



JURIDISKA FAKULTETEN
vid Lunds universitet

Fredrik Jorstadius

Inspektion av elektroniskt lagrad information i dispositiva tviste- mål

En komparativ studie av on-site inspections av elektroniskt lagrad
information enligt Federal Rules of Civil Procedure och en analys
av editionspliktens gränser

Examensarbete
30 högskolepoäng

Handledare
Professor Peter Westberg

Ämnesområde
Processrätt/Avtalsrätt

Vårterminen 2010

Innehåll

SUMMARY	1
SAMMANFATTNING	3
FÖRORD	5
FÖRKORTNINGAR	6
1 INLEDNING	7
1.1 Introduktion	7
1.2 Syfte	7
1.3 Avgränsning	8
1.4 Metod och material	9
1.5 Disposition	10
1.6 Definitioner och terminologi	10
2 ON-SITE INSPECTIONS AV ELEKTRONISKT LAGRAD INFORMATION ENLIGT FEDERAL RULES OF CIVIL PROCEDURE	11
2.1 Allmänt om e-discovery	11
2.2 On-site inspections av elektroniskt lagrad information	13
2.3 Problem kopplade till on-site inspections av elektroniskt lagrad information	15
2.4 Under vilka omständigheter beviljas en inspektion av motpartens elektroniskt lagrade information?	18
2.4.1 Inspektion som kontrollmekanism	19
2.4.2 Tvistefrågans direkta koppling till elektroniskt lagrad information	21
2.5 Riktlinjer för inspektionen	23
2.5.1 Vem genomför inspektionen och under vilkas närvaro?	24
2.5.2 Hur bevaras orginalkällans äkthet vid insamling av elektronsikt lagrad information?	27
2.5.3 Inspektionens omfattning	29
2.5.4 Hur hanteras och granskas informationen på speglingen?	31
3 INSPEKTION AV ELEKTRONISKT LAGRAD INFORMATION INOM RAMEN FÖR EDITIONSPLIK TEN	36

3.1	Processuell editionsplikt	36
3.2	Materiell editionsplikt	36
3.2.1	Precisionkrav	38
3.2.2	Skriftlig handling	40
3.2.3	Bevis efter forskning	40
3.2.4	Verkställighet och vitesföreläggande	42
4	KONKLUSION OCH AVSLUTANDE SYNPUNKTER	44
	BILAGA A	46
	KÄLL- OCH LITTERATURFÖRTECKNING	61
	RÄTTSFALLSFÖRTECKNING	64

Summary

A party's ability to access electronic information stored on an opponent's hard disks – e.g. on a computer or on other electronic storage devices – has become increasingly challenging due to the technological development. In order to get hold of such information and to identify and/or recover deleted electronic information relevant to a dispute, parties sometime include an inspection clause in their agreement, giving one or both contracting parties the right to inspect the opponent's hard disks.

The purpose of this thesis is to analyze whether it is possible for a court to permit an inspection of an adversary's hard disks within the scope of a production order under Chapter 38 Swedish Code of Judicial Procedure (»rättegångsbalken»), especially focusing on Chapter 38 § 3, which recognizes the right for a party to move for a production order based on an agreement. The thesis will also discuss protocols for on-site inspections of hard disks, established by federal courts in the U.S. under the Federal Rules of Civil Procedure, in order to provide guidance for contracting parties when constructing an inspection clause.

The conclusion reached regarding American law, is that in the U.S., litigants are increasingly utilizing the tactic of moving for permission to inspect their adversary's computers. Federal courts have recognized that there are certain technical issues associated with on-site inspections of hard disks under Rule 34 Federal Rules of Civil Procedure and accordingly have set forth protocols to protect producing parties from e.g. destruction of data and invasion of privacy. Courts have established protocols, pursuant to which a computer expert extracts the raw electronic data in a way in which it can be verified and then allows the producing party to remove privileged, confidential, and unresponsive information that should not be produced. The producing party shall then produce to the adversary all responsive information that is properly discoverable.

The conclusion reached regarding Swedish law, is that an inspection clause gives party's access to different and more extensive information than the Swedish procedural rules governing document production permits. In other words, it is not possible for a Swedish court to allow a party to inspect an adversary's hard disks within the scope of a procedural production order (»processuell edition») under Chapter 38 § 2 Swedish Code of Judicial Procedure. In order to enforce an agreement including an inspection clause, a party can move for permission to inspect their adversary's hard disks within the scope of a production order based on an agreement under Chapter 38 § 3 Swedish Code of Judicial Procedure (»materiell edition»). In comparison with a procedural production order, it appears possible to enforce an inspection clause under Chapter 38 § 3.

Regardless of whether a motion to compel has been filed in an ongoing liti-

gation or if a claim is made regardless of a trial, the requirement for a party to specify the motion to compel or claim should be linked to the agreement and, it should be sufficient for a party to describe in the application for a summons, which agreement the production order should be based on, as long as the claim is as precise as Chapter 42 § 2 Swedish Code of Judicial Procedure requires.

Furthermore, no guarantees can be given that the designated computer expert will be able to assist KFM in the enforcement, or that other agreed upon terms for the inspection will be met, as KFM under Chapter 16 § 12 paragraph 3 Swedish Code of Dept Enforcement («utsökningsbalken»), has the power to reconsider and abandon the courts regulations if necessary.

Sammanfattning

Den tekniska utvecklingen har lett till att parts möjlighet att komma åt för tvisten relevant elektronisk lagrad information från motparten, blivit en allt större utmaning. För att komma sådan information förekommer det därför att parter ingår inspektionsavtal. Avtalen ger en eller båda avtalsparter rätt att genomsöka motpartens elektroniskt lagrade information, i syfte att identifiera och/eller återskapa raderade filer relevanta för tvisten.

I uppsatsen utreds dels huruvida en inspektion av motpartens elektroniskt lagrade information kan tillåtas inom ramen för editionsplikten. I utredningen riktas särskild uppmärksamhet mot att avgöra vilka verkningar en inspektionsklausul kan få inom ramen för den materiella editionsplikten. Dels utreds, i syfte att belysa viktiga aspekter som bör beaktas vid utformning av en inspektionsklausul, hur inspektioner av elektroniskt lagrad information läggs upp i USA enligt Federal Rules of Civil Procedure.

Gällande amerikansk rätt, där parter i allt större utsträckning ansöker om att få genomföra en inspektion av motpartens elektroniskt lagrade information, kan följande slutsats dras. Federala domstolarna har uppmärksammat att en inspektion av elektroniskt lagrad information är förknippad med särskilda risker, exempelvis att företagshemlig information röjs, att information manipuleras eller att mjukvaruapplikationer eller operativsystem äventyras om programvara används felaktigt. För att minimera riskerna kopplade till förfarandet har de federala domstolarna utarbetat särskilda riktlinjer, som generellt angett att en opartisk dataexpert ska insamla den elektroniskt lagrade informationen på ett sätt varpå insamlad data kan verifieras. Informationen ska sedan överlämnas till den »discoverysvarande» partens juridiska ombud, som genom en »privilege screening» sorterar bort irrelevant eller skyddad information, varefter dokumentationen överlämnas till motparten i digital form.

Den konklusion som nås gällande svensk rätt är att en inspektion av motpartens elektroniskt lagrade information, som närmast kan liknas vid en privat "husrannsakan", är något som den svenska rättegångsbalken inom ramen för processuell edition står främmande inför. Det synes dock möjligt för parter att genom fristående avtal – ett avtal som alltså ger part tillgång till annan och mer omfattande information än vad de processuella reglerna om informationsåtkomst medger – åstadkomma ett sådant långtgående tvångsmedel som en inspektionsklausul innebär, vilken kan genomdrivas genom ett editionsföreläggande enligt 38 kap. 3 § rättegångsbalken. Materiell edition präglas alltså inte av samma tankesätt som den processuella editionsplikten gällande inspektioner av motpartens elektroniskt lagrade information.

Någon garanti kan dock inte lämnas för att den av parterna utpekade dataexperten får biträda KFM vid verkställighet eller att det överenskomna tillvägagångssättet för inspektionen kommer att efterföljas, eftersom KFM enligt

16 kap. 12 § 3 stycket utsökningsbalken har befogenhet att ompröva och frångå domstols föreskrifter i exekutionstiteln om så behövs.

Oavsett om yrkandet framställs oberoende av rättegång eller om begäran om materiell edition framställs som en rättegångsfråga i en pågående process, bör preciseringskravet kopplat till 38 kap. 3 § rättegångsbalken vara uppfyllt om stämningsansökan innehåller tillräckliga upplysningar om den omständighet som utlöser editionsplikten. Preciseringskyldigheten får sedan bedömas mot bakgrund av den rättsliga grunden som editionsplikten vilar på, exempelvis ett avtal. Parts preciseringskyldighet måste dock ytterst avgöras av att yrkandet om vad svarande parten ska förpliktigas att göra eller tåla måste vara bestämt enligt 42 kap. 2 § rättegångsbalken.

Förord

Jag vill passa på att tacka alla som delat med sig av sina erfarenheter och hjälpt mig med att färdigställa denna uppsats. Ett särskilt tack vill jag rikta till John Daerr och Magistrate Judge Tim Baker, som lämnat värdefulla synpunkter beträffande amerikanska federala rättsreglers tillämpning. Ett varmt tack riktas dessutom till Peter Bayer, som bistått med information om hur inspektioner av datorer genomförs. Ett särskilt tack riktas även till Kevin Häggström, Gunnar Svedberg och min mormor Birgitta Börjesson, som hjälpsamt korrekturläst uppsatsen och kommit med givande synpunkter.

Jag vill slutligen ta tillfället i akt att tacka min handledare professor Peter Westberg, som bidrog till inspiration att skriva denna uppsats och som kommit med värdefulla råd under arbetets gång.

Göteborg i maj 2010

Fredrik Jorstadius

”Corruptissima re publica plurimae leges” - Tacitus

Förkortningar

Cardozo L. Rev.	Cardozo Law Review
E-discovery	Electronic discovery
Fed. Cts. L. Rev.	Federal Courts Law Review
Fed. R. Civ. P.	Federal Rules of Civil Procedure
FHL	Lag (1990:409) om skydd för företagshemligheter
J.L. Tech. & Pol'y	Journal of Law, Technology & Policy
JT	Juridisk Tidskrift vid Stockholms universitet
KFM	Kronofogdemyndigheten
Loy. L. Rev.	Loyola Law Review
Nat'l L.J.	The National Law Journal
NJA	Nytt Juridiskt Arkiv
Nw. J. Tech. & Intell. Prop.	Northwestern Journal of Technology and Intellectual Property Proposition
Prop.	Proposition
RICH. J.L. & TECH.	Richmond Journal of Law & Technology
Santa Clara Computer & High Tech. L.J	Santa Clara Computer & High Technology Law Journal
SOU	Statens Offentliga Utredningar
SvJT	Svensk Juristtidning

1 Inledning

1.1 Introduktion

I dagens samhälle lagras mer än 99 % av all information som skapas elektroniskt.¹ För att komma åt information som lagras elektroniskt, vilket p.g.a. den tekniska utvecklingen blivit en allt större utmaning, förekommer det att parter avtalar om tillgången till elektroniska informationskällor. Inspektionsklausuler² är ett exempel på en sådan avtalskonstruktion. En inspektionsklausul gällande elektroniskt lagrad information ger en eller båda avtalsparter rätt att genomöka motpartens datorer – inbegripet även andra externa lagringsenheter – i syfte att identifiera och/eller återskapa raderad elektronisk information relevant för tvisten (nedan »inspektion av rer»³). Förfarandet kan närmast liknas vid en 'privat husrannsakan' och ger part tillgång till annan och mer omfattande information än vad de processuella reglerna om informationsåtkomst medger. För svenskt vidkommande erbjuds genom materiell edition ett förfarande som täcker åtkomsten av informationskällor, som grundar sig på avtal. Det är dock svårt att finna några exempel på inspektionsklausuler i svensk domstolspraxis, trots att de i praktiken förekommer. För att erhålla kunskap om och förståelse för hur inspektioner av datorer lämpligen läggs upp för att minimera riskerna med förfarandet, flyttas blicken i denna framställning istället till de amerikanska federala rättsreglerna, Federal Rules of Civil Procedure (nedan »Fed. R. Civ. P.»). Enligt Rule 34 Fed. R. Civ. P. erbjuds nämligen part möjlighet att under vissa omständigheter genomföra en inspektion av motparten datorer. De federala domstolarna har, för att undvika de många problem och risker som finns kopplade till ett sådant förfarande, utarbetat särskilda riktlinjer för hur inspektionen lämpligen utformas.

1.2 Syfte

Det övergripande syftet med denna uppsats är tudelat. För det första eftersträvas att ge läsaren en god inblick i hur inspektioner av datorer enligt Federal Rules of Civil Procedure läggs upp för att minimera riskerna, som ett sådant förfarande kan medföra. Denna framställning syftar dock inte till att

¹ Isom, *Electronic Discovery Primer for Judges*, 1 Fed. Cts. L. Rev. 26 2006, s. 26.

² En inspektionsklausul betecknar i denna framställning ett avtal där parterna kommit överens om att en eller båda parter har rätt att, antingen själv eller genom utsedd dataexpert, genomföra en inspektion av motpartens datorer, i syfte att identifiera och/eller återskapa raderade filer relevanta för tvisten.

³ Med »inspektion av datorer» avses alltså i denna framställning en inspektion av meningsinnehållet i datorn, d.v.s. den elektroniskt lagrade informationen. Begreppet ska således inte sammanblandas med en inspektion av datorns fysiska beståndsdelar. Begreppet »dator» används i uppsatsen som ett samlingsbegrepp för samtliga digitala lagringsenheter vars hårddiskar kan bli föremål för inspektion, t.ex. en extern hårddisk, USB-minnen, mobiltelefoner e.d.

ge konkreta avtalsförslag, eftersom omständigheterna i varje enskilt fall avgör avtalsupplägget. Däremot är min förhoppning att läsaren genom uppsatsen kan få en god förståelse för vad parter bör beakta vid utformningen av inspektionsklausuler. För det andra syftar uppsatsen till att utreda och analysera huruvida ett yrkande om att genomföra en inspektion av motpartens datorer kan bifallas inom ramen för den svenska editionsplikten. I utredningen riktas särskild uppmärksamhet mot att avgöra vilka verkningar en inspektionsklausul kan få inom ramen för den materiella editionsplikten.

Syftet med uppsatsen är sålunda följande:

- Att beskriva och utreda hur »on-site inspections» av datorer läggs upp i USA enligt Federal Rules of Civil Procedure.
- Att utreda och analysera huruvida inspektioner av motpartens datorer tillåts inom ramen för den svenska editionsplikten, med särskilt fokus på materiell edition.

1.3 Avgränsning

Beträffande amerikansk rätt kommer denna framställning att begränsas till att enbart behandla »on-site inspections» av datorer enligt Federal Rules of Civil Procedure. Det bör dock påpekas att de delstatliga och de federala domstolarna i USA har sina egna »discoveryregler». Anledningen till att uppsatsen enbart kommer att behandla Federal Rules of Civil Procedure är att det federala regelverket i stor utsträckning tjänar som förebild för delstatliga regler. Uppsatsen kommer även att bortse från s.k. »local rules», som utfärdas av olika domsagor vid sidan av de delstatliga eller federala reglerna.

Uppsatsen avser inte att behandla »on-site inspections» inom ramen för traditionell »discovery», d.v.s. »discovery» av information som finns på papper, film eller annan typ av media, som kan läsas utan hjälp av en dator. Anledningen härför är att traditionell »discovery» på en fundamental nivå skiljer sig från »electronic discovery», både vad gäller hur förfarandet praktiskt genomförs samt vilka problem som finns kopplade till förfarandet. Andra aspekter av »electronic discovery» (d.v.s. utöver »on-site inspections» av datorer) kommer inte heller att beröras i uppsatsen, exempelvis skyldigheten att bevara information, olika proportionalitetsbedömningar, sanktioner när part försummat sina »discoveryförpliktelser» och »cost-shifting» frågor. I framställningen kommer de många olika problemområden, som finns kopplade till »discovery» av elektroniskt lagrad information inte heller att behandlas, exempelvis problem rörande omfång, sökbarhet, metadata, autenticitet, raderade data och resurskrav.

Beträffande svensk rätt kommer uppsatsen inte att behandla editionsplikten avseende allmänna handlingar. Framställningen kommer att begränsas till att enbart behandla möjligheten för part att inom ramen för editionsplikten

genomföra en inspektion av motpartens datorer. Andra aspekter av editionsplikten kommer alltså inte att beröras. I uppsatsen kommer både materiell och processuell edition att diskuteras. Rättsläget gällande parts möjlighet att genomföra en inspektion av motpartens datorer inom ramen för processuell edition är dock relativt väl klarlagt, varför detta område enbart kommer att behandlas i korthet. Den materiella editionsplikten ter sig mer öppen beträffande denna fråga, vilket ger skäl för en mer utförlig redogörelse. Gällande den materiella editionsplikten kommer uppsatsen enbart att behandlas utifrån en editionsplikt som grundas på civilrättsliga föreskrifter i ett avtal. Andra aspekter av den materiella editionsplikten, exempelvis *documentum commune*, kommer inte att avhandlas. Uppsatsen kommer heller inte att beröra reglerna om syn enligt 39 kap. rättegångsbalken, eftersom framställningen främst rör möjligheterna för part att erhålla 'meningsinnehållet' i datorer för att granska denna, vilket handlar om edition inte om exhibition.

Framställningen kommer vidare inte att diskutera reglerna i personuppgiftslagen. Läsaren bör dock uppmärksamma att en inspektion av datorer kan aktualisera bestämmelser i regelverket.

Uppsatsen kommer inte djupare att gå in på behandling av material, som innehas av tredje man eller information som är skyddad p.g.a. sekretess, exempelvis advokatsekretess eller liknande.

1.4 Metod och material

I den första delen av uppsatsen (avsnitt 2) försöker jag fastställa gällande amerikansk rätt genom att lagar, förarbeten, rättsfall, doktrin, ändamålssynpunkter etc. beaktas utifrån ett domstolsperspektiv.

I den andra delen av uppsatsen (avsnitt 3) utreder och analyserar jag gällande svensk rätt genom att lagtext, förarbeten, rättsfall, doktrin, ändamålssynpunkter etc. beaktas på det sätt, som domstolarna och då främst HD kan förväntas göra. Analysen utgår följaktligen från ett domarperspektiv.

Jag har eftersträvat ett brett och gediget underlag för mina slutsatser. Det amerikanska perspektivet har naturligen krävt flitigt användande av amerikansk litteratur och rättspraxis. Härvid förtjänar *Electronic Discovery: Law and Practice* av Cohen och Lender ett särskilt omnämnande. Det finns en riklig tillgång på fall, som angår »on-site inspections» av datorer i amerikansk federal domstolspraxis. Härvid har jag valt att behandla de som jag bedömt vara mest betydelsefulla eller som av andra skäl varit intressanta för att belysa viktiga aspekter av federal rättstillämpning.

1.5 Disposition

Avsnitt 2 behandlar hur »on-site inspections» av datorer enligt Federal Rules of Civil Procedure läggs upp. Syftet är att ge läsaren en god förståelse för vilka problem som finns kopplade till en inspektion av motpartens datorer, när en sådan inspektion tillåts av de federala domstolarna och hur inspektionen läggs upp för att minimera riskerna. Avsnittet är i stor utsträckning av deskriptiv karaktär.

I avsnitt 3 utreds och analyseras rättsläget beträffande huruvida en inspektion av datorer kan tillåtas inom ramen för editionsplikten. I avsnittet behandlas både processuell och materiell edition.

Uppsatsen slutförs med en konklusion och avslutande synpunkter i avsnitt 4.

1.6 Definitioner och terminologi

I denna framställning kommer aktuella amerikanska termer att användas av främst två skäl. Det kan för det första vara svårt att översätta juridiska begrepp, i synnerhet när ett institut saknar en motsvarighet i det andra språket. För det andra kan det vara fördelaktigt för svenska jurister, som allt oftare kommer i kontakt med amerikanska förfaranden att stifta bekantskap med den ursprungliga terminologin.

I uppsatsen kommer termen »discoverysvarande» att användas för att beteckna vad som i USA kallas för »the producing party» och »discoverysökande» för att beteckna »the requesting party».

Beträffande svensk editionsplikt kommer begreppen »editionssökande» och »editionssvarande» användas, eftersom både käranden och svaranden kan begära ut information från den andra parten i processen.

Med »inspektion av datorer» avses i denna framställning en inspektion av meningsinnehållet i datorn, d.v.s. den elektroniskt lagrade informationen. Begreppet ska således inte sammanblandas med en inspektion av datorns fysiska beståndsdelar. Begreppet »dator» används i uppsatsen som ett samlingsbegrepp för samtliga digitala lagringsenheter vars hårddiskar kan bli föremål för inspektion, t.ex. en extern hårddisk, USB-minnen, mobiltelefoner e.d.

2 On-site inspections av elektroniskt lagrad information enligt Federal Rules of Civil Procedure

2.1 Allmänt om e-discovery

Den 1 december 2006 trädde *the 2006 amendments to the Federal Rules of Civil Procedure* i kraft i de federala domstolarna i USA. De nya federala rättsreglerna⁴ är ämnade att bemöta de många unika problem⁵ som är kopplade till »electronic discovery»⁶ (nedan »e-discovery»), exempelvis problem rörande omfång, sökbarhet, metadata, autenticitet, raderade data, skyldigheten att bevara information och resurskrav. De nya rättsreglerna utgör en produkt av en process, som pågick under flera år där privata organisationers utarbetade riktlinjer, med *The Sedona Principles* i spetsen, kom att spela en central roll.⁷

Rule 34(a) Fed. R. Civ. P. klargör att »electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations – stored in any medium from which information can be obtained» kan bli föremål för »discovery».⁸ Regeln syftar genom sin formulering till att omfatta en mängd olika typer av

⁴ Federal Rules of Civil Procedure kan laddas ner från www.uscourts.gov/rules/CV2009.pdf, hämtad 2010-05-14.

⁵ För en genomgång av de unika problem som är kopplade till »e-discovery» se exempelvis *The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 Nw. J. Tech. & Intell. Prop. 171 2005-2006, s. 171 ff och Withers, *Computer-Based Discovery in Federal Civil Litigation*, 1 Fed. Cts. L. Rev. 65 2006, s. 65 ff.

⁶ I Black Law Dictionary anges att »discovery» syftar till »[the c]ompulsary disclosure, at a party's request, of information that relates to the litigation.» »Discovery» kan således i enkelhet beskrivas, som rättsregler som tvingar en part att tillhandahålla eller överlämna information, som äger relevans som bevisning i en civilprocess. »E-discovery» innebär i »discovery» av elektroniskt lagrad information.

⁷ Se t.ex. *The Sedona Conference*, <http://www.thesedonaconference.org>, hämtad 2010-03-03, American Bar Association Section of Litigation, <http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf> hämtad 2010-03-03, National Conference of Commissioners on Uniform State Laws, <http://www.nccusl.org/update/committeeresearchresult.aspx?committee=248> hämtad 2010-03-03.

⁸ Innan 2006 års tillägg trädde ikraft, kunde en part enbart begära »e-discovery» av »documents». Begreppet medförde att vissa oklarheter uppstod beträffande om vissa typer av elektroniskt lagrad information omfattades, t.ex. dynamiska databaser. Se *The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s.11.

information lagrad på olika media, vilket tydligt klargörs i *The Committee Note*:

»Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common example often sought in discovery is electronic communications, such as e-mail. The rule covers [...] electronically stored information [...] 'stored in any medium,' to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.»⁹

Det vida begreppet »electronically stored information» (nedan »elektroniskt lagrad information») innefattar således i princip allt som kan lagras på ett datamedium, exempelvis omfattas e-post, hemsidor, ordbehandlingsfiler, ljud- eller videofiler, bilder, säkerhetskopior, databaser och raderade data.¹⁰ Tekniskt sett är all information som existerar på ett datamedium 'elektronisk' om informationen kan erhållas med hjälp av en dator. »E-discovery» skiljer sig på så vis från traditionell »discovery», där informationen finns lagrad på papper, film eller annan typ av media och kan erhållas utan en dators hjälp. Uttrycket »stored in any medium» innebär att en mängd olika typer av datamedia kan bli föremål för »e-discovery», alltifrån traditionella elektroniska media som datorer och servrar till föremål som iPhones, BlackBerrys, MP3-spelare, minneskort, externa hårddiskar, USB-minnen, flash-minnen, CD-ROM skivor, DVD-skivor, Internetbaserade röstbrevlådor (»voicemail») och framtida elektroniska media omfattas.¹¹

I detta sammanhang bör påpekas att det är viktigt att skilja på

- (a) huruvida viss information är föremål för »discovery» i enlighet med Rule 34(a) Fed. R. Civ. P. och
- (b) huruvida informationen bör tillhandahållas eller lämnas ut.¹²

⁹ The Committee Note to the 2006 amendments to Rule 34(a) Fed. R. Civ. P. (kurs här).

¹⁰ Viktigt att notera i detta sammanhang är att raderad information ofta beaktas »not reasonably accessible» i enlighet med 2006 års tillägg till Rule 26(b)(2)(B) Fed. R. Civ. P. vilket innebär att en proportionalitetsprövning måste göras, en s.k. »good cause inquiry», för att bedöma huruvida informationen ska omfattas av den »discoverysvarande» partens »discoveryförpliktelser». Se The Committee Note to Fed. R. Civ. P. 26(b)(2). Se även *Ameriwood Industries, Inc., v. Liberman, et al.*, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006) där domstolen bedömde att begärd inspektion avsåg information som var »not reasonably accessible» i enlighet med Rule 26(b)(2)(B). Efter att ha genomfört den s.k. »good cause inquiry» bedömde domstolen att inspektionen ändå skulle beviljas.

¹¹ Fliegel & Entwisle, *Electronic Discovery in Large Organizations*, 15 Rich. J.L. & Tech. 1 2008-2009, s. 3 och *The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s. 1 och s. 11.

¹² The Committee Note to the 2006 amendments to Rule 34(a) Fed. R. Civ. P., *The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s. 1 och Withers, *Electronically Stored Information: The December 2006*

Den senare frågan måste avgöras mot bakgrund av Rule 26(c) och 34(b) Fed. R. Civ. P. samt de proportionalitetsbedömningarna som regleras i Rule 26(b) Fed. R. Civ. P. I nämnda regler anges bl.a. att den »discoverysvarande» parten inte genom förfarandet ska utsättas för »undue burden», »expense[s]», att skyddad information röjs eller bli tvingad att framställa information som är »not reasonably accessible». ¹³ Dessa proportionalitetsbedömningar kommer dock inte närmare att beröras inom ramen för denna uppsats.

Parterna har vidare en skyldighet att i ett så tidigt skede av processen som möjligt träffas för att diskutera och försöka enas kring olika »discoveryfrågor». I samband med mötet ska parterna bl.a. utarbeta en »discovery plan» som ska behandla när obligatorisk »disclosure» ska äga rum, vilken information som är föremål för kommande »discoveryförfaranden», tidsschema, på vilket sätt informationen ska tillhandahållas, behovet av domstolsbeslut som begränsar eller modifierar skyldigheterna enligt lag samt behovet av andra domstolsbeslut som kan komma att krävas i »discoveryförfarandet». ¹⁴ »Discovery» sker normalt utan domstolens inverkan. Domstolens medverkan kan dock vara nödvändig om en part ställer obefogade krav på motparten eller om en part försummar sina »discoveryförpliktelser».

I enlighet med 34(a) Fed. R. Civ. P. kan en part begära att viss elektroniskt lagrad information ska överlämnas – om inte annat avtalats mellan parterna ska informationen överlämnas i ett i enlighet med Rule 34(b)(2)(E) Fed. R. Civ. P. godtagbart format ¹⁵ – eller tillhandahållas för inspektion hos motparten, en s.k. »on-site inspection». ¹⁶

2.2 On-site inspections av elektroniskt lagrad information

I amerikanska tvistemål har ansökningar om få genomföra »on-site inspections» av motpartens datorer blivit ett allt vanligare inslag. Den främsta anledningen till att parter i amerikanska civilmål i allt större utsträckning begär att få genomföra inspektioner av motparters datorer är möjligheten att identifiera och/eller återskapa raderad information relevant för tvisten, exempelvis raderade e-postmeddelanden, som motparten försökt dölja eller förstöra. Moderna datorer innehåller normalt hårddiskar med flera hundratal

Amendments to the Federal Rules of Civil Procedure, *Northwestern Journal of Technology and Intellectual Property* 2006, s. 199.

¹³ Rule 26(b) Fed. R. Civ. P. Se även Cohen & Lender, *Electronic Discovery: Law and Practice*, 10-4 f.

¹⁴ Rule 16(b), 26(f) och 34(b) Fed. R. Civ. P. Se även Friedenthal, Kane & Miller, *Civil Procedure*, s. 420.

¹⁵ Rule 34(b)(2)(E) Fed. R. Civ. P. stadgar att informationen ska överlämnas in »a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms».

¹⁶ Georg, *Someone's watching: Protecting privilege on both sides of the table during electronic discovery*, 2004 *J.L. Tech. & Pol'y* 283 2004, s. 286 f. och Withers, *Computer-Based Discovery in Federal Civil Litigation*, 1 *Fed. Cts. L. Rev.* 65 2006, s. 78.

gigabytes lagringsutrymme, vari information finns lagrad som i många fall enbart är tillgänglig för en dataexpert.¹⁷

En »on-site inspection» av datorer innebär att en part eller neutral expert får tillträde till motpartens lokaler för att på plats genomföra en inspektion och/eller skapa en spegling (»mirror image»)¹⁸ av motpartens hårddiskar, datasystem eller annan digital media som är föremål för »discovery», för att söka efter viss elektronisk data med tillhörande metadata¹⁹. Omfattningen av en »on-site inspection» kan följaktligen variera, inspektionen kan innebära allt från att en enskild dator speglas till att en full forensisk undersökning av ett helt nätverk genomförs.²⁰

I de federala domstolarna kan rätten att genomföra en »on-site inspection» härledas till Rule 34 Fed. R. Civ. P. I 2006 års tillägg till Rule 34 anges uttryckligen att elektroniskt lagrad information kan bli föremål för en inspektion genom »testing» och »sampling».²¹ I *The Committee Note* anges dessutom att:

»Rule 34(a)(1) is also amended to make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying them. That opportunity may be important for both electronically stored information and hard-copy materials. The current rule is not clear that such testing or sampling is authorized; the amendment expressly provides that such discovery is permitted.»²²

Redan innan tilläggen trädde i kraft 2006 ansågs dock en »on-site inspection» av motpartens datorer omfattas av Federal Rules of Civil Procedure. Rule 34(a) Fed. R. Civ. P. gav tidigare en part rätt att kopiera och inspektera »documents and things» från motparten. 1970 års tillägg till Federal Rules of Civil Procedure stadgade att »[t]he inclusive description of 'documents' is revised to accord with changing technology.»²³ Rule 34(b) Fed. R. Civ. P. gav i sin tur part rätt att beträda motpartens lokaler i syfte att genomföra en inspektion, vilket i kombination med Rule 34(a) ansågs utgöra grund för en inspektion av motpartens datorer.²⁴ Den praxis som vuxit fram innan 2006

¹⁷ Cohen & Lender, *Electronic Discovery: Law and Practice*, 10-3.

¹⁸ En »spegling» innebär att datorns hårddisk kopieras. Detta kan ske genom att en andra hårddisk installeras eller genom att en extern hårddisk kopplas till datorn varefter ett dataprogram speglar (klonar) hårddisken. Ett annat sätt varpå en dator kan speglas är genom att temporärt avlägsna hårddisken från datorn och spegla den till en annan dators hårddisk. Se Cohen & Lender, *Electronic Discovery: Law and Practice*, 10-6.

¹⁹ Metadata är ett begrepp som kan uttryckas som »data om andra data», t.ex. e-postuppgifter om avsändare, mottagare, cc, bcc eller datum. Se Perhard, Lars, Något om elektronisk edition i tvistemål och skiljeförfarande, JT 2007-08, s. 401 f.

²⁰ Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2).

²¹ 34(a) Fed. R. Civ. P.

²² The Committee Note to the 2006 amendments to 34(a) Fed. R. Civ. P.

²³ The Committee Note to the 1970 amendments to 34(a) Fed. R. Civ. P. (kurs här).

²⁴ Se t.ex. *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000) och *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999).

års tillägg till Federal Rules of Civil Procedure har på många sätt varit vägledande för senare domstolsavgöranden.²⁵

2.3 Problem kopplade till on-site inspections av elektroniskt lagrad information

En oinskränkt »on-site inspection» av motpartens datorer kan ge upphov till en rad olika problem, varför det krävs att särskilda riktlinjer eller avtal utarbetas för att bemöta dessa (se nedan i kapitel 2.5). En uppenbar risk med en oinskränkt inspektion av datorer är att motparten kan få fri insyn och därmed få tillgång till information, som denne inte har rätt att granska eller insamla. Parterna har ofta en stark strävan efter att skydda för bolaget skyddsvärd information och begränsa motpartens tillgång till för tvisten irrelevant information. Sättet varpå elektronisk information lagras gör det dock ofta mycket svårt (i många fall omöjligt) att fullt ut skydda företags- eller yrkeshemlig information. En inspektion av exempelvis en jobbdator kan vidare leda till att för den anställda känslig eller personlig information insamlas eller granskas av motparten (exempelvis lösenord, bankinformation eller personliga e-postmeddelanden).²⁶ En inspektion av datorer kan dessutom leda till att »privileged information»²⁷ (t.ex. information som skyddas under »the attorney-client privilege» eller »the work product doctrine») röjs, varpå motparten kan få en inblick i processtaktiska överväganden och strategier.²⁸

En anledning till varför det är särskilt svårt att värja sig mot att motparten granskar skyddad eller för tvisten irrelevant information är den enorma

²⁵ Till detta ska dock läggas att senare domstolsavgöranden varit färgade av den förändring som 2006 års tillägg till Federal Rules of Civil Procedure innebar för tillämpning av Rule 26(b)(2)(B), som efter tilläggen reglerar att en proportionalitetsbedömning ska göras för att avgöra om part har rätt till information som är »not reasonably accessible». Cohen & Lender, *Electronic Discovery: Law and Practice*, 10-3.

²⁶ En granskning av för den anställda personlig eller känslig information kan dessutom leda till att integritets- eller personuppgiftsskyddande lagstiftning överträds. The Sedona Principles, *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s. 39.

²⁷ Det är framförallt genom »common law» som begreppet »privileged information» har definierats. Syftet är att skydda viss typ av information som är av särskild betydelse för parten. Två vanligt förekommande typer av information som skyddas är information som hänför sig till »the work product doctrine» och »attorney-client privilege». »The work product doctrine» skyddar i civilmål material som part förberett inför en kommande eller pågående rättegångsprocess. I Fed R. Civ. P. regleras »the work product doctrine» av Rule 26(b)(3), som stadgar att en part som huvudregel inte kan erhålla »discovery of documents and tangible things... prepared in anticipation of litigation or for trial». »Attorney-client privilege» skyddar (kuriosa: enda sedan Elisabeth I:s tid) kommunikation och dokument som upprättats mellan klient och advokat. Se vidare Georg, *Someone's watching: Protecting privilege on both sides of the table during electronic discovery*, 2004 J.L. Tech. & Pol'y 283 2004, s. 288 f och Cohen & Lender, *Electronic Discovery: Law and Practice*, 7:4 ff och 8:5 ff.

²⁸ Withers, *Computer-Based Discovery in Federal Civil Litigation*, 1 Fed. Cts. L. Rev. 65 2006, s. 76.

mängden material som omfattas av en inspektion av en dator. Som exempel kan nämnas att den initiala genomsökningen av två jobbdatorer i rättsfallet *Northwest Airlines, Inc. v. Local* resulterade i information motsvarande 75,200 sidors pappersutskrift. ²⁹

En inspektion av motpartens datorer har även lett till en rad unika problem som traditionell pappersbaserad discovery inte gav upphov till. Med hjälp av olika typer av dataprogram kan den »discoverysvarande»³⁰ parten lättare övervaka och dokumentera vad den »discoverysökande»³¹ parten har använt för sökord och vilka dokument som granskats eller kopierats, s.k. »electronic eavesdropping» och »keystroke and command logging». Genom att identifiera vilka dokument som granskats och vilka sökord som använts kan den »discoverysvarande» parten avslöja och analysera motpartens processstrategier, vilket kan leda till att reglerna om »the attorney-client privilege» och »the work product doctrine» kringgås. ³²

En inspektion av motpartens datorer kan även orsaka störningar i den pågående verksamheten. Det går inte att jämföra en inspektion av pappersutskrift i ett konventionellt arkivrum – vilket sällan påverkar den pågående verksamheten – med en inspektion av datorer. För att kunna genomföra en inspektion eller en spegling av en hårddisk krävs i vissa situationer att den pågående verksamheten tillfälligt avbryts. ³³ När inspektionen avser mer komplicerade datasystem, exempelvis nätverk eller e-postservrar, kan det även hända att systemen eller olika applikationer skadas eller på annat vis äventyras om programvaror används felaktigt. ³⁴

Vid en inspektion finns också en risk att data manipuleras eller förstörs av den »discoverysökande» parten, dennes representanter eller anlita expert. ³⁵ Ett bra exempel på denna problematik är rättsfallet *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*, som gällde otillåtet röjande av företags-hemlig information. Käranden lade fram bevis som tydde på att svaranden, efter att processen inletts, förstört elektroniskt lagrad information relevant för tvisten. Käranden beviljades därav rätten att inspektera och kopiera filer på motpartens datorer. ³⁶ Inspektionen genomfördes av en anlita dataexpert

²⁹ *Northwest Airlines, Inc. v. Local* 2000, Int'l Bd. of Teamsters, No. Civ. 00-08 (DWF/AJB) (D. Minn. Feb. 2, 2000).

³⁰ Med den »discoverysvarande» parten avses i denna framställning den part som förpliktas att framställa information (»producing party»).

³¹ Med den »discoverysökande» parten avses i denna framställning den part som begär viss information av motparten (»requesting party»).

³² Georg, *Someone's watching: Protecting privilege on both sides of the table during electronic discovery*, 2004 J.L. Tech. & Pol'y 283 2004, s. 290.

³³ Withers, *Computer-Based Discovery in Federal Civil Litigation*, 1 Fed. Cts. L. Rev. 65 2006, s. 77.

³⁴ Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2) och *The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s. 39.

³⁵ Withers, *Computer-Based Discovery in Federal Civil Litigation*, 1 Fed. Cts. L. Rev. 65 2006, s. 76.

³⁶ *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*, 167 F.R.D. 90 (D. Colo. May 1, 1996), s.100.

som bland annat försökte återskapa raderad information från motpartens datorer. Dataexperten använde dock ett program som slumpmässigt skrev över 7-8 % av informationen lagrad på datorn, vilket resulterade i att informationen raderades för gott. Dataexperten genomförde dessutom insamlingen och kopieringen av filerna i strid med de standardmetoder som utarbetats för bevaring och insamling av databevis. Följden blev att kärandens begäran om att svaranden skulle drabbas av sanktioner för bevisförstörelse avlogs, trots att bevis på sådan förstörelse dokumenterats vid inspektionen.³⁷

Eftersom elektroniskt lagrad information generellt sett är lätt att manipulera kan dessutom svåra bevisvärderingsfrågor uppstå om äktheten av insamlad data ifrågasätts, särskilt om data insamlats utan beaktande av utarbetade standardmetoder.³⁸

Sammanfattningsvis kan konstateras att »on-site inspections» av motpartens datorer kan skapa problem såsom:

- att yrkeshemligheter avslöjas,
- att företagshemligheter eller annan konfidentiell eller privat information röjs, t.ex. personalutvärderingar, löneinformation eller annan för de anställda känslig information,
- att information som omfattas av »the attorney-client privilege» eller »the work doctrine» röjs,
- att orimliga störningar uppstår i den pågående affärsverksamheten,
- att stabiliteten hos operativsystem, mjukvaruapplikationer och elektroniska filer äventyras om programvaror används felaktigt,³⁹
- att information manipuleras,⁴⁰ eller
- att strategier avslöjas genom »electronic eavesdropping» eller »keystroke and command logging».⁴¹

³⁷ Gates Rubber Co. v. Bando Chemical Industries, Ltd., 167 F.R.D. 90 (D. Colo. May 1, 1996), s. 112.

³⁸ Cohen & Lender, Electronic Discovery: Law and Practice, 6-4 ff och Perhard, Lars, Något om elektronisk edition i tvistemål och skiljeförfarande, JT 2007-08, s. 406 f. Se även Lorraine v. Markel American Ins. Co., 241 F.R.D. 534 (D. Md. May 4, 2007) som behandlar olika autencitetsproblem som elektroniskt lagrad information kan medföra.

³⁹ The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production, s. 39.

⁴⁰ Withers, Computer-Based Discovery in Federal Civil Litigation, 1 Fed. Cts. L. Rev. 65 2006, s. 76.

⁴¹ Georg, Someone's watching: Protecting privilege on both sides of the table during electronic discovery, 2004 J.L. Tech. & Pol'y 283 2004, s. 290.

2.4 Under vilka omständigheter beviljas en inspektion av motpartens elektroniskt lagrade information?

I ett »discoveryförfarande» tillåts normalt parterna själva att framställa och överlämna begärd information. I jämförelse härmed kan en »on-site inspection» av motpartens datorer sägas utgöra ett omvänt förfarande och är i regel ett undantag när det gäller »discovery» av elektroniskt lagrad information.⁴² I *The Committee Note* nämns särskilt att Rule 34(a) Fed. R. Civ. P. inte är ämnad att ge en part en »routine right of direct access to a party's electronic information system» och att domstolarna bör vara särskilt vaksamma för »undue intrusiveness» vid sådana inspektioner.⁴³

Likväl finns situationer då en »on-site inspection» av motpartens datorer kan rättfärdigas och tillåtas. I de federala domstolarna har »on-site inspections» beviljats när den »discoverysökande» parten visat att »the burden and intrusion are justified by the need»⁴⁴ och

(a) när det förekommer bevisning som tyder på att den »discoverysvarande» parten inte fullgjort sina »discoveryförpliktelser», genom att denne exempelvis undanhållit eller raderat för tvisten relevant information⁴⁵ eller

⁴² The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production, s. 39 och Catlin, How Private Is the Home Computer?, Minnesota Public Radio, http://news.minnesota.publicradio.org/features/200002/08_catlinb_privacy/ hämtad 2010-05-11.

⁴³ The Committee Note to the 2006 amendments to Rule 34(a) Fed. R. Civ. P. (kurs här).

⁴⁴ Arent, Brownstone & Fenwick, Ediscovery: Preserving, requesting & producing electronic information, 19 Santa Clara Computer & High Tech. L.J. 131 2002-2003, s. 144 (kurs här). När domstolen gör denna bedömning beaktas ofta samma faktorer som vid den s.k. »good cause inquiry», nämligen: »(1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.» The Committee Note to Fed. R. Civ. P. 26(b)(2) (kurs här).

⁴⁵ Se t.ex. *ACMG of Louisiana, Inc. v. Towers Perrin, Inc.*, 2007 WL 4373604 (N.D. Ga. Dec. 11, 2007) där domstolen beviljade inspektion av motpartens hårddisk innehållande relevant information som flyttats, raderats eller på annat vis manipulerats från hårddisken; *Sims v. Lakeside School*, 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007) som behandlade en inspektion av en spegling av motpartens bärbara dator samt inspektion av e-postmeddelanden som skickats och mottagits via ett webbaserat e-postkonto.

(b) när den centrala tvistefrågan har ett nära samband med elektronisk information lagrad i de för målet aktuella datorerna.⁴⁶

En begäran om en »on-site inspection» beviljas dock inte i syfte att genomföra utpräglade s.k. »fishing expeditions».⁴⁷ En inspektion kommer således inte att beviljas om den ansökande parten enbart vill söka efter information utöver vad som begärts i partens »document request». Den ansökande parten bör därför ange vilket datasystem och vilken information som ska bli föremål för inspektion. Notera emellertid att parterna inom ramen för »discovery» kan begära att få granska information som i sin tur kan leda till relevant information – denna typ av bevis efterforskning är alltså tillåten.⁴⁸

2.4.1 Inspektion som kontrollmekanism

Har den »discoverysvarande» parten på ett övertygande sätt argumenterat för att den av parten överlämnade relevanta elektroniska informationen från datasystem och databaser varit fullgod för att partens »discoveryförpliktelser» skall anses uppfyllda, finns sällan någon grund eller rättsligt intresse att genomföra en »on-site inspection» i mål där den centrala tvistefrågan hänför sig till information lagrad på ett elektroniskt medium (d.v.s. inte själva datasystemet i sig).⁴⁹

I praxis förekommer dock att »on-site inspections» av motpartens datorer beviljas. Kravet i dessa fall är att det framkommit bevisning som visar eller tyder på att den »discoverysvarande» parten inte uppfyllt sina »discoveryförpliktelser» genom att parten antingen undanhållit eller raderat information som varit föremål för »discovery».⁵⁰ I *Simon Property Group L.P. v.*

⁴⁶ See exempelvis *Performance Chevrolet, Inc. v. Market Scan Information Systems, Inc.*, 2006 WL 980727 (D. Idaho April 11, 2006) vari domstolen beviljade en inspektion av motpartens datorer för att kontrollera huruvida ett datasystem användes felaktigt, *Ferron v. Search Cactus, L.L.C.*, 2008 WL 4458864 (S.D. Ohio April 28, 2008) där en inspektion av motpartens dator beviljades eftersom datorn innehöll »the only available documentary evidence of his visits to the websites at issue», *Cenveo Corp. v. Slater, et al.*, 2007 WL 442387 (E.D. Pa. Jan. 31, 2007) där en spegling av motpartens hårddisk beviljades »because of the close relationship between plaintiff's claims and defendant's computer equipment» och där karendens anspråk grundade sig på att datautrustningen används för att utnyttja »confidential information and trade secrets to divert business from plaintiff to defendants», *Frees, Inc. v. McMillian*, 2007 WL 184889 (W.D. La. Jan. 22, 2007) där domstolen beviljade speglingar med motiveringen att den saknade informationen sannolikt lagrats eller nedladdats på de i målet aktuella datorer, *In re Honza*, 242 S.W.3d 578 (Tex. App. Waco Jan. 2, 2008) där domstolen, i likhet med underinstansen, beviljade en inspektion av motpartens datorer genomförd av en dataexpert i syfte att finna vissa dokument och utkast med tillhörande metadata för att kunna fastslå när vissa ändringar av dokumenten skett.

⁴⁷ See t.ex. *Balfour Beatty Rail, Inc. v. Vaccarello*, 2007 WL 169628 (M.D. Fla. Jan. 18, 2007), p. *3 vari domstolen avtog karendens ansökan med motiveringen att karenden inte hade specificerat vad denne letade efter eller i vilket datasystem denne avsåg att genomföra varför inspektionen skulle vara en »fishing expedition».

⁴⁸ See exempelvis *McCurdy Group v. American Biomedical Group, Inc.*, 9 Fed. Appx. 822, 2001 WL 536974 (10th Cir. May 21, 2001), s. 831.

⁴⁹ *The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s. 39.

⁵⁰ Noteras kan att en part som bryter mot sina »discoveryförpliktelser» riskerar att drabbas av kraftiga sanktioner i rättegångsprocessen, vilket t.ex. rättsfallet *Lauren Corp. v. Century*

mySimon, Inc. beviljades exempelvis en inspektion av motpartens datorer med hänvisning till att käranden hade påvisat »some troubling discrepancies with respect to defendant's document production.»⁵¹ I målet Playboy Enterprises v. Welles beviljades kärandens begäran om att få inspektera svarandens hårddisk i syfte att återskapa e-postmeddelanden, vilka var högst relevanta för processen, som systematiskt raderats efter det att rättegångsprocessen inletts. Domstolen bedömde att svaranden inte vidtagit nödvändiga åtgärder för att bevara de aktuella e-postmeddelandena.⁵² I Illinois Tool Works, Inc. v. Metro Mark Prod. Ltd. beviljades ansökan efter det att motparten vid upprepade tillfällen lämnat icke trovärdiga och motsägelsefulla förklaringar till varför dennes datasystem inte kunde genomsökas efter relevant information.⁵³

En inspektion av motpartens datorer beviljas dock inte »just to adress the bare possibility of discovery misconduct», det räcker alltså inte med bevis av rent spekulativ karaktär.⁵⁴ Den ansökande parten måste lägga fram bevisning som visar på att »conventional discovery methods have failed to produce the information they need to litigate their case.»⁵⁵ Beviskravet är

Geophysical Corp., 953 P.2d 200 (Colo. App. Jan. 22, 1998), s. 200-202. väl exemplifierar. Svaranden hade i målet förstört all relevant hårdvara innan inspektionen ägde rum. Agerandet ledde till att domstolen presumerade att svaranden använt det i målet aktuell programvara på det vis käranden hävdade, vilket ledde till att svaranden förlorade målet. Se även t.ex. Minnesota Mining & Manufacturing Co. v. Pribyl, 259 F.3d 587 (7th Cir. 2001) och Communications Center, Inc. v. Hewitt, 2005 WL 3277983 (E.D. Cal. April 5, 2005).

⁵¹ Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639 (S.D. Ind. June 7, 2000), s. 641 (kurs här).

⁵² Playboy Enterprises v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999), s. 1053.

⁵³ Illinois Tool Works, Inc. v. Metro Mark Prod. Ltd., 43 F.Supp. 2d 951 (N.D. Ill. April 22, 1999).

⁵⁴ Diepenhorst v. City of Battle Creek, 2006 WL 1851243 (W. D. Mich. June 30, 2006) (kurs här). Se även t.ex. Bethea v. Comcast, 218 F.R.D. 328 (D.D.C. Dec. 3, 2003) vari i domstolen avslag ansökan med motiveringen att en ansökan i enlighet med Rule 34 Fed. R. Civ. P. måste påvisa att relevant information kan påträffas vid en inspektion och att det inte räcker med en »vague assertion» att information undanhållits och McCurdy Group v. American Biomedical Group, Inc., 9 Fed. Appx. 822, 2001 WL 536974 (10th Cir. May 21, 2001), s. 831 p. *7 där domstolen uttryckte att det inte var »sufficient to warrant such a drastic discovery measure» baserat på att svaranden var skeptisk till att käranden hade överlämnat all relevant och »non-privileged» material (i målet ville svaranden själv genomföra inspektionen, d.v.s. parten ville inte att en neutral utomstående expert skulle genomsöka motpartens datorer).

⁵⁵ Lawyers Title Ins. Corp. v. United States Fidelity & Guaranty Co., 122 F.R.D. 567 (N.D. Cal. Nov. 10, 1988) (kurs här). Se även t.ex. det omdebatterade målet In re Ford Motor Company, 345 F.3d 1315 (11th Cir. Sep. 22, 2003) där domstolen återförvisade målet efter att underinstanserna beviljat en Rule 34 Fed. R. Civ. P. ansökan, bl.a. med motiveringen att det inte fanns några bevis som tydde på att motparten försummat sina discovery-åligganden. Se vidare Williams v. Massachusetts Mutual Life Insurance Co., 226 F.R.D. 144 (D.C. Mass. Feb. 2, 2005), s. 146 »The court is similarly disinclined to allow Plaintiff to conduct the forensic study at his own expense. Before permitting such an intrusion into an opposing party's information system - particularly where, as here, that party has undertaken its own search and forensic analysis and has sworn to its accuracy - the inquiring party must present at least some reliable information that the opposing party's representations are misleading or substantively inaccurate. Here, Plaintiff has provided no reliable or competent information to show that Defendants' representations regarding the one "e-mail" are misleading or substantively inaccurate.»

högt ställt vilket domstolen i *Scotts Co. LLC v. Liberty Mut. Inc. Co.* uttryckte genom formuleringen:

»[i]n the absence of a strong showing that the responding party has somehow defaulted in his [discovery] obligation, the court should not resort to extreme, expensive, or extraordinary means to guarantee compliance.»⁵⁶

För det fall en part oavsiktligt misskött sina »discoveryförpliktelser» och den 'skada' som uppstått går att reparera, utgör det generellt inte en tillräcklig grund för en »on-site inspection».⁵⁷

Rule 34(a) Fed. R. Civ. P. kan följaktligen beskrivas som en slags kontrollmekanism som den »discoverysökande» parten kan använda sig av för att verifiera att denne erhållit all relevant information som parten är berättigad till inom ramen för »discovery».⁵⁸

2.4.2 Tvistefrågans direkta koppling till elektroniskt lagrad information

Generellt har de federala domstolarna varit mer benägna att bevilja en begäran om en »on-site inspection» av motpartens datorer när den centrala tvistefrågan har ett nära samband med elektronisk information lagrad i de för målet aktuella datorerna.⁵⁹

I *Performance Chevrolet, Inc. v. Market Scan Information Systems* tillät exempelvis domstolen att svaranden genomförde en inspektion av kändans datasystem. Kändanden hade i målet gjort gällande att svarandens programvara var behäftad med fel, mot vilket svarande invände att kändanden själv orsakat felet genom att programvaran använts på ett felaktigt sätt. Domstolen beviljade svarandens ansökan om att få genomföra en inspektion av aktuellt datasystem i syfte att identifiera relevant elektronisk information om hanteringen av programvaran.⁶⁰

Det förefaller även vara så att domstolar i större utsträckning, under särskilda omständigheter, beviljar inspektioner av datorer om förfarandet syftar till att inspektera finansiella handlingar eller data ur redovisningssystem.⁶¹

⁵⁶ *Scotts Co. LLC v. Liberty Mut. Ins. Co.*, 2007 WL 1723509 (S.D. Ohio June 12, 2007), p. *1-2.

⁵⁷ *Se t.ex. Butler v. Kmart Corp, et al*, 2007 WL 2406982 (N.D. Miss. Aug. 20, 2007), p. *3.

⁵⁸ Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2).

⁵⁹ *The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s. 39.

⁶⁰ *Performance Chevrolet, Inc. v. Market Scan Information Systems, Inc.*, 2006 WL 980727 (D. Idaho April 11, 2006).

⁶¹ *Se t.ex. Etzion v. Etzion*, 62 A.D.3d 646; 880 N.Y.S.2d 79 (2nd Dep't May 5, 2009). *Se även Adam I. & Lender, David J., Electronic Discovery: Law and Practice*, s. 10-9.

I de federala domstolarna har »on-site inspections» av datorer beviljats i särskilt stor utsträckning i mål där en f.d. anställd på ett otillåtet sätt använt eller spridit företags- eller yrkeshemlig information.⁶² I *Cenveo Corp. v. Slater* gjorde kändanden gällande att svaranden använt sin datautrustning för att sprida företags- och yrkeshemlig information till konkurrenter. Domstolen beviljade kändandens begäran om att få genomföra en inspektion av de i målet aktuella datorerna, trots att svaranden visat sig villig att genomföra begärd genomsökning, med hänvisning till »the close relationship between plaintiff's claims and defendant's computer equipment».⁶³

Det är dock inte säkert att det räcker med ett samband mellan tvistefrågan och aktuell datautrustning för att en begäran om en »on-site inspection» ska beviljas. I *Calyon v. Mizuho Securities USA Inc.*, som gällde ett påstått röjande av företags- och yrkeshemlig information, beviljade domstolen inte kändandens ansökan om att få genomföra en inspektion av motpartens datorer bl.a. med hänvisning till att inga »discrepancies or inconsistencies» kunnat påvisas i svarandens »discoveryförpliktelser». I många rättsfall gällande spridandet av företagshemligheter återkommer istället ett resonemang liknande det som domstolen förde i *Ameriwood Industries, Inc., v. Liberman, et al.*⁶⁴ I målet gjorde kändanden gällande att svarandena, f.d. anställda hos kändanden, använt och spridit företags- och yrkeshemlig information i syfte att skada kändandens affärsrelationer och knyta kändandens kunder till sitt eget bolag. Domstolen beviljade kändandens ansökan om att få genomföra en »on-site inspection» av motpartens datorer med hänvisning till (a) det nära sambandet mellan tvistefrågan och svarandens datorer samt (b) att det fanns fakta som antydde att svaranden inte fullgjort sina »discoveryförpliktelser».⁶⁵

En inspektion av motpartens datorer måste även genomföras på ett sätt så att båda parternas intressen kan tillgodoses.⁶⁶ En domstol kan således inte i enlighet med Federal Rules of Civil Procedure lämna tillstånd till en inspektion som är »overly broad, setting no parameters or limitations on the inspection of [...] computer system[s]».⁶⁷ Särskilda riktlinjer har därför utarbetats i praxis, vilka kommer att behandlas nedan i kapitel 2.5.

⁶² Cohen & Lender, *Electronic Discovery: Law and Practice*, 10-10.

⁶³ *Cenveo Corp. v. Slater, et al.*, 2007 WL 442387 (E.D. Pa. Jan. 31, 2007) (kurs här). Jfr dock med *Calyon v. Mizuho Sec. USA Inc.*, 2007 WL 1468889 (S.D.N.Y. May 18, 2007), p. *5 där en begäran om att få utföra en »on-site inspection» av motpartens datorer avslögs till följd av att motpartens gått med på att låta sin egen dataexpert genomföra begärd genomsökning och där domstolen inte hade någon »basis to question this representation».

⁶⁴ Cohen & Lender, *Electronic Discovery: Law and Practice*, 10-10.

⁶⁵ *Ameriwood Industries, Inc., v. Liberman, et al.*, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006). Se även *Equity Analytics, LLC v. Lundin*, 248 F.R.D. 331 (D.D.C. March 7, 2008) som gällde en tvist vari i svaranden använt sig av information från salesforce.com (svarandes f.d. arbetsgivare) för att kontakta befintliga och potentiella kunder till företaget. Domstolen beviljade efter ansökan av kändanden en spegling (*mirror image*) av motpartens dator.

⁶⁶ *The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s. 39.

⁶⁷ *Southern Diagnostic Association v. Bencosme, et al.*, 833 So. 2d 801 (Fla. Dist. Ct. App. 2002), s. 803 (kurs här). Se även *Strasser v. Yalamanchi*, 669 So.2d 1142 (Fla. 4th Dist. Ct.

2.5 Riktlinjer för inspektionen

För att förhindra att en part får mer eller mindre fri insyn i en mängd skyddad och för tvisten irrelevant information samt i syfte att undvika de många andra problem som inspektioner av datorer kan medföra (se t.ex. 'Gates Rubber'-situationen i kapitel 2.3 ovan), sluter parter särskilda avtal om hur förfarandet kring en »on-site inspection» av datorer ska läggas upp. I de fall parterna inte kan enas kring förfarandet för inspektionen utarbetas särskilda riktlinjer av domstolen, definierade i protokoll, men det står parterna fritt att genom avtal modifiera de av domstolen angivna riktlinjerna (om särskilt intresse finns för att närmare studera ett urplock av de riktlinjer som tillämpats av federala domstolar hänvisas till Bilaga A).⁶⁸

Den praxis som utvecklats i de federala domstolarna före 2006 års tillägg till Federal Rules of Civil Procedure har i många hänseenden varit vägledande även för senare avgöranden gällande »on-site inspections».⁶⁹ Den kompromisslösning som vuxit fram innebär generellt att:

- (a) en partsneutral dataexpert utses som genomför inspektionen, i ett flertal fall i egenskap av en »officer of the court»,
- (b) dataexperten skapar en spegling (»mirror image») av den digitala lagringsenhetens hårddisk,
- (c) med användning av dataforensiska verktyg granskar experten speglingen och återskapar raderade filer samt andra delar eller fragment av data,
- (d) med hjälp av sökprogram genomsöker dataexperten filerna med användning av förutbestämda sökkriterier (t.ex. nyckelordssökningar, sökningar efter filer som skapats mellan vissa datum eller av viss angiven person e.d.), som utarbetats av parterna i samråd med dataexperten för att identifiera för tvisten relevant information,
- (e) dataexperten sammanställer alla för tvisten relevanta filer i en databas eller på utskrivet papper varpå den »discoverysvarande» partens juridiska ombud granskar informationen och avlägsnar för tvisten irrelevant eller skyddad information,
- (f) den »discoverysvarande» parten överlämnar sedan »non-privileged» och för tvisten relevant information till motparten och

App. 1996), *rev. den.*, 805 so.2d 810 (Fla. 2001) vari domstolen, efter överklagande, ansåg att en »unfettered access» inte var tillåten.

⁶⁸ *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002), s. 432 »[t]he protocol [...] is necessarily only a set of guidelines, and the parties are free to add detail and otherwise modify the protocol agreement.»

⁶⁹ Cohen & Lender, *Electronic Discovery: Law and Practice*, 10-21.

- (g) kan parterna inte enas kring objektiva kriterier för vad som ska anses vara relevant information kan domstolen, med dataexpertens hjälp, i ett protokoll ange lämpliga kriterier.⁷⁰

Nedan kommer några centrala frågor att behandlas som är av vikt för parterna vid utformningen av avtal om »on-site inspections» av datorer. Det är särskilt viktigt att parterna angett (a) vem som ska genomföra inspektionen, (b) vilka som får närvara vid inspektionen, (c) datum och tid för inspektionen, (d) vilka datasystem som ska genomsökas eller speglas, (e) vem som ska genomföra själva speglingen, (f) hur speglingen får användas, (g) vilka som får lov att söka igenom speglingen, (h) sökord eller andra sökkriterier som anger omfattningen av inspektionen, (i) hur irrelevant och skyddad information ska hanteras, (j) hur tvister med anledning av inspektionen ska lösas (denna fråga kommer dock inte att närmare beröras i denna framställning), (k) hur speglingen eller andra kopior av insamlad information ska hanteras efter avslutad process och (l) andra typer av skyldigheter som parterna eller experterna har innan, under och efter inspektionen.⁷¹

2.5.1 Vem genomför inspektionen och under vilkas närvaro?

Sällan tillåts en part själv genomföra inspektionen av motpartens datorer, eftersom ett sådant förfarande skulle aktualisera de flesta av de i kapitel 2.3 behandlade problemen. I *In re: Triton Energy Ltd. Securities Litigation* nekades käranden att själv inspektera motpartens datorer med hänvisning till att en sådan inspektion »would potentially violate [defendant], employees, and outside directors right to privacy and privileges.»⁷² Inspektionen genomförs istället av en eller flera dataexperter.⁷³ Dataexperten utses normalt av antingen domstolen i enlighet med Federal Rules of Evidence 706 (dataexperten utses då i egenskap av »officer of the court») eller av parterna gemensamt. Påpekas kan att dataexperten inte bör agera rådgivare i juridiska spörsmål. Uppstår därför en situation som kräver juridisk kunskap bör parts juridiska ombud rådgöras.⁷⁴

⁷⁰ Withers, Computer-Based Discovery in Federal Civil Litigation, 1 Fed. Cts. L. Rev. 65 2006, s. 77.

⁷¹ Goldberg, Discovery and the Reluctant Host, 3/10/2008 Nat'l L.J.S1, (Col. 2) och Withers, Computer-Based Discovery in Federal Civil Litigation, 1 Fed. Cts. L. Rev. 65 2006, s. 77.

⁷² *In re: Triton Energy Ltd. Securities Litigation*, 2002 WL 32114464 (E.D. Tex. 7 mars 2002), s. 43 p. *6 (kurs här).

⁷³ Goldberg, Discovery and the Reluctant Host, 3/10/2008 Nat'l L.J.S1, (Col. 2)

⁷⁴ Cohen & Lender, Electronic Discovery: Law and Practice, 10-21 och Goldberg & McGowan, Electronic Discovery Behind Enemy Lines: Inspection Of An Adversary's Network Pursuant To Fed. R. Civ. P. 34(a), The Metropolitan Corporate Counsel, November 2007, s. 56 fotnot 5, <http://www.metrocorpocounsel.com/pdf/2007/November/56.pdf> hämtad 2010-04-12.

I *Playboy Enterprises, Inc. v. Welles*⁷⁵, som i många avseenden blivit ett vägledande mål för vilka riktlinjer som ska gälla vid »on-site inspections», gjorde käranden gällande att svaranden, en före detta anställd hos Playboy Enterprises, Inc., på ett otillåtet sätt använt sig av Playboys varumärke på sin hemsida. Efter att processen inletts fick käranden vetskap om att svaranden systematiskt raderade alla lästa och skickade e-postmeddelanden. I syfte att återskapa nämnda e-postmeddelanden ansökte käranden om få genomföra en »on-site inspection» för att kunna spegla Welles datahårdisk.⁷⁶ Domstolen bedömde att det fanns för tvisten relevant information på Welles dator (som användes för både privat bruk i svarandens affärsverksamhet) och förpliktade svaranden att tillhanda sin dator för inspektion. Riktlinjerna klargjorde att inspektionen skulle genomföras av en dataexpert som parterna i första hand skulle utse gemensamt. För det fall parterna inte kunde enas skulle domstolen utse experten, dock med beaktande av parternas förslag.⁷⁷ Den av domstolen eller parterna utsedda dataexperten skulle vidare agera i egenskap av »officer of the court».⁷⁸ Ofta anges även ett slutdatum för när parterna senast ska lämna in det gemensamma förslaget.⁷⁹

För att tillvarata båda parter intressen vid en inspektion av datorer – särskilt för att skydda den »discoverysvarande» parten från skadlig hantering av dennes datasystem samt partens rätt till »privacy and privileges» – förekommer det att domstolen utser en oberoende och partsneutral dataexpert.⁸⁰

I praxis har även förekommit att domstolen angett att den »discoverysökande» parten (i dessa mål har den »discoverysökande» parten ofta varit kärande part) ska utse dataexperten. I *Simon Property Group L.P. v. mySimon Inc.*⁸¹, där en »on-site inspection» beviljades i syfte att utreda huruvida svaranden agerat i ond tro vid val av firmanamn och logga, angav domstolen att käranden skulle utse dataexperten. Efter att käranden gjort sitt val skulle svaranden meddelas och ges möjlighet att invända mot valet.⁸² I ett flertal mål, i vilka den »discoverysökande» parten utsett dataexperten, har dock

⁷⁵ *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999).

⁷⁶ *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999) s. 1051.

⁷⁷ *Ibid.* s. 1055. Samma modell användes även i exempelvis *Coburn v. PN II, Inc.*, 2008 WL 879746 (D. Nev. March 28, 2008) och *Bank of Magnolia v. M & P Global Financial Services, Inc.*, 258 F.R.D. 514, 2009 WL 1117312 (S.D. Fla. April 24, 2009). Jfr även *Koo-sharem Corp. v. Spec Personnel, LLC*, 2008 WL 4458864 (D.S.C. Sept. 29, 2008).

⁷⁸ *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999), s. 1055. Se även *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), *Coburn v. PN II, Inc.*, 2008 WL 879746 (D. Nev. March 28, 2008) och *Bank of Magnolia v. M & P Global Financial Services, Inc.*, 258 F.R.D. 514, 2009 WL 1117312 (S.D. Fla. April 24, 2009).

⁷⁹ Se t.ex. *Coburn v. PN II, Inc.*, 2008 WL 879746 (D. Nev. March 28, 2008) och *Bank of Magnolia v. M & P Global Financial Services, Inc.*, 258 F.R.D. 514, 2009 WL 1117312 (S.D. Fla. April 24, 2009).

⁸⁰ *In re: Triton Energy Ltd. Securities Litigation*, 2002 WL 32114464 (E.D. Tex. 7 mars 2002) s. 43 (kurs här).

⁸¹ *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000)

⁸² Denna modell användes även i t.ex. *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002).

den »discoverysvarande» parten bara haft rätt att bli informerad om valet utan någon möjlighet att invände mot det.⁸³

Parterna bör lämpligen utse dataexperten med omsorg och eftertanke. Dataexpertens erfarenhet och expertis kan vara avgörande för hur väl inspektionen genomförs, särskilt med beaktande av att existerande standardmetoder för inspektioner av datorer inte är färdigutvecklade och dataexperter använder olika typer av programvara samt tillvägagångssätt för att genomföra inspektionerna.⁸⁴

Riktlinjerna eller avtalen bör även ange vilka som får lov att närvara vid inspektionen. För att minimera riskerna för att yrkes- eller företagshemlig information röjs anges vanligtvis att den »discoverysökande» parten eller dennes juridiska ombud inte har rätt att närvara vid inspektionen.⁸⁵ I sällsynna fall tillåts den »discoverysökande» partens ombud närvara vid inspektionen för att granska dokument, som identifierats vid en sökning med tillämpning av överenskomna sökkriterier (se kapitel 2.5.3 nedan), men då på en »attorneys'-eyes-only basis».⁸⁶

Ofta anges även att all kommunikation mellan den »discoverysökande» parten och utsedd dataexpert ska övervakas av den »discoverysvarande» parten, antingen genom att båda parter juridiska ombud närvarar vid mötena med experten eller genom att en kopia av e-postkommunikation översändes till den »discoverysvarande» partens ombud.⁸⁷

I enlighet med Rule 26(f) Fed. R. Civ. P. uppmanas parterna att utarbeta särskilda »protective orders» i syfte att skydda »privileged information» för det fall sådan information oavsiktligt överlämnats till motparten för granskning (s.k. »inadvertent production»).⁸⁸ Domstolarna har normalt angett att utsedd dataexpert ska underteckna de »protective orders» som är i bruk i målet samt andra typer av avtal ämnade att skydda företagshemlig eller annan skyddad information.⁸⁹ Avtal med dataexperten bör skraddarsys med

⁸³ Se exempelvis *The Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. April 29, 2002), *Ameriwood Industries, Inc., v. Liberman, et al.*, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006), *Frees, Inc. v. McMillian*, 2007 WL 184889 (W.D. La. Jan. 22, 2007), *Cenveo Corp. v. Slater, et al.*, 2007 WL 442387 (E.D. Pa. Jan. 31, 2007) och *Northwest Airlines, Inc. v. Local 2000*, No. Civ. 00-08 (DWF/AJB) (D. Minn. Feb. 2, 2000).

⁸⁴ *The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s. 40.

⁸⁵ Se t.ex. riktlinjerna som tillämpades i *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999), s. 1055.

⁸⁶ *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002).

⁸⁷ Se t.ex. *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), s. 642.

⁸⁸ Cohen & Lender, *Electronic Discovery: Law and Practice*, 2-28.8-21.

⁸⁹ Se exempelvis *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999), *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002) och *Cenveo Corp. v. Slater, et al.*, 2007 WL 442387 (E.D. Pa. Jan. 31, 2007).

beaktande av inspektionens omfattning för att i möjligaste mån undvika att skyddad information röjs.⁹⁰ För att ett erforderligt skydd ska uppnås är det viktigt att alla inblandade parter är väl införstådda i vilken information som är konfidentiell eller skyddad samt vem som får lov att granska informationen. Avtalen eller riktlinjerna bör därför noga ange vilken information (a) dataexperten, (b) den »discoverysökande» partens juridiska ombud samt (c) den »discoverysökande» parten har rätt att granska. Särskilda dataprogram har utvecklats som möjliggör att information kan märkas (t.ex. genom färgkodning) och enbart göras tillgänglig för granskning av viss angiven person.⁹¹

I regel anger även riktlinjer eller avtalen att dataexperternas och/eller den »discoverysökande» partens juridiska ombuds granskning av dokumenten inte en utgör en »waiver»⁹² av konfidentiell eller »privileged» information.⁹³

2.5.2 Hur bevaras originalkällans äkthet vid insamling av elektronsikt lagrad information?

Domstolarna har i riktlinjerna ofta angett att dataexperten (eller annan av parterna utsedd person) vid inspektionen ska skapa en spegling av de i målet aktuella hårdiskarna – lokaliserade i ett datamedium – med tillämpning av standardiserade dataforensiska metoder. Genom att spegla en hårdisk med tillämpning av sådana metoder kan äktheten av insamlad data verifieras.⁹⁴ En spegling innebär att hela hårdisken dupliceras, d.v.s. en identisk kopia skapas av varje bit, varje sektor, all allokerat och icke allokerat utrymme som såväl raderade filer.⁹⁵

Genom att tillämpa standardmetoden kallad »MD5 hashing» (vilket är en tids- och kostnadseffektiv kontrollmekanism inom en »de-duplication» pro-

⁹⁰ The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production, s. 53.

⁹¹ The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production, s. 40.

⁹² En »waiver» av privileged information innebär förenklat att parten, genom att t.ex. överlämna »attorney-client» skyddad information, avsagt sig sitt skydd. För en närmare genomgång se Cohen & Lender, *Electronic Discovery: Law and Practice*, 7.02[C], 7.05 och 8.05.

⁹³ Se exempelvis *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999), s. 1055, *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), s. 642 och *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002), s. 433.

⁹⁴ Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2).

⁹⁵ Raysman & Brown, *Examining Hard Drives During Discovery*, *Law Technology News*, <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=900005495808> hämtad 2010-03-25.

cess) kan de checksummor⁹⁶ (s.k. »hash values») som genereras vid speglingen användas för att kontrollera om minsta information ändrats (t.ex. om ett kommotecken ändrats i ett dokument). För att undvika tvister om insamlad informations äkthet bör bågge parterna känna till checksummorna för all speglad data.

Andra kontrollmekanismer finns även att tillgå beroende på vilken information inspektionen avser och var informationen finns lagrad. Avser inspektionen information om olika typer av nätverk kan parterna t.ex. avtala om att dela med sig av särskilda metadata för att verifiera äktheten av viss information. Oavsett vilken kontrollmekanism parterna avtalar om är det viktigt att båda parterna kan verifiera äktheten av viss information. Ofta kan utsedd dataexpert, som är väl insatt i denna problematik, föreslå lämpliga kontrollmekanismer skraddarsyddade för den enskilda situationen.⁹⁷

Genom att spegla hela hårddisken kan dataexperten analysera informationen och finna fragment eller hela raderade filer vilka potentiellt kan återskapas. Ofta speglas hårddiskar med hjälp av särskilt utvecklade programvara och hårdvara.⁹⁸

En förutsättning för att dataexperten ska kunna genomföra en inspektion av krypterade e-postklienter, såsom exempelvis Microsoft Outlook och IBM Lotus Notes, är att experten får tillgång till lösenord. Dataexperten kan vidare möta särskilda utmaningar när inspektionen avser e-postklienter som Yahoo, Hotmail, GMail e.d. För att få tillgång till hela användarens e-postlåda i sådana situationer krävs ofta att lösenord och användarnamn överlämnas till dataexperten.⁹⁹

Vid mindre komplicerade inspektioner finns det sällan någon anledning för parterna att ange att någon annan än utsedd dataexpert ska skapa speglingen

⁹⁶ En checksumma eller »hash value» är en algoritm som skapar elektroniska fingeravtryck av ett elektroniskt dokument. Se Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2).

⁹⁷ Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2) och Cohen & Lender, *Electronic Discovery: Law and Practice*, 9-10 f.

⁹⁸ Serverar kan ofta vara särskilt problematiska att kopiera till följd av mängden data som ofta lagras på dess hårddiskar. Generellt insamlas data genom att dataexperten skapar en »logical copy», med erforderliga tekniska parametrar för att bevara metadata, på en extern hårddisk med hjälp av särskilda kopieringsverktyg. Databaser innehåller många gånger relevant information för en tvist. Databaser kan kopieras, dock inte utan problem. Ofta är kopian läsbar enbart om den används på exakt samma hårdvara som den tidigare kördes på. Problemet kan dock lösas t.ex. genom att skicka en »static data output» från databasen till en annan databas som skapats i syfte att analysera informationen. För denna typ av analys krävs dock tillgång ett s.k. »database schema», vilket är datadiagram av databasens struktur and dess »tables». I många företag används idag e-postklienter såsom exempelvis Microsoft Outlook och IBM Lotus Notes. Flera alternativ står till buds för att extrahera hela e-postlådor. T.ex. kan ett av program kallat ExMerge utvecklade av Microsoft användas för att kopiera e-postlådor i .pst format, vilka kan granskas i t.ex. Microsoft Outlook. Viktigt att tänka på är att både Microsoft Outlook och IBM Lotus Notes lagrar »cache» filer i datorns användarmapp, vilket kan vara viktigt att ha i åtanke när inspektionens omfattning bestäms. Cohen & Lender, *Electronic Discovery: Law and Practice*, 9-3 ff.

⁹⁹ Cohen & Lender, *Electronic Discovery: Law and Practice*, 9-3 ff.

med beaktande av dataforensiska standardmetoder.¹⁰⁰ Avser däremot inspektionen komplicerade datasystem, är det av stor vikt att parterna noga överväger och specificerar vem som ska skapa speglingen. Riskerna att exempelvis ett nätverk eller en e-postserver skadas vid inspektionen – vilket potentiellt kan orsaka stora skador genom t.ex. produktionsstopp eller andra typer av störningar i den ordinarie verksamheten – är ofta alltför stora för att låta en utomstående dataexpert utföra speglingen. I dylika fall bör riktlinjerna eller avtalen ange att den »discoverysvarande» parten ska skapa speglingen under dataexpertens uppsikt och efter dennes direktiv.¹⁰¹

2.5.3 Inspektionens omfattning

Omfattningen av inspektionen bör vidare regleras i riktlinjerna eller avtalen. För att en ansökan om en »on-site inspection» ska beviljas krävs, som ovan nämnts, att den »discoverysökande» parten specificerar vad denne avser att inspektera. I kommersiella tvister avser inspektionen vanligtvis t.ex. e-postsystem, arkiverade e-postmeddelanden (t.ex. Outlook .PST¹⁰² filer), stationära och bärbara datorer, externa hårddiskar, mobiltelefoner, USB-minnen, nätverksservrar, delade mappar eller säkerhetskopior av olika slag. Inspektionen bör i möjligaste mån begränsas till att enbart avse de datamedia och de mapparna mest sannolika att innehålla information relevant för tvisten.¹⁰³ Ofta är IT-personalen på företagen bäst insatta i vilka delar av nätverken som används av olika personer. För att i möjligaste mån skydda mot att irrelevant eller skyddad information röjs, är det viktigt att kunskap om nätverken samt om var »non-discoverable» information finns lagrad förmedlas till den »discoverysvarande» partens juridiska ombud. Kunskapen kan användas av ombuden när riktlinjerna eller avtalen arbetas fram.¹⁰⁴

För att begränsa omfattningen av inspektionen bör olika sökkriterier användas för att identifiera relevant material och för att kunna sortera ut för tvisten irrelevant eller skyddad information.¹⁰⁵ Den enorma mängden data som inspektioner av datasystem generellt omfattar, gör det ofta nödvändigt för dataexperten att använda särskilda sökprogram utvecklade för att samla in och framställa »types of files reasonably likely to contain material potentially relevant to [the]case».¹⁰⁶ Relevant information kan identifieras genom exempelvis nyckelordssökningar (»keyword searches»), där sökningen kan

¹⁰⁰ Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2).

¹⁰¹ Goldberg & McGowan, *Electronic Discovery Behind Enemy Lines: Inspection Of An Adversary's Network Pursuant To Fed. R. Civ. P. 34(a)*, The Metropolitan Corporate Counsel, November 2007, s. 56.

¹⁰² .PST står för Microsoft Outlook Personal Folder File.

¹⁰³ Goldberg & McGowan, *Electronic Discovery Behind Enemy Lines: Inspection Of An Adversary's Network Pursuant To Fed. R. Civ. P. 34(a)*, The Metropolitan Corporate Counsel, November 2007, s. 56.

¹⁰⁴ Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2).

¹⁰⁵ The Sedona Principles, *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, s. 47 och *Northwest Airlines, Inc. v. Local 2000*, No. Civ. 00-08 (DWF/AJB) (D. Minn. Feb. 2, 2000).

¹⁰⁶ *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), s. 641 (kurs här).

avse t.ex. namn på nyckelpersoner, vissa angivna datumspann och annan terminologi, som kan relateras till ett specifikt skeende. Parterna bör i ett så tidigt skede av processen som möjligt enas (läs: i den ideala situationen) om särskilda sökmetoder och sökord som dataexperten ska använda vid inspektionen. Parterna bör dock hålla i åtanke att överenskomna sökmetoder och sökord lämpligen kan behöva ändras när mer kunskap om inspektionen erhålls i ett senare skede av förfarandet.¹⁰⁷ Sökmetoder och sökord bör utarbetas i samarbete med antingen utsedd dataexpert eller tillsammans med parternas egna anlidade dataexperter, då de besitter kunskap om olika tekniska aspekter av inspektionen som parterna ofta saknar. Ofta krävs även juridisk kunskap vid utformningen av sökmetoder och sökord varför parts juridiska ombud bör rådgöras.¹⁰⁸

För det fall parterna inte kan enas får domstolen i riktlinjerna bestämma hur och av vem sökmetoderna ska anges. I *Northwest Airlines, Inc. v. Local 2000* angav domstolen att dataexperten skulle använda sig av olika sökmetoder – utan att specificera någon särskild metod – för att identifiera relevanta ord, fraser, data, dokument, meddelanden eller fragment av dessa. Omfattningen av inspektionen begränsades till att enbart avse data upprättad mellan den 1 april 1999 och den 8 februari 2000.¹⁰⁹ I andra mål, exempelvis *Bank of Magnolia v. M & P Global Fin. Servs., Inc* och *Rowe Entertainment, Inc. v. William Morris Agency, Inc.* angav riktlinjerna istället att den »discoverysökande» parten skulle utarbeta särskilda sökkriterier, som skulle användas för att identifiera relevanta dokument. När sökkriterierna hade utarbetats skulle den »discoverysvarande» parten delges kriterierna, för att inom angiven tidsgräns kunna invända mot de sökmetoder motparten angett (t.ex. för att skydda viss konfidentiell information).¹¹⁰

För att dataexperten på förhand ska kunna planera och koordinera inspektionen är det viktigt att denne förses med teknisk och logistisk information om exempelvis nätverksstrukturer och lösenord. Riktlinjerna eller avtalen bör således reglera den »discoverysvarande» partens skyldighet att både innan och under inspektionen identifiera var och hur eftersökt elektronisk information lagras. Detta är särskilt viktigt när eftersökt information finns lagrad i delade mappar. Delade mappar innehåller ofta enorma mängder filer, vilket gör planeringen och samarbetet mellan parterna oerhört viktigt för att undvika kostsamma och betungande bördor för båda parterna. Denna information erhålles normalt genom diskussioner med »discoverysvarandens» IT-

¹⁰⁷ The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production, 2007, s. 57.

¹⁰⁸ Withers, Computer-Based Discovery in Federal Civil Litigation, 1 Fed. Cts. L. Rev. 65 2006, s. 78.

¹⁰⁹ *Northwest Airlines, Inc. v. Local 2000*, No. Civ. 00-08 (DWF/AJB) (D. Minn. Feb. 2, 2000).

¹¹⁰ Se exempelvis *Bank of Magnolia v. M & P Global Financial Services, Inc.*, 258 F.R.D. 514, 2009 WL 1117312 (S.D. Fla. April 24, 2009) och *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002).

personal eller genom intervjuer med de personer, som råder över de datorer eller datasystem inspektionen avser.¹¹¹

För att minimera olika slags störningar, som inspektionen kan medföra bör dessutom en ansvarig person utses, exempelvis den »discoverysvarande» partens egen dataexpert, som kan vidarebefordra olika ansökningar hänförliga till inspektionen till rätt part och person. Vidare bör en utsedd IT-person kontrollera att inga skador uppstått på inspekterade media. Har skador eller andra typer av störningar uppstått till följd av inspektionen bör dessa förtecknas, eftersom den »discoverysökande» parten i vissa situationer kan bli skadeståndsskyldig för skadorna eller störningarna.¹¹²

2.5.4 Hur hanteras och granskas informationen på speglingen?

När dataexperten skapat en spegling av i målet aktuella media, genomför dataexperten en analys av spegelkopian samt genomför sökningar med användning av de sökkriterier, som parterna eller domstolen angivit för att identifiera och eventuellt återskapa relevant information.¹¹³ I *Playboy Enterprises, Inc. v. Welles* angavs även, för det fall viss information inte kunde återskapas, att svarandens juridiska ombud skulle överlämna en rapport, undertecknad av dataexperten, som angav anledningarna till varför vissa dokument inte kunnat återskapas.¹¹⁴ I andra rättsfall har riktlinjerna även angett att den »discoverysvarande» partens juridiska ombud har rätt att få ta del av information om när en raderad fil återskapats, all tillgänglig information om dess innehåll samt information om vilka filer som inte kunnat återskapas.¹¹⁵

Det förekommer även att dataexperten måste förteckna vilken information som återskapats samt från vilka datorer informationen insamlats från (s.k. »chain of custody» dokumentation), vilket t.ex. kan vara av värde när inspektionen avser flera datorer.¹¹⁶

¹¹¹ Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2) och Goldberg & McGowan, *Electronic Discovery Behind Enemy Lines: Inspection Of An Adversary's Network Pursuant To Fed. R. Civ. P. 34(a)*, The Metropolitan Corporate Counsel, November 2007, s. 56. Se även t.ex. *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002).

¹¹² Goldberg, *Discovery and the Reluctant Host*, 3/10/2008 Nat'l L.J.S1, (Col. 2).

¹¹³ Se t.ex. *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002), s. 433, *Northwest Airlines, Inc. v. Local 2000*, No. Civ. 00-08 (DWF/AJB) supra notes 46-56 och infra notes 74-87 (D. Minn. Feb. 2, 2000) och *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), s. 641.

¹¹⁴ *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999), s. 1055.

¹¹⁵ Se t.ex. *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), s. 641.

¹¹⁶ *Northwest Airlines, Inc. v. Local 2000*, No. Civ. 00-08 (DWF/AJB) supra notes 46-56 och infra notes 74-87 (D. Minn. Feb. 2, 2000). Se även Cohen, Adam I. & Lender, David J., *Electronic Discovery: Law and Practice*, 6-39 f.

Gemensamt för alla riktlinjer gällande »on-site inspections» av datorer är att de anger att ingen information får överlämnas till den »discoverysökande» parten förrän den »discoverysvarande» partens juridiska ombud haft möjlighet att granska och sortera bort irrelevant eller skyddad information (s.k. »privilege screening».¹¹⁷ I praxis har även vikten av att »no employee of [the requesting party], or its counsel, will inspect or otherwise handle the equipment produced» betonats.¹¹⁸ Undantagsvis förekommer dock, som i *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, att den »discoverysökande» partens juridiska ombud fått lov att granska informationen innan en s.k. »privilege screening» ägt rum, men då på en »attorneys-eyes-only basis».¹¹⁹

Sättet varpå den av dataexperten identifierade relevanta informationen överlämnas till den »discoverysvarande» parten för granskning varierar. En metod är att informationen överförs till en särskild databas. På databasen installeras sedan särskilda »document review systems», som erbjuder omfattande verktyg för att hantera och granska informationen. Med hjälp av installerad programvara kan den »discoverysvarande» partens juridiska ombud bl.a. genomföra sökningar i metadata och dokument, färgkoda och klassificera dokument, markera eller stryka särskilda stycken i ordbehandlingsfiler, gruppera dokument efter klassificering eller färgkodning (t.ex. i listor, mappar e.d.). Därtill kan skannade dokument, e-postmeddelanden samt »voice-mail» t.ex. sammanföras och sparas på en gemensam plats. Genom att granska och klassificera informationen kan skyddad och irrelevant information sorteras bort eller på annat vis göras oåtkomlig för motparten.¹²⁰

Det förekommer dock att även andra metoder används. I *Simon Property Group L.P. v. mySimon Inc* angavs exempelvis att dataexperten skulle överlämna alla ordbehandlingsfiler, kalkylblad, e-postmeddelanden eller liknande i ett »reasonably convenient form», varefter de juridiska ombuden hade möjlighet att granska och sortera bort irrelevant eller skyddad information.¹²¹ I *The Antioch Co. v. Scrapbook Borders, Inc.* skulle utsedd dataexpert skapa två kopior av speglingen samt övrig insamlad data av »discoverysvarandenas» hårddiskar, varav en kopia skulle ges in till domstolen och den andra kopian skulle översändas till svarandena. De »discoverysvarande» parterna förpliktades sedan att genomsöka den data som de erhållit från ex-

¹¹⁷ Tvister hänförliga till klassificeringen av viss information, t.ex. klassificeringen »privileged», löses ofta genom en s.k. »in camera review». De omtvistade dokumenten översänds då till domaren som granskar dem, varefter domaren beslutar huruvida informationen behöver överlämnas eller inte. Se t.ex. *The Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. April 29, 2002).

¹¹⁸ *The Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. April 29, 2002) (kurs här).

¹¹⁹ *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002), s. 433.

¹²⁰ Cohen & Lender, *Electronic Discovery: Law and Practice*, 9-12 f.

¹²¹ *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), s. 641 (kurs här)

perten, för att identifiera relevant och efterfrågad information i enlighet med de av käranden framställda »document requests».¹²²

Ett något ovanligt upplägg användes i *In re: Triton Energy Ltd. Securities Litigation*. Den av domstolen utsedda dataexperten skulle identifiera och återskapa information från speglingarna av »discoverysvarandens» hårddiskar och servrar, för att sedan överlämna informationen till en i enlighet med Rule 53 Fed. R. Civ. P. utsedd »special master». »The special master» hade i uppdrag att granska överlämnad information i syfte att avgöra vilka dokument som »[bore] significantly on the claims and defenses» i processen.¹²³ En rapport om huruvida svaranden fullgjort sina »discoveryförpliktelser» skulle sedan sammanställas och översändas till domstolen tillsammans med ett utlåtande för att avgöra om ett »sanction hearing» skulle hållas.¹²⁴

Det förekommer att en »special master» utses i komplicerade »discoverytvister» för att bistå med expertis. En »special master» skiljer sig från en av domstolen utsedd expert på så vis att denne har rätt att utöva viss domarmakt. Även om förekomsten av »special masters» i »discoveryförfaranden» ökat, är målen vari de används fortfarande relativt få. Den begränsade förekomsten av »special masters» i »discoveryförfaranden» beror ofta på att det kan vara tidsödande och kostsamt att ta in en utomstående expert, som inte är insatt i den aktuella tvisten, särskilt när parternas eller av domstolen utsedd dataexpert i många fall kan lösa uppkomna problem.¹²⁵

Det är en mycket kostsam börda för den »discoverysvarande» parten att granska speglade kopior efter »privileged» eller annan konfidentiell information. I viss mån kan olika nyckelordssökningar identifiera skyddad information. Sällan identifieras dock alla skyddade dokument vid en sådan genomsökning, vilket i stor utsträckning beror på att företag i allmänhet har dåliga kategoriseringsrutiner för dokument (t.ex. genom att skyddade dokument flyttas till särskilda mappar eller på annat sätt markeras). Detta leder till att parterna i många fall måste granska dokumenten manuellt. Manuella granskningar innebär ofta mycket stora kostnader, särskilt med beaktande av mängden information som måste granskas.¹²⁶ För att minska kostnaderna för granskningen samt för att skydda »privileged information», förekommer att parter bl.a. avtalar om s.k. »claw back agreements». En »claw back agreement» innebär att parterna avtalar om att den »discoverysökande» parten ska lämna tillbaka skyddad information, som den »discoverysvarande» parten

¹²² *The Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. April 29, 2002).

¹²³ *In re: Triton Energy Ltd. Securities Litigation*, 2002 WL 32114464 (E.D. Tex. 7 mars 2002), s. 43 p. *6 (kurs här).

¹²⁴ *In re: Triton Energy Ltd. Securities Litigation*, 2002 WL 32114464 (E.D. Tex. 7 mars 2002).

¹²⁵ Scheindlin & Redgrave, *Special masters and e-discovery*, 30 *Cardozo L. Rev.* 347 2008-2009, s. 369 och s. 382.

¹²⁶ Kindall, *Electronic Discovery: Substantially increasing the risk of inadvertent disclosure and the costs of privilege review - do the proposed amendments to the federal rules of civil procedure help?*, 52 *Loy. L. Rev.* 839 2006, s. 852 f. och Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 *Nw. J. Tech. & Intell. Prop.* 171 2005-2006, s. 185 f.

oavsiktligt överlämnat. Trots att den faktiska kostnaden för tvisten typiskt sett inte minskas p.g.a. sådana avtal, då tvister om huruvida informationen som begärs tillbaka är skyddad eller inte ofta uppstår, kan denna typ av överenskommelser minska på 'spänningarna' mellan parterna i tvisten.¹²⁷

Den information som sorteras bort bör anges i en särskild »privilege log».¹²⁸ I loggen har traditionellt sett information om dokumentet (t.ex. författarens namn, avsändare, mottagare e.d.) förtecknats tillsammans med en förklaring till varför informationen är skyddad. Upprättandet av dessa loggar är dock oerhört tidskrävande, även i »discoveryförfaranden» som rör relativt få dokument. Med beaktande av de enorma mängder filer som normalt omfattas av en inspektion av datasystem förstärks problemen, vilket ofta gör loggarna nästintill oanvändbara.¹²⁹ För att komma till rätta med problemet kan parterna enas om att exempelvis initialt acceptera att grupper eller kategorier av dokument klassificeras som »privileged». För det fall oenighet angående klassificeringen uppstår, kan tvisten t.ex. lösas genom en »document-by-document review»^{130 131}.

När den »discoverysvarande» parten sorterat bort och klassificerat skyddad och irrelevant information, överlämnas relevant information till motparten. I detta sammanhang är det viktigt att parterna angett

- (a) vilka personer hos motparten som får ta del av informationen samt
- (b) på vilket sätt de ska få ta del av informationen.

Det förekommer att enbart vissa namngivna personer har rätt att ta del av informationen på exempelvis en neutral plats eller i informationsägarens lokaler. Informationen kan även överlämnas i pappersform eller i digital form, exempelvis på en extern hårddisk. Överlämnas informationen i digital form konverteras den i normalfallet till TIFF eller PDF (exakt vilken filtyp

¹²⁷ Withers, Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure, 4 Nw. J. Tech. & Intell. Prop. 171 2005-2006, s. 202 f.

¹²⁸ Se t.ex. *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999), *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002), *The Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. April 29, 2002), *Koosharem Corp. v. Spec Personnel, LLC*, 2008 WL 4458864 (D.S.C. Sept. 29, 2008) och *Ameriwood Industries, Inc., v. Liberman, et al.*, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006).

¹²⁹ The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production, s. 23 f.

¹³⁰ The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production, s. 23 f (kurs här).

¹³¹ The Committee Note to Rule 26(b)(5) (1993) »The rule does not attempt to define for each case what information must be provided when a party asserts a claim of privilege or work product protection. Details concerning time, persons, general subject matter, etc., may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected, particularly if the items can be described by categories.»

som används och hur informationen är strukturerad beror dock på vilket datasystem som använts för att granska materialet).¹³²

Riktlinjerna eller avtalen brukar vidare ange att dataexperten ska behålla speglingen fram till laga kraft vunnna dom, varpå speglingen samt alla andra kopior av information, som kan härledas till speglingen ska förstöras.¹³³

¹³² Cohen & Lender, *Electronic Discovery: Law and Practice*, 9-14 f.

¹³³ Se t.ex. *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), s. 642, och *Northwest Airlines, Inc. v. Local 2000*, No. Civ. 00-08 (DWF/AJB) (D. Minn. Feb. 2, 2000).

3 Inspektion av elektroniskt lagrad information inom ramen för editionsplikten

Ovan har parts möjlighet att ansöka om en »on-site inspection» av motpartens datorer enligt Federal Rules of Civil Procedure behandlats. Utredningen och därtill analysen nedan ska utröna huruvida det finns möjlighet för part att inom ramen för den processuella och materiella editionsplikts gränser genomföra en inspektion av motpartens datorer. Den processuella editionsplikten är förhållandevis tydlig vad gäller inspektioner av motpartens datorer, varför detta område enbart kommer att behandlas i korthet. Den materiella editionsplikten ter sig mer öppen beträffande denna fråga, vilket ger skäl för en mer utförlig redogörelse.

3.1 Processuell editionsplikt

Den processuella editionsplikten regleras av 38 kap. 2 § rättegångsbalken, som enligt sin lydelse ger part möjlighet att utverka ett editionsföreläggande avseende skriftliga handlingar (se nedan under kapitel 3.2.2 för innebörden av begreppet »skriftlig handling») som är både rättsligt relevanta och av betydelse som bevis i rättegång. Grundtanken bakom den processuella editionsplikten är att den editionssvarande¹³⁴ parten kan förpliktigas att till domstolen överlämna viss information. Syftet med regeln är alltså inte att ge motparten tillstånd att bedriva egna undersökningar eller inspektioner av eftersökt information. Att tillåta en inspektion av motpartens datorer, en slags 'privat husrannsakan', inom ramen för processuell edition är något, som den svenska rättegångsbalken enligt Westberg står främmande inför.¹³⁵ Ett sådant långtgående tvångsmedel kan parterna enbart åstadkomma genom fristående avtal. Parterna förfogar dock inte över vilka tvångsmedel domstolen ska tillgå vid tillämpning av den processuella bevisanskaffningen.¹³⁶

3.2 Materiell editionsplikt

Redogörelsen nedan kommer att utgå ifrån antagandet att två parter medtagit en inspektionsklausul i ett avtal vari parterna använt de amerikanska federala domstolarnas upplägg vid en »on-site inspection» av datorer som förebild. En inspektionsklausul är konstruerad för att ge en eller båda parter tillgång

¹³⁴ Eftersom både käranden och svaranden kan begära ut information från den andra parten i processen, används »editionssökande» och »editionssvarande» som begrepp i denna uppsats.

¹³⁵ Westberg, Anskaffning av bevisning i dispositiva tvistemål, s. 202 och 541 f.

¹³⁶ Westberg, Anskaffning av bevisning i dispositiva tvistemål, s. 202.

till annan eller mer omfattande information än vad de processuella reglerna medger. Ett avtal, som vidgar åtkomsten till information, främjar ambitionen att parterna ska eller bör ha lika tillgång till information i en rättegång, för att kunna föra sin talan på lika villkor och väcker enligt Westberg i sig inte några betänkligheter.¹³⁷ Genom inspektionsklausulen har parterna skapat en materiell grund, som ligger vid sidan av den processuella grunden för informationsåtkomst som följer av rättegångsbalken.

För att genomdriva ett avtal med en inspektionsklausul erbjuder svensk rätt materiell edition i enlighet 38 kap. 3 § rättegångsbalken.¹³⁸ Rättsregeln anger bl.a. att ett editionsföreläggande kan grundas på rättsförhållandet mellan parter, vilket följaktligen innebär att föreläggandet kan grundas på civilrättsliga föreskrifter i ett avtal.¹³⁹ En begäran om materiell edition kan enligt lagmotiven framställas i en särskild process eller, som en rättegångsfråga i en redan pågående rättegång.¹⁴⁰ Att begäran kan framställas i en särskild process innebär att ett yrkande om materiell edition ska handläggas enligt reglerna för tvistemål och avgöras genom dom.¹⁴¹

Framställs begäran i en särskild process behöver den elektroniskt lagrade informationen som omfattas av yrkandet – till skillnad från processuell edition – varken ha varken bevisbetydelse i eller något samband med en tvist. Den materiella editionsplikten är därav i allmänhet inte villkorad av att det uppkommit någon domstolstvist mellan parterna.¹⁴² Framställs begäran om materiell edition som en rättegångsfråga i en pågående process framgår det dock av lagmotiven att yrkandet enbart kan bifallas om parternas processuella intresse fodrar att handlingen företes. Processlagberedningen har alltså utgått ifrån att informationen måste ha bevisbetydelse i det aktuella målet.¹⁴³ Processlagberedningens inställning i denna fråga ter sig dock enligt Westberg märklig, eftersom det slår under själva poängen med ett avtal om informationsåtkomst, nämligen att en part vill undvika en prövning av huruvida informationen har bevisbetydelse i sammanhanget.¹⁴⁴ Part saknar vidare möjlighet att före en rättegång om huvudtvisten få frågan om materiell edition prövad i en förenklad ordning, t.ex. som domstolsärende.¹⁴⁵

När domstolen ska ta ställning till parts begäran om informationsåtkomst enligt 38 kap. 3 § rättegångsbalken, ska bedömning enbart göras mot bak-

¹³⁷ Westberg, *Anskaffning av bevisning i dispositiva tvistemål*, s. 200. Jfr även Ekelöf m.fl., *Rättegång IV*, s. 274 vari ett exempel ges på att ett avtal kan innebära längre gående rättigheter för en part, exempelvis rätten att få göra inspektioner av motpartens datorer.

¹³⁸ Utöver de verkningar som den materiella editionsplikten medför kan en inspektionsklausul givetvis även sanktioneras med vanliga kontraktsrättsliga sanktioner (t.ex. skadestånd).

¹³⁹ Lindell, *Civilprocessen*, s. 452.

¹⁴⁰ SOU 1938:44 s. 414.

¹⁴¹ Ekelöf m.fl., *Rättegång IV*, s. 274 och Westberg, *Anskaffning av bevisning i dispositiva tvistemål*, s. 199. Käranden kan även vända sig direkt till KFM om parten bedömer att svarenden inte kommer att bestrida dennes anspråk. Heuman, *Specialprocess*, s. 65 f.

¹⁴² Ekelöf m.fl., *Rättegång IV*, s. 274.

¹⁴³ Fitger, *Rättegångsbalken*, 38:11 och Westberg, *Anskaffning av bevisning i dispositiva tvistemål*, s. 199.

¹⁴⁴ Westberg, *Anskaffning av bevisning i dispositiva tvistemål*, s. 199 f.

¹⁴⁵ Westberg, *Anskaffning av bevisning i dispositiva tvistemål*, s. 199.

grund av de avtalsvillkor parterna kommit överens om. Omfattningen av parts rätt att få tillgång till handlingar bestäms därav uteslutande av den materiella rättens regler och berörs inte av de begränsningar, som finns för processuell edition.¹⁴⁶ För att domstol ska kunna bifalla editionsyrkandet krävs dock att yrkandet är bestämt enligt 42 kap. 2 § rättegångsbalken. Vid ett bifall av yrkandet måste den förelagde kunna avgöra hur långt hans skyldighet sträcker sig och KFM måste veta vilken innebörd domslutet har så att verkställighet kan ske.¹⁴⁷ Inspektionsklausulen bör därför noga ange vilka förpliktelser avtalet omfattar för editionssvaranden, t.ex. att parten ska tillåta en dataexpert att spegla och genomöka editionssvarandens datorer. Inspektionsklausulen bör även med fördel ange i vilken form och på vilket sätt informationen ska överlämnas till editionskäranden.

3.2.1 Precisionkrav

Gällande parts preciseringskyldighet vid begäran om materiell edition, finns anledning att närmare granska två situationer;

- (a) dels då yrkandet framställs oberoende av rättegång
- (b) dels då begäran om materiell edition framställs som en rättegångsfråga i en pågående process.

Framställs yrkandet oberoende av rättegång bör precisionskravet kopplat till 38 kap. 3 § rättegångsbalken vara uppfyllt om begäran om edition innehåller tillräckliga upplysningar om den omständighet som utlöser editionsplikten.¹⁴⁸ Preciseringskyldigheten får sedan bedömas mot bakgrund av den rättsliga grunden som editionsplikten vilar på. Resonemanget bottnar i att den materiella editionsplikten i grunden vilar på ett rättsförhållande mellan parter, varför rättsförhållandet närmast bör avgöra hur preciserat yrkandet behöver vara. Om editionsplikten kan hänföras till en inspektionsklausul, avgör således avtalet hur preciserat yrkandet behöver vara. Noteras bör dock att parts preciseringskyldighet ytterst måste avgöras av att yrkandet om vad svarande ska förpliktigas att göra eller tåla måste vara bestämt enligt 42 kap. 2 § rättegångsbalken.

¹⁴⁶ Fitger, Rättegångsbalken, 38:11 och Westberg, Anskaffning av bevisning i dispositiva tvistemål, s. 202. Eftersom 38 kap. 3 § rättegångsbalken inte omfattas av de begränsningar som 38 kap. 2 § ställer upp är det tänkbart att en avtalspart ska lämna ut handlingar som rör yrkeshemligheter eller minnesanteckningar. Avtalet bör dock inte tolkas så att part är skyldig att lämna ut korrespondens med sin advokat med anledning av tvisten. Ekelöf m.fl., Rättegång IV, s. 274.

¹⁴⁷ Westberg, Anskaffning av bevisning i dispositiva tvistemål, s. 200 not 20 och Heuman, Editions förelägganden i civilprocesser och skiljetvister, Del I, JT 1989-90, 6 f.

¹⁴⁸ Jfr Skoghøy, Tvistemål, s. 622. I norsk rätt finns regler om *edisjonsplikt*, som uppvisar likheter med de svenska reglerna i 38 kap. rättegångsbalken. Enligt de norska reglerna om *materiell edisjonsplikt* räcker det att ansökan innehåller tillräckliga upplysningar om den omständighet som utlöser editionsplikten för att preciseringskravet ska vara uppfyllt. Enligt Skoghøy får preciseringskyldigheten bedömas mot bakgrund av den rättsliga grunden som den materiella editionsplikten vilar på.

Viss osäkerhet får anses föreligga i rättsläget beträffande parts preciserings-skyldighet då begäran om materiell edition framställs som en rättegångsfråga i en pågående rättegångsprocess. Processberedningen har, som ovan angivits, utgått ifrån att den information som omfattas av parts editionsyrkande måste ha bevisbetydelse i det aktuella målet för att yrkandet ska kunna bifallas.¹⁴⁹ En sådan utgångspunkt ger enligt Westberg för handen att regeln om materiell edition inte kan ges ett självständigt syfte.¹⁵⁰ Om regeln ges en sådan innebörd bör materiell edition alltså närmast tillämpas som ett substitut till den processuella editionsplikten, med följderna att parts preciserings-skyldighet vid processuell edition blir gällande även för ett yrkande om materiell edition. För att uppfylla preciserings-skyldigheten skulle alltså krävas att part identifierar handlingarna, anger vilken kategori av handlingar som avses (exempelvis alla e-postmeddelanden i motpartens servrar som utväx-lats mellan vissa angivna personer) eller genom att sökanden noga beskriver bevissteman till vilka handlingarna kan hänföras.¹⁵¹

Processberedningens uttalande är dock märkligt – oavsett om beredning menade att en pågående rättegång inte ska få tyngas med frågor om materiell edition som inte är till nytta för tvistens handläggning eller avveckling eller om andra skäl låg bakom uttalandet – eftersom det, vilket även Westberg framhåller, slår under själva poängen med ett avtal om informationsåtkomst, nämligen att en part vill undvika en prövning av huruvida informationen har bevisbetydelse i sammanhanget.¹⁵² Dessutom ger ordalydelsen i 38 kap. 3 § rättegångsbalken inte stöd för att ett bifall av ett editionsyrkande kräver att handlingen som begärs ut måste ha bevisbetydelse i sammanhanget. Om hänsyn tas till Processberedningens uttalande, kan part enbart – i strid med ordalydelsen i 38 kap. 3 § rättegångsbalken – utfå elektronsikt lagrad information, som inte uppfyller precisionskravet för processuell edition, om en begäran om detta väcks som en självständig civilrättslig talan.

Mot bakgrund av syftet med 38 kap. 3 § rättegångsbalken och regelns ordalydelse, bör enligt min mening samma precisionskrav gälla oavsett om en begäran om materiell edition framställs som en rättegångsfråga i en pågående process eller då yrkandet framställs oberoende av rättegång. Precisionskravet kopplat till regeln om materiell edition bör alltså vara uppfyllt – förutsatt att yrkandet om vad svarande ska förpliktigas att göra eller tåla är bestämt enligt 42 kap. 2 § rättegångsbalken – om begäran om materiell edition innehåller tillräckliga upplysningar om den omständighet som utlöser editionsplikten, varefter parts preciserings-skyldighet får bedömas mot bakgrund av den rättsliga grunden som editionsplikten vilar på.

¹⁴⁹ SOU 1938:44 s. 414.

¹⁵⁰ Westberg, *Anskaffning av bevisning i dispositiva tvistemål*, s. 199 f.

¹⁵¹ NJA 1998 s. 590, Perhard, Något om elektronisk edition i tvistemål och skiljeförfarande, JT 2007-08, s. 399, Heuman, Editions-förelägganden i civilprocesser och skiljetvister, Del I, JT 1989-90, s. 13.

¹⁵² Westberg, *Anskaffning av bevisning i dispositiva tvistemål*, s. 199 f.

3.2.2 Skriftlig handling

För att en inspektionsklausul ska kunna läggas till grund för ett yrkande om materiell edition krävs att elektroniskt lagrad information ska jämföras med begreppet »skriftlig handling». Utvecklingen i domstolspraxis tyder på att så är fallet och att innebörden av begreppet »skriftlig handling» kommit att anpassas efter den teknologiska utvecklingen.

Denna utveckling började i och med Högsta domstolens avgörande i NJA 1998 s. 829, där domstolen klargjorde att editionsplikten avseende skriftliga handlingar dels inrymmer en skyldighet att lämna ut existerande datautskrift, dels en skyldighet för den editionsvarande parten att ta fram utskrift av information i en dator och ta fram programvara som gör det möjligt att framställa dokumenterad elektronisk information.¹⁵³ Utvecklingen tyder dock på att begreppet »skriftlig handling» inte bara inrymmer en skyldighet att skriva ut information i en dator, utan även en skyldighet att överlämna informationen i digital form om informationen redan finns i sådan form. I ett nyligen avgjort mål förelades editionsvaranden av Svea hovrätt att lämna ut för tvisten relevanta källkoder i digital form (på en CD-ROM skiva).¹⁵⁴ Uppfattningen om att elektroniskt lagrad information ska jämföras med skriftliga bevis synes även delas av doktrin.¹⁵⁵

Mycket tyder alltså på att elektroniskt lagrad information sannolikt jämföras med skriftliga bevis, var de i praxis utvecklade principerna för skriftliga handlingar blir vägledande även för denna typ av information. Något hinder för att lägga inspektionsklausulen till grund för ett editionsföreläggande finns därav sannolikt inte avseende denna fråga.

3.2.3 Bevis efterforskning

En inspektionsklausul kan i vissa avseenden liknas vid en 'privat husrannsakning' och har inslag av bevis efterforskning (»fishing expeditions»), även om det grundläggande syftet med inspektionen är att komma åt informationskällor och säkra bevisning. Inspektionsklausulen främjar alltså i första hand ambitionen att parterna ska ha lika tillgång till information i en rättegång för att kunna föra sin talan på lika villkor. Bevis efterforskning kan vid en första anblick te sig som ett främmande inslag i svensk rätt.¹⁵⁶ Trenden under de senaste åren talar dock för att bevis efterforskning tillåts i allt större utsträckning. Inom civilprocessens ramar har främst rättsinstitutet intrångs-

¹⁵³ NJA 1998 s. 829 och Heuman, Editions-förelägganden avseende ADB-baserad information och proportionalitetsgrundsatsen, JT 1999-2000, s. 152 f.

¹⁵⁴ Svea hovrätt Ö 4004-09.

¹⁵⁵ Se t.ex. Ekelöf m.fl., Rättegång IV, s. 255.

¹⁵⁶ Lindell har t.ex. framfört att det, inom länder som saknar »discovery», är vedertaget att rätten till materiell edition inte föreligger om den editionsyrkande parten genom editionen syftar till att undersöka om det finns underlag för ett anspråk mot 2008motparten. Vad Lindell åsyftar borde vara att bevis efterforskning anses vara ett främmande inslag i svensk rätt. Se Lindell, Civilprocess, s. 452.

undersökning och informationsföreläggande, tvångsåtgärder som kan initieras av privata parter i immaterialrättsliga tvister, utvidgat möjligheten till bevis efterforskning.¹⁵⁷ En intrångsundersökning innebär i korthet att domstolen, redan innan talan har väckts, får besluta om att KFM ska göra en undersökning hos den som skäligen kan antas ha gjort ett immaterialrättsintrång, för att söka efter handlingar som kan antas ha betydelse för utredningen i målet i syfte att säkra bevisning.¹⁵⁸ Ett informationsföreläggande ger en rättighetsinnehavare en civilrättslig möjlighet att t.ex. få ut information från en Internetleverantör om vem som har ett abonnemang som använts vid ett immaterialrättsligt intrång via Internet. Genom ett informationsföreläggande kan en kärandepart alltså – innan denne väckt talan i tvistemål – tvinga fram bevis och omständigheter som kan ha betydelse för kärandens talan.¹⁵⁹

Möjligheten till bevis efterforskning finns även i viss begränsad omfattning inom ramen för den processuella editionsplikten. Vid ett editionsyrkande i enlighet med 38 kap. 2 § rättegångsbalken kan en part, som ovan angivits, fullgöra sin preciseringskyldighet på tre olika sätt. Antingen uppfylls preciseringskyldigheten genom att handlingarna (a) identifieras, (b) genom att parten anger vilken kategori av handlingar som avses eller (c) genom att sökanden noga beskriver bevissteman till vilka handlingarna kan hänföras.¹⁶⁰ Det senare kan nog beskrivas som en möjlighet till bevis efterforskning. De relativt vaga krav som har uppställts på parts preciseringskyldighet för ett editionsyrkande kan även få till följd att stora mängder information måste utges vari part kan tänkas hitta bevis för sin talan.

En part har vidare i begränsad utsträckning möjlighet att genom ett editionsförhör i enlighet med 38 kap. 4 § rättegångsbalken eftersöka handlingar relaterade till det händelseförlopp eller saksammanhang som är aktuellt i målet.¹⁶¹ Förhöret behöver inte begränsas till bevis beträffande redan åberopade rättsfakta, utan bör enligt Fitger även kunna syfta till att ta ställning till om ett visst ytterligare och av part eventuellt förekommande rättsfaktum

¹⁵⁷ Även om det grundläggande syftet med intrångsundersökning är att säkra bevisning har det praktiska syftet påtagliga inslag av bevis efterforskning. Ekelöf m.fl., Rättegång IV, s. 320.

¹⁵⁸ Prop. 2008/09:26 s. 113. I betänkandet SOU:63 *Förstärkt skydd för företagshemligheter* föreslås dessutom att ett nytt rättsinstitut kallat »bevisundersökning» ska införas i svensk rätt. Enligt förslaget bör bevisundersökningen utformas på ett sätt som i stort stämmer överens med vad som gäller för intrångsundersökning i immaterialrättsliga mål. Bevisundersökningen ska kunna användas om det skäligen kan antas att någon har angripit en företagshemlighet enligt FHL och gälla om angreppet är straffbart eller grundar rätt till skadestånd. En bevisundersökning syftar till att säkra bevisning om ett misstänkt försök eller misstänkt förberedelse till olovligt utnyttjande av företagshemlighet, exempelvis i syfte att kunna föra en talan om vitesförbud. SOU 2008:63 s. 260 ff.

¹⁵⁹ Prop. 2008/09:67 s. 127 ff.

¹⁶⁰ NJA 1998 s. 590, Perhard, Något om elektronisk edition i tvistemål och skiljeförfarande, JT 2007-08, s. 399, Heuman, Editions-förelägganden i civilprocesser och skiljetvister, Del I, JT 1989-90, s. 13.

¹⁶¹ Westberg, Anskaffning av bevisning i dispositiva tvistemål, s. 522 och Rudvall, Till minnet av Södra Roslags tingsrätt, s. 160.

föreligger.¹⁶² Processlagberedningen har även framhållit att editionsförhör får hållas för att eftersöka vilka handlingar motparten innehar, som kan vara av betydelse i målet.¹⁶³ Det bör vidare inte krävas att den part som begär editionsförhör anger vilka bevisstämata som denne vill styrka genom de handlingar som efterfrågas. Enligt Heuman bör det däremot krävas att den part som yrkar att editionsförhör ska hållas anger förhörstemat på ”ett funktionellt men vagt sätt”,¹⁶⁴ så att rätten kan bedöma huruvida förhör ska hållas.¹⁶⁵ Ett editionsförhör med stöd av bestämmelserna i 41 kap. rättegångsbalken ger även möjlighet för part, under förutsättning att farerekvisitet är uppfyllt, att bedöma om tillräcklig bevisning föreligger för att inleda en rättegång eller inte.

I sammanhanget bör även 42 kap. 8 § 1 stycket rättegångsbalken nämnas, som tydligt främjar tanken på att parterna ska ha lika tillgång till information i en rättegång och är därtill ett gott exempel på att bevis efterforskning tillåts inom civilprocessens ramar. Av regeln, som inte är förenad med någon omedelbar sanktion, framgår att part är skyldig att på yrkande av motpart uppge vilka skriftliga handlingar som denne innehar utöver de handlingar som denne åberopat till sin förmån och som kan vara av relevans för motpartens talan. Den part som söker relevant information behöver således inte ens känna till handlingens existens eller närmare precisera vilka handlingar som eftersöks.¹⁶⁶

Mot bakgrund av vad som nyss angivits saknas anledning för domstol att avslå parts begäran om edition grundat på en inspektionsklausul med hänvisning till att inspektionen i viss mån möjliggör för part att efterforska bevis. Inspektionen utgör inte heller ett främmande inslag i svensk rätt.

3.2.4 Verkställighet och vitesföreläggande

Om editionsföreläggandet grundar sig på en inspektionsklausul vari parterna angett att en opartisk dataexpert ska spegla och genomsöka vissa angivna datorer, kan dataexperten - eller part för den delen - inte ges befogenhet att verkställa inspektionen mot den editionssvarande partens vilja.¹⁶⁷ I sammanhanget kan även påpekas att reglerna i 40 kap. 5 § rättegångsbalken om besiktning och granskning inte gäller privat sakkunnig (partssakkunnig),

¹⁶² Fitger, Rättegångsbalken, 38:13.

¹⁶³ NJA II 1943 s. 500. Se även Rudvall, Till minnet av Södra Roslags tingsrätt, s. 159 som framhåller att ett editionsförhör bör tillåtas om det vid en sammanlagd bedömning framstår som sannolikt att editionsförhöret kommer att kunna leda till identifiering av bevis i motpartens förvar av betydelse för saken.

¹⁶⁴ Heuman, Editions-förelägganden i civilprocesser och skiljetvister, Del I, JT 1989-90, s. 19 (kurs här).

¹⁶⁵ Se även Stockholms tingsrätts mål T 112-74, här hämtat från Heuman, Editions-förelägganden i civilprocesser och skiljetvister, Del I, JT 1989-90, s. 17 ff. I målet angavs inte bevisstämata för editionsförhören utan endast förhörstemata. Se vidare Rudvall, Till minnet av Södra Roslags tingsrätt, s. 159.

¹⁶⁶ Lindblom, Rättssfärernas harmoni, SvJT 1996, s. 820 f.

¹⁶⁷ Jfr SOU 2008:63 s. 263.

alltså den som parten själv anlitar genom en civilrättslig överenskommelse. Den private experten kan således inte utrustas med den rätt till besiktning respektive granskning som regleras i denna bestämmelse.¹⁶⁸ För att framtvunga fullgörelse kan emellertid domstol i enlighet med 38 kap. 5 § rättegångsbalken vitesförelägga den editionssvarande parten att tillhandahålla sina lokaler för en inspektion av partens datorer i enlighet med partsöverenskommelsen. Om föreläggandet inte följs kan rätten besluta att KFM ska verkställa editionsföreläggandet. Om rätten finner det lämpligt kan den dock redan i editionsbeslutet föreskriva att informationen skall tillhandahållas genom KFM:s försorg. Med stöd av 17 kap. 14 § 3 stycket rättegångsbalken kan tingsrätten vidare förordna om att beslutet omedelbart får verkställas.¹⁶⁹

Har parterna angett en särskilt ordning för hur dataexperten ska utses eller andra föreskrifter för hur inspektionen ska genomföras kan domstol i exekutionstiteln föreskriva vem som ska genomföra inspektionen och lämna andra föreskrifter om sättet för verkställighet. Avser inspektionen komplicerade digitala nätverk bör domstolen i möjligaste mån tillmötesgå parternas önskemål, eftersom det finns risk för att systemet äventyras eller skadas vid inspektionen. Parterna bör dock vara uppmärksamma på att KFM i enlighet med 16 kap. 12 § 3 stycket utsökningsbalken har befogenhet att ompröva och frångå domstols föreskrifter i exekutionstiteln om så behövs, t.ex. om föreskriften p.g.a. ändrade förhållanden inte kan tillämpas eller är klart oförmånlig för parterna.¹⁷⁰ Det är alltså ytterst KFM som ska besluta om vilka experter som ska vara sakkunniga biträden och sättet för verkställighet. Det finns alltså inte någon garanti för att den av parterna angivna dataexperten får bistå KFM vid inspektionen.¹⁷¹

¹⁶⁸ Inget hindrar förvisso att parten begär att få ett förordnande på en domstolssakkunnig för att granska viss elektroniskt lagrad information och utifrån materialet dra slutsatser om dess innehåll. Det blir då fråga om en besiktning enligt 40 kap. 5 § rättegångsbalken. Den sakkunnige kan även biträdas av en dataexpert vid eftersökning och insamling av relevant information. En given utgångspunkt är att både den sakkunnige och dataexperten saknar någon koppling till någondera parten eller att de drar nytta av målets utgång. Se Westberg, *Anskaffning av bevisning i dispositiva tvistemål*, s. 453 f.

¹⁶⁹ Heuman, *Editionsförelägganden i civilprocesser och skiljetvister*, Del I, JT 1989-90, s. 44.

¹⁷⁰ Walin m.fl., *Utsökningsbalken - en kommentar*, s. 630.

¹⁷¹ KFM är ingalunda främmande för att en opartisk expert bistår vid verkställighet. I intrångsundersökningar i mål om immaterialrättsliga intrång anlitas frekvent sakkunniga för att biträda vid undersökningen för att garantera dess effektivitet. Inte sällan lämnar sökanden redan vid ansökan om intrångsundersökning förslag på experter som kan vara sakkunniga biträden, men KFM måste i varje enskilt fall göra en självständig prövning av den föreslagna expertens lämplighet. Se Prop. 1998/99:11 s. 73 f.

4 Konklusion och avslutande synpunkter

Rätten att få inspektera motpartens datorer har kategoriserats som ett undantag av de federala domstolarna vid tillämpning av Federal Rules of Civil Procedure. I särskilda situationer kan dock »on-site inspections» visa sig värdefulla och tillåts generellt när det finns bevisning, som tyder på att den »discoverysvarande» parten inte uppfyllt sina »discoveryförpliktelser» samt i situationer när den centrala tvistefrågan har ett nära samband med digital information lagrad i de för målet aktuella datorerna.

Med hänsyn till problematiken kring »on-site inspections» av datorer har de federala domstolarna utarbetat särskilda riktlinjer, såsom exempelvis de som tillämpades i *The Antioch Co. v. Scrapbook Borders, Inc.*, *Playboy Enterprises v. Welles*, *Simon Property Group L.P. v. mySimon, Inc.*, *Northwest Airlines, Inc. v. Local 2000* och *Rowe Entertainment, Inc. v. William Morris Agency, Inc.* Rättsfallen ger för handen att inspektionen bör regleras av avtal eller riktlinjer som: (a) är snävt utformade för att begränsa inspektionens omfattning, (b) är utformade för att undvika att den »discoverysökande» parten får tillgång till för tvisten irrelevant eller skyddad information, (c) är utformade för att minimera störningar och skydda datasystem från skadlig användning och (d) tar hänsyn till utomstående intressen (exempelvis anställda, patienter eller annan tredje part). För att ta hänsyn till dessa punkter har riktlinjerna generellt angett att en opartisk dataexpert ska insamla den elektroniskt lagrade informationen på ett sätt varpå insamlad data kan verifieras. Informationen överlämnas sedan till den »discoverysvarande» partens juridiska ombud, som genom en »privilege screening» sorterar bort irrelevant eller skyddad information, varefter dokumentationen överlämnas till motparten i digital form.¹⁷² Det är dock viktigt att hålla i åtanke att avtalen eller riktlinjerna bör skraddarsys för att i möjligaste mån anpassas till omständigheterna i varje enskilt fall.

Att den svenska rättegångsbalken står främmande inför att tillåta en inspektion av editionssvarandens datorer inom ramen för processuell edition, är tydligt. Materiell edition präglas dock inte av samma tankesätt. Istället synes det möjligt för parter att genom fristående avtal åstadkomma ett sådant långtgående tvångsmedel som en inspektionsklausul innebär, vilket kan genomdrivas genom ett editionsföreläggande enligt 38 kap. 3 § rättegångsbalken. Inslaget av bevis efterforskning, som förknippas med en inspektion av motpartens datorer, utgör inte hinder för ett editionsföreläggande enligt nyss

¹⁷² *The Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. April 29, 2002), *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999), *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. June 7, 2000), *Northwest Airlines, Inc. v. Local 2000*, No. Civ. 00-08 (DWF/AJB) supra notes 46-56 och infra notes 74-87 (D. Minn. Feb. 2, 2000) och *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002).

nämnt lagrum och utgör inte heller ett främmande inslag i svensk rätt. Numer synes även elektroniskt lagrad information likställas med begreppet »skriftlig handling». Hinder föreligger därför inte att förelägga part att överlämna information hänförlig till det editionsgrundande avtalet i digital form, vilket är en förutsättning för att kunna skapa en spegling (»mirror image») av en dators hårddisk eller andra externa lagringsenheter.

Oavsett om yrkandet framställs oberoende av rättegång eller om begäran om materiell edition framställs som en rättegångsfråga i en pågående process, bör preciseringskravet kopplat till 38 kap. 3 § rättegångsbalken vara uppfyllt om stämningsansökan innehåller tillräckliga upplysningar om den omständighet som utlöser editionsplikten. Preciseringskyldigheten får sedan bedömas mot bakgrund av den rättsliga grunden som editionsplikten vilar på, exempelvis ett avtal. Parts preciseringskyldighet måste dock ytterst avgöras av att yrkandet om vad svarande parten ska förpliktigas att göra eller tåla måste vara bestämt enligt 42 kap. 2 § rättegångsbalken.

Någon garanti kan dock inte lämnas för att den av parterna utpekade dataexperten får biträda KFM vid verkställighet eller att det överenskomna tillvägagångssättet för inspektionen kommer att efterföljas, eftersom KFM enligt 16 kap. 12 § 3 stycket utsökningsbalken har befogenhet att ompröva och frångå domstols föreskrifter i exekutionstiteln om så behövs.

Med beaktande av den amerikanska rättens ökade inflytande över svensk rättsutveckling kan det förväntas att editionsplikten, inte minst materiell edition, framöver kommer att få en alltmer framträdande roll inom det svenska rättssystemet. Trots att de amerikanska federala domstolarnas rättsliga konstruktioner gällande »on-site inspections» av datorer inte har sett sin slutgiltiga form, finns ändå goda skäl att beakta den amerikanska rättsordnings erfarenheter och riktlinjer vid utformning av inspektionsklausuler.

Bilaga A

Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d. 1050 (S. D. Cal. Aug. 2, 1999)

- 1) The Court will appoint a computer expert who specializes in the field of electronic discovery to create a “mirror image” of Defendant's hard drive. The Court requests the parties to meet and confer to agree upon the designation of such an expert. If the parties cannot agree on an expert, the parties shall submit suggested experts to the Court by August 13, 1999. The Court will then appoint the computer specialist. Defendant asserts that the computer expert may be acting as an agent of Plaintiff because Plaintiff will be paying the costs. However, the Court finds this argument is moot, as the computer expert will either be agreed to by both parties or appointed by the Court and will act as an Officer of the Court. Further, Defendant's attorney-client privilege and privacy concerns will be protected by the protective order, which will be signed by the expert, and this Court's Order finding that this process will not waive any attorney-client privilege.
- 2) The Court appointed computer specialist will serve as an Officer of the Court. To the extent the computer specialist has direct or indirect access to information protected by the attorney-client privilege, such “disclosure” will not result in a waiver of the attorney-client privilege. Plaintiff herein, by requesting this discovery, is barred from asserting in this litigation that any such disclosure to the Court designated expert constitutes any waiver by Defendant of any attorney-client privilege. The computer specialist will sign the protective order currently in effect for this case. Lastly, any communications between Plaintiff and/or Plaintiff's counsel and the appointed computer specialist as to the payment of fees and costs pursuant to this Order will be produced to Defendant's counsel.
- 3) The parties shall agree on a day and time to access Defendant's computer. Plaintiff shall defer to Defendant's personal schedule in selecting this date. Representatives of both parties shall be informed of the time and date, but only Defendant and defense counsel may be present during the hard drive recovery.
- 4) After the appointed computer specialist makes a copy of Defendant's hard drive, the “mirror image” (which the Court presumes will be on or transferred to a disk) will be given to Defendant's counsel. Defendant's counsel will print and review any recovered documents and produce to Plaintiff those communications that are responsive to any earlier request for documents and relevant to the subject matter of this litigation. All documents that are withheld on a claim of privilege will be recorded in a privilege log.

- 5) Defendant's counsel will be the sole custodian of and shall retain this "mirror image" disk and copies of all documents retrieved from the disk throughout the course of this litigation. To the extent that documents cannot be retrieved from defendant's computer hard drive or the documents retrieved are less than the whole of data contained on the hard drive, defense counsel shall submit a Declaration to the Court together with a written report signed by the designated expert explaining the limits of retrieval achieved.
- 6) The Court orders that the "mirror image" copying of the hard drive, and the production of relevant documents, shall be completed by September 10, 1999.

Simon Property Group, L.P., v. mySimon, Inc., 194 F.R.D. 639 (S. D. Ind. 2000)

- 1) In essence, plaintiff shall select and pay an expert who will inspect the computers in question to create a "mirror image" or "snapshot" of the hard drives. Cf. *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*, 167 F.R.D. 90, 111-13 (D.Colo.1996) (describing problems that arose when one party's effort to preserve and recover files resulted in overwriting of 7 to 8 percent of hard drive contents). Defendant shall have a chance to object to the selection of the expert. The court will appoint the expert to carry out the inspection and copying as an officer of the court.
- 2) The expert shall then use his or her expertise to recover from the "mirror image" of the hard drive of each computer, and to provide in a reasonably convenient form to defendant's counsel, all available word-processing documents, electronic mail messages, powerpoint or similar presentations, spreadsheets, and similar files. The court intends that files making up operating systems and higher level programs in the computer not be duplicated, and that the copying be limited to the types of files reasonably likely to contain material potentially relevant to this case. Cf. *Adobe Systems, Inc. v. South Sun Products, Inc.*, 187 F.R.D. 636, 642-43 (S.D.Cal.1999) (noting that Microsoft Office 97 occupies more than 200 mega-bytes on hard drive of a personal computer). To the extent possible, the expert shall also provide to defendant's counsel: (a) the available information showing when any recovered "deleted" file was deleted, and (b) the available information about the deletion and contents of any deleted file that cannot be recovered.
- 3) After receiving these records from the expert, defendant's counsel shall then have to review these records for privilege and responsiveness to plaintiff's discovery requests, and shall then supplement defendant's responses to discovery requests, as appropriate.

- 4) The expert shall sign the protective order in the case and shall retain until the end of this litigation the “mirror image” copies of the hard drives and a copy of all files provided to defendant's counsel. At the end of this litigation, the expert shall then destroy the records and confirm such destruction to the satisfaction of defendant. The expert shall not disclose the contents of any files or documents to plaintiff or its counsel or other persons. Because the expert will serve as an officer of the court, disclosure of a communication to the expert shall not be deemed a waiver of the attorney-client privilege or any other privilege. The expert may designate assistants to help in this project. Each assistant shall sign the protective order in this case and shall be subject to all provisions applicable to the expert.
- 5) The expert shall file a report with the court setting forth the scope of the work performed and describing in general terms (but without disclosing the contents) the volume and types of records provided to defendant's counsel. See *McGuire v. Acufex Microsurgical, Inc.*, 175 F.R.D. 149, 157 n. 12 (D.Mass.1997) (noting that printouts of only the filenames for two years totaled 478 pages in length). After the expert has been selected, all communications between the expert and plaintiff's counsel shall take place either in the presence of defendant's counsel or through written or electronic communication with a copy to defendant's counsel.

Northwest Airlines, Inc. v. Local 2000, No. Civ. 00-08 (DWF/AJB) (D. Minn. Feb. 2, 2000)

- 1) **Place of Production.** Any discovery requests and/or subpoenas issued by Northwest for equipment shall specify that the equipment will be produced at the offices of Ernst & Young nearest to the site of the equipment. Northwest will advise you further, if, at the request of any respondent, or by Order of the Court, alternative arrangements are to be made for you to review the equipment either at the site where it is located or at some other site.
- 2) **Minimize Disruption or Interference.** Consistent with the schedule of this litigation, you shall endeavor to conduct your inspection to the extent possible, in a manner which is least intrusive or disruptive of the normal activities or business operations of the person or organization producing the equipment.
- 3) **Only Ernst & Young to Review.** When any equipment is produced to you, the only persons authorized to inspect or otherwise handle such equipment, computer manufacturer, model number and serial number; hard drive manufacturer, model number and serial number; and network card manufacturer, model number, serial number, and MAC address wherever possible. Likewise, you should obtain a similar receipt when you return the equipment. Ernst & Young

should document the chain of custody of the equipment and of any copies or information drawn from the equipment.

- 4) **Limit Scope of Inspection.** It is understood from your representations that the standard practice among experts in computer forensics is to make a “mirror image” of any disc drive, or other storage device and then to utilize search methodologies to locate responsive words, phrase, data, documents, messages or fragments thereof (hereinafter “data”) contained on the mirror image. The Court has limited discovery to the period between April 1, 1999, and February 8, 2000. In order to protect the privacy interest of the person producing the equipment, except to the extent necessary to search for responsive Data, you shall not read or review Data on the equipment which does not fall within the discovery period and does not relate to the persons or subject matter listed on Attachment A to these instructions. Ernst & Young shall retain custody of the mirror image until conclusion of this litigation, at which time you shall destroy the mirror image and shall issue written confirmation of that fact to us and to the person or organization who produced the equipment.

- 5) **Produce Copies of Responsive Information.** Whenever you inspection of equipment belonging to Griffin and Reeve identifies Data that you deem to be responsive to Attachment A, you shall designate the item on a checklist/index. The listing form shall contain a line for each item of data followed by separate spaces/boxes which may be checked (by defendants only) to designate any objections based upon (1) privilege; (2) negotiation or strike strategy; (3) relevance; (4) other (specified). You shall make three paper copies of each such item, retaining one copy for your records and delivering one copy, along with the prepared checklist, to Paul Alan Levy, Esq., Public Citizen Litigation Group, 2000 P Street NW, Suite 700, Washington, D.C. 20036. Upon notification by defense counsel you shall release particularly identified documents to counsel for plaintiff Northwest. Copies of documents not released to Northwest shall be submitted to the Court for safekeeping pending determination of discoverability. Upon request of the person producing the equipment, you may provide to that person a copy of any document you have copied for Northwest. You shall not otherwise copy, or disclose, the contents of the equipment.

- 6) **Qualification of Personnel; Verification of Procedures.** You shall be responsible for ensuring that all personnel assigned to this project are qualified and experienced in the field of computer forensic investigations and operate under the direction and control of one or more individuals qualified to serve as expert witness on the subject of computer forensic investigations. You shall also be responsible for confirming in writing, and testify under oath, if necessary, that you have strictly followed the foregoing procedures.

- 7) **No changes to these Procedures Without Written Notice.** There shall be no change in the foregoing instructions without prior written notice to the parties. Please confirm such notice before accepting any propose changes to these procedures.
- 8) **Acknowledgement and Agreement.** Please confirm by an authorized signature below you receipt of, and agreement to be bound by, the foregoing procedures.

Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645 (D. Minn. April 29, 2002)

- 1) First, Antioch will select an expert of its choice, in the field of computer forensics (“the Expert”), to produce the “mirror image” of the Defendants’ computer equipment. Once the Expert is chosen, Antioch will notify the Defendants, and the Defendants will make available to the Expert, at their place of business, and at a mutually agreeable time, all of their computer equipment.
- 2) The Expert will use its best efforts to avoid unnecessarily disrupting the normal activities or business operations of the Defendants while inspecting, copying, and imaging, the Defendants’ computer equipment, up to and including the retention of the computer equipment on the Defendants’ premises. Moreover, the only persons authorized to inspect, or otherwise handle such equipment, shall be employees of the Expert assigned to this project. No employee of Antioch, or its counsel, will inspect or otherwise handle the equipment produced. The Expert will also maintain all information in the strictest confidence.
- 3) Within ten days of its inspection, copying, and imaging, of the computer equipment produced by the Defendants, the Expert shall provide the parties with a report as to what computer equipment was produced by the Defendants, and the actions taken by the Expert with respect to each piece of computer equipment. This report shall include a detailed description of each piece of computer equipment inspected, copied, or imaged, by the Expert, including the name of the manufacturer of the equipment and its model number and serial number; the name of the hard drive manufacturer and its model number and serial number; and the name of any network card manufacturer and its model number, serial number, and MAC address wherever possible. The Expert shall document the chain of custody for any copies and images drawn from the equipment. These reports shall be produced to both of the parties.
- 4) Once the Expert has created copies and images of the Defendants’ hard drives, it will produce two copies of the resulting data. One copy will be transmitted to the Court, and the other copy will be transmitted to the Defendants. Thereafter, once Antioch pro- pounds any doc-

ument requests, the Defendants will sift through the data provided by the Expert to locate any relevant documents.

- 5) The Defendants shall then produce to Antioch all responsive documents that are properly discoverable, as well as a privilege log, which describes the nature of any privileged documents or communications, in a manner that, without revealing information that is privileged or protected, will enable Antioch to assess the applicability of the privilege or protection claimed. At that time, the Defendants shall also forward the privilege log to the Court for potential in camera review.
- 6) Once it has reviewed the documents produced by the Defendants, as well as the privilege log, if the Plaintiff raises a dispute as to any of the documents, by providing a cogent basis for doubting the claim of privilege, or for believing that there are further relevant documents, the Court will conduct an in camera review, limited to the issues raised. This procedure will govern the recovery of deleted information from the Defendants' computers unless and until modified by a Court of competent jurisdiction.
- 7) With this procedure in mind, we direct the parties to "meet and confer" on an appropriate time for the Expert to access the Defendants' computer equipment, keeping in mind our directive to minimize the burden and inconvenience caused to the Defendants. To that extent, we grant the Plaintiff's Motion to Compel, and to Appoint a Neutral Expert in Computer Forensics.

Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002)

- 1) Initially, the plaintiffs shall designate one or more experts who shall be responsible for isolating each defendant's e-mails and preparing them for review. The defendants shall have the opportunity to object to any expert so designated. The expert shall be bound by the terms of this order as well as any confidentiality order entered in the case.
- 2) With the assistance and cooperation of the defendants' technical personnel, the plaintiffs' expert shall then obtain a mirror image of any hard drive containing e-mails as well as a copy of any back-up tape. The plaintiffs may choose to review a sample of hard drives and tapes in lieu of all such devices.
- 3) Plaintiffs' counsel shall formulate a search procedure for identifying responsive e-mails and shall notify each defendant's counsel of the procedure chosen, including any specific word searches. Defendants' counsel may object to any search proposed by the plaintiffs.
- 4) Once an appropriate search method has been established, it shall be implemented by the plaintiffs' expert. Plaintiffs' counsel may then review the documents elicited by the search on an attorneys'-eyes-only

basis. The plaintiffs may choose the format for this review; they may, for example, view the documents on a computer screen or print out hard copy. Once plaintiffs' counsel have identified those e-mails they consider material to this litigation, however, they shall provide those documents to defendants' counsel in hard copy form with Bates stamps. The plaintiffs shall bear all costs associated with the production described thus far. However, the defendants shall pay for any procedures beyond those adopted by the plaintiffs, such as the creation of TIFF files.

- 5) Defendants' counsel shall then have the opportunity to review the documents produced in order to designate those that are confidential and assert any privilege. Any purportedly confidential or privileged document shall be retained on an attorneys'-eyes-only basis until any dispute about the designation is resolved. The fact that such a document has been reviewed by counsel or by the expert shall not constitute a waiver of any claim of privilege or confidentiality.
- 6) Should any defendant elect to review its database prior to production, it shall do so at its own expense. In that event, the defendant shall review those hard drives and back-up tapes selected by the plaintiffs and shall create copies from which privileged or confidential and unresponsive material has been deleted. The defendant shall then provide plaintiffs' counsel with each "redacted" hard drive or tape, together with a privilege log identifying the documents removed. The process would then continue as described above.

Bank of Magnolia v. M & P Global Financial Services, 258 F.R.D. 514, 2009 WL 1117312 (S.D. Fla. April 24, 2009)

- 1) An independent third party computer expert shall be appointed by the Court and shall mirror image M & P Defendants' computer system.
- 2) The parties have until April 30, 2009, to meet and confer regarding their designation of an independent computer expert. If the parties cannot agree on an independent computer expert, each party shall submit its recommendation for an independent expert to the Court, and the Court shall select the expert.
- 3) The appointed independent computer expert shall serve as an Officer of the Court. Thus, to the extent that this computer expert has direct or indirect access to information protected by attorney-client privilege, such disclosure will not result in any waiver of the M & P Defendants' privilege.
- 4) The independent expert shall sign a confidentiality order. Additionally, the expert shall be allowed to hire other outside support if necessary in order to mirror image M & P Defendants' computer system. Any outside support shall be required to sign the same confidentiality order.

- 5) The expert shall mirror image the M & P Defendants' computer system.
- 6) Plaintiff shall provide a list of search terms to the Court to identify responsive documents to Plaintiff's document requests by April 30, 2009. After Plaintiff has submitted the search terms to the Court, the M & P Defendants shall have 5 days to submit their objections to the Court regarding any of the search terms, which the Court will rule upon. The Court will provide the search terms to the independent expert.
- 7) Once the expert has mirror imaged the M & P Defendants' computer system, the expert shall search the mirror image results using the search terms. The results of the search terms will be provided to the M & P Defendants and to the Court, along with an electronic copy of all responsive documents (also to be provided to both the M & P defendants and the Court).
- 8) The M & P Defendants shall review the search term results provided by the Court's expert and identify all responsive documents. The M & P Defendants shall either produce all responsive documents to Plaintiff or identify those responsive documents not produced on a privilege log to Plaintiff within 20 days of the date that the M & P Defendants receive the search term results from the independent expert. *Any privilege log produced shall comply strictly with the Local Rules for the Southern District of Florida.*
- 9) Plaintiff shall pay for all fees and costs of hiring the independent expert at this time. However, if at a later time there is evidence of the M & P Defendants' improper deletion of electronic documents or any other associated improper conduct, the Court will revisit this issue and consider charging the M & P Defendants for the fees and costs of the independent expert or imposing the fees and costs on the parties in a duly appropriate proportioned manner.
- 10) The independent expert shall provide a signed affidavit detailing the steps he or she took in mirror imaging the M & P Defendants' computer system and searching the mirror image for the search terms within 5 days of providing the M & P Defendants and the Court with the results of the search for search terms in the mirror image.

Cenveo Corporation v. Slater, 2007 WL 442387 (E.D. Pa. Jan. 31, 2007)

- 1) Plaintiff shall select a computer forensics expert trained in the area of data recovery to produce a digital or mirror image of all computers and portable hard drives that have been in defendants' custody, possession, or control since January 2006. Once the expert is chosen, plaintiff shall notify the defendants, and the expert shall execute a confidentiality agreement agreed to by the parties and sign a copy of

the protective order in place in this matter (Document No. 20). The expert shall further agree to submit to the jurisdiction of this Court and be bound by the terms of this memorandum and order.

- 2) Defendants shall then make all of the computer equipment described above available to plaintiff's expert at their place of business or residences at mutually agreeable times. Plaintiff's expert shall use his or her best efforts to avoid unnecessarily disrupting the normal activities and business operations of defendants while inspecting and imaging defendants' computer equipment. Plaintiff's expert may not remove defendants' computer equipment from defendants' premises, and only plaintiff's expert and his or her employees assigned to this project are authorized to inspect the equipment produced. Defendants may also have an electronic data recovery expert present during the inspection and imaging of their computer equipment. After the inspection and imaging, plaintiff's expert may perform the remainder of his or her responsibilities outside defendants' premises. Plaintiff's expert shall maintain all information in the strictest confidence. Plaintiff's expert will maintain a copy of the mirror images and all recovered materials until sixty days after the unappealable conclusion of this litigation.
- 3) Within ten days of inspection and imaging, plaintiff's expert shall provide the parties with a report describing the computer equipment defendants produced and the actions plaintiff's expert took with respect to each piece of equipment. This report shall include a detailed description of each piece of equipment inspected, including the name of the manufacturer and model and serial number of the equipment, wherever possible.
- 4) Plaintiff's expert shall recover all documents from the mirror images, including but not limited to all word-processing documents, email messages, PowerPoint or similar presentations, spreadsheets and other files, including "deleted" files. Plaintiff's expert shall provide the recovered files to defendants in a reasonably convenient and searchable form, along with, to the extent possible, information showing when any files were created, accessed, copied, or deleted. Plaintiff's expert shall also provide plaintiff notice of when the recovered materials were provided to defendants.
- 5) Within forty-five days of receipt, defendants shall review the recovered materials for privilege and responsiveness, supplement defendants' responses to plaintiff's discovery requests, and send to plaintiff's counsel all non-privileged responsive documents, as well as a privilege log complying with Federal Rule of Civil Procedure 26(b)(5)(A). Plaintiff shall have the opportunity thereafter to propound any additional discovery requests, and defendants shall produce any non-privileged responsive materials to plaintiff as described above. Nothing in this order shall prevent plaintiff from filing a motion to compel if it is unable to resolve a claim of privilege or relev-

ance with defendants, but the parties are strongly encouraged to resolve these issues without Court intervention.

- 6) This procedure shall govern the recovery of discoverable materials located on defendants' computer equipment. The Court directs the parties to meet and confer to determine how they will carry out the terms of this order, keeping in mind the Court's directive to minimize the burden and inconvenience to defendants.

Frees, Inc. v. Phil McMillian, 2007 WL 184889 (W.D. La. Jan. 22, 2007)

- 1) Frees' computer forensics expert will be allowed to make images of the hard drives of the computers at issue;
- 2) Copies of the imaged hard drives are to be provided to McMillian and the Court ten (10) days before Frees' computer forensics expert may begin any investigation into those imaged drives;
- 3) After McMillian has had time to identify and seek protection for any objectionable information (such as privileged or work-product information) on the imaged hard drives, Frees' forensic expert will then be permitted to perform keyword searches of the hard drives and, subsequently, will provide to both Frees and McMillian a list of the file names identified through such searches;
- 4) McMillian will then have an additional ten (10) days to object to production of the requested files and files not objected to will be produced to Frees at the end of this period;
- 5) Depending on the number of "hits" produced through the particular key words used in the search, the above process may need to be repeated using different lists of key words based on actual issues in the case;
- 6) In any event, the forensics expert is authorized to search for any indications that external devices were used with the subject computers and, if so, to attempt to identify such memory devices.

Ameriwood Industries, Inc. v. Liberman, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006)

- 1) The Court has carefully reviewed the procedures adopted by courts addressing similar problems in *Antioch*, 210 F.R.D. at 653-54, *Simon Property Group*, 194 F.R.D. at 643-44, and *Playboy Enterprises v. Welles*, 60 F.Supp.2d 1050, 1054 (S.D.Cal.1999). The following three-step imaging, recovery, and disclosure process provides the requesting party sufficient access to information that is not reasonably accessible and ensures the process does not place an undue burden on the responding party.

- 2) First, plaintiff will select a computer forensics expert of its choice (“the Expert”), that has been trained in the area of data recovery, to produce mirror images of all computers and portable or detachable hard drives in defendants' possession, custody, or control and used by defendants Liberman, Fridley, or Kleist since May 2005, including but not limited to any computer or portable or detachable hard drive in their homes. Once the Expert is chosen, plaintiff will notify defendants. The Expert will then execute a confidentiality agreement agreed to by the parties and sign a copy of and abide by the protective order in place in the instant action.
- 3) Defendants will then make available to the Expert, at their places of business or residences, and at mutually agreeable times, all of the computer equipment described above. The Expert will use its best efforts to avoid unnecessarily disrupting the normal activities or business operations of defendants while inspecting, copying, and imaging defendants' computer equipment. The Expert may not remove defendants' computer equipment from defendants' premises. Moreover, only the Expert and its employees assigned to this project are authorized by this order to inspect, or otherwise handle such equipment. No employee of plaintiff, or its counsel, will inspect or otherwise handle the equipment produced. The Expert will also maintain all information in the strictest confidence. Furthermore, the Expert will maintain a copy of the mirror images and all recovered data and documents until sixty days after the conclusion of litigation. After the inspection, copying, and imaging of defendants' computer equipment, the Expert may perform the remainder of its responsibilities outside defendants' premises.
- 4) Within ten days of the inspection, copying, and imaging of each item of computer equipment produced by defendants, the Expert shall provide the parties with a report describing the computer equipment defendants produced and the Expert's actions with respect to each piece of the equipment. This report shall include a detailed description of each piece of computer equipment inspected, copied, or imaged by the Expert, including the name of the manufacturer of the equipment and its model number and serial number; the name of the hard drive manufacturer and its model number and serial number; and the name of any network card manufacturer and its model number, serial number, and the media access control address wherever possible.
- 5) Once the Expert has created copies and images of defendants' hard drives, it shall recover from the mirror images all available word-processing documents, incoming and outgoing email messages, PowerPoint or similar presentations, spreadsheets, and other files, including but not limited to those files that were “deleted.” The Expert shall provide the recovered documents in a reasonably convenient and searchable form to defendants' counsel, along with, to the extent

possible, the information showing when any files were created, accessed, copied, or deleted, and the information about the deletion and the contents of deleted files that could not be recovered. The Expert shall also provide plaintiff notice of when the documents and data were provided to defendants' counsel.

- 6) Within twenty days of the receipt of the recovered documents and data, defendants' counsel shall review the records for privilege and responsiveness, appropriately supplement defendants' responses to discovery requests, and send to plaintiff's counsel all responsive and non-privileged documents and information, in addition to a privilege log, which claims each privilege expressly and describes "the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection." Fed.R.Civ.P. 26(b)(5)(A). Thereafter, once plaintiff propounds any further discovery requests, defendants will search through the information provided by the Expert to locate all responsive documents and data, and shall then produce to plaintiff all properly discoverable documents and data, as well as a privilege log, as described above. Once plaintiff has reviewed the documents produced by defendants, as well as the privilege log, if plaintiff raises a dispute as to any of the documents by providing a cogent basis for doubting the claim of privilege, or for believing that there are further relevant documents, plaintiff may file a motion to compel.
- 7) This procedure will govern the recovery of information and other data from defendants' computer equipment. With this procedure in mind, the Court directs the parties to "meet and confer" to determine the contents of the aforementioned confidentiality agreement and an appropriate time for the Expert to access defendants' computer equipment, keeping in mind the Court's directive to minimize the burden and inconvenience caused to defendants.

Koosharem Corporation v. Spec Personnel, LLC, 2008 WL 4458864 (D.S.C. Sept. 29, 2008)

- 1) Defendants will make available for forensic analysis and data recovery to be conducted by an expert forensics firm ("Expert") any business computers and/or any personal computers used to conduct business, correspond in any way regarding business, Spec and/or its current or employees, and/or plaintiffs and/or their current or former employees, for Steve Arnold, Walter Chudowsky, Benita Dillard, Trevor Doyle, Ken Fuston, Kevin Moore, Steve Roberson, and Jude Tallman.
- 2) The time frame for the forensic analysis and data recovery will encompass the period September 1, 2007, to present.

- 3) The parties will jointly agree within five (5) calendar days after entry of this order on an Expert that will be used to conduct the data recovery and forensic analysis.
- 4) Defendants will produce to the Expert within ten (10) calendar days after entry of this order the computers identified in paragraph 1.
- 5) The Expert will recover only the documents and email account or accounts used by individuals identified in paragraph 1 (or those accounts and documents accessed remotely using another computer).
- 6) The Expert also will conduct a search or run other appropriate programs to determine whether any emails or documents have been deleted, destroyed, altered, or otherwise compromised since January 25, 2008, and whether any programs have been installed that would alter, destroy, erase, modify, or otherwise compromise any portion of each computer or its contents as of January 25, 2008. The Expert also will be permitted to conduct such search efforts as are necessary to form an opinion as to whether any procedures were put into place to preserve emails and documents as of January 25, 2008.
- 7) The recovery of emails will include all emails in any form whatsoever including, but not limited to, deleted emails, forwarded emails, copied ("cc") and blind-copied ("bcc") emails and draft emails. The recovery of documents will include all documents including drafts, multiple versions, and final versions.
- 8) The Expert will securely maintain the original data recovered in order to establish a chain of custody.
- 9) The Expert will produce a copy of the recovered data to defendants' local counsel of record attorney John Glancy ("defendants' counsel").
- 10) Defendants' counsel will review the data to identify any privileged or personal emails that it seeks to withhold from document production.
- 11) Within ten (10) business days of obtaining the recovered data from the Expert, defendants' counsel will prepare and provide to counsel for plaintiffs: (I) a log of privileged emails ("Privileged Email Log") protected against disclosure by a relevant legal privilege and include the identity of the email, the sender and recipient (and any individuals identified in the "cc" and "bcc" fields), the date sent, the nature of the privilege, a general description of the email and the basis for asserting the privilege; and (ii) a log of personal emails ("Personal Email Log") and include the identity of the email, the sender and recipient (and any individuals identified in the "cc" and "bcc" fields), the date sent, a general description of the email and the basis for claiming it is a personal email. To the extent that defendants' counsel asserts privilege as to any documents obtained from the forensic analysis, such

documents also must be set forth on a document privilege log (“Privileged Document Log”) and be produced within ten (10) business days of obtaining the recovered data.

- 12) Together with the Privileged Email Log, Personal Email Log, and Privileged Document Log, defendants shall produce (within 10 business days after obtaining the recovered data from the Expert) all emails and documents recovered by the Expert, which are not identified on the Logs.
- 13) For purposes of the procedure described herein, a personal email is one that does not relate to or in any way concern: defendants' employment, whether it deals with past, present, future or prospective employment; plaintiffs' business; plaintiffs' customers and former customers (including contacts at customers and former customers); plaintiffs' employees and former employees; defendants' drivers or plaintiffs' former drivers; plaintiffs and any of its employees; or Spec Personnel and any of its employees, including but not limited to, communications regarding Spec's closing of offices staffed by plaintiffs' former employees or efforts to have anyone take over, purchase or otherwise assume responsibility for any Spec office staffed by plaintiffs' former employees.
- 14) If any document attachment to an email is identified through the discovery of an email, and such document was opened, saved from, detached or otherwise transferred or reproduced on the hard-drive of defendants' computers, such attachment shall be produced or the Expert shall be given access to defendants' computer to conduct further data recovery in order to obtain such document(s).
- 15) If any document is identified by the Expert as being opened, saved, altered, transferred or reproduced and it falls within the scope of the request, such document must be produced by the Expert and handled by defendants' counsel in the same manner as though it was an email communication.
- 16) If plaintiffs disagree with the assertion of any privileges, the parties shall submit to the court the disputed documents and Logs for the court to view *in camera* and determine whether the documents must be produced.
- 17) Defendants are responsible for any and all fees, costs and expenses associated with gathering the computers and transmitting them to the Expert.
- 18) At this time, the parties will share equally the fees, costs and expenses charged by the Expert. When the Expert is retained, the Expert will be jointly informed that any billing or retainer must be split evenly between the parties. If any retainer is required, the parties are obli-

gated to provide the retainer within three (3) business days of the Expert's request so that the process is not delayed in any way. Neither party waives its right to seek reimbursement or payment of any fees, costs and expenses charged by the Expert if it is determined that award of such is appropriate pursuant to the Federal Rules of Civil Procedure, Local Rules or case law.

19) By agreeing to this order, no party waives its rights or objections to the discovery sought herein.

20) The parties understand and agree that this order addresses the preliminary scope for the computer production and forensic analysis. If the initial production and analysis determines that additional searches are necessary, either party may petition the court to re-visit the scope of this order

Käll- och litteraturförteckning

Litteratur

Böcker och monografier

Black Law Dictionary, 8:e uppl., USA 2004
[Westlaw databasidentifiering: BLACKS]

Cohen, Adam I. & Lender, David J., Electronic Discovery: Law and Practice, The 2010 Supplement, USA 2010

Ekelöf, Per Olof, Edelstam, Henrik & Heuman, Lars, Rättegång, Fjärde häftet, 7:e uppl., Stockholm 2009
[Citeras: Ekelöf m.fl., Rättegång IV]

Fitger, Peter, Rättegångsbalken, Del III, Stockholm 2009

Friedenthal, Jack H., Kane, Mary Kay & Miller, Arthur R. Civil Procedure, Fourth Edition, USA 2005

Heuman, Lars, Festskrift till Peter Seipel, Processrätten och den digitala tekniken, Stockholm 2006, s. 249 ff.

Heuman, Lars, Specialprocess, 6:e uppl., Stockholm 2007

Lindell, Bengt, Civilprocessen, 2:a uppl., Uppsala 2003

Rudvall, Samuel, Till minnet av Södra Roslags tingsrätt, Bevisafterforskning avseende skriftliga handlingar hos motparten, Stockholm 2007, s. 140 ff.

Skoghøy, Jens Edvin A., Tvistemål, 2:a uppl., Oslo 2001

The Sedona Principles, Best Practices Recommendations & Principles for Addressing Electronic Document Production, 2:a uppl., USA 2007
[Tillgänglig på www.thesedonaconference.org, hämtad 2010-03-03]

Walin, Gösta, Gregow, Torkel, Löfmarck, Peter, Millqvist, Göran & Persson, Annina H., Utsökningsbalken - en kommentar, 4:e uppl., Stockholm 2009.
[Citeras: Walin m.fl., Utsökningsbalken - en kommentar]

Westberg, Peter, Anskaffning av bevisning i dispositiva tvistemål, Stockholm 2010

Artiklar och uppsatser

Arent, Brownstone & Fenwick, Ediscovery: Preserving, requesting & producing electronic information, Santa Clara Computer & High Technology Law Journal, Volume 19, 2002-2003, s. 131 ff.

[Citeras: 19 Santa Clara Computer & High Tech. L.J. 131 2002-2003]

Catlin, Bill, How Private Is the Home Computer?, Minnesota Public Radio, 8 Februari, 2000

[Tillgänglig på

http://news.minnesota.publicradio.org/features/200002/08_catlinb_privacy/,

hämtad 2010-05-11]

Fliegel, Jason & Entwisle, Robert, Electronic Discovery in Large Organizations, Richmond Journal of Law & Technology, Volume XV, Issue 3, 2008-2009, s. 1 ff.

[Citeras: 15 RICH. J.L. & TECH. 7.]

Georg, Christopher N., Someone's watching: Protecting privilege on both sides of the table during electronic discovery, Journal of Law, Technology & Policy, Volume 4, 2004, s. 283 ff.

[Citeras: 2004 J.L. Tech. & Pol'y 283 2004]

Goldberg, Nolan M., Discovery and the Reluctant Host, The National Law Journal, Volume 30, Number 26, 2008.

[Citeras: 3/10/2008 Nat'l L.J.S1, (Col. 2)]

Goldberg, Nolan M. & McGowan, Michael F., Electronic Discovery Behind Enemy Lines: Inspection Of An Adversary's Network Pursuant To Fed. R. Civ. P. 34(a), The Metropolitan Corporate Counsel, November 2007, s. 56.

[Tillgänglig på

<http://www.metrocorpccounsel.com/pdf/2007/November/56.pdf>, hämtad

2010-04-12]

Heuman, Lars, Editions förelägganden i civilprocesser och skiljetvister, Del I, Juridisk Tidskrift 1989-90, s. 3 ff.

Heuman, Lars, Editions förelägganden avseende ADB-baserad information och proportionalitetsgrundsatsen, Juridisk Tidskrift 1999-2000, s. 152 ff.

Kindall, James C., Electronic Discovery: Substantially increasing the risk of inadvertent disclosure and the costs of privilege review - do the proposed amendments to the federal rules of civil procedure help?, Loyola Law Review, Volume 52, 2006, s. 839 ff.

[Citeras: 52 Loy. L. Rev. 839 2006]

Lindblom, Per Henrik, Rättssfärernas harmoni, Svensk Juristtidning 1996, s. 793 ff.

Perhard, Lars, Något om elektronisk edition i tvistemål och skiljeförfarande, Juridisk Tidskrift 2007-08, s. 395 ff.

Raysman, Richard & Brown, Peter, Examining Hard Drives During Discovery, Law Technology News, 13 november 2007.

[Tillgänglig på

<http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=900005495808>, hämtad 2010-03-25]

Scheidlin, Shira A. & Jonathan M. Redgrave, Special masters and e-discovery, Cordozo Law Review, Volume 30:2, 2008, s. 347 ff.

[Citeras: 30 Cardozo L. Rev. 347 2008-2009]

Withers, Kenneth J., Computer-Based Discovery in Federal Civil Litigation, Federal Courts Law Review, Volume 1, 2006, s. 65 ff.

[Citeras: Fed. Cts. L. Rev. 65 2006]

Withers, Kenneth J., Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure, Northwestern Journal of Technology and Intellectual Property, Volume 4, Number 2, 2006, s. 171 ff.

[Citeras: 4 Nw. J. Tech. & Intell. Prop. 171 2005-2006]

Offentligt tryck

NJA II 1943 s. 500

Prop. 1998/99:11

Prop. 2008/09:67

SOU 1938:44

SOU 2007:92

SOU 2008:63

The Committee Note to the 1970 amendments

The Committee Note to the 1993 amendments

The Committee Note to the 2006 amendments

Rättsfallsförteckning

USA

ACMG of Louisiana, Inc. v. Towers Perrin, Inc., 2007 WL 4373604 (N.D. Ga. Dec. 11, 2007)

Ameriwood Industries, Inc., v. Liberman, et al., 2006 WL 3825291 (E.D. Mo. December 27, 2006)

Balfour Beatty Rail, Inc. v. Vaccarello, 2007 WL 169628 (M.D. Fla. Jan. 18, 2007)

Bank of Magnolia v. M & P Global Financial Services, Inc., 258 F.R.D. 514, 2009 WL 1117312 (S.D. Fla. April 24, 2009)

Bethea v. Comcast, 218 F.R.D. 328 (D.D.C. Dec. 3, 2003)

Butler v. Kmart Corp, et al, 2007 WL 2406982 (N.D. Miss. Aug. 20, 2007)

Calyon v. Mizuho Sec. USA Inc., 2007 WL 1468889 (S.D.N.Y. May 18, 2007)

Cenveo Corp. v. Slater, et al., 2007 WL 442387 (E.D. Pa. Jan. 31, 2007)

Coburn v. PN II, Inc., 2008 WL 879746 (D. Nev. March 28, 2008)

Communications Center, Inc. v. Hewitt, 2005 WL 3277983 (E.D. Cal. April 5, 2005)

Diepenhorst v. City of Battle Creek, 2006 WL 1851243 (W. D. Mich. June 30, 2006)

Etzion v. Etzion, 62 A.D.3d 646; 880 N.Y.S.2d 79 (2nd Dep't May 5, 2009)

Equity Analytics, LLC v. Lundin, 248 F.R.D. 331 (D.D.C. March 7, 2008)

Ferron v. Search Cactus, L.L.C., 2008 WL 4458864 (S.D. Ohio April 28, 2008)

Frees. Inc. v. McMillian, 2007 WL 184889 (W.D. La. Jan. 22, 2007)

Gates Rubber Co. v. Bando Chemical Industries, Ltd., 167 F.R.D. 90 (D. Colo. May 1, 1996)

Illinois Tool Works, Inc. v. Metro Mark Prod. Ltd., 43 F.Supp. 2d 951 (N.D. Ill. April 22, 1999)

In re Ford Motor Company, 345 F.3d 1315 (11th Cir. Sep. 22, 2003)

In re Honza, 242 S.W.3d 578 (Tex. App. Waco Jan. 2, 2008)

In re Triton Energy Ltd. Securities Litigation, 2002 WL 32114464 (E.D. Tex. 7 mars 2002)

Koosharem Corp. v. Spec Personnel, LLC, 2008 WL 4458864 (D.S.C. Sept. 29, 2008)

Lauren Corp. v. Century Geophysical Corp., 953 P.2d 200 (Colo. App. Jan. 22, 1998)

Lawyers Title Ins. Corp. v. United States Fidelity & Guaranty Co., 122 F.R.D. 567 (N.D. Cal. Nov. 10, 1988)

McCurdy Group v. American Biomedical Group, Inc., 9 Fed. Appx. 822, 2001 WL 536974 (10th Cir. May 21, 2001)

Minnesota Minning & Manufacturing Co. v. Pribyl, 259 F.3d 587 (7th Cir. 2001)

Northwest Airlines, Inc. v. Local 2000, No. Civ. 00-08 (DWF/AJB) (D. Minn. Feb. 2, 2000)

Performance Chevrolet, Inc. v. Market Scan Information Systems, Inc., 2006 WL 980727 (D. Idaho April 11, 2006)

Playboy Enterprises v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. Aug. 2, 1999)

Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002)

Scotts Co. LLC v. Liberty Mut. Ins. Co., 2007 WL 1723509 (S.D. Ohio June 12, 2007)

Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639 (S.D. Ind. June 7, 2000)

Sims v. Lakeside School, 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007)

Southern Diagnostic Association v. Bencosme, et al, 833 So. 2d 801 (Fla. Dist. Ct. App. 2002)

Square D Co. v. Scott Electric Co., 2008 WL 2779067 (W.D. Pa. July 15, 2008)

Strasser v. Yalamanchi, 669 So.2d 1142 (Fla. 4th Dist. Ct. App. 1996), *rev. den.*, 805 so.2d 810 (Fla. 2001)

The Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645 (D. Minn. April 29, 2002)

Williams v. Massachusetts Mutual Life Insurance Co., 226 F.R.D. 144 (D.C. Mass. Feb. 2, 2005)

Sverige

NJA 1998 s. 590

NJA 1998 s. 829

Stockholms tingsrätts mål T 112-74

Svea hovrätt Ö 4004-09