa kan inbegripa sådant agerande som förekommer vid social manipulation.

3.2.1 Företagsspioneri och olovlig befattning med företagshemlighet

Bestämmelsen om *företagsspioneri* utgör den första straffansvarsbestämmelsen i LFH.[233] Flertalet av de metoder som används i samband med företagsspioneri är emellertid sedan tidigare försedda med straffansvar i BrB. I det fall att den tilltalade frias från ansvar enligt bestämmelsen om företagsspioneri i LFH utesluter det inte att denne likväl kan dömas till ansvar för någon annan typ av brottslighet som företogs parallellt med att denne beredde sig tillgång till informationen. Om det å andra sidan bedöms föreligga straffansvar enligt bestämmelsen om företagsspioneri i LFH, men bestämmelsen står i konflikt med den grundlagsstadgade anskaffarfriheten kan straffansvar enligt LFH inte ådömas den tilltalade.[234] Med anledning av att skyddsobjektet i LFH utgörs av företagshemligheter kan såväl privata som offentliga närings-

[229] Fahlbeck 2019, s. 482.
[230] Ibid. s. 477.
[231] Straffansvar för *företagsspioneri* stadgades tidigare i 3 § FHL, numera 26 § LFH. Tidigare stadgades *olovlig befattning med företagshemlighet* i 4 § FHL, numera 27 § LFH.
[232] Fahlbeck 2019, s. 748.
[233] 26 § LFH.
[234] Aspegren, Jacob, lag om företagshemligheter (2018:558), kommentar till 26 § JUNO.

verksamheter omfattas av straffansvarsbestämmelsen. Det finns emellertid ett fåtal undantag där anskaffarfriheten inte gäller för företagshemligheter inom den offentliga näringsverksamheten.[235]

Bestämmelsen om *olovlig befattning med företagshemlighet* utgör lagstiftningens andra straffbestämmelse.[236] På motsvarande sätt som för bestämmelsen om *företagsspionerі* innefattar *olovlig befattning med företagshemlighet* företagshemligheter inom såväl privata som offentliga näringsverksamheter. På liknande sätt som för föregående straffbestämmelse kan den grundlagsstadgade anskaffarfriheten inverka på sådan information som finns inom den offentliga sektorn.[237] Utöver kravet på att samtliga objektiva och subjektiva ansvarsförutsättningarna måste vara uppfyllda för att straffansvar ska kunna utdömas, krävs det även att angreppet är *obehörigt*.[238]

3.2.2 Objektiva och subjektiva ansvarsförutsättningar

För att straffansvar ska kunna åläggas i enlighet med bestämmelsen om *företagsspionerі* krävs det att tre objektiva rekvisit är uppfyllda. De objektiva rekvisiten är identiska med de rekvisit som formulerats i lagstiftningens föregående paragrafer. Inledningsvis krävs det att den tilltalade har *berett sig tillgång till* informationen. Rekvisitet, *bereder sig tillgång till*, har i denna kontext samma innebörd som i 3 § LFH.[239] För straffansvar enligt 26 § LFH erfordras inget krav på att den tilltalade ska ha utnyttjat eller röjt informationen, utan *beredandet* är i sig tillräckligt.[240] Ett ytterligare ofrånkomligt krav är att beredandet ska ha skett *olovligen*. Innebörden i begreppet *olovligen* kan och ska ges olika tolkningar, eftersom omständigheterna inte sällan skiljer sig åt från fall till fall. Det som kan bli avgörande för huruvida den tilltalade *berett sig tillgång till* informationen på *olovlig* väg är i vilken mån som informa-

[235] Fahlbeck 2019, s. 749.
[236] 27 § LFH.
[237] Fahlbeck 2019, s. 769.
[238] Se närmre kap. 3.1.5.
[239] Se närmre kap. 3.1.5.
[240] Aspegren 2018, kommentar till 26 § JUNO.

tionsinnehavaren har framhållit vikten av att hemlighålla informationen samt hur åtkomst till informationen kunnat ske på lovlig väg. Det aktivitetskrav som i 2 § LFH åvilar informationsinnehavaren får således även betydelse i fråga om straffansvar. Den gärningsperson som har för avsikt att bereda sig tillgång till en viss typ av information måste, i enlighet med legalitetsprincipen, på förhand ges möjlighet att kunna värdera presumtiva konsekvenser av sitt uttänkta agerande.[241] Utgångspunkten för bedömningen om huruvida ett beredande skett *olovligen* sker således utifrån beaktandet av i vilken omfattning som den tilltalade har brutit mot informationsinnehavarens avsikt att hemlighålla informationen.[242] Om exempelvis den tilltalade överträder en eller flera av informationsinnehavarens explicit eller implicit uppställda skyddsåtgärder föreligger *olovlighet*.[243] Huruvida den metod som den tilltalade använt sig av då denne berett sig tillgång till företagshemligheten är rättsstridig har ingen betydelse vid bedömning av straffansvar.[244] Rekvisitet *företagshemlighet* har i denna kontext samma innebörd som i 2 § LFH.[245]

Till skillnad från det objektiva rekvisitet, *bereder sig tillgång till*, som uppställs i 26 § LFH, innefattar bestämmelsen om *olovlig befattning med företagshemlighet* endast rekvisitet *anskaffar*. Fahlbeck hänvisar till 2016 års utredning, vari det anförs att de två begreppen har en likvärdig innebörd i de båda straffansvarsbestämmelserna.[246] Begreppet *anskaffar* har samma betydelse som i 2 § LFH.[247] På motsvarande sätt som för straffansvarsbestämmelsen om företagsspioneri har det, vid tillämpning av 27 § LFH, ingen relevans vilket syfte som föranleder anskaffandet. Det andra objektiva rekvisitet som uppställs utgör ett krav på att den som anskaffar företagshemligheten måste ha vetskap om att den som tillhandahåller informationen har berett sig tillgång till denna genom att bedriva företagsspioneri. Till skillnad från 26 § LFH föreligger det i straffansvarsbestämmelsen om *olovlig*

[241] Fahlbeck 2019, s. 753–754.
[242] Prop. 2017/18:200, s. 121.
[243] Fahlbeck 2019, s. 755.
[244] Aspegren 2018, kommentar till 26 § JUNO.
[245] Se närmre kap. 3.1.1.
[246] Fahlbeck 2019, s. 770; SOU 2017:45, s. 63.
[247] Se närmre kap. 3.1.5.

befattning med företagshemlighet således inget krav på att den tilltalade ska ha tillägnat sig informationen.[248] Förklaringen till detta är att det vid ett tillägnande fordras att den tilltalade redan har tillgång till informationen.[249] Bedömningen avseende huruvida kravet på att den tilltalade måste inneha vetskap om att företagsspionerі har begåtts, är förhållandevis lågt ställt. Det är tillräckligt att den tilltalade borde ha insett att företagsspionerі begåtts. Detsamma gäller om den tilltalade får kännedom om informationen först efter att denna vidareförmedlats genom ett större antal personer. Länken kan emellertid brytas om den sista personen i kedjan inte innehar sådan vetskap, vilket innebär att straffansvar enligt 27 § LFH i sådana fall inte kan utdömas.[250] Den tredje och sista objektiva ansvarsförutsättningen utgörs av kravet på att informationen ska utgöra en *företagshemlighet*.[251]

Under kategorin subjektiva ansvarsförutsättningar faller endast ett rekvisit – *uppsåt*. För att straffansvar ska föreligga för såväl *företagsspionerі* som *olovlig befattning med företagshemlighet* är det tillräckligt med likgiltighetsuppsåt och att uppsåtet omfattar samtliga objektiva ansvarsförutsättningar. Under förutsättning att de övriga rekvisiten är uppfyllda föreligger inget ytterligare krav på att den tilltalade måste ha haft särskilda avsikter med anskaffandet för att kunna dömas för företagsspionerі.[252] I sammanhanget är det emellertid väsentligt att ånyo poängtera den situation där den tilltalades anskaffande grundar sig på dennes avsikt att avslöja ett misstänkt brott eller andra missförhållanden, vilket kan resultera i straffrihet enligt LFH.[253]

[248] Fahlbeck 2019, s. 771–772.
[249] Aspegren, Jacob, lag om företagshemligheter (2018:558), kommentar till 27 § JUNO.
[250] Fahlbeck 2019, s. 772–773.
[251] Se närmre kap. 3.1.1.
[252] Fahlbeck 2019, s. 761–762.
[253] 2 § 3 st. LFH och 4 § 2 st. p. 1–2 LFH.

4 Presumtiva hot och angrepp på företagshemligheter

4.1 Introduktion

Följande kapitel har till syfte att vidga det skyddsperspektiv som lagstiftningen och övriga rättskällor uppvisar avseende företagshemligheter. Detta sker i huvudsak genom att synliggöra betydelsen av verksamheternas skyddsvärda informationstillgångar. På motsvarande sätt som för materiell utrustning utgör information en värdefull tillgång för att verksamheter ska kunna bedrivas och utvecklas.[254] I syfte att kunna inplacera företeelsen social manipulation i sitt rättmätiga sammanhang är det nödvändigt att inledningsvis klargöra informationssäkerhetsbegreppet och försöka utröna vilka potentiella hot och angrepp som bedrägerimetoden kan förorsaka.

4.2 Informationssäkerhet

Intresset av att skydda information i privata och offentliga verksamheter avspeglas inte enbart i det rättsliga skyddet som lagstiftningen erbjuder. Som exempel på annan typ av information som lagstiftaren har ansett skyddsvärd är personuppgifter vars rättsliga skydd erhålls genom dataskyddsförordningen (2018:218). Även sekretessbelagda allmänna handlingar ges rättsligt skydd i tryckfrihetsförordningen (1949:105) (TF) och OSL. Vidare erhåller information rörande rikets säkerhet rättsligt skydd i säkerhetsskyddslagen (2018:585).[255]

I sammanhanget kan det diskuteras huruvida det rättsliga skyddet som LFH erbjuder är tillräckligt för att verksamheternas informationstillgångar ska

[254] MSB (2015), *Detta är informationssäkerhet*, <https://www.informationssakerhet.se/om-informationssakerhet2/vad-ar-informationssakerhet/>, (hämtad 2020-03-27).
[255] MSB (2018b), *Rättsligt skydd för viss typ av information*, <https://www.informationssakerhet.se/lagar--regelverk/rattsligt-skydd-for-viss-typ-av-information/>, (hämtad 2020-03-23).

anses ha ett fullgott skydd. Svensson[256] hävdar att så inte är fallet. Svensson betonar att lagstiftningens skydd i denna del är otillräckligt, men att det rättsliga skyddet likväl har en viktig funktion som signallagstiftning. Svensson menar att verksamheterna, i syfte att komplettera lagstiftningen, har ett individuellt ansvar att tillgodose skyddsbehovet utifrån verksamhetens enskilda förutsättningar.[257] Detta konstaterande gör det berättigande att ånyo erinra om det aktivitetskrav som åvilar informationsinnehavaren i 2 § LFH.[258]

Informationssäkerhet handlar om att vara införstådd med vilka säkerhetsrisker som finns avseende hantering av verksamhetens information och utifrån denna insikt vidta såväl tekniska som andra lämpliga rutinåtgärder.[259] Den nära förbindelsen som råder mellan informationssäkerhet och teknik- och datavetenskap har medfört att arbetet med säkerhetsåtgärder ofta uttrycks genom det förenade begreppet *informations- och cybersäkerhet*.[260] Arbetet med informationssäkerhet har till syfte att säkerställa verksamhetens information så att denna inte förvanskas, offentliggörs eller undanröjs. Detta ska ske parallellt med att informationens tillgänglighet inte försvåras.[261]

Informationssäkerhetsarbetet är av vikt för såväl privata som offentliga verksamheter och begreppets innebörd är detsamma oavsett i vilken verksamhet det förekommer.[262] Vid hantering av information eftersträvas ett särskilt vidmakthållande av konfidentialitet, riktighet och tillgänglighet, varav samtliga komponenter utgör grundpelarna i informationssäkerhetsbegreppet.[263]

---

[256] Tommy Svensson är verksam som jurist inom säkerhetsjuridikens område och är ansvarig för säkerhetsfrågor inom bl.a. Svenskt Näringsliv.
[257] Svensson 2011, s. 83.
[258] Se närmre kap. 3.1.4.
[259] MSB (2018a), *Informationssäkerhet för små företag – rekommendationer för dig som driver eget företag med upp till 10 anställa*, <https://rib.msb.se/filer/pdf/28741.pdf>, (hämtad 2020-03-17), s. 4.
[260] Jfr MSB (2019b), *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022*, <https://rib.msb.se/filer/pdf/28804.pdf>, (hämtad 2020-04-01).
[261] Svenska institutet för standarder, *Informationssäkerhet*, <https://www.sis.se/iso27000/informationssakerhet/>, (hämtad 2020-03-27).
[262] MSB (2019a) *Informationssäkerhet, cybersäkerhet och säkra kommunikationer*, <https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/>, (hämtad 2020-04-01).
[263] Jfr Säkerhetspolisen (2019). *Vägledning i säkerhetsskydd. Informationssäkerhet*, <https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c673/1560952186689/Vagledning-Informationssakerhet.pdf>, (hämtad 2020-05-18).

Endast personer med särskild behörighet ska ha tillgång till informationen och denna ska för dessa vara lättåtkomlig och användbar. Innehållet i informationen får inte riskeras att utsättas för manipulering eller förvanskning, utan måste alltid vara tillförlitlig till sitt innehåll.[264] Informationssäkerhet inbegriper såväl administrativa som tekniska säkerhetsåtgärder, vilka primärt syftar till att verksamhetens informationstillgångar ska omges av ett starkt utomrättsligt skydd. På lång sikt ska arbetet med informationssäkerhet bidra till ett förhöjt förtroende för verksamhetens arbete.[265]

4.2.1 Underrättelseverksamhet och öppna källor

I sammanhanget bör uppmärksammas den skiljelinje som föreligger mellan å ena sidan den legala affärsunderrättelse som utgör ett led i den fria konkurrensen, å andra sidan den illegala underrättelseverksamheten som bland annat kan föreligga i samband med företagandet av företagsspioneri. Svensson menar att den legala underrättelseverksamheten som sker i företag i första hand syftar till att granska och kartlägga konkurrerande företag som är verksamma på marknaden. En sådan form av granskning utgör ett naturligt inslag i hur vissa företag väljer att bedriva sitt säkerhetsarbete. Syftet kan exempelvis vara att försvåra utomstående aktörers åtkomst till konfidentiell information och att således möjliggöra en obesvärad utveckling av den egna verksamheten.[266]

I detta sammanhanget bör begreppet *competitive intelligence* nämnas. Begreppet *competitive intelligence* innebär att företagandet av omvärldsbevakning i syfte att optimera verksamhetens konkurrenskraft. Metoden innefattar all typ av bevakning som kan vara av värde för verksamheten, dess kunder och samhället i stort.[267] Metoden tillämpas i ett flertal industrialiserade länder och har bedömts vara etiskt vedertagen. Insamlandet och

[264] MSB (2009) *Samhällets informationssäkerhet: lägesbedömning 2009*, <https://www.msb.se/RibData/Filer/pdf/24593.pdf>, (hämtad 2020-03-20), s. 13.
[265] Jfr Säkerhetspolisen, *Informationssäkerhet*, <https://www.sakerhetspolisen.se/sakerhetsskydd/informationssakerhet.html>,(hämtad 2020-03-20).
[266] Svensson 2011, s. 85.
[267] Nobicon (2015). *Competitive intelligence och annan begreppsförvirring*, <https://www.nobicon.se/nyheter/competitive-intelligence/>, (hämtad 2020-03-26).

analyserandet av information har för avsikt att öka förståelsen för de konkurrerande verksamheternas strategier, kapacitet och målsättningar och metoden tjänar således som en typ av strukturell analys.[268]

Underrättelseverksamhet kan följaktligen ske på laglig eller illegal väg samt med mer eller mindre etiska vedertagna metoder. Som exempel på etisk vedertagen underrättelseverksamhet kan nämnas sådan informationsinhämtning som sker med hjälp av öppna källor. Samlingsbegreppet *öppna källor* utgör en viktig komponent i begreppet *competitive intelligence*.[269] *Öppna källor* innefattar sådan information som bland annat går att finna i tidskrifter, litteratur och på internet. Information om en viss verksamhet kan även inhämtas från mer specifika källor i form av årsredovisningar, marknadsföringsåtgärder, utställningsmässor, leverantörer och kunder, vilka tillika utgör *öppna källor*. Information som påträffas i sådana allmänt tillgängliga källor och som samlas in och sammanställs är, till skillnad från kriminella handlingar som begås inom ramen för företagsspionerі, såväl etiskt vedertagna som lagliga. Trots att informationen enbart härrör från *öppna källor* kan utbudet likväl vara stort. Den totala mängden information kan sammantaget frambringa en tämligen heltäckande och djupgående bild över den verksamhet som granskas.[270]

4.2.2 Externa och interna hot

Om företagen är införstådda med vilka säkerhetsrisker som finns och vart dessa vanligtvis påträffas är det möjligt att i ett tidigt skede utarbeta och vidta förebyggande skyddsåtgärder.[271] Frågan är emellertid hur vanligt förekommande det är att företagen själva innehar tillräckligt med kunskap för att

[268] Nasheri, Hedieh (2005). *Economic espionage and industrial spying*. New York: Cambridge University Press, s. 72–73.
[269] Begreppet *öppna källor* kan på engelska översättas till *open source intelligence*, vilket betyder *undersökning med öppna källor* och inbegriper sådan information som är tillgänglig för allmänheten. Om det krävs någon form av specialkompetens, verktyg eller genomförandetekniker för att få åtkomst till källan bör det rimligtvis inte betraktas som en öppen källa.
[270] Svensson 2011, s. 84–85.
[271] MSB 2015, s. 4.

identifiera och konkretisera riskerna och utifrån en säkerhetsprognos utarbeta lämpliga skyddsåtgärder?

Säkerhetsriskerna kan, för enkelhetens skull, beskrivas utifrån informationssäkerhetens fyra dimensioner, varav externa och interna hot utgör de två första. Såväl de externa som interna hoten kan sedermera kategoriseras i mänskliga respektive omänskliga hot. Inom teknik- och datavetenskapens område är forskningen huvudsakligen inriktad på att identifiera och granska de säkerhetsrisker som härrör från externa hot. Resultaten från den vetenskapliga forskningen har bland annat påvisat att verksamheter i hög grad prioriterar sådana säkerhetsåtgärder vars primära syfte är att förhindra företagandet av externa angrepp på verksamhetens datorsystem.[272] Med *externa angrepp* avses i denna kontext angrepp på information som företas av individer som, i relation till den aktuella verksamheten, är att betrakta som utomstående.[273] Oavsett om arbetet med informationssäkerhet sker inom en privat eller en offentlig verksamhet är det vanligt att informationssäkerhetsarbetet diskuteras utifrån ett cybersäkerhetsperspektiv.[274]

Att diskussionerna om potentiella säkerhetsrisker till övervägande del inriktas på IT-relaterade hot är troligtvis inte speciellt anmärkningsvärt. I takt med utvecklandet av IT, den ökade användning av internet i allmänhet och sociala medier i synnerhet, har insamlingen av konkurrensfördelaktig information effektiviserats. En stor mängd information finns att tillgå via internet. Ökad globalisering har medfört att flertalet av samhällets kommunikationskanaler har inplacerats i den digitala miljön.[275] Digitaliseringens reformerande har gett upphov till ett flertal nya kommunikationsmedel, varav majoriteten bidrar till att stora delar av den vardagliga kommunikationen underlättas.[276]

[272] Warkentin, Merrill, Willison, Robert (2009). *Behavioral and policy issues in information systems security: the insider* threat, European Journal of Information Systems, 18, s. 101.
[273] Fahlbeck 2019, s. 755; Uttrycket *utomstående angrepp* har i den juridiska litteraturen används i samband med beskrivning av *olovlig åtkomst* samt utgjort en motpol till sådana interna angrepp som företas av arbetstagare.
[274] Svensson 2011, s. 185.
[275] Warkentin och Willison 2009, s. 101.
[276] Nasheri 2005, s. 74.

Genom att särskilt inrikta informationssäkerhetsarbetet på cybersäkerhet är det möjligt att vidmakthålla den ständigt pågående digitaliseringsutvecklingen. Detta inbegriper att viktiga värden, exempelvis rättssäkerhet, demokrati och mänskliga fri- och rättigheter, skyddas från hot och faktiska angrepp.[277]

Systematiskt informationssäkerhetsarbete syftar huvudsakligen till att statliga myndigheter, företag och andra organisationer ska verka för att införskaffa sig vetskap om potentiella underliggande hot och risker samt att individuellt ansvara för att informationssäkerhetsarbetet fortskrider.[278] Regeringen har uttryckt att den nationella målsättningen är att vara bland de bästa länderna i världen på att nyttja digitaliseringens möjligheter.[279] Den senaste framtagna nationella strategin omfattar både myndigheter, företag och privatpersoner. Det primära syftet med strategin är att öka den allmänna medvetenheten samt att samhälleliga aktörer ska uppbära goda förutsättningar för att kunna bedriva ett långsiktigt och produktivt arbete med information- och cybersäkerhet. De nationella strategierna markerar vikten av att samtliga aktörer arbetar konsekvent med information- och cybersäkerhetsfrågor, eftersom dessa frågor berör majoriteten av den information som figurerar i samhället.[280]

Förenklad digital kommunikation är i ett flertal situationer av väsentlig betydelse. Lättillgänglig och tillförlitlig information är en nödvändighet för att såväl företag som privatpersoner ska kunna fatta snabba och tydligt motiverade beslut. Besluten kan sedermera komma att inverka på kvalitén i all den kontakt som sker mellan verksamheter.[281] Trots att det finns ett flertal konkreta fördelar med att frekvent bedriva kommunikation i den digitala miljön bör inte riskerna underskattas. Effektiviteten och lättillgängligheten i att snabbt

[277] Skr. 2016/17:213, *Nationell strategi för samhällets informations- och cybersäkerhet*, s. 4.
[278] Ibid. s. 9.
[279] Bet. 2011/12:TU1, *Utgiftsområde 22 Kommunikationer*, s. 1.
[280] Jfr MSB, 2019b, s. 11; Mouton, F., Leenen, L., Venter, H.S. (2016). *Social engineering attack examples, templates and scenarios,* Computers and security 59, s. 186.
[281] Skr. 2016/17:213, s. 6.

finna och tillgodogöra sig information kan resulterar i fler situationer som inbjuder till en ökad användning av bedrägerimetoder.[282] Den utbreda användningen av sociala medier utgör ett exempel som kan föranleda att det brister i värnandet av den personliga integriteten eller i det enskilda företagets intressen.[283] Bundenheten till internet kan således komma att inverka negativt på sårbarheten i den information som rör enskilda individers privata sfär samt i den information som finns inom oumbärliga samhällsledande organisationer.[284] Samverkan och interaktionen på nätet mellan privata och offentliga aktörer ligger i ständig utveckling. Gränsdragningen mellan det privata och det offentliga är emellertid inte alltid tydlig. Privata aktörer är ofta styrande inom den tekniska utvecklingen, vilket får betydelse då dessa äger och driver samhällsviktiga verksamheter.[285]

I en undersökning från 2019, utförd av Statistiska centralbyrån (SCB) på uppdrag av regeringen, var målsättningen att identifiera och kartlägga sådana säkerhetsåtgärder som gick att härleda till cybersäkerhet. Det fordrades att de säkerhetsåtgärderna som studerades hade tillkommit i syfte att tillförsäkra informationens integritet, validitet och tillgänglighet. Undersökningens utfall påvisar att de vanligaste förekommande säkerhetsåtgärderna som företag vidtar för att undvika angrepp och intrång på konfidentiell information är genom att uppdatera operativsystemet och programvaror.[286] Den säkerhetsåtgärd som i ringa utsträckning nyttjas är biometriska metoder.[287] Närmast till hands står att finna sådan beteendevetenskaplig forskning där studiet utgörs av arbetstagarnas bristande efterlevnad av informationssystemets säkerhetspolicys, vilka kan utgöras av såväl avsiktliga som oavsiktliga handlingar.[288]

---

[282] Nasheri 2005, s. 74.
[283] Svensson 2011, s. 84.
[284] Warkentin och Willison 2009, s. 101.
[285] Skr. 2016/17:213, s. 3.
[286] SCB (2019). *Digitalisering och säkerhet i svenska företag*, <https://www.scb.se/hitta-statistik/statistik-efter-amne/naringsverksamhet/naringslivets-struktur/it-anvandning-i-foretag/pong/statistiknyhet/it-anvandning-i-foretag-2019/>, (hämtad 2020-04-01).
[287] Med *biometriska metoder* eller *biostatistik* åsyftas sådan statistik vars data rör människans fysiologiska eller beteendemässiga egenskaper. Egenskaperna kan t.ex. utgöras av ansikts- och fingeravtryck, vilka kan användas inom biometrisk teknik i syfte att säkerställa identifiering eller verifiering.
[288] Warkentin och Willison 2009, s. 101.

Oavsett vilken nivån av tekniskt skydd som verksamheten vidtagit kvarstår de mänskliga riskfaktorerna. Detta innebär att samtliga säkerhetsrisker aldrig fullständigt kan undanröjas. Genom att arbeta för förhöjd cybersäkerhet finns det emellertid en ökad möjlighet att reducera ett flertal säkerhetsrisker.[289] Från den nationella fältstudien som företogs av 1983 års utredning kan det utrönas att arbetstagare inom ett företag utgör en avsevärd riskfaktor för att konfidentiell information ska hamna i fel händer.[290] Även senare tillkomna studier påvisar att arbetstagare utgör en betydande säkerhetsrisk avseende informationssäkerhet.[291]

Interna hot och angrepp i form av arbetstagarnas avsiktliga eller oavsiktliga handlanden kan medföra stor invärtes skada i verksamheten. Problematiken kan i viss mån relateras till cybersäkerhet då merparten av riskerna inom IT är förenade med arbetstagares beteenden.[292] Utan hänsyn till befattning har arbetstagare ofta någon form av åtkomst till den information som finns lagrad på verksamhetens nätverksservrar. Den inverkan som arbetstagare har i förhållande till verksamhetens integritet har benämnts som *säkerhetsproblemets slutpunkt*, eftersom arbetstagare ofta utgör ändpunkten i arbetet med informationssäkerhet.[293] Den totala mängd konfidentiell information som en arbetstagare har kännedom om kan naturligtvis variera beroende på sakförhållanden inom den specifika verksamheten.[294] MSB beskriver hotbilden som allvarlig och tillägger att bedrägerierna blir alltmer sofistikerade då gärningspersonerna i allt högre utsträckning utnyttjar mänskliga svagheter i avsikt att få åtkomst till information.[295] MSB uttrycker en farhåga över att informationssäkerheten inte förmår hålla jämt tempo med den tekniska samhällsutvecklingen. Till följd av det avstånd som därav uppstår förhöjs

[289] *Nationalencyklopedin,* IT-säkerhet, <http://www.ne.se/uppslagsverk/encyklopedi/lång/it-säkerhet>, (hämtad 2020-03-30).
[290] Se närmre kap. 1.4.1.3.
[291] Jfr bl.a. Warkintin och Willison 2009.
[292] Flores, Rocha, W. (2016). *Shaping Information Security Behaviors Related to Social Engineering Attacks,* <https://kth.diva-portal.org/smash/get/diva2:925493/FULLTEXT02.pdf>, (hämtad 2020-03-14), s. 3.
[293] Warkintin och Willison 2009, s. 102.
[294] MSB 2009, s. 44.
[295] Ibid. s. 7.

riskerna avseende IT-relaterade angrepp på verksamheter. Genom att fästa avseende vid såväl teknik som mänskligt beteende kan verksamheten påverka i vilken mån som informationssäkerheten upprätthålls.[296] Mitnick påpekar att företagen ofta är medvetna om att informationssäkerheten bör ha en hög prioritet. Detta kommer bland annat till uttryck då merparten av verksamheternas utgifter ofta går till att införskaffa högkvalitativ säkerhetsteknik.[297] Trots att företaget kan ha investerat i andra typer av säkerhetsrutiner – utarbetade säkerhetsföreskrifter, inhyrda vaktbolag etcetera – hävdar Mitnick att verksamheterna inges av en obefogad känsla av säkerhet. Mitnick menar att upprättandet av sådana skyddsåtgärder inte reducerar risken att verksamheten utsätts för angrepp. Sårbarheten, som består av den utsatthet som uppstår då en arbetstagare utsätts för manipulativa metoder, kvarstår. I de situationer där arbetstagaren manipuleras har gärningspersonen utnyttjat det kryphål som tekniska skyddsåtgärder aldrig kan förmå täcka. Arbetstagaren beskrivs således utgöra den svagaste länken i verksamheternas säkerhetskedja.[298]

4.3 Social manipulation inom de brottsförebyggande myndigheterna

I samverkan med övriga brottsbekämpande myndigheter har Brottsförebyggande rådet (Brå) sedan den 1 januari 2019 tilldelat bedrägerimetoden *social manipulation* en brottskod.[299] Tidigare hade indelningen av bedrägeribrottens brottstyper i 9 kapitlet BrB en annan utformning. Termen *social manipulation* förekom inte heller uttryckligen vid framställandet av kriminalstatistik.[300] Härvid bör emellertid noteras att även om de brottsförebyggande

[296] MSB 2018a, s. 3.
[297] Mitnick, Kevin D. & Simon, William (2002a). *Bedrägerihandboken: hantera den mänskliga säkerhetsfaktorn*. Sundbyberg: Pagina, s. 9.
[298] Ibid. s. 21–29.
[299] Jfr Brå (2019a). *Klassificering av brott. Anvisningar och regler*, <https://www.bra.se/download/18.7d27ebd916ea64de530d0ac/1576675852400/2019_Klassificering_av_brott_v8_0.pdf>, (hämtad 2020-04-02). – Brottskoder ger upplysning om vilka typer av brott som anmäls och utgör, tillsammans med annan information, en viktig faktor för att de brottsförebyggande myndigheterna ska förmå framställa underlag och upprätta statistik.
[300] Brå (2019b). *Kriminalstatistik 2019. Anmälda brott. Slutlig statistik*, <https://www.bra.se/download/18.7d27ebd916ea64de5304e10e/1585653308304/Sammanfattning_anmalda_2019.pdf>, (hämtad 2020-04-03), s. 37–38.

myndigheterna har avgett sin begreppsförklaring samt uttalat vilka möjliga tillämpningsområden som företeelsen kan verka inom, är området på intet sätt fullständigt utrönt. Att social manipulation, av de brottsförebyggande myndigheterna, bekräftats förekomma i illegala sammanhang utgör i denna bemärkelsen inte ett fullgott klargörande över i vilken mån social manipulation inverkar på eller beaktas i den juridiska kontexten.

Brå:s implementering av brottskoder syftar primärt till att kvalitetssäkra den officiella statistiken genom att effektivisera och öka trovärdigheten bland statistikens framställande.[301] Genom att koda vissa typer av brott kan bedrägeribrotten enklare följas upp och således bidra till utarbetandet av detaljerad kriminalstatistik.[302] Vid införandet av nya brottskoder uppställs de alternativa kraven på att det aktuella brottet, enligt regeringen eller rättsväsendets bedömning, antingen ska ges särskild prioritet, anses utgöra allvarlig brottslighet eller utgöra sådan typ av brottslighet som i större omfattning än andra brott anmäls. Ett alltför generöst införande av nya brottskoder är emellertid, av praktiska skäl, inte eftersträvansvärt.[303] Givetvis är det nödvändigt att fästa avseende vid att det i princip alltid föreligger en viss risk för att felkodning kan uppstå i samband med att ett brott anmäls.[304] Brottskoden för bedrägerimetoden social manipulation har av Brå definierats som

> *”Gärningspersonen tar kontakt med en person och förmår hen att begå eller låta bli att begå en handling genom att utnyttja en förtroenderelation, i syfte att ge ekonomisk vinning till gärningspersonen.”*[305]

[301] Brå 2019a, s. 12.
[302] Polisen (2016). Nationellt bedrägericenter, *Intressant just nu om bedrägerier*, <https://www.ekobrottsmyndigheten.se/Documents/NBC_Informationsblad_December_2016.pdf>, (hämtad 2020-04-12), s. 2.
[303] Jfr Brå 2019a.
[304] Jfr Brå (2012). *Användningen av brottskoder. En kvalitetsstudie inom kriminalstatistiken*, <https://www.bra.se/download/18.1ff479c3135e8540b29800021266/1371914739137/2012_Anv_ndningen_av_brottskoder.pdf>, (hämtad 2020-05-02).
[305] Brå 2019a, s. 64.

I en rapport framtagen av Brå redovisas slutlig statistik rörande antalet anmäla brott under 2019. Statistikens primära syfte är att beskriva det rådande läget avseende utvecklingen av anmälda och registrerade brott.[306] Vid tolkning av statistiken är det emellertid särskilt viktigt att klargöra att antalet anmälda brott kan variera över tid samt att de anmälda brotten vanligtvis är färre till antalet än den totala mängden brott som i själva verket begås.[307] Rapporten framhåller att det totala antalet anmälda bedrägeribrott under 2019 uppgick till 245 000 brott. I jämförelse med antalet bedrägeribrott som anmäldes under 2018 har anmälningarna blivit färre till antalet med en procentuell minskning på sex procent.[308] Mellan åren 2010–2019 har emellertid det totala antalet bedrägeribrott påvisat en progressiv utvecklingskurva med en total ökning på 113 procent.[309]

Med anledning av att brottskoderna för bedrägeribrotten reviderades i början av 2019 gavs bedrägeribrotten en ny brottstypsindelning. Bedrägerimetoden *social manipulation* är numera indelad i fyra brottstypskategorier – romansbedrägeri, investeringsbedrägeri, befogenhetsbedrägeri samt bedrägeri av annan typ. Inom respektive underkategori görs ytterligare en indelning i huruvida brottet begåtts gentemot en äldre eller funktionshindrad. En anledning till att en sådan uppdelning görs just avseende bedrägeribrotten kan vara då social manipulation är den bedrägerimetod som framställs vara vanligast förekommande bland äldre och funktionshindrade.[310] Bedrägerier som begåtts genom social manipulation, inberäknat samtliga fyra nyssnämnda underkategorier, uppgick under 2019 till totalt 14 760 anmälda brott. Med anledning av 2019 års revidering av brottskoder finns det för 2018 ingen motsvarande siffra att tillgå.[311] Den kriminalstatistik som Brå tillhandahåller avseende antalet anmälda brott inbegriper såväl privatpersoner som företag.

[306] Brå 2019b, s. 45.
[307] Ibid. s. 8–9.
[308] En minskning på sex procent motsvarar en minskning med 15 600 anmälda bedrägeribrott.
[309] Brå 2019b, s. 37.
[310] SVT nyheter (2020). *Så fungerar vishing och social manipulation*, <https://www.svt.se/nyheter/lokalt/skane/sa-har-fungerar-vishing-och-social-manipulation>, (hämtad 2020-03-31).
[311] Brå 2019b, s. 37.

Differentierad statistik där det tydligt framgår vem som är anmälaren finns dessvärre inte att undfå.[312]

Den Nationella trygghetsundersökningen (NTU) påpekar att ökningen av antalet anmälda bedrägeribrott förvisso uppvisar att rättsväsendet uppmärksammar fler brott än tidigare. Vid tolkning av statistiken krävs det emellertid att adressaten likaså beaktar att vissa bedrägerimetoder anmäls i större utsträckning än andra. Detta kan bland annat ha sin grund i det sammanlagda värdet som bedrägeriet i det enskilda fallet förorsakar eller vem gärningspersonen är. Faktorer som kan påverka minskad anmälningsbenägenhet är sådana brott som genomförs med hjälp av internet. Benägenheten att anmäla ett brott minskar likaså om de som utsatts för brottet upplever en känsla av skam eller rädsla för att företagets trovärdighet och dess goodwillskapande verksamhet ska lida skada. De bedrägeribrott som företas i en verksamhet kan tillika vara synnerligen svåra att upptäcka. Brå har således bedömt att det finns ett stort mörkertal över hur många företag som de facto utsätts för bedrägeribrott.[313]

4.4 Social manipulation i en utomrättslig kontext

Med undantag från straffrätten förekommer bedrägerimetoden social manipulation i såväl sociologiska och beteendevetenskapliga som datavetenskapliga kontexter. Företeelsen förekommer nästintill dagligdags i större eller mindre utsträckning. Som illustrerande exempel kan nämnas de situationer då föräldrar manipulerar sina barn i syfte att barnen ska göra det som föräldrarna anser är bäst för dem.[314] Ett annat typexempel är då en lärare interagerar med sina studenter.[315] Dessa situationer illustrerar manipulation som till synes

[312] Brå 2020, mailkorrespondens.
[313] Brå (2015). *Brottsutvecklingen i Sverige fram till år 2015,* <https://www.bra.se/download/18.4a33c027159a89523b1b134e/1488273427834/8_Bedrageri.pdf>, (hämtad 2020-04-21), s. 171–189, s. 174–175.
[314] Mitnick och William 2002a, s. 30.
[315] Hadnagy, Christopher (2011). *Social engineering: the art of human hacking*. Hoboken, N.J.: Wiley, s. 10.

används i syfte att förmå en individ att förfara på ett, av manipulatören, önskvärt sätt. Hadnagy vill framhålla att social manipulation inte alltid företas i negativt syfte och har således valt att anlägga en tämligen bred och generell definition av social manipulation.

> *"Social engineering is any act that influences a person to take an action that may or may not be in his or her best interest.*[316]

En annan begreppsförklaring av social manipulation är den som Mitnick formulerat. Till skillnad från Hadnagy har Mitnick för avsikt att framhäva den negativa aspekten av social manipulation, vilken huvudsakligen åsyftar sådana manipulativa metoder som sker i illegala syften.[317]

> *"Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."*[318]

På motsvarande sätt som Mitnick har Nohlberg i sin begreppsförklaring låtit avspegla den negativa aspekten av social manipulation.

> *"Social engineering is a term used for techniques to con, or trick, victims into given the attacker sensitive information or to get them to perform actions that the attacker wants them to do."*[319]

---

[316] Hadnagy, Christopher (2018). *Social engineering: the science of human hacking*. Second edition Indianapolis, IN: Wiley, s. 7.
[317] Mitnick, Kevin D. & Simon, William L. (2002b). *The art of deception: controlling the human element of security*. New York: Wiley, s. 3.
[318] Mitnick och William 2002b, s. 1.
[319] Nohlberg, M., Kowalski, S. (2008). *The Cycle of Deception - A Model of Social Engineering Attacks, Defences and Victims*, School of Humanities and Informatics, University of Skövde, s. 1.

Social manipulation kan beskrivas utgöra ett paraplybegrepp för ett antal olika manipulativa metoder. För samtliga metoder är den grundläggande innebörden densamma – att utnyttja generella socialpsykologiska mänskliga sårbarhetsfaktorer i syfte att manipulera individer att ge ifrån sig konfidentiell information som sedermera kan utnyttjas i illegala syften.[320] Manipulatören använder sig av beteendepsykologiska verktyg, vilket i praktiken innebär att manipulatören skapar en illusion av känslor hos individen. Med hjälp av psykologiska katalysatorer kan manipulatören utöva inflytande över en individ. Manipulatören kan få individen att infria, det som enligt manipulatören är ett önskvärt resultat, utan att individen företar någon ingående analys.[321] Mitnick koncentrerar de vanligaste formerna av dessa psykologiska katalysatorer till sympati, skuldkänslor och hotelser.[322]

Mitnick hänvisar till den amerikanska forskaren Cialdini,[323] som sammanställt flera års beteendevetenskaplig forskning.[324] Såväl Cialdini som Mitnick hävdar att det finns ett antal fundamentala kvaliteter som manipulatören avsiktligt eller oavsiktligt förlitar sig på. Individer som erhåller krav från en auktoritet har en benägenhet att vilja åtlyda dessa. På motsvarande sätt föreligger det en inneboende vilja hos människor att rätta sig efter de krav som framförs av en, till synes, sympatisk person. En individ som känner behov av att återgälda någon till följd av att denna erhållit eller utlovats en gåva, har på jämförbart sätt en tendens att hörsamma den person som överlämnar gåvan. Mitnick framhåller även vikten av social bekräftelse och menar att individens benägenhet att lyda ökar om andra individer agerar på ett likartat sätt. Likaså har denne en tendens att vilja vara konsekvent genom att hålla ett uttalat löfte eller om individen får uppfattningen om att det som manipulatören söker efter

[320] Brå (2016). *Bedrägeribrottsligheten i Sverige. Kartläggning och åtgärdsförslag*, <https://www.bra.se/download/18.358de3051533ffea5ea2ec64/1458044205141/2016_9 Bedrägeribrottsligheten_i_Sverige.pdf >, (hämtad 2020-04-02), s. 102.
[321] Mitnick och William 2002a, s.137.
[322] Ibid. s. 163.
[323] Robert B. Cialdini är professor i socialpsykologi vid Arizona State University.
[324] Robert B. Cialdini (2001). Scientific American. *The Science of Persu*, <https://digitalwellbeing.org/downloads/CialdiniSciAmerican.pdf>, (hämtad 2020-04-19), s. 76.

är eftertraktat och endast förekommer i ringa omfattning.[325] Hadnagy framhåller metodens beständighet då social manipulation i grunden handlar om att uppbära förståelse för hur individer fattar beslut, vad som motiverar besluten samt hur individen kontrollerar sina känslor.[326]

4.4.1 IT-relaterade säkerhetsrisker

Social manipulation är inte uteslutande ett begrepp som påträffas inom beteendevetenskapen. Begreppet härrör ursprungligen från säkerhetsområdet.[327] Verksamheternas förmåga att vara konkurrenskraftiga är till stora delar beroende av användandet av IT-system, vilket medför att IT-relaterade säkerhetsrisker är ett faktum som bör uppmärksammas. Några av dessa IT-relaterade riskerna kan kopplas till tekniska systemfel, medan andra risker i högre grad relaterar till hotelser av extern karaktär. Företag har traditionellt sett primärt prioriterat vidtagandet av tekniska säkerhetsåtgärder. Trots styrkan i sådana åtgärder har sårbarheten i verksamheterna inte minskat. Flertalet av de IT-relaterade säkerhetsriskerna sammanhänger i själva verket med beteendet hos verksamhetens arbetstagare.[328] Bedrägerier som utförs med hjälp av IT kan ta sig varierande uttryck. Likaså kan konsekvenserna av den företagna gärningen skifta. Det som emellertid gör att dessa typer av bedrägerier sammanstrålar är då de, till skillnad från andra bedrägerimetoder, ofta utgör ett förstadium till utförandet av andra förestående bedrägeribrott. Det finns en rikhaltig flora av litteratur som behandlar bedrägliga beteenden i relation till information- och cybersäkerhet.[329]

I den mån social manipulation behandlas utifrån dess negativa aspekter och i förhållande till cybersäkerhet kan bedrägerimetoden, i grova drag, brytas ned i fyra olika grupper. Hadnagy benämner dessa grupper för phishing, vishing, smishing och imitation. Samtliga metoder utgår från att manipulatören, i

[325] Mitnick och William 2002a, s. 301–304.
[326] Hadnagy 2018, s. 7.
[327] Nohlberg och Kowalski 2008, s. 2.
[328] Flores, Rocha 2016, s. 3.
[329] Se bl.a. Marie-Helen Maras (2015). *Computer Forensics; Second Edition,* Jones and Bartlett Learning.; Watson, Gavin, Ackroyd, Richard, Mason, Andrew & Seaman, Jim (2014). *Social Engineering Penetration Testing*. Syngress.

större eller mindre utsträckning, nyttjar tekniska hjälpmedel i samband med sitt sätt att handla.[330] Via exempelvis mail, SMS eller andra typer av chattjänster ämnar manipulatören få en individ att besöka en specifik webbplats, öppna eller ladda ner en viss fil. Avsikten kan vara att angripa mottagarens IT-utrustning för att erhålla information som sedermera kan underlätta vid ett förestående angrepp.[331] SCB har i samband med en vidtagen undersökning avseende den svenska befolkningens internetanvändning samlat in data. Denna data anger att phishing, som vidtagits genom utskick av bedrägliga e-postmeddelanden till privatpersoner i åldrarna 16–85 år, uppgick till nästan tre miljoner personer under 2018.[332] Enligt en global undersökning från 2018–2019 avseende informationssäkerhet i globala organisationer, genomförd av Ernst & Young (EY), utpekas phishing som den bedrägerimetod som organisationerna själva upplever utgör det främsta hotet. Phishing är placerad på första plats på den topp tio-lista över presumtiva cyberrelaterade hot som organisationer kan utsättas för. Av de totalt tillfrågade 1 400 högt uppsatta verksamhetsledarna inom information- och cybersäkerhet ansåg 22 procent att phishing är den angreppsmetod som utgör det största hotet gentemot verksamheten.[333] Komparabelt med det uppskattade mörkertalet som Brå påtalade i samband med redogörelsen över kriminalstatistik, förefallet det även inom den beteendevetenskapliga disciplinen svårt att påträffa statistik avseende sådana angrepp som vidtas mot företag genom social manipulation. Förklaringen till denna avsaknad är i princip likartad den förklaring som anförts av Brå.[334] Brå:s konstaterande bekräftas i viss mån av Mitnick som bedömer att förefintligheten av angrepp på företag som företas genom social manipulation ofta är svåra att upptäcka, vilket inte föranleder någon brottsanmälan.

[330] Hadnagy 2018, s. 9–10.
[331] Sentor, *Nätfiske/Phishing*, <https://www.sentor.se/kunskapsbank-it-sakerhet/natfiske-phishing/>, (hämtad 2020-04-15).
[332] Resultatet inhämtades med hjälp av SCB:s statistikdatabas för cybersäkerhet under rubriken *Säkerhetsrelaterade problem vid användning av internet. År 2019*. I tabellsökning markerade jag det totala antalet kvinnor och män i åldrarna 16–85 år som under 2019 tagit emot e-postmeddelanden från bedragare (s.k. phishing), vilket gav en precis siffra på totalt 2 960 700 privatpersoner.
[333] EY (2018–2019). *Is cybersecurity about more than protection?*, <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf>, (hämtad 2020-04-17), s. 9 och 34. – Notera att EY är ett privatägt företag, vars intressen kan avspeglas i det material som de sammanställt.
[334] Se närmre kap. 4.3.

Mitnick framhåller emellertid att om sådan statistik existerat hade den sannolikt inte varit särskilt tillförlitlig, eftersom mörkertalet presumeras vara stort.[335]

4.4.2 Traditionell och humanistisk interaktion

Nohlberg belyser och utvecklar den distinktion som ofta framställs föreligga mellan, det som Nohlberg själv betecknar som, traditionell social manipulation och sådan social manipulation som primärt företas genom tekniskt inriktade angrepp. De traditionella typfallen är vanligtvis för handen då manipulatören vidmakthåller en tämligen direkt mänsklig interaktion med den individ som utsätts för angreppet. Övriga angrepp fordrar en lägre grad av mänsklig kontakt samt att tekniska hjälpmedel använts i manipulationsprocessen.[336]

Nohlberg har i samarbete med Kowalski[337] utvecklat en modell, vilken de benämner *the cycle of deception*. Modellen syftar till att ge en generell beskrivning av bedrägeribrott i allmänhet och social manipulation i synnerhet. Modellen avser skildra olika varianter av de angreppssätt som användandet av social manipulation kan föranleda. Modellen fungerar således som ett pedagogiskt hjälpmedel och som ramverk för att möjliggöra utvecklandet av effektiva skyddsåtgärder. Nohlberg och Kowalskis modell utgår bland annat från den grundtanke som förekommer i Mitnicks förklaringsmodell – *the social engineering cycle* – vars innebörd syftar till att identifiera och uppmärksamma de faser som föreligger innan, under samt efter ett inträffat angrepp. Mitnick har demolerat processens olika faser till fyra åtgärder – grundforskning, upprättande av kontakt, utnyttjande av förtroende samt utnyttjande av information.[338] Nohlberg och Kowalski menar emellertid att

[335] Mitnick och William 2002a, s. 315.
[336] Nohlberg, Marcus (2008). *Securing information assets: understanding, measuring and protecting against social engineering attacks*. Diss. (sammanfattning) Stockholm: Stockholms universitet, 2009, <http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-8379>, (hämtad 2020-04-12), s. 10.
[337] Stewart Kowalski är verksam professor i informationssäkerhet vid Norwegian University of Science and Technology.
[338] Mitnick och William 2002b, s. 397.

strukturen i Mitnicks förklaringsmodell är något förenklad och diffus. De tillät sig således att utveckla Mitnicks grundtanke och låta denna utgöra underlaget för en reviderad modell. Nohlberg och Kowalskis modell inbegriper en framställning av beteendet hos samtliga involverade aktörer – angriparen, försvararen och offret.[339]

Inledningsvis beskriver duon ett antal faser som de olika aktörerna genomgår vid ett pågående angrepp. För att angreppet ska vinna gehör krävs det emellertid att ytterligare komponenter i form av kontroll, påverkan och tid impliceras. Om angriparen, under kort tid, förmår upprätthålla låg påverkan på den kontrollnivå som organisationen eller offret uppfört kan angriparen uppnå sitt mål. Modellen inrymmer de aktiviteter som företas av angriparen, försvararen och offret, vilket bidrar till att en lättbegriplig och holistisk syn appliceras på den brottsliga angreppsprocessen. Framställningen kan främja verksamheternas säkerhetsarbete avseende ökad förståelse för konsekvenserna av ett angrepp. Modellen kan även ge en fingervisning om var verksamheten bör förlägga sina resurser. Nohlberg och Kowalski betonar värdet av att modellen uppbär en generell struktur då den kan tillämpas på ett antal olika brottstyper samt, ur ett vetenskapligt perspektiv, vara bistående till den forskning som företas inom informationssäkerhetens område.[340]

Hadnagy menar att bedrägerimetoden innehar en dynamisk karaktär, vilket i princip omöjliggör att på förhand organisera varje enskild fas i angreppsprocessen.[341] Trots detta konstaterande har Hadnagy utarbetat en egen modell – *the SE pyramid*. Syftet med modellen är jämförbart med såväl Nohlberg och Kowalskis som Mitnicks förklaringsmodeller. Hadnagys modell identifierar det händelseförlopp samt de verktyg som vanligtvis används under ett angrepp som företas genom social manipulation. Till skillnad från de övriga förklaringsmodellerna betonar Hadnagy vikten av att särskilt fokusera på den

[339] Nohlberg och Kowalski 2008, s. 2–10.
[340] Ibid. s. 2–10.
[341] Hadnagy 2018, s. 225.

inledande fasen i angreppsprocessen, vilken utgörs av underrättelser som sker med hjälp av öppna källor.[342]

4.5 Framtida hot och forskning

Angrepp som genomförs genom bedrägerimetoden social manipulation begrundas även i framtiden utgöra ett kontinuerligt överhängande hot. Nohlberg är emellertid övertygad om att hotet, inom en snar framtid, kommer att manifesteras i en mer sofistikerade skepnad än dess nuvarande yttringar. Detta kräver att diskussionen kring utarbetandet av preliminära skyddsåtgärder påbörjas inom en nära förestående tid.[343] Nohlberg och Kowalski menar att deras framtagna modell kan användas för att underlätta genomförandet av automatiserad social manipulation i form av en AI-programvara. Genom att utveckla en enkel programvara baserad på artificiell intelligens (AI) kan mänskligt beteende simuleras.[344] Framställning av autentiska socialtekniska hot är en potentiell metod för att möjliggöra utbildandet av de individer som riskerar att, i större utsträckning än andra, utsättas för angrepp.[345] Myndigheten för samhällsskydd och beredskap (MSB) har i korthet vidareutvecklat Nohlbergs resonemang. MSB menar att utvecklandet av en AI-programvara, vars huvudsakliga syfte är att manipulera användaren, i förlängningen kan ge upphov till en utbredd förtroendeförlust gentemot de tjänster som bedrivs online. MSB påpekar därutöver risken med att social manipulation kan få en särskild slagkraftig effekt i tider av ekonomisk kris.[346]

Likt Nohlberg, menar Hadnagy att social manipulation inte är ett övergående fenomen. Tillämpningsområdet för social manipulation är stort då dess principer kan användas i såväl legala som illegala syften och adresseras mot dels privatpersoner och juridiska personer.[347] Uppsåtlig mänsklig aktivitet i förening med utökade och sofistikerade tekniska möjligheter kan få skadlig inverkan på informationstillgångar, oavsett om det rör sig om sökandet efter

[342] Hadnagy 2018, s. 11.
[343] Nohlberg 2008, s. 81.
[344] Nohlberg och Kowalski 2008, s. 9–10.
[345] Nohlberg 2008, s. 81.
[346] MSB 2009, s. 45.
[347] Hadnagy 2018, s. 285.

företagshemligheter eller annan typ av konfidentiell information.[348] Hadnagy vidmakthåller sitt ställningstagande avseende att det även i framtiden är erforderligt att utbilda för att på så vis medvetandegöra om manipulationsmetodens utmärkande egenskaper.[349] Hadnagy menar att så länge som mänsklig arbetskraft existerar är den mänskliga sårbarheten en beständig faktor. På liknande sätt som Nohlberg och Kowalski uppskattar Hadnagy att framtidens ingenjörskonst, i betydande omfattning, kommer att inbegripa såväl AI som annan teknik för att motverka denna typen av angrepp.[350]

Sandgren, som har avhandlat förhållandet mellan kunskap och juridik, framhåller den inverkan som lagstiftningen har på utvecklingen av ny kunskap – i synnerhet ny teknik. Sandgren framhåller problematiken avseende användandet av *kunskapsteknik* i den rättsliga kontexten. Med *kunskapsteknik* avser Sandgren användandet av de metoder som forskningen om AI har utvecklat i syfte att behandla kunskap för att sedermera framställa datorbaserade system, vilka kan nyttjas vid juridisk problemlösning. Enligt Sandgren består problematiken av kunskapsteknikens bristande förmåga att uppfånga grundläggande komponenterna som förekommer inom rättsvetenskapen – exempelvis skälighetsresonemang och skönsmässiga bedömningar. Trots den oförmåga som kunskapstekniken besitter råder det ändå en intressant förbindelse gentemot juridiken. Utvecklandet av ny kunskapsteknik kan likaså influera lagstiftningens utformning och det övriga juridiska arbetet. Sandgren utesluter inte att utvecklandet av kunskapsteknik även kan reformera den juridiska tekniken som primärt manifesteras i rättskälleläran och i den juridiska argumentationen.[351]

Med undantag från ökad kunskap och medvetenhet kring social manipulation kan insikten om att åstadkomma en beteendeförändring vara av minst lika stor betydelse för att kunna hantera potentiella hot och skydda verksamhetens information.[352] Mitnick framhåller människans goda uppfinningsförmåga som

[348] Warkentin och Willison, s. 101.
[349] Hadnagy 2018, s. 285–286.
[350] Ibid. s. 254–255.
[351] Sandgren 1995, s. 56–57.
[352] Flores, Rocha 2016, s. 21.

ytterligare en faktor som kan inverkan på att det finns ett stort antal framgångsrika bedrägerimetoder där risken för upptäckt är låg. För att försvaret gentemot bedrägerimetoderna ska få effekt krävs det således att skyddsåtgärderna är dynamiska och nyskapande.[353] Trots den kontinuerliga utvecklingen av tekniska skyddsåtgärder kan inte ett absolut försvar gentemot social manipulation erhållas. Mitnick menar att det krävs en kombination av säkerhetstekniska åtgärder, säkerhetsföreskrifter samt utbildning av arbetstagare för att förmå upprätthålla ett fullgott skydd. Den tekniska utvecklingen bidrar till utökandet av försvarsåtgärder gentemot säkerhetsbrott i företag. Med hjälp av de principer som social manipulation utgör kan manipulatören kringgå de tekniska skyddsåtgärderna och istället bedriva en mer traditionell och humanistisk interaktion med individen.[354]

[353] Mitnick och William 2002a, s. 299–300.
[354] Ibid. s. 315–316.

5 Analys

5.1 Introduktion

Följande kapitel har för avsikt att inledningsvis ge en metodisk och objektiv sammanfattning av de resultat som uppsatsarbetet påvisat. Därefter diskuteras resultatet, vilket sker med utgångpunkt i uppsatsens syfte – *att undersöka om straffrätten korrelerar med social manipulation.* Den avslutande diskussionen har även för avsikt att besvara uppsatsens frågeställning – *i vilken mån beaktar straffrätten den mänskliga sårbarhetsfaktorn som utnyttjas vid social manipulation?* Ambitionen är placera in resultatet i en bredare rättslig kontext och utifrån ett subjektivt förhållningssätt diskutera rättsreglernas funktion i förhållande till den beteendevetenskapliga företeelse som social manipulation utgör.

I syfte att åstadkomma en öppen och utförlig analys är den kombinerade tillämpningen av den rättsdogmatiska och den rättsanalytiska metoden viktig att ånyo framhålla. Trots att den rättsdogmatiska metoden i viss mån bedöms kunna tillämpas i perspektivvidgande syfte, genom att inte uteslutande begränsas till gällande rätt, erhålls stöd i den rättsvetenskapliga doktrinen som antyder vikten av att tydligt särskilja beskrivande fakta från värderingar. I föregående kapitel har avsikten varit att, i enlighet med såväl den rättsdogmatiska som den rättsanalytiska metoden, framhålla argumentens ursprung. Min förhoppning är att framställningen i föregående kapitel ska bidra till utvecklandet av en transparent och fri diskussion som inger en hög grad av tillförlitlighet.

5.2 Rekvisiten och den straffrättsliga bedömningen

Skyddsobjektet i LFH utgörs av företagshemligheter, närmare bestämt information om affärs- eller driftförhållanden i en näringsidkares rörelse eller i en forskningsinstitutions verksamhet. Såväl begreppet *information* som *näringsidkare* kan anses ha ett vidsträckt innehåll. Detta innebär att ett brett spektrum av uppgifter och kunskaper har potential att kategoriseras som företagshemligheter. Kravet på att det ska röra sig om en *näringsidkare* bidrar i viss mån till denna vidsträckthet då rekvisitet inte fordrar några särskilda krav på vare sig verksamhetens ledning eller syfte.[355]

Vid en granskning av hur bedömningen av lagstiftningens övriga rekvisit ska genomföras, blir det emellertid tydligt att det rättsliga skyddet kan komma att få begränsad tillämplighet. Den avsedda informationen måste hemlighållas och får inte vara allmänt känd eller lättillgänglig. Informationsinnehavaren behöver inte framföra skälen till varför ett hemlighållande är för handen. Det fordras emellertid att denne aktivt har vidtagit rimliga åtgärder för att hemlighålla informationen. Trots att aktivitetskravet vid en första anblick kan uppfattas som tämligen strikt, uppställs inget krav på vare sig en viss typ av aktivitet eller en lägstanivå på graden av skydd som aktiviteten bör föranleda. Bedömningen grundar sig i huvudsak på informationens karaktär och omständigheterna i det enskilda fallet. Den företagna aktiviteten tillåts således ta sig olika uttryck.[356]

Informationsinnehavarens avsikt att hemlighålla viss typ av information grundar sig ofta på att inte gå miste om informationens kommersiella värde. Lagstiftningens krav på att röjandet av informationen ska ha en negativ inverkan på verksamhetens konkurrensförmåga, utgör många gånger en viktig del i en sådan förlust. Förlusten kan resultera i att verksamheten anser sig lida ekonomisk eller icke-ekonomisk skada. Även om förlusten inte alltid uppstår

[355] Se närmre kap. 3.1.1.
[356] Se närmre kap. 3.1.4.

vid tidpunkten för informationens röjande kan skadan få väsentlig betydelse för verksamheten. Detta gäller inte minst för de forskningsinstitutioner som, inte i lika hög omfattning som kommersiella företag, bedriver konkurrerande verksamhet.[357]

Kravet på att angreppet måste vara *obehörigt* för att det rättsliga skyddet ska inträda har, på motsvarande sätt som för rekvisiten information och näringsidkare, en vidsträckt innebörd. Detta framgår av de i lagen specificerade angreppssätten – *bereder sig tillgång till*, *tillägnar sig* eller *på något annat sätt anskaffar* företagshemligheten eller *utnyttjar* eller *röjer* företagshemligheten. Vid bedömning av rekvisitet *bereder sig tillgång till* avses anskaffanden av sådan information som gärningspersonen inte redan förfogar över. Huruvida gärningspersonen *tillägnar sig* företagshemligheten bedöms med utgångspunkt i om gärningspersonen, med något som denne redan innehar, gör till sitt eget. Vid bedömning av generalklausulen – om gärningspersonen *på något annat sätt anskaffar* företagshemligheten – utgår bedömningen från sådana omständigheter där anskaffandet kan anses strida mot god sed inom näringslivet eller om anskaffandet har skett genom byte, köp eller gåva och informationsinnehavaren inte avgett sitt samtycke till denna typ av förvärv. I sammanhanget bör ånyo erinras om den teknikneutralitet som åvilar rekvisitet *anskaffar*. Denna teknikneutralitet kan vara en ytterligare bidragande faktor till att anskaffarbegreppet har en vidsträckt innebörd. För att ett *utnyttjande* ska vara för handen krävs det att gärningspersonen i sin egen verksamhet praktiskt använder sig av informationen. Ett *röjande* fordrar att gärningspersonen avslöjar företagshemligheten för någon annan.[358]

Vid bedömning av straffansvar ska rättstillämparen bland annat utgå från om den tilltalade *olovligen berett sig tillgång till* företagshemligheten. Rättstillämparen ska härvid utgå från omständigheterna i det enskilda fallet. Av betydelse är i vilken mån som informationsinnehavaren framhållit vikten av att informationen hemlighålls samt på vilka sätt som åtkomst till informa-

[357] Se närmre kap. 3.1.3.
[358] Se närmre kap. 3.1.5.

tionen kan ske på lovlig väg i enlighet med legalitetsprincipen. Har den tilltalade överträtt klart uttalade eller underförstådda skyddsåtgärder kan kravet på olovlighet anses uppfyllt. Av förarbeten framgår det uttryckligen att rättstillämparen, vid bedömning av straffansvar, inte ska utgå från huruvida den metod som den tilltalade använt sig av är rättsstridig. De metoder som vanligtvis används i samband med genom-förandet av företagsspioneri är ofta redan försedda med straffansvar i BrB. Straffrihet enligt LFH utesluter således inte automatiskt straffrihet enligt BrB.[359]

5.3 Informationssäkerhet och social manipulation

Trots att flertalet av rekvisiten har tämligen generösa bedömningsmarginaler och att aktivitetskravet som åläggs informationsinnehavaren är tämligen lågt ställt har det rättsliga skyddet i LFH inte alltid bedömts som tillräckligt. Oberoende av lagstiftningens krav på att informationsinnehavaren ska företa rimliga åtgärder för att hemlighålla informationen finns det likväl ett egenintresse från verksamhetens sida att skydda sina företagshemligheter. Syftet med systematiskt informationssäkerhetsarbete är att verksamhetens informationstillgångar ska omges av ett starkt utomrättsligt skydd. Detta baseras på idéen om att vidmakthålla informationens konfidentialitet, riktighet och tillgänglighet. Arbetet med informationssäkerhet uppställer emellertid ett slags undertryckt krav på att företaget har god insikt om vilka presumtiva hot och angrepp som verksamheten kan komma att utsättas för. Verksamheten bör även kunna identifiera och konkretisera hoten för att i ett tidigt skedde förmå vidta lämpliga och effektiva säkerhetsåtgärder.[360]

Forskningen har påvisat att verksamheter ofta väljer att prioritera säkerhetsåtgärder av teknisk karaktär. Detta är troligtvis inte särskilt anmärkningsvärt med tanke på den kontinuerliga utvecklingen av digitaliseringen, vilket bland annat ger upphov till nya och förenklade kommunikationsmedel. På så vis

[359] Se närmre kap. 3.2.
[360] Se närmre kap. 4.2.

kan kvalitén i all den kontakt som sker mellan olika verksamheter förbättras. Trots att åtgärdsplanerna i de framtagna nationella strategierna inte har enskilda verksamheter som sin primära adressat, markeras det samhälleliga intresset av att skydda informationstillgångar samt vikten av att bedriva ett konsekvent information- och cybersäkerhetsarbete. Trots att det finns ett flertal fördelar med digitaliseringen är verksamheterna sårbara. Företagen väljer ofta att prioritera och inrikta säkerhetsarbetet på IT-relaterade hot och angrepp. Konstruerandet av säkerhetsåtgärder med utgångspunkt i den beteendevetenskaplig forskningen sker i ringa omfattning. Onekligen är fördelarna med den ständigt pågående tekniska utvecklingen och de enskilda företagens medvetenhet kring IT-relaterade hot betydelsefullt för att fortsätta bedriva och utveckla arbetet med informationssäkerhet. Trots att merparten av de IT-relaterade säkerhetsriskerna kan härledas till arbetstagarnas avsiktliga eller oavsiktliga beteende är den mänskliga sårbarheten ett bestående faktum.[361]

Utnyttjandet av mänsklig kontakt och förtroende i syfte att erhålla information utgör grunden för sådan social manipulation som företas med hjälp av IT eller genom mer traditionell och humanistisk interaktion. Risken att en arbetstagare utsätts för sådant utnyttjande har i såväl äldre som senare tillkommen forskning bedömts vara stor. Den befintliga statistiken avseende antalet anmälda bedrägeribrott som företagits genom social manipulation påvisar inte uttryckligen hur stor andel av det totala antalet anmälningar som utförts av företag. De brottsförebyggande myndigheterna har påpekat svårigheten i att överhuvudtaget identifiera och upptäcka social manipulation, eftersom metoden kan företas i mer eller mindre moraliskt klandervärda sammanhang. Metodens många yttringar kan således tyda på ett befintligt mörkertal. Verksamheterna riskerar att invaggas i en falsk känsla av trygghet om skyddsåtgärderna primärt koncentreras till hot och angrepp av teknisk karaktär.[362]

[361] Se närmre kap. 4.2.2.
[362] Se närmre kap. 4.4.1 och 4.4.2.

Medvetandegörandet av social manipulation kan bland annat ske med hjälp av framtagna modeller, vars syfte är att illustrera bedrägerimetodens olika faser och beteenden hos samtliga inblandade aktörer. Modellerna kan även appliceras på andra typer av brott och syftar således till att ge en generell illustrering av ett brotts olika faser. Modellernas primära syfte är att tjäna som pedagogiska hjälpmedel, men de kan även utgöra ett stöd i den vetenskapliga forskningen. Då social manipulation i framtiden bedöms påträffas i en alltmer automatiserad form, har det uttryckts en strävan efter att öka medvetenheten kring metodens förefintlighet och uttryckssätt.[363]

5.4 Avslutande diskussion

Den genomförda undersökningen av rättskällorna påvisar att angreppssättens struktur har något av en, som jag här valt att benämna, teknisk prägel. Rekvisiten i den straffrättsliga bedömningen koncentreras i huvudsak till huruvida gärningspersonen förfogar, använder eller avslöjar information. Rättskällorna ger ingen antydan om att den metod som gärningspersonen använder sig av för att genomföra angreppet har någon betydelse i denna delen av den juridiska bedömningen. Naturligtvis kan det förekomma enskilda fall där rättstillämparen, i den straffrättsliga bedömningen, har beaktat den tilltalades beteende i samband med utnyttjandet av en förtroenderelation. Då övriga rättskällor inte uttryckligen föreskriver att rättstillämparen konsekvent ska beakta denna typen av utnyttjande, ställer jag mig tveksam till om utfallen i sådana potentiella avgöranden ensamt kan ligga till grund för ett besvarande av uppsatsens frågeställning.

I fråga om straffansvar har förarbetena uttryckligen angett att den straffrättsliga bedömningen inte ska grundas på huruvida den metod som den tilltalade använt sig av är rättsstridig. Anskaffarbegreppet, som utgör ett samlingsbegrepp för de i lagen uppräknade handlingarna som kan företas gentemot företagshemligheter, beskrivs ha en teknikneutral utformning. Detta kan emellertid tolkas som att det i den straffrättsliga bedömningen finns ett visst

[363] Se närmre kap. 4.5.

utrymme för rättstillämparen att fästa avseende vid vilken metod den tilltalade har använt sig av i det enskilda fallet. Vid en granskning av befintliga rättsfallssammanställningar på området tycks emellertid den tilltalades handlingssätt ofta utgöras av sådana angreppet som företagits med hjälp av tekniska hjälpmedel, exempelvis genom kopiering eller fotografering. Vad som i sammanhanget utgör den ursprungliga och förtäckta påtryckningsmetoden framhålls inte.[364]

En viss gynnsam effekt kan möjligtvis ha uppkommit i samband med att social manipulation tilldelades en egen brottskod.[365] Brottskoden kan indicera att de brottsförebyggande myndigheterna uppmärksammar och erkänner existensen av social manipulation som bedrägerimetod. Den definition av social manipulation som Brå deklarerar är emellertid förhållandevis snäv, eftersom den inte i tillräckligt stor utsträckning framhåller den socialpsykologiska aspekten av bedrägerimetoden. På motsvarande sätt som för utformningen av lagstiftningens rekvisit, kan Brå:s definition beskrivas ha en teknisk prägel. Definitionens formulering skapar emellertid mer otydlighet än vad den bringar klarhet. Vad åsyftas exempelvis med utnyttjande av en förtroendeställning? Brottskoden ger således, enligt min mening, på intet sätt en fullgod redogörelse över vad som inryms i begreppet social manipulation eller hur metoden ska beaktas i den straffrättsliga kontexten.

Syftet med LFH är framför allt att främja rättvis konkurrens. Rättsreglernas primära funktion är att tjäna som skyddslagstiftning för företagshemligheter.[366] På lång sikt ökar företagens incitament att bedriva innovativt arbete, vilket gynnar den dynamiska utvecklingskurvan för ekonomisk tillväxt och sysselsättning. De straffrättsliga rekvisiten är konstruerade på ett sådant sätt att de iakttar ett flertal olika tillvägagångssätt som angrepp på företagshemligheter kan ske. Vid bedömning av straffansvar uppfattar jag det som att det är de faktiska omständigheterna som beaktas. I ringa eller obefintlig grad före-

[364] Se bl.a. Bengtsson och Kahn 2002; Bengtsson och Kahn 2018.
[365] Se närmre kap. 4.3.
[366] Se närmre kap. 2.4.2.

faller rättstillämparen fästa avseende vid mänskligt beteende i samband med missbruk av en förtroenderelation. Beteendevetenskaplig forskning har i viss mån kunnat styrka vilka grundläggande emotioner som offret i allmänhet upplever i samband med ett fortgående angrepp genom social manipulation. Trots denna påvisade vetskap torde reaktionen hos varje enskild individ aldrig med säkerhet på förhand kunna förutspås. Oförutsägbarheten i hur olika individer reagerar och upplever en viss situation kan troligtvis hänga samman med bland annat individens personlighet och erfarenheter samt de rådande omständigheterna före, under och efter ett angrepp.

Straffrätten har bland annat till syfte till att påverka människors beteende och uppmärksamma oönskade beteenden. Den situation där en gärningsperson utnyttjar en förtroenderelation genom att angripa mänskliga sårbarhetsfaktorer bör, enligt min mening, anses klandervärd. Genom att begagna sig av lagstiftningen för att uttryckligen uppmärksamma social manipulation, kan detta klandervärda tillvägagångssätt markeras. Detta kan i sin tur bidra till ökad rättssäkerhet och i synnerhet ökad förutsägbarhet. Förarbetena framhåller att rättstillämparen, vid bedömning av straffansvar, inte ska beakta om den metod som den tilltalade använt sig av är rättsstridig. Detta kan insinuera att den tilltalades utnyttjande av en förtroenderelation inte beaktas i samband med bedömning av straffansvar. Det finns i vart fall ingen uttrycklig antydan på att ett sådant utnyttjande specifikt ska beaktas i den straffrättsliga bedömningen. Att social manipulation i viss mån uppmärksammats i den straffrättsliga kontexten får i detta sammanhanget ringa betydelse. Rättstillämparen instrueras inte uttryckligen om att tillåtas beakta den tilltalades manipulativa beteende eller målsägandens reaktion på ett sådant beteende.

Problematiken med att inordna social manipulation i en straffrättslig kontext kan vara att metoden har en förmåga att yttra sig på ett flertal olika sätt och att det således är svårt att rättsligt och systematiskt konstruera metoden. Konsekvenserna av metodens tillämpande kan få olika skadeverkningar beroende på vem som tillämpar metoden, i vilket syfte som tillämpandet sker, vem som utnyttjas samt i vilket sammanhang som utnyttjandet sker. Därutöver finns

det givetvis en mängd olika sakförhållanden som kan få betydelse i det enskilda fallet. Den beteendevetenskapliga forskningen har visserligen konstaterat ett antal emotioner och mänskliga sårbarhetsfaktorer som en gärningsperson huvudsakligen väljer att utnyttja i samband med företagandet av social manipulation. Det kan således finnas potential att i lagstiftningen upprätta och införa rättsliga ramar för hur en straffrättslig bedömning avseende social manipulation bör utföras. Om lagstiftningen ger rättstillämparen uttrycklig tillåtelse att beakta mänskliga sårbarhetsfaktorer och utnyttjandet av dessa, finns det emellertid en risk att principen om objektivitet försvagas. Kravet på att domstolarna ska vara sakliga och opartiska kan försvåras om den straffrättsliga bedömningen ska inbegripa ett hänsynstagande till emotionella triggers och effekterna utav dessa. Ett sådant hänsynstagande kan mot förmodan redan beaktas av rättstillämparen – exempelvis i enlighet med generalklausulen i 3 § p. 1 LFH. Då rättskällorna, enligt min bedömning, uppvisar en avsaknad rörande om och hur en sådan bedömning ska genomföras, kan det i detta avseende föreligga en allvarlig brist i legalitetsprincipen. I de situationer då rättstillämparen beaktar påverkansmedel som inbegriper starka drag av emotioner, kan de eventuella skillnaderna i bedömningarna blir indirekt avhängig av andra faktorer. Dessa faktorer kan associeras till vissa typer av beteenden eller exempelvis könstillhörighet, ålder etcetera. Detta kan riskera att medföra att den straffrättsliga bedömningen överlag inte bidrar till dannandet av en enhetlig och opartisk rättstillämpning.

Diskussionen bör även belysas utifrån verkningsgraden med att ytterligare kriminalisera det skyddsvärda intresset. I förhållande till det skyddsvärda objektet – *företagshemligheter* – kan en alltför generös straffrättslig bedömning resultera i att det kriminaliserade området blir för omfattande. I uppsatsens inledande kapitel redogjorde jag för LFH:s funktion i rättssystemet och hur rättsreglerna i LFH tangerar ett flertal andra rättsområden. Möjligheten att sprida och erhålla information har bland annat föreskrivits grundlagsskydd i TF och YGL. Om rättstillämparen tillåts att inkludera ett större antal faktorer i straffansvarsbedömningen, kan detta således komma att inverka på de rättsområden som tangerar LFH. Under sådana förhållanden ställer jag mig

således tveksam till om rättstillämparen bör fästa avseende vid faktorer som kräver omfattande subjektiva ställningstaganden. För den händelsen att sådana faktorer tillåts att beaktas i den straffrättsliga bedömningen, bör det i vart fall krävas att lagstiftaren noggrant överväger hur en sådan bedömning skulle komma att påverka närliggande lagstiftning och dess skyddsvärden. En ytterligare invändning mot att beakta de faktorer som omfattas av bedrägerimetoden social manipulation kan vara de befarade farhågorna som huvudsakligen rör automatiserad simulering av mänskligt beteende. Risken finns att mänskliga sårbarhetsfaktorer inom en snar framtid kan komma att utnyttjas genom mer avancerade metoder. Flertalet av de vetenskapliga avhandlingarna som jag granskat utmynnar ofta i ett konstaterande om att lagstiftningen måste vara tidsenlig i förhållande till den tekniska utvecklingen som sker. Detta kan exempelvis infrias genom utvecklandet av nya kommunikationsmedel. I syfte att öka rättssäkerheten, i synnerhet förutsägbarheten, bör åtminstone effekterna av utnyttjanden av mänskligt beteende inkluderas i de diskussioner som rör modernisering av svenska rättsregler.

Sammanfattningsvis finns det, enligt min mening, en betydelse med att straffrätten beaktar utnyttjandet av mänskliga sårbarhetsfaktorer i samband med angrepp av skyddsvärda intressen. Beaktandet kan visserligen innebära en viss svårighet för rättstillämparen att skilja på individens subjektiva uppfattning av hur denna upplevt situationen. Trots detta är min uppfattning att det finns tillräckligt med stöd inom den beteendevetenskapliga disciplinen för att i någon mån initiera en diskussion kring vilken potential straffrätten har att beakta och bedöma utnyttjandet av mänskliga sårberhetsfaktorer. Det är i nästintill obefintliga mån som straffrätten för närvarande tillkännager social manipulation i den straffrättsliga bedömningen som företas i LFH. De förekommande antydningarna i förarbetena, om att rättstillämparen kan tillåtas att beakta andra omständigheter eller förfaranden än vad lagstiftningen uttryckligen föreskriver, är på intet sätt tillräckliga. Inte heller Brå:s uppmärksammande av bedrägerimetoden kan anses utgöra ett tillräckligt stöd i detta avseendet.

Straffrätten torde vara i behov av att uppmärksamma social manipulation. Inte minst för att identifiera, belysa och medvetandegöra en tämligen förtäckt problematik som, i större eller mindre omfattning förekommer, men vars företeelse ännu inte uttryckligen har påvisats i vare sig rättskällorna eller i den officiella kriminalstatistiken. Genom att särskilt framhålla det rättsliga och det utomrättsliga skyddet för företagshemligheter och hur undermåligt detta kan anses vara vid angrepp genom social manipulation, placeras emellertid problematiken in i en befintlig rättslig kontext. Hot och angrepp som riktas mot företagshemlig information kan förorsaka omfattande skadeverkningar för verksamheten, potentiella kunder och för det allmänna. Även om det finns en befogad distinktion mellan rättsvetenskapen och andra vetenskapliga discipliner bör lagstiftaren sträva efter att i det närmaste återspegla verkliga sakförhållanden. Mänsklig interaktion och påverkan utgör ett sådant centralt och vedertaget faktum. Emotionell interaktion inverkar på hur en individ väljer att agera och reagera i det sociala sammanhang som denne befinner sig i – något som även kan få betydande konsekvenser i den straffrättsliga kontexten.

Käll- och litteraturförteckning

Tryckta källor

Offentligt tryck

Sverige

Propositioner

Prop. 2017/18:200 — *En ny lag om företagshemligheter.*

Prop. 1987/88:155 — *Om skydd för företagshemligheter.*

Utredningsbetänkanden m.m.

Bet. 2011/12:TU1 — *Utgiftsområde 22 Kommunikationer.*

Bet. 1988/89:LU30 — *Skydd för företagshemligheter*.

Skr. 2016/17:213 — *Nationell strategi för samhällets informations- och cybersäkerhet.*

SOU 2017:45 — *Ny lag om företagshemligheter.*

SOU 1983:52 — *Företagshemligheter.*

SOU 1966:71 — *Otillbörlig konkurrens.*

PM 1988/89:KU2y — *Skydd för företagshemligheter.*

Protokoll 1989/90:131 — *Riksdagens protokoll.*

Litteratur

Arvidson, Markus (2007). *Den fabricerande människan*, doktorsavhandling Karlstad universitet, 2007:20.

Aspegren, Jacob, lag om företagshemligheter (2018:558), kommentar till 2, 3, 4, 26 och 27 §§ JUNO.

Bengtsson, Henrik, Kahn, Johan (2002). Ny juridik 4:02, *Företagshemligheter i domstolarnas praxis*, <http://kahnpedersen.se/wp-content/uploads/2017/06/Johan-Kahn-Foretagshemligheter-i-domstolarnas-praxis-–-del-I-Ny-Juridik-nr-4-2002-s.-7.pdfs.>, (hämtad 2020-04-06).

Bengtsson, Henrik, Kahn, Johan (2018). Ny juridik 3:05, *Företagshemligheter i domstolarnas praxis – del 2*, <https://www.delphi.se/uploads/2018/07/05foretagshemligheteridomstolarnaspraxisdel2henrik-bengtsson.pdf>, (hämtad 2020-04-06).

Domeij, Bengt (2016). *Från anställd till konkurrent: lojalitetsplikt, företagshemligheter och konkurrensklausuler*. 1. uppl. Stockholm: Wolters Kluwer.

Fahlbeck, Reinhold (2019). *Lagen om företagshemligheter: en kommentar och rättsöversikter*. Fjärde upplagan Stockholm: Norstedts Juridik.

Fahlbeck, Reinhold, *Kan forskning ske de lege ferenda? Några ord om vetenskap och den lag som bör införas*, JT Nr 2 2016/17, s. 526–532.

Hadnagy, Christopher (2018). *Social engineering: the science of human hacking*. Second edition Indianapolis, IN: Wiley.

Hadnagy, Christopher (2011). *Social engineering: the art of human hacking*. Hoboken, N.J.: Wiley.

Helgesson, Christina (2000). *Affärshemligheter i samtid och framtid*. Diss. Stockholm: Univ.

Industrispionage - ett svårarbetat fält. (2019). Copenhagen: Saga.

Jareborg, Nils, *Rättsdogmatik som vetenskap*, SvJT 2004 s. 4.

Korling, Fredric & Zamboni, Mauro (red.) (2013). *Juridisk metodlära*. 1. uppl. Lund: Studentlitteratur.

Lehrberg, Bert (2019). *Praktisk juridisk metod*. Elfte upplagan Uppsala: Iusté.

Marie-Helen Maras (2015). *Computer Forensics; Second Edition,* Jones and Bartlett Learning.

Mitnick, Kevin D. & Simon, William (2002a). *Bedrägerihandboken: hantera den mänskliga säkerhetsfaktorn*. Sundbyberg: Pagina.

Mitnick, Kevin D. & Simon, William L. (2002b). *The art of deception: controlling the human element of security*. New York: Wiley.

Mouton, F., Leenen, L., Venter, H.S., *Social engineering attack examples, templates and scenarios,* Computers and security 59 (2016), s. 186–209.

Nasheri, Hedieh (2005). *Economic espionage and industrial spying*. New York: Cambridge University Press.

Nohlberg, Marcus (2008). *Securing information assets: understanding, measuring and protecting against social engineering attacks*. Diss. (sammanfattning) Stockholm: Stockholms universitet, 2009, <http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-8379>, (hämtad 2020-04-12).

Nohlberg, M., Kowalski, S., *The Cycle of Deception - A Model of Social Engineering Attacks, Defences and Victims* (2008), School of Humanities and Informatics, University of Skövde.

Nordblom, Charlie (1984). *Industrispionage*. Stockholm: Timbro.

Peczenik, Aleksander, *Rätt och moral*, SvJT 1982 s. 609.

Peczenik, Aleksander, *Rättsordningens struktur*, SvJT 1974 s. 369.

Sandgren, Claes (2018). *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*. Fjärde upplagan Stockholm: Norstedts Juridik.

Sandgren, Claes (2007). Juridikavhandlingar vid Stockholms universitet 1957–2006, *ingår i Juridiska fakulteten 1907–2007. En minnesskrift (2007)*, s. 440–485.

Sandberg, Claes, *Är rättsdogmatiken dogmatisk?,* TfR 2005 s. 648.

Sandgren, Claes & Andersson, Anderz (red.) (1995). *Kunskapsföretaget i ett rättsligt perspektiv: [bolagsrätt, arbetsrätt, familjerätt, immaterialrätt, avtalsrätt, köprätt, skadeståndsrätt, skatterätt]*. 1. uppl. Stockholm: Fritze.
Schelin, Johan (2018). *Kritiska perspektiv på rätten*. [Stockholm]: Poseidon Förlag.

Strömholm, Stig, *Något om sociologins betydelse för juridiken*, SvJT 1970 s. 97–125.

Svensson, Eva-Marie, *De lege interpretata – om behovet av metodologisk reflektion*, Juridisk publikation, jubileumsnummer 2014, s. 211–226.

Svensson, Tommy (2011). *Lönsam säkerhetsjuridik: om konsten att skydda sig själv och sina tillgångar*. 5. omarb. utg. Hässelby: M I J media.

Wahlgren, Peter (2014). *Manipulation – ny strategi för skattelagstiftaren?*, Ingår i: Skattelagstiftning: att lagstifta om skatt / [ed] Anders Hultqvist, Peter Melz, Robert Påhlsson, Stockholm: Norstedts Juridik AB, 2014, s. 33–43.

Wainikka, Christina (2010). *Företagshemligheter: en introduktion*. 1. uppl. Lund: Studentlitteratur.

Warkentin, Merrill, Willison, Robert, *Behavioral and policy issues in information systems security: the insider* threat, European Journal of Information Systems (2009), 18, p. 101–105.

Watson, Gavin, Ackroyd, Richard, Mason, Andrew & Seaman, Jim (2014). *Social Engineering Penetration Testing*. Syngress.

Övriga källor

Applegate, D. Scott. (2009). *Social Engineering: Hacking the Wetware!* Information Security Journal: A Global Perspective, 40-46.

Baker & McKenzie Study on Trade Secrets and Confidential Business Information in the Internal Market, MARKT/2011/128/D.

Bradshaw, S., Howard, N. P., *The Global Disinformation Order*, 2019 Global Inventory of Organised, Social Media Manipulation, University of Oxford, Oxford Internet Institute, Computational Propaganda Research Project.

Brå (2012). *Användningen av brottskoder. En kvalitetsstudie inom kriminalstatistiken*, <https://www.bra.se/download/18.1ff479c3135e8540b29800021266/1371914739137/2012_Anv_ndningen_av_brottskoder.pdf>, (hämtad 2020-05-02).

Brå (2016). *Bedrägeribrottsligheten i Sverige. Kartläggning och åtgärdsförslag*, <https://www.bra.se/download/18.358de3051533ffea5ea2ec64/1458044205141/2016_9_Bedrägeribrottsligheten_i_Sverige.pdf >, (hämtad 2020-04-02).

Brå (2015). *Brottsutvecklingen i Sverige fram till år 2015,* <https://www.bra.se/download/18.4a33c027159a89523b1b134e/1488273427834/8_Bedrageri.pdf>, (hämtad 2020-04-21), s. 171–189.

Brå (2019a). *Klassificering av brott. Anvisningar och regler*, <https://www.bra.se/download/18.7d27ebd916ea64de530d0ac/1576675852400/2019_Klassificering_av_brott_v8_0.pdf>, (hämtad 2020-04-02).

Brå (2019b). *Kriminalstatistik 2019. Anmälda brott. Slutlig statistik*, <https://www.bra.se/download/18.7d27ebd916ea64de5304e10e/1585653308304/Sammanfattning_anmalda_2019.pdf>, (hämtad 2020-04-03).

Robert B. Cialdini (2001). Scientific American. *The Science of Persu*, <https://digitalwellbeing.org/downloads/CialdiniSciAmerican.pdf>, (hämtad 2020-04-19).

Dagens industri (2019). *Mexico godkänner ”nya Nafta”*, <https://www.di.se/live/mexiko-godkanner-handelsavtalet-usmca/>, (hämtad 2020-01-29).

Europeiska kommissionen (2013). *COM (2013) 813 final*, <https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52013PC0813&from=EN >, (hämtad 2020-01-30).

EY (2018–2019). *Is cybersecurity about more than protection?*, <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf>, (hämtad 2020-04-17).

Falasca, Kajsa, Mikolaj, Dymek, & Grandien, Christina, (2019) *Social media election campaigning: who is working for whom? A conceptual exploration of digital political labour*, Contemporary Social Science, 14:1, p. 89-101, DOI:10.1080/21582041.2017.1400089.

Flores, Rocha, W. (2016). *Shaping Information Security Behaviors Related to Social Engineering Attacks,* <https://kth.diva-portal.org/smash/get/diva2:925493/FULLTEXT02.pdf>, (hämtad 2020-03-14).

Hogan Lovells (2012) International, Study on Trade Secrets and Parasitic Copying (Look-alikes), MARKT/2010/20/D: Report on Trade Secrets for the European Commission.

Investopedia (2020). *USMCA*, <https://www.investopedia.com/usmca-4582387>, (hämtad 2020-01-29).

Kommerskollegium (2019a) National Board of Trade Sweden, *Handelsrelationen mellan USA, Kanada och Mexico – En jämförande analys mellan USMCA och Nafta, CPTPP respektive EU:s frihandelsavtal*, <https://www.kommers.se/Documents/dokumentarkiv/publikationer/2019/Publ_Analys-av-USMCA.pdf>, (hämtad 2020-01-29).

Kommerskollegium (2017). Omförhandling av NAFTA och svenska företag i Mexico, <https://www.kommers.se/Documents/dokumentarkiv/publikationer/2017/publ-omforhandling-av-nafta.pdf>, (hämtad 2020-01-28).

Kommerskollegium (2019b) National Board of Trade Sweden, *TRIPS-avtalet i WTO,* <https://www.kommers.se/verksamhetsomraden/Handelsfragor/Immaterialratt/Utanfor-EU/TRIPS-avtalet-i-WTO/>, (hämtad 2020-01-27).

Mittuniversitetets forskningscenter (2018). DEMICOM, *Hur används sociala medier inför ett val*, <https://www.miun.se/Forskning/forskningscentra/demicom/nyheter/2018-4/hur-anvands-sociala-medier-infor-ett-val/>, (hämtad 2020-04-07).

MSB (2015), *Detta är informationssäkerhet*, <https://www.informationssakerhet.se/om-informationssakerhet2/vad-ar-informationssakerhet/>, (hämtad 2020-03-27).

MSB (2019a) *Informationssäkerhet, cybersäkerhet och säkra kommunikationer*, <https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/>, (hämtad 2020-04-01).

MSB (2018a), *Informationssäkerhet för små företag – rekommendationer för dig som driver eget företag med upp till 10 anställa*, <https://rib.msb.se/filer/pdf/28741.pdf>, (hämtad 2020-03-17).

MSB (2018b), *Rättsligt skydd för viss typ av information*, <https://www.informationssakerhet.se/lagar--regelverk/rattsligt-skydd-for-viss-typ-av-information/>, (hämtad 2020-03-23).

MSB (2019b), *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022*, <https://rib.msb.se/filer/pdf/28804.pdf>, (hämtad 2020-04-01).

MSB (2009) *Samhällets informationssäkerhet: lägesbedömning 2009*, <https://www.msb.se/RibData/Filer/pdf/24593.pdf>, (hämtad 2020-03-20).

Nationalencyklopedin, IT-säkerhet, <http://www.ne.se/uppslagsverk/encyklopedi/lång/it-säkerhet>, (hämtad 2020-03-30).

Nationalencyklopedin, manipulation, <http://www.ne.se/uppslagsverk/encyklopedi/lång/manipulation>, (hämtad 2020-04-14).

Nationalencyklopedin, NAFTA, <http://www.ne.se/uppslagsverk/encyklopedi/lång/nafta>, (hämtad 2020-01-29).

Nobicon (2015). *Competitive intelligence och annan begreppsförvirring*, <https://www.nobicon.se/nyheter/competitive-intelligence/>, (hämtad 2020-03-26).

Office of the United States Trade Representative, *United States – Mexico – Canada Agreement*, <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>, (hämtad 2020-01-29).

Pieters, W., Montoya, L., Bullee, J. H., Junger, M., & Hartel, P. (2015), *The persuasion and security awareness experiment: reducing the success of social engineering attacks*, Journal of Experimental Criminology, 11(1), 97. doi:10.1007/s11292-014-9222-7.

Polisen (2020). *Kraftfullare informationsåtgärder krävs för att minska bedrägeribrott mot äldre*, <https://polisen.se/aktuellt/nyheter/2020/februari/kraftfullare-informationsatgarder-kravs-for-att-minska-bedrageribrott-mot-aldre/>, (hämtad 2020-05-11).

Polisen (2016). Nationellt bedrägericenter, *Intressant just nu om bedrägerier*, <https://www.ekobrottsmyndigheten.se/Documents/NBC_Informationsblad_December_2016.pdf>, (hämtad 2020-04-12).

Rådets beslut 94/800/EG av den 22 december 1994 om ingående, på Europeiska gemenskapens vägnar – vad beträffar frågor som omfattas av dess behörighet – av de avtal som är resultatet av de multilaterala förhandlingarna i Uruguayrundan (1986–1994).

SCB (2019). *Digitalisering och säkerhet i svenska företag*, <https://www.scb.se/hitta-statistik/statistik-efter-amne/naringsverksamhet/naringslivets-struktur/it-anvandning-i-foretag/pong/statistiknyhet/it-anvandning-i-foretag-2019/>, (hämtad 2020-04-01).

Sentor, *Nätfiske/Phishing*, <https://www.sentor.se/kunskapsbank-it-sakerhet/natfiske-phishing/>, (hämtad 2020-04-15).

Svenska institutet för standarder, *Informationssäkerhet*, <https://www.sis.se/iso27000/informationssakerhet/>, (hämtad 2020-03-27).

SVT nyheter (2020). *Så fungerar vishing och social manipulation*, <https://www.svt.se/nyheter/lokalt/skane/sa-har-fungerar-vishing-och-social-manipulation>, (hämtad 2020-03-31).

Säkerhetspolisen, *Informationssäkerhet,*
<https://www.sakerhetspolisen.se/sakerhetsskydd/informationssakerhet.html
>, (hämtad 2020-03-27).

Säkerhetspolisen (2019). *Vägledning i säkerhetsskydd.*
Informationssäkerhet,
<https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c673/15
60952186689/Vagledning-Informationssakerhet.pdf>, (hämtad 2020-05-18).

The Wall Street Journal (2020). Canada Begins USMCA Ratification
Process That Won´t Necessarily Be Smooth Sailing,
<https://www.wsj.com/articles/canada-begins-nafta-ratification-process-
that-wont-necessarily-be-smooth-sailing-11580152748>, (hämtad 2020-01-
30).

Otryckta källor

Mailkorrespondens med företrädare för Brå, den 20 april 2020.

Rättsfallsförteckning

Rättsfall m.m.
Sverige

Högsta domstolen
NJA 2001 s. 362.

Svea Hovrätt
Svea hovrätt, dom den 20 oktober 2003, mål nr B 5221-03.