# La búsqueda y conservación de los datos informáticos en el Derecho norteamericano. E-discovery

Antonio Evaristo Gudín Rodríguez-Magariños
Doctor en Derecho
Secretario del Juzgado Central de Instrucción n.º 6 de la Audiencia Nacional de España

Recibido: 13.11.2010
Aceptado: 20.12.2010

**Resumen:** La incorporación de la información electrónicamente almacenada al proceso, es una de las cuestiones más candentes en el derecho norteamericano. El enorme volumen de información que contienen los soportes informáticos y la mutabilidad de sus contenidos han determinado una reconsideración de los derechos y deberes de las partes en el proceso, creando un especial deber de diligencia en la preservación de este tipo de información. El cambio que se opera, tras la reforma procesal de diciembre de 2006 y que se continúa en enero del año 2009, se centra en que dicho deber se verá conculcado no sólo cuando las partes se enfrentan a un concreto proceso sino también cuando resulte previsible que este tenga lugar. De este modo, este deber que surge en el ámbito estrictamente procesal, se ha hecho extensivo a todos los ámbitos del derecho desde la protección de los datos de carácter personal, a los aspectos contables, administrativos, etc… atendida la eventualidad de la judicialización de las cuestiones que a aquellos se refiere.

**Palabras clave:** Búsqueda electrónica, Información electrónicamente almacenada, información especialmente protegida

**Abstract:** *The incorporation of electronically stored information to lawsuit is one of the most pressing issues in American law. The enormous volume of information contained in the computer media has implied a review of the parties' procedural rights and duties, to create a special duty of care to preserve information. The change that were made law by amendment of December 2006 and continues by amendment of January last year 2009, has led now, that this duty will be contravened not only when the parties face to a particular process but also when it is expected that it can take place. As a result of which, this duty purely procedural, it has been extended to all areas of law like the protection of personal data, accounting issues, administrative matters, etc. given that the judicial prosecution of these matters can be always possible.*

**Key words:** *e-discovery, inadvertent privilege waiver, electronic evidence*

## 1. **Cuestión previa: borrar no es suprimir**

Nuestro acervo jurídico, creado bajo la cultura del soporte papel, nos presenta la noción de documento como una unidad de información terminada y definitiva, en la que resulta imposible escindir el continente y el contenido. En el documento en papel no cabe alteración en cuanto que, una vez impresa en el papel, la tinta queda fijada de modo indeleble al soporte, resultando imposible materialmente separar uno de otro. En el documento electrónico por el contrario el vínculo entre continente y contenido es puramente convencional, por cuanto que la información contenida en un soporte informático está continuamente modificándose.[1]

En tal sentido, **en los documentos electrónicos puede diferenciarse, el continente -el soporte electrónico- del contenido del documento o -documento electrónico propiamente dicho-**.[2] El soporte electrónico es cual-

[1] Lo cierto sin embargo, es que aún tratándose de soporte papel, siempre existió la posibilidad de realización de documentos por otros medios que no presentaban ese carácter inescindible. En el documento realizado en lápiz es posible borrar el contenido, en este, ciertamente cabe la realización de una pericial que nos permitiese reconstruir lo borrado, pero resultaría imposible determinar si ha habido ulteriores adiciones o modificaciones en el documento. En este sentido, el documento tendría carácter auténtico, en el sentido que por medio de un análisis pericial podría identificarse su autor y su contenido, pero no resultaría definitivo.

[2] Así en el ordenamiento jurídico español, en el art. 3.5 de la Ley de Firma Electrónica en la redacción dada por la ley 56/2007, de 28 de diciembre de medidas de impulso a la sociedad de la información, dispuso que se consideran documentos electrónicos, *la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado* para señalar a continuación en su apartado 6 que *los documentos electrónicos serán soporte* tanto de los documentos públicos, como por los expedidos por funcionarios públicos, como de los documentos privados, con lo que existe una clara distinción del documento electrónico cuando actúa como soporte de otro documentos (art. 3.6), que cuando tiene sustantividad propia como información considerada en sí misma (art. 3.5).

quier medio apto para recibir y tratar la información, que permite en mayor o menor medida la identificación de su origen, y las alteraciones que se produzcan en el mismo, pero en el que en puridad no cabe identificar un contenido propio, pues éste va cambiando conforme a las necesidades del sistema donde se encuentra integrado. El documento electrónico exige además, el carácter ultimado e íntegro de dicha información, de modo que no sea posible alteración del mismo, sirviendo como medio de prueba del hecho que motiva su otorgamiento y la fecha de este, (1218 Cc.) o únicamente de la fecha de éste (1227 Cc). Se exige por tanto que a través de medios físicos o técnicos se impida la alteración de su contenido, véase mediante el volcado de su información a un medio indeleble, empleo de programas bloqueadores o a través de programas que permitan encriptar la información mediante la firma electrónica.[3]

De este modo resulta patente, que la inescendibilidad entre continente y contenido, no se presenta en los documentos electrónicos. Así si lo característico de los documentos es el carácter preconstituido y su virtualidad propia por la perfecta identificación entre la información y su soporte, tal característica no es del todo trasladable a los documentos electrónicos. Por lo pronto la corroboración de un documento en formato papel parte de la noción de evidencia, de aquello que es patente a la vista sin necesidad de entrar en otros razonamientos, mientras que en el documento electrónico su contenido está representado por signos, contenidos en códigos binarios, que deben ser descodificados mediante un programa con un procedimiento lógi-

[3] Esta confusión entre el alcance del soporte electrónico y el documento electrónico es bastante común. Así en el ámbito de la Administración Pública Española pese a la grandilocuencia con la que se suele presentar la importancia de dichos documentos su eficacia es bastante limitada. Así la Ley 11/2007, de 22 de junio, sobre el Acceso Electrónico de los Ciudadanos a los Servicios Públicos, pese al reconocimiento explicito del documento electrónico, a la alusión a "procedimientos administrativos gestionados en su totalidad electrónicamente" (art. 37), a "su iniciación "a solicitud del interesado por medios electrónicos" (art. 35.1) y a una "instrucción por medios electrónicos" (art. 36), incluso a la "terminación de los procedimientos por medios electrónicos" o la "resolución de un procedimiento utilizando medios electrónicos" (art. 38), lo cierto es, que de forma más discreta, establece algunas reservas frente a la digitalización del procedimiento administrativo, como la previsión del posible requerimiento de cotejo con sus originales de las copias digitalizadas aportadas al procedimiento (art. 35.2) y, sobre todo, la salvedad (formulada por el art. 38.2) de que "podrán adoptarse las resoluciones en forma automatizada en aquellos procedimientos en los que así esté previsto". Como señala Mira Ros, a la hora de la verdad, el acto administrativo por antonomasia que es la resolución administrativa, salvo que la norma lo permita especialmente, por regla general, no cabe en formato electrónico. Ese mismo escepticismo legal frente a la digitalización administrativa asoma también detrás de la obligación de mantener, en todo caso, las llamadas "oficinas de atención presencial", art. 7,2,a. de la Ley 11/2007 de 22 de junio, (Mira Ros, Corazón. "¿Una justicia por ordenador?" Revista del Notariado", Marzo Abril 2010,n.º 30).

co que convierta la expresión en codificación informática al lenguaje natural. Se exige, por ello, mecanismos técnicos que no están al alcance de la mayoría de las personas, y que de otra parte, aun conociendo su funcionamiento interno, tampoco presentan aquel carácter manifiesto que caracteriza al cotejo de la documental. En estos, se hace preciso aparte de la autenticación o cotejo de la información, el reconocimiento judicial del soporte informático no como elementos documentales, sino como efecto de convicción susceptible de reconocimiento judicial. Es por esto por lo que, el artículo 384.3 de la Ley de Enjuiciamiento Civil remite para la valoración de su contenido a las reglas de la sana crítica y no de la prueba tasada propia de los documentos propiamente dichos.

Pese a estas limitaciones, **el reconocimiento judicial de los soportes electrónicos permite la realización de operaciones que van a más allá de lo pretendido por los documentos tradicionales** y que dan píe a una nueva consideración de las diligencias de averiguación y cotejo de la información. Siguiendo los principios expuestos por la conferencia de SEDONA[4], caben destacar las siguientes características de los soportes electrónicos, que determinan el carácter sui generis de las diligencias de reconocimiento judicial de aquellos:

– Apariencia. Lo que se nos aparece a la vista cuando abrimos un documento electrónico, no se corresponde con una realidad tangible, sino que es mera apariencia, es lo que se conoce como entorno gráfico. La información a que accedemos presenta sólo el nivel más superficial del Iceberg que soporta el sistema, por debajo de aquel existen varios niveles sistemas de lenguaje informático que realmente son los que hacen que el documento se nos muestre de modo accesible, pero que a parte de esta función instrumental, contienen también a su vez otro tipo de información tales como metadatos, índices contadores, etc que son decisivos para conocer el origen y la eficacia de la información.
– Volumen y transmisibilidad de la información, la información contenida en los soportes informáticos es notoriamente superior a los medios tradicionales de documentación. Esto se debe al modo en que se transmite y se recopila la información. Pese a que no se ha llegado a un sistema de software libre propugnado por ciertas iniciativas como *Linux* es lo cierto que el entorno informático *Microsoft*, *Apple*, etc. se ha caracterizado en mayor o menor medida por el principio de libre transmisión de información sobre la base de códigos compartidos. Esto ha

[4] VVAA; *The Sedona Principles. Best practices & principles for adressing Electronic Document Production*,annoted versión, Coordinador Jonathan M. Redgrave, 2005, p. 7 y 8.

permitido la más fácil transmisión de información pero también la desprotección de los derechos de propiedad intelectual y la vulnerabilidad del sistema, (virus, *spam*, *spyware*, etc.).

– Metadatos. La existencia de estos sistemas que soportan la información, hace que junto a los datos que son visibles existan otra serie de datos que son estrictamente necesarios para el tratamiento informático de la información. La conferencia de Sedona define los metadatos como la información sobre la que los documentos o archivos quedan registrados que permiten al ordenador y al usuario la localización y el tratamiento de la información contenida en los documentos propiamente dichos.
– Persistencia. En un soporte electrónico cuando procedemos a suprimir un documento, en realidad lo único que hacemos es desvincular ese documento dentro del entorno visual, pero aquél permanece siempre, bien a través de las distintas copias de seguridad, *cookies* etc., bien a través código basura del documento, información que en la mayoría de los casos es perfectamente recuperable
– Contenido dinámico. Como hemos visto la información contenida en un documento digital no puede considerarse como algo definitivo, pues nunca cabe decir que esta es la versión definitiva del escrito que estoy haciendo, y siempre que dicha información no se salga de su entorno cabe una modificación posterior del documento. De este modo obtenemos tantas versiones del documento como modificaciones realicemos, de tal modo que no es tanto la consideración definitiva del documento como el marco temporal del mismo lo que determina su eficacia. Así, por ejemplo en un registro de una cuenta corriente obtenemos una situación distinta por cada movimiento contable que hacemos, sin embargo son tales movimientos los que proporcionan la unidad documental a la información. La consideración temporal del documento electrónico es pues esencial. Esto no sólo es predicable, de una tabla de datos, sino de cualquier documento. Como luego veremos la mayoría de las empresas proceden a la realización periódica de copias de seguridad. Antiguamente se realizaban diariamente por la noche cuando los sistemas no se encuentran operativos, pero actualmente en la mayoría de las empresas estas copias de seguridad se realizan continuamente a intervalos cada vez más cortos, de una hora o menos, copias de seguridad que nos permiten conocer cuál era la versión de cada documento, casi en cada momento. Por consiguiente, lo relevante no es tanto el carácter definitivo del documento sino cualquier versión del mismo durante el tiempo el que esté el ordenador encendido.

Por todo ello, cada una de las distintas unidades de almacenamiento informático, en su multiplicidad de versiones, puede ser considerada bien

como un solo documento en sí mismo, la totalidad de la información del soporte electrónico, o bien en consideración a cada uno de los documentos que se contienen en el mismo, cuyo carácter definitivo dependerá de la eficacia que pretendamos dar a la información contenida en aquellos al salir del entorno en que se encuentra.

Si el derecho europeo se ha centrado, en el segundo aspecto, particularmente en los aspectos relativos al **cotejo de los documentos electrónicos** propiamente dichos, aspectos en los que recientemente nos hemos ocupado[5], en el sistema jurídico norteamericano, se ha centrado en los aspectos relativos a la **averiguación y reconocimiento, no tanto de los documentos como de los soportes informáticos**, particularmente el alcance del deber de preservación, y los límites y garantías de acceso aquellos soportes, como medio de prueba en el proceso, aspectos en los que se centrará el objeto del presente estudio.

## 2. Tratamiento de la cuestión en el derecho norteamericano. La configuración del deber de preservación de la información electrónicamente almacenada.

Las diligencias de reconocimiento judicial de los soportes electrónicos o averiguación electrónica, (e-discovery) han supuesto en los Estados Unidos, una verdadera revolución del derecho procesal. El enorme volumen de información que se contienen en los soportes informáticos y la mutabilidad de sus contenidos han determinado una reconsideración de la eficacia procesal de la prueba documental. Como veremos el principio fundamental que inspira la regulación de esta cuestión, se encuentra en el denominado deber de preservación. Este deber de preservar los datos potencialmente relevantes en el proceso se fundamenta en el deber de diligencia y en las reglas de la buena fe. El cambio que se opera por las últimas reformas procesales en los Estados Unidos, se encuentra en que dicho deber de diligencia se verá conculcado no sólo cuando las partes se enfrentan a un concreto proceso sino también cuando resulte previsible que este tenga lugar. De este modo, este deber que surge en el ámbito estrictamente procesal, se ha hecho extensivo a todos los ámbitos del derecho desde la protección de los datos de carácter personal, a los aspectos contables, administrativos, etc… atendida la eventualidad de la judicialización de las cuestiones que a aquellos se refiere.

El principio básico en la materia procesal viene contenido en la regla 26 a) apartados (i) y (ii) de las reglas federales del proceso Civil que señalan:[6]

---

[5] Gudín Rodríguez-Magariños, Antonio Evaristo. "La diligencia de cotejo de los documentos electrónicos". Revista General de Derecho Procesal, Iustel, n.º 11, 2010.

[6] (A) In General. Except as exempted by Rule 26(a)(1)(B) or as otherwise stipulated or ordered by the court, a party must, without awaiting a discovery request, provide to the other parties: (i) the name and, if known, the address and telephone number of each individual

En general, salvo en aquellos actos procesales que encuentren exentos por la regla 26 (a) (1) (b) o cuando exista una disposición en contrario acordada por las partes u ordenada por el Tribunal, cada parte debe proceder, sin esperar la solicitud de averiguación, a proporcionar a las otras partes:

(i) El nombre y si lo sabe, la dirección y el número de teléfono de cualesquiera individuos que probablemente puedan tener información de interés, y que la parte revelante pueda usar para respaldar sus alegaciones, a menos que su empleo sólo lo fuese para reprobar la actuación de aquellos. [7]

(ii) Una copia o una descripción por clases y locación de todos los documentos, información electrónicamente almacenada y soportes tangibles que la parte tenga en su posesión, custodia o control y debe de usar para mantener su demanda o defensa, a menos que su empleo sólo lo fuese para reprobar otros medios de prueba.[8]

Todo esto determina un deber de diligencia a la hora de la preservación de nuestra información electrónicamente almacenada, creando un especial

---

[78] likely to have discoverable information — along with the subjects of that information — that the disclosing party may use to support its claims or defenses, unless the use would be solely for impeachment; (ii) a copy — or a description by category and location — of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment; (iii) a computation of each category of damages claimed by the disclosing party — who must also make available for inspection and copying as under Rule 34 the documents or other evidentiary material, unless privileged or protected from disclosure, on which each computation is based, including materials bearing on the nature and extent of injuries suffered; *(Una relación de los daños reclamados por la parte aportante, quien debe también permitir la exhibición y copia conforme a las previsiones de la regla 34 de los documentos u otros materiales de prueba en los cuales se fundamenta el cálculo de los perjuicios, salvo aquellos que se encuentren protegidos o excluidos de la revelación. Se incluyen entre estos los materiales que sustenten el carácter y la extensión de los perjuicios.)* and (iv) for inspection and copying as under Rule 34, any insurance agreement under which an insurance business may be liable to satisfy all or part of a possible judgment in the action or to indemnify or reimburse for payments made to satisfy the judgment. *Dentro de la revisión y copia conforme a las previsiones de la regla 34, deberá de entenderse incluidos cualquier acuerdo de aseguramiento con una empresa de seguros que pueda ser responsable de satisfacer en toda o parte la eventual condena o indemnizar o reembolsar los pagos hechos para evitar el juicio.*

[7] Literalmente "….for impeachment", con carácter genérico reprobación o descalificación, así article impeachment o witness impeachment, expresión que debe de interpretarse en el sentido que los datos aportados lo sean para el ejercicio de derecho de defensa y no para impugnar otras pruebas o testimonios.

[8] Literalmente "…for impeachment", véase nota anterior.

deber de custodia a la hora de conservar la información contenida en nuestros archivos. No es necesario que exista un concreto requerimiento en orden a la preservación de información en vistas a la celebración del juicio, sino que las partes como sujetos de derecho tienen el deber, no sólo de preservar toda la información incorporada a sus sistemas informáticos, sino también de procurar que la misma sea accesible con vistas al proceso. De este modo, cualquier alteración o destrucción de aquella información determinará que nos veamos privados de un medio de prueba cuando no una presunción en contra de la existencia de los datos desaparecidos de nuestros soportes informáticos.

## 3. **El origen del problema el caso United states v. Quattrone**

Hasta no hace mucho tiempo no era inusual en las empresas o en la Administración que los ejecutivos o funcionarios cuando cesaban en su trabajo procediesen a hacer limpieza de los archivos que han venido almacenando de forma asistemática durante años. Dado el enorme volumen de los documentos inservibles, borradores, notas, apuntes, etc… que normalmente solemos emplear, nunca tenemos el tiempo bastante para proceder a eliminar de forma sistemática los archivos realmente innecesarios y muchas veces forzados por la necesidad se procede a realizar un barrido de documentos a fin de evitar que queden en el sistema documentos comprometedores o de carácter estrictamente personal. Esta práctica adquirió tintes de escándalo en los Estados Unidos a finales de 2002 y durante todo el año 2003. En aquel tiempo los periódicos de mayor difusión de los Estados Unidos, publicaron una serie de artículos en los que se señalaba como muchas compañías animaban a sus empleados a suprimir archivos cuando fuese de esperar el inicio de un proceso o de un expediente de la administración tributaria.[9] El caso más sonado fue el de *United States v. Quattrone,* (USCA 2d Cir, Mar. 22, 2005)[10], en este proceso penal se analizaba el comportamiento del Sr. Frank Quattrone, quien se encontraba a la espera de una investigación federal dentro de una emisión de oferta pública de acciones sometida al control de la comisión de valores. En vistas de dicha visita de inspección, el señor Quattrone envió a sus empleados un e-mail, en el que se recomendaba encarecidamente que se realizase una limpieza a fondo de los archivos antes de salir de vacaciones. Por este hecho Mr. Quattrone fue sentenciado a 18 meses de prisión por un delito de obstrucción a la acción de la agencia federal y de manipulación de testigos. La sentencia, sin embargo fue anulada y se orde-

[9] SCHEINDLIN Shira A. & WANGKEO, Kanchana. "Electronic Discovery Sanctions in the Twenty-First Century", Mich. Telecomm. Tech. L. Rev. 71. 2004.

[10] *United States v. Quattrone*, 402, f.3d, 304, S. Sotomayor, (USCA 2d Cir, Mar. 22, 2005).

nó un nuevo juicio por una mala instrucción del jurado. Mr. Quattrone alcanzó finalmente un acuerdo de suspensión del proceso, antes de llegar al nuevo juicio.

Sin embargo, es el caso *Arthur Andersen LLP v. United States (USCA 2005)*[11], el que realmente determinó un cambio de mentalidad sociedad americana y puso en la palestra los problemas que se derivan de la preservación de documentos electrónicos. Este caso, surge como una derivación de la quiebra de la mercantil ENRON una empresa de energía con sede en Houston que constituía, con anterioridad a su quiebra, la séptima mayor empresa del país y la primera en el sector energético. La cobertura dada por la sociedad de auditoría Arthur Andersen, en la que algunos de sus empleados estaban en nómina también en ENRON, convirtió la quiebra de ENRON en el más grande fraude empresarial de la historia de los EEUU y en el arquetipo de fraude empresarial planificado. Se acusaba a Arthur Anderesen, de que durante el tiempo que estuvo encargada de la auditoria, y en vistas de que la investigación se dirigiese también frente a la sociedad auditora, los responsables de Arthur Andersen dieron instrucciones concretas a fin de proceder a la destrucción sistemática de información en relación a la empresa ENRON, esto dio lugar en mayo de 2002 a la presentación de cargos contra Arthur Andersen, siendo encontrado culpable por el jurado del subdistrito Sur de Tejas por estos hechos, por veredicto pronunciado el 8 de junio de aquel año. Apelada la sentencia ante el Tribunal Supremo de los Estados Unidos, en una decisión unánime, el Tribunal Supremo anuló la condena de Arthur Andersen. En la sentencia de la que era ponente William Rehnquist se estimó que no había existido una voluntad manifiesta de que la empresa pretendiera persuadir a sus empleados para que procediesen a la supresión de documentos. Los gerentes de Arthur Andersen, reconocían que dieron instrucciones a sus empleados para eliminar los archivos relacionados con ENRON, pero esas medidas estaban dentro de su política de retención de documentos de la empresa y de supresión de la información de índole privada de sus empleados. Si la infraestructura del sistema de gestión de documentos estaba construida para mantener cierta información privada, Arthur Andersen carecía de facultades para persuadir a sus empleados para mantener o destruir dicha información. En opinión del tribunal, las instrucciones remitidas por Andersen a sus empleados, no eran lo bastante concretas para demostrar que la empresa sabía que había violado la ley o que quedase constatada una voluntad de vulnerar de forma sistemática la normas que prohíbe la destrucción de documentos cuando estos se deben de aportar al proceso. Las instrucciones eran tan vagas, escribió Rehnquist, que *«simplemente no transmitían la conciencia necesaria de su mala conducta»*. Pese al carácter del fallo dictado, el

[11] *Arthur Andersen LLP v. United States,* 544 U.S. 696, R.J. Rehnquist (USCA 5.º Cir. 2005), 374 f.3d 281, ponente

caso supuso un cuestionamiento determinadas prácticas y la necesidad de escindir el ámbito privado de acceso a los datos y el propio de la gestión empresarial, atendida la vinculación que muchos de estos asesores tenían con la sociedad ENRON.

Estos dos casos, y los cientos de casos, exactamente iguales, que le siguieron, pusieron de relieve el peligro que supone la eliminación de archivos indiscriminada y la necesidad de preservar la información electrónicamente almacenada. La jurisprudencia norteamericana a raíz del caso Quattrone y de la experiencia del caso Arthur Andersen fue evolucionando hacia imponer unas mayores exigencias a la hora de la conservación de la información. Al igual que sucede en materia contable el principio de transparencia, se imponía como una exigencia insoslayable en el tratamiento de la información electrónicamente almacenada, no sólo cuando se había iniciado un proceso, sino cuando hubiese visos de que pudiese ser plantearse.

La cara contraria de la moneda, se producía cuando requerida una parte para la aportación de los documentos informáticos, se hacía aportación indiscriminada de los archivos sin tener en cuenta que entre aquellos archivos pudiese encontrarse información comprometida o confidencial. En estos casos, conocidos como *privilege inadvertent waiver* o simplemente *privilege waiver*, (renuncia al privilegio) se producía el efecto contrario, al perder la información aportada el carácter de especialmente protegida como consecuencia de su falta de celo a la hora discriminar lo que se facilita a la parte contraria. Esto dio lugar a un conflicto jurisprudencial, así si muchos tribunales norteamericanos preservaban el derecho a la confidencialidad de esos datos y reaccionaban frente a la parte que se había beneficiado de la buena fe del que hizo aportación de aquellos, otros fallos por el contrario imputaban las consecuencias de este error a la parte que no había guardado la diligencia necesaria en la clasificación y conservación de dicha información.

Por otra parte, si los tribunales norteamericanos empezaron a exigir cada vez mayor diligencia en la clasificación y ordenación de la información electrónicamente almacenada, también se encontraron con los excesos de celo de quienes en el ejercicio del derecho de defensa solicitaban la exhibición o aportación de información, que por su volumen o difícil acceso, excedía notoriamente de los medios y recursos de las empresas, resultando en muchos casos abusivo la paralización de los sistemas informáticos (*smoking gun*), cuando no el acceso torticero a información confidencial o al know how de las empresas competidoras por estos medios, (*phishing expedition*).

Así en el *In re Ford Motor Company*, (USCA 11th Cir. 2003),[12] el tribunal de apelación revocó la decisión del tribunal de distrito, por la que ordenaba a Ford dar al demandante acceso a los sistemas de relación con los pro-

[12] *In re Ford Motor Company*, 345, F.3d 1315, J.L. Edmondson, (USCA 11th Cir., september 22, 2003).

pietarios (MORS) y las bases de datos de los sistemas de indicadores de calidad (CQIS) de Ford, por estimar abusiva dicha petición. Posteriormente numerosa jurisprudencia incidió en estos abusos, así *Bethea v. Comcast.,* (D.D.C 2003)[13], *Simon Prop. Group L.P. v. Simon Inc.* (S.D. Ind. Jun 7, 2000)[14], *Balboa Threadworks Inc. V. Stucky* (D. Kan. Mar. 24, 2006)[15], sin embargo fue el caso Zubulake el que estableció el standard jurisprudencial en orden a fijar los criterios a tener en cuenta para la valoración de los costes y las cargas y el derecho de la parte a acceder a información de interés para la defensa de sus intereses.

## 4. **El caso Zubulake y la reforma procesal de 2006. La accesibilidad de la información electrónicamente almacenada.**

Esta situación dio lugar en el año 2006, a una de las reformas procesales de mayor calado en la historia de los Estados Unidos. Junto a otras modificaciones se incluyen revisiones a las reglas 16, 26, 33, 34, 37 y 45 de las Reglas Federales del Proceso civil, (*The Federal Rules of Civil Procedure*, en adelante FRCP) a lo largo de las cuales se proporciono las líneas generales del sistema legal, en los supuestos de decisiones sobre información electrónicamente almacenada, incluyendo cuestiones tales como la publicidad, la posibilidad de averiguación, la renuncia anticipada, los deberes de protección y el coste. La regla fundamental en esta materia se encuentra incorporada a la regla 26 de las FRCP que debe de completarse recientemente por la modificación del art. 502 de las Reglas Federales de la Prueba, (*Federal Rule of Evidence*, en adelante FRE). La regla 26(b)(2)(B), es consecuencia de la modificación operada en diciembre de 2006 en la regulación de la diligencia de averiguación, «discovery», semejante a nuestras diligencias preliminares. La nueva regulación del precepto parte del principio de que todo documento es revelable y debe de aportarse a las actuaciones si es razonablemente accesible. La modificación a la regla 26 (b) (2) fue diseñada para resolver las cuestiones surgidas como consecuencia de las dificultades en la localización, recuperación y aportación de información electrónicamente almacenada. Los sistemas de almacenamiento de información con frecuencia facilitan bastante la localización y recuperación de información, pero en ocasiones el acceso a estos medios puede implicar importantes costes o la imposición de cargas no justificadas, como la renuncia a la confidencialidad de la información empresarial o imponiendo restricciones al derecho de defensa de las partes.

---

[13] *Bethea v. Comcast.,* 281 FRD 328, 329-30, John M. Facciola, (D.D.C 2003).

[14] *Simon Prop. Group L.P. v. Simon Inc.,* 194 FRD 639, 641, David Hamilton, (S.D. Ind. Jun 7, 2000)

[15] *Balboa Threadworks Inc. V. Stucky, WL,* 763668, Donald Bostwick, (D. Kan. Mar. 24, 2006).

En supuestos concretos, estas cargas y costes pueden dar lugar a que la información contenidos en dichos soportes no sea razonablemente accesible.

Esta reforma legal, es consecuencia de la doctrina que en torno a la accesibilidad de los documentos electrónicos surge a raíz del caso *Zubulake v. UBS Warburg* (SDNY, May 13, 2003)[16], conocido comúnmente como Zubulake I. En el caso Zubulake, se solventaba una reclamación por discriminación en el empleo, y se discutía las consecuencias de la falta de aportación de varios meses de correos electrónicos, desechados por la compañía USB Warburg luego de que se presentase una denuncia ante la Agencia Federal de Estados Unidos encargada de supervisar la igualdad de oportunidades ante el empleo.

El tribunal hizo saber entonces a los abogados de la defensa, que la empresa era parcialmente culpable de la destrucción de documentos, imputando a la misma las consecuencias de la falta de cumplimiento de su obligación de localizar esa información electrónica relevante, de preservar esa información y del deber procesal de aportación de dicha información en su momento procesal. El tribunal afirmó entonces: *Consuel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched*, «los asesores jurídicos de la empresa deben de poner los medios necesarios para vigilar que todas las fuentes de información revelable este identificadas y localizadas». Esto implicaba la asunción de responsabilidad por encubrir la ausencia de documentos que se estimaban decisivos para la resolución de la cuestión. De este modo, el tribunal dictó una instrucción inferencia adversa o presunción en contrario, a los miembros del jurado, en el sentido de asumir como ciertos aquellos correos electrónicos, desechados por UBS, después de que Zubulake presentase una denuncia ante la agencia federal de Estados Unidos encargada de supervisar la igualdad de oportunidades ante el empleo. Esta presunción sería decisiva en el caso, y así, en Abril de 2005, después de tres años del litigio, el juicio culminó con el veredicto por el que el jurado encontró a la compañía culpable de haber discriminado a Laura Zubulake y la indemnización de aquella en más de $ 29 millones por daños y perjuicios.

Para llegar estas conclusiones, el tribunal en el caso Zubulake distinguió la existencia de dos niveles según el carácter accesible o no de la información, esto es, según si la información puede identificarse a primera vista o por medio de un simple muestreo, o por el contrario exige el análisis forense de los soportes informáticos:

– El primer nivel está compuesto por la información que es identificada como accesible. La información accesible en este primer nivel debe de

[16] *Zubulake v. UBS Warburg,* WL 2003 21087884, Shira Sheindlin, (SDNY, May 13, 2003)

aportarse automáticamente cuando se es requerido de contrario. En este primer nivel, la parte requerida soporta la carga de la prueba de demostrar que la información inicialmente identificada como accesible resulta inaccesible debido a que implicaría asumir unas cargas desproporcionadas o costes innecesarios asociados a su aportación al proceso. Si la parte requerida justifica satisfactoriamente esta carga la información debida será identificada como inaccesible.
– En el segundo nivel, se parte del supuesto contrario, en el que la información es en principio inaccesible. La carga de probar se traslada a la parte requirente, debiendo dar una justa causa que justifique la intromisión a pesar de los costes o de las cargas que esto implique.

Para discriminar si una información es accesible o no, en la sentencia dictada en el caso Zubulake se identifican cinco categorías de datos, relacionados estos por orden desde los más accesibles a los menos accesibles, y se afirma que las tres primeras categorías pueden identificarse por regla general como supuestos típicos de información en principio accesible, mientras que los dos segundos son supuestos de documentos inaccesibles en el sentido anteriormente expuesto. Pese a que no se tratan de categorías rígidas, como señala LANGE & NIMSGER,[17] tales categorías nos resultarán muy útiles como modelo para determinar la accesibilidad de los datos y poder entonces sopesar los costes y cargas frente al acceso a la información.

Las cinco categorías de datos son las siguientes:

– Datos en soportes fijos. (*Active on line*). Son aquellos que se pueden ver y acceder, al arrancar nuestro sistema informático y se conocen como activos, o datos on-line. Estos datos están generalmente almacenados en nuestra unidad central o servidor y son los que presentan el acceso más directo para los usuarios.
– Datos en componentes extraíbles. (*Near Line*). Estos datos pueden crearse y leerse desde instrumentos de almacenamiento, si se conectan al ordenador. Dentro de estos, cabría hacer una distinción según si los soportes pueden ser regrabados o no, y dentro de los primeros si puede modificarse el archivo o tiene que ser reconstruido para poder ser alterado. Estos datos son de fácil acceso siempre que se reconozca el soporte por el ordenador.
– Almacenamiento de registros (*Offline storages*). Los datos puede ser creados y reproducidos por el sistema informático del ordenador pero carecen de virtualidad por sí mismos. La probabilidad de recuperar

[17] LANGE, Michele C.S. y NIMSGER, Kristin M. *Electronic Evidence and discovery: what every lawyer should know now*, American Bar Asociation, Section of Science of technology Law, 2nd edit., 2010, p.75

estos datos es mínima y la accesibilidad es mucho más lenta que las dos anteriores.
– Copias de seguridad. Los datos contenidos en una copia de seguridad son creados por un dispositivo al igual que una cinta de registro que lee datos desde el sistema informático y los transcribe a una cinta. Los datos contenidos en cintas backup no son de fácil acceso porque las búsquedas de la organización de los datos en la cinta y las características del software, hacen precisa la reconstrucción de los datos.
– Datos eliminados, fragmentados o dañados. Estos datos no son accesibles para la generalidad de los usuarios, quedando reservado su acceso a los expertos especializados en ingeniería informática forense, quienes son los únicos que pueden analizar y recuperar los datos haciéndoles accesibles.

Una vez que se constate, que la información de un soporte electrónicamente almacenado no es razonablemente accesible, la parte contraria podrá todavía obtener la averiguación aduciendo una justa causa. La decisión sobre si la información solicitada no es razonablemente accesible depende no sólo de las cargas y costes, sino también sobre si esas cargas pueden estar justificadas en las circunstancias del caso. La sentencia agrupa estas circunstancias en tres grupos:

– El primer grupo de factores atiende al margen de utilidad. Estos factores incluyen (1) La especificación de una concreta información relevante y (2) la disponibilidad de tal información desde otras fuentes. La esencia del margen de utilidad fue correctamente descrita en *Mcpeek v. Ashcroft* (DDc, Jun 9, 2003)[18]. En este asunto, las copias de seguridad, contenían sólo parcialmente la información de modo que había periodos de tiempo en que los datos se encontraban completos y otros periodos de tiempo en que se había perdido la información. Los abogados de las partes no se ponían de acuerdo sobre el modo y sobre quien tenía que soportar el coste de la aportación de dicha información. El juez John M. Facciola señaló entonces que en dichas cintas se podrían encontrar datos relevantes tanto para una como para otra parte, sin embargo lo menos probable sería lo más injusto, estimando que dicho gasto debería de imputarse a quien presentase mayores visos de utilidad. Para determinar la probabilidad el tribunal ordenó hacer un muestreo de la información contenida en uno de los ordenadores de un empleado durante el periodo de un año, y en función de estos resultados adoptó la decisión que le pareció más justa.

[18] *Mcpeek v. Ashcroft,* U.S. Dist. LEXIS 172, John M. Facciola, (DDc, Jun 9, 2003).

– El segundo grupo de factores se dirige a valorar el coste de estas cuestiones. Cuánto costará la aportación de la información y quien manejará estos costes. Estos factores incluyen el total coste de aportación de la información en relación con la entidad de la controversia y con las fuentes a disposición de cada una de las partes, así como la relativa capacidad de cada parte para controlar los costes y los incentivos necesarios para llevarlo a efecto.
– El tercer grupo, atiende a la importancia de la litigación en sí misma, y como se indicó anteriormente tal previsión raramente entra en juego dado el desconocimiento último de la información que puede ser encontrada. Este factor, sin embargo, tiene el potencial de predominar sobre los otros.

El tribunal precisó que estos factores no deberían ser equiparados, pues su determinación quedaba condicionada a los costes implícitos en el cambio y el traslado de la información. Sopesando los factores por su importancia decreciente se pueden solventar los problemas que se derivan de una rígida aplicación de la regla.

Conforme a estas premisas, la sentencia ordenó a UBS aportar todos los *e-mails* de interés que existían su disco duro o en sus servidores a costa suya. Se ordenó también a UBS aportar por su cuenta, los *e-mails* indicados desde cualquier de las cinco cintas de back-up seleccionadas por Zubulake. UBS debería también de realizar una declaración jurada detallando los resultados de la búsqueda como también el tiempo y el dinero invertido. Después de revisar los contenidos de las cintas de back-up y a la vista de la certificación aportada por UBS el tribunal debía de llevar también a cabo un análisis adecuado de los costes de desplazamiento.

## 5. **La regla 26 de las reglas federales del proceso civil.**

La regla 26 acoge esta doctrina y configura el marco legal para llevar a cabo la aportación de la información electrónicamente almacenada sobre la base de la regla de la buena fe. Conforme a esta regla, las partes deben de facilitar la información electrónicamente almacenada que resulte relevante, que no esté especialmente protegida y que resulte accesible, estando sujeta a las limitaciones comunes a todos los medios de prueba. Como hemos visto, las partes deben también aportar copia, o identificar por categorías o modo de localización, los soportes que la parte aportante tenga en su poder, custodia o control y que puedan contener potencialmente información de interés para sostener su pretensión o para su defensa. La identificación, en la medida de lo posible, debe de proporcionar suficientes detalles para permitir al solicitante de la prueba evaluar las cargas y costes, que implique la averiguación y la probabilidad de encontrar la información solicitada, en los soportes correspondientes.

Siguiendo el sistema de dos niveles propuesto por el caso Zubulake, el artículo 26 prevé que una vez que se constate, que la información de un soporte electrónicamente almacenado no es razonablemente accesible, la parte contraria podrá todavía obtener la averiguación aduciendo una justa causa, dentro de las limitaciones de la regla 26 y luego de que el tribunal sopese los costes y los potenciales beneficios de la averiguación. Se deberán de tener en cuenta para ello las siguientes consideraciones ya referidas en el caso Zubulake:

– La especificidad de la solicitud de averiguación.
– La cuantía de la información disponible a través de otros medios de más fácil acceso.
– La imposibilidad de reproducir la información relevante que probablemente puede haber existido, pero que no se encuentre disponible en las fuentes de más fácil acceso.
– La probabilidad de encontrar información de interés que no pueda obtenerse por otros modos de más fácil acceso.
– Las predicciones sobre la importancia y la utilidad de la información ausente.
– La importancia de las cuestiones pendiente en el litigio.
– Los recursos con que cuenten las partes para hacer frente a las cargas y costes de la averiguación.

Si las fuentes identificadas no son razonablemente accesibles en atención a las cargas y costes exigidos, la parte contraria tendrá la carga de demostrar que la necesidad de acceder a dicha información supera las cargas y costes de localización. La determinación de la justa causa, sin embargo, puede resultar bastante complicada porque los tribunales y las partes suelen saber poco de antemano acerca de la información que pueda llegarse a encontrar en los soportes electrónicos. En tales casos, las partes deberán centrar su atención, en la realización de muestreos de los soportes electrónicos, para poder aprender más sobre que cargas y costes se encuentran implicados en el acceso a la información de que se trate. Como veremos después, en esta tarea será especialmente relevante la forma en que se haya podido exteriorizar dicha información, así contestación a un correo electrónico anterior, datos contenidos en balances o documentos contables, etc.

En todo caso, como señala el comentario a la regla 26, el Tribunal tiene casi completa discrecionalidad en la determinación de lo que deba de entenderse por justa causa. En general el tribunal comparará las necesidades de las partes en la búsqueda de averiguación frente a las cargas de la parte contraria, la existencia de otros medios y la importancia de poder acreditar algún extremo de prueba relevante para el resultado del litigio.[19] El examen de la

[19] BAICKER- MCKEE, Steven, JANSSEN, Willian y CORR, Jhon Bernard. *Federal Rule of Civil Procedure* handbook, West Group, 2004, pp. 529-593.

justa causa y la consideración de las limitaciones previstas en la regla 26 (b) (2) (C), se deben de conjugar también con la autoridad que tenga el juez para poner condiciones para la averiguación dentro de la particular posición que ostenta el juez en el proceso norteamericano. Las condiciones pueden llevar la forma de límites sobre la cantidad, el modo o las fuentes de información exigidas para que se acceda a la información. Las condiciones deben también incluir la propuesta de pago de parte o de todo de lo costas razonables por la obtención de información desde fuentes que no sean razonablemente accesibles, así como su voluntad de soportar los costes que puedan ser adelantados por el tribunal para la determinación si había o no justa causa.

La identificación por la parte de los soportes electrónicos que contengan información electrónicamente almacenada como no racionalmente accesibles no releva a la parte de sus deberes de preservar los medios de prueba. El volumen y la capacidad para buscar información electrónicamente almacenada implican que en muchos casos la parte contraria será capaz de aportar dicha información desde otras fuentes razonablemente accesibles que satisfarán por completo las necesidades de averiguación por las partes. En muchas ocasiones la solicitud habrá de partir de la evaluación de la posibilidad de acceso a la información desde otros soportes, antes de insistir en que la parte contraria busque y presente la información contenida sobre soportes que no son razonablemente accesibles. Si la parte continúa buscando información sobre soportes identificados como no razonablemente accesibles, las partes deberán discutir las cargas y los costes del acceso y revisión de esta información, la necesidad que deba de establecer una justa causa para requerir todo o parte de la averiguación solicitada incluso si la información solicitada, no es razonablemente accesible y las condiciones para la obtención y aportación de la información puedan ser inapropiadas.

## 6. **Sanciones por expoliación**

En el derecho norteamericano presenta una extraordinaria importancia el principio de transparencia, cualquier ocultación de información que se detecte en el curso del proceso, es vista como una actuación torticera que determina una presunción en contrario, pues si algo se oculta es que no existe una convicción bastante para demostrar la realidad de los hechos. Es lo que se conoce en el derecho norteamericano como expoliación, «*spoliation*». Cualquier alteración destrucción o fracaso en la obligación legal de preservación de las pruebas, así como cualquier conducta que dé lugar a inaccesibilidad de la prueba, determina la existencia de una expoliación.

De este modo, la expoliación implica un prejuicio injusto para la parte contraria, en cuanto que se restringe o imposibilita el acceso a la realidad de los hechos, lo que da lugar a que está situación sea corregida por el juez. Los Tribunales en Estados Unidos tienen a este efecto autoridad bastante para imponer sanciones contra las partes que violen la ley o las resoluciones de

los tribunales dictadas en el seno del proceso, dentro del ámbito de su competencia y conforme a las reglas del procedimiento civil. Las sanciones pueden dictarse por una incorrecta averiguación, por la aportación de la documentación fuera de plazo, por realizar la aportación en un formato inadecuado, por el incumplimiento de cualesquiera otras resoluciones del tribunal, etc. En este sentido, en *Zubulake v. UBS Warburg* (DC SDNY, Oct. 22, 2003),[20] conocido comúnmente como Zubulake IV, se insiste en que la determinación de la severidad de las sanciones es una determinación confiada a la discreción del juez cuya concreta evaluación debe de hacerse caso por caso, (ver también *Linnen v. A.H. Robins Co.* [Mass. Super. June. 16, 1999][21]). Tales sanciones, que son inherentes al poder de policía que corresponde al juez en el ejercicio de la dirección del proceso, presentan unas especiales características en el derecho procesal norteamericano en la medida que no corresponde al juez la apreciación última de la prueba sino al jurado, lo que determina cierta distorsión del sistema cuando el juez interfiere excluyendo un medio de prueba.

Sin embargo, a diferencia del derecho continental, los tribunales norteamericanos no se encuentran constreñidos a las normas del procedimiento a la hora hacer valer las facultades de policía en orden a la dirección del procedimiento, previendo la imposición de una gran diversidad de sanciones. Así siguiendo a GEORGE & NEARON (2006, p. 46),[22] podemos señalar las siguientes:

– Imponiendo sanciones pecuniarias.
– Permitiendo al tribunal dirigir instrucciones al jurado sobre la presunción en contra de determinados hechos.
– Preclusión de medios de prueba.
– Imponiendo un veredicto dirigido.
– Penalizando la conducta de las partes por obstrucción a la justicia.
– Imponiendo sanciones disciplinarias a los abogados.
– Deduciendo responsabilidades civiles.
– Anulación del proceso, restringir el objeto del proceso o sobreseerlo.

Estas sanciones son por otra parte **acumulables**. Un buen ejemplo de un caso de acumulación de las más diversas sanciones, es el del caso *William T.*

---

[20] *Zubulake V. UBS Warburg,* LLC 220, FRD 212, US Dis Lexis 18771, Shira Sheindlin, (DC SDNY, Oct. 22, 2003).

[21] *Linnen v. A.H. Robins Co.* 1999, WL 462015, Raymond J. Brassard (Mass. Super. June. 16, 1999).

[22] PAUL, George, L. y NEARON, Bruce H. *The discovery revolution, e discovery amendments to the federal Rules of Procedure*, American Bar Asociation, 2006, p. 46.

*Thompson Co. v. General Nutrition*, (3d cir. CD Cal. 1984).[23] En este asunto, los ejecutivos que estaban al frente de la empresa, contraviniendo la orden de preservación dictada por el tribunal, dirigieron a sus empleados directrices para que continuasen con el reciclaje de cintas de *back-up*, indicando que esto estaba permitido conforme a dicha resolución. El tribunal desaprobó esta actuación, declaró la nulidad del juicio, e individualmente impuso sanciones a los ejecutivos que lo ordenaron por importe de hasta 450.000 $.

De estas sanciones la más relevante es la que se refiere a la **instrucción al jurado de presunción en contrario**, (*adverse inference*). Esta instrucción permite al jurado presumir la existencia de determinados hechos en contra de la parte responsable de la pérdida o destrucción de las pruebas. El *standard* de este tipo de instrucciones, fue articulado en el caso Zubulake:

> La expoliación dirigida a evitar que se profundice en la averiguación de ciertos elementos de prueba puede suponer una presunción de que la prueba no habría sido favorable para la parte culpable de la destrucción de dicha información. Para que esto pueda darse deben de concurrir los siguientes requisitos:
> (1) que la parte que ostente el control sobre la prueba tenga una obligación de preservarla en el momento que fue destruida.
> (2) Que los registros que hayan sido destruidos teniendo conocimiento de esta circunstancia la parte que debiera de aportarla,
> (3) que las pruebas destruidas resulten relevantes para la pretensión de la parte o su defensa, de modo tal, que se pudiese deducir una más que probable conclusión sobre la certeza del hecho, de haberse desenvuelto plenamente este medio de prueba.

En el caso *Hodge v. Wal Mart (*USCA 4th Cir., Mar. 10, 2004),[24] se muestran, sin embargo, las limitaciones de estos remedios. Allí, el tribunal sostuvo que la imposibilidad de la parte demandada de obtener información para contactar con el testigo, que había visto como se cayeron los espejos y como se causaron las lesiones al cliente, no garantizaba que se pudiese hacer una presunción en contrario. El pretendido expoliador, no tenía el control sobre la prueba y no perdió o alteró voluntariamente las pruebas, no se apreció por ello la existencia de una expoliación bastante como para hacer una presunción en contra. Según PAUL Y NEARON,[25] esta es línea en la que se mue-

---

[23] *William T. Thompson Co. v. General Nutrition*, 593 F. Supp.1443, 1455, Robert A. McQuaid, (3d. cir. CD Cal. 1984).

[24] *Hodge v. Wal Mart*, n.º 03-1597, 360 F.3d-446, Michael Lutting, (USCA 4th Cir., Mar. 10, 2004)

[25] PAUL, George, L. y NEARON Bruce H. *The discovery revolution, e discovery amendments to the federal Rules of Procedure*, American Bar Asociation, 2006, p. 48

ve las políticas que propugna la nueva regla 37 (f), en el que las sanciones por expoliación no son procedentes cuando la prueba está más allá del control de la parte que la discute.

También como consecuencia de la imposición de esta presunción en contra, el tribunal puede excluir todos o algún medio de prueba de la parte contraria. En el caso *Trigon Insurance Co. v. United States* (Ed VA Nov. 9, 2001)[26] el tribunal consideró que debería de excluir la declaración de los expertos designados por la empresa consultora a quien se había encomendado por la Administración que le asistiese en el caso, como medio para suplir el hecho de la pérdida de información ocasionada por la política de gestión de datos de la compañía concesionaria. El Tribunal declaró entonces que la administración americana, no había cumplido con su deber de preservación de documentos y que la ratificación de los peritos era improcedente, máxime cuando se había podido recuperar parte de la información por los expertos forenses. En el caso, *Vodusek v. Bayliner Marine Corp.* (USCA 4th Cir. 1995), [27] el tribunal sancionó a Mrs. Vodusek con la descalificación de uno de sus testigos porque aquellos había participado en la expoliación de pruebas relevantes. Expresamente el testigo empleaba métodos destructivos que privaban a los soportes de utilidad para los abogados y sus peritos.

La sanción más grave que puede imponer el tribunal norteamericano es que el tribunal dirija el veredicto imponiendo las preguntas que deban de someterse al jurado, sobre la base de una situación de hecho deducida de una inferencia adversa. Por ejemplo en *Dempsey v. Pfizer* (Tex. App. Jul. 3, 1991),[28] el tribunal rechazó la solicitud del demandante de someter determinadas cuestiones al jurado, por que el demandante destruyó pruebas cruciales con el intento de eludir la averiguación. Una sanción de este tipo implicando información electrónicamente almacenada, tiene lugar en el caso *Coleman v. Morgan Stanley & Co. Inc.* (Flo. Cir. Ct, Mar.1 y 22, 2005).[29] Como veremos estos y otros fallos dieron una importancia decisiva a la valoración de la conducta de las partes en la preservación de los documentos, siendo generalizados los fallos que preveían como presupuesto de la expoliación el solo hecho del manejo incorrecto de la información. Todas estas sentencias serán el punto de partida de la reforma del año 2009, de la regla 502 de las Reglas Federales sobre la Prueba, (*Federal rule of the evidence*) que vendrá a establecer definitivamente el alcance de la obligación de dili-

---

[26] *Trigon Insurance Co. v. United States,* 204 FRD 277, 2001, Robert E. Payne, (Ed VA Nov. 9, 2001)

[27] *Vodusek v. Bayliner Marine Corp.* 71 E3d, 148, 1996, Victor Niemeyer, (USCA 4th Cir. 1995).

[28] *Dempsey v. Pfizer,* 813 S.W.2d.205, 206, J. *Hill* (Tex. App. Jul. 3, 1991)

[29] *Coleman v. Morgan Stanley & Co. Inc.* 2005 WL 679071, Elisabeth T. Maass (Flo. Cir. Ct, Mar., 1 y 22, 2005).

gencia en la preservación de los documentos. En todo caso, se ha de señalar que cuando el tribunal opta por una sanción de esta envergadura, debe de argumentar concienzudamente su decisión, por que las posibilidades de anulación del juicio al apelar la sentencia aumentan exponencialmente.

Para la imposición de sanciones de este tipo, hay una serie de factores que los tribunales suelen considerar para apreciar la existencia y extensión de las sanciones por el incumplimiento de las obligaciones de diligencia, pudiéndose citar sin carácter exhaustivo, los siguientes:

– La naturaleza y alcance del deber de preservación, por ejemplo si la conservación de dicha información debe de considerarse como una precaución razonable, si existía una resolución del tribunal que ordenase la preservación de los datos que fueron eliminados por la expoliación, etc.
– Las circunstancias concurrentes alrededor del incumplimiento del deber de preservación. Así por ejemplo, si hay elementos prueba que nos permitan afirmar que el incumplimiento fue deliberado, arriesgado, negligente, o que por el contrario, fue debido a la gestión ordinaria del sistema operativo o a una actuación de buena fe dentro de los recursos ordinarios del sistema de gestión.
– Las consecuencias del incumplimiento, por ejemplo la extensión del perjuicio a la parte contraria.
– El factor clave en la determinación de la adecuación y de la gravedad de la sanción, a la vista de los últimos fallos jurisprudenciales y de la nueva redacción de la regla 502 FRE parecen seguir siendo los tradicionales criterios de culpa y diligencia.

Las nuevas previsiones, contenidas en las últimas reformas de las reglas del proceso civil norteamericano, son consecuencia de la configuración del deber abstracto de diligencia en la preservación de documentos que surge tras la reforma del año 2006. Tales previsiones restringieron los supuestos de exoneración para el caso de acceso no intencional a la información. Así, se crean un apartado e) en la norma de la regla 37 de las reglas federales del procedimiento civil, que restringe la posibilidad de alegar la falta de conocimiento, como excusa absolutoria frente a la eventual imposición de sanciones, apartado este, que es de gran trascendencia a estos efectos y que a continuación transcribimos:

> Falta de aportación de información electrónicamente almacenada. Salvo en circunstancias excepcionales, el tribunal no deberá imponer sanciones conforme a estas reglas a la parte que no aporte la información electrónicamente almacenada, si esta se perdió como resultado de una operación rutinaria realizada de buena fe en el sistema de gestión informático; (*Absent exceptional circumstances, a*

*court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system).*

El apartado ha añadido ahora esta previsión a las reglas del proceso civil, implicando una protección limitada frente a la alegación del carácter no intencional de la pérdida de información en la gestión del sistema informático. Así, es importante hacer notar que la regla no excluye la posibilidad de sanciones por toda expoliación no intencionada, en cuanto que en primer lugar se refiere, a un supuesto excepcional *«absent excepcional circunstances»*, lo que configura sino un verdadero suceso de fuerza mayor, cuando menos de caso fortuito muy excepcional. Por otra parte exige para que la conducta puede exonerar a quien gestiona el sistema, que la gestión que realice tenga el carácter de rutinaria. La nota del Comité a la regla 37, se refiere concretamente al alcance que deba darse a esta expresión, señalando que la operaciones de gestión rutinaria del sistema ha de entenderse en el sentido de que (la gestión del sistema) ha sido realizada en el modo en que generalmente fue diseñada programada y ejecutada para satisfacer las finalidades propuestas por los programadores y las necesidades comerciales a que se destina el sistema informático. Es por ello que una gestión negligente o arriesgada del sistema informático puede determinar la imposición de sanciones.

Se ha de precisar, sin embargo, que la jurisprudencia norteamericana ha moderado la rígida aplicación de esta regla. Así, en el caso de *Diabetes Center of América v. Healthpia Am. Inc.* (D. Tex., Feb. 5, 2008),[30] el tribunal denegó la solicitud de sanciones después de determinar que había una falta de mala fe, en un caso en el que ninguna de las partes fue capaz de recuperar las copias de seguridad o de cualquier otro modo preservar los e-mails de más interés para el resultado del pleito. Por otra parte, los tribunales que han apreciado la deliberada destrucción de pruebas electrónicas suelen vacilar al ordenar la imposición de sanciones. En el caso *Treppel V. Biovail Corp. (*SDNY Apr. 2th, 2008),[31] en el que el demandante estaba asistido del mismo letrado que ostentó la representación de Laura Zubulake, las cintas de back-up eran de especial importancia porque en ellas estaba la única fuente de datos que permitía aportar pruebas para la resolución de la controversia. En este asunto, aunque Biovail tenía los medios para preservar los datos que mensualmente se iban incorporando a las copias de seguridad, luego de presentar la demanda, la empresa no hizo uso de estos medios y no es sino has-

[30] *Diabetes Center of América v. Healthpia Am. Inc.* 2008, WL 336382, Nancy F. Atlas, (D. Tex., Feb. 5, 2008),

[31] *Treppel v. Biovail Corp.* 2008, WL 866594, James C. Francis, *(*SDNY Apr. 2th, 2008)

ta que se le dirige un requerimiento de preservación, *preservation letter*, cuando comienza a guardar las copias de seguridad. A juicio del Tribunal esta falta resulta más que criticable, pues al tiempo en el que se inicia el litigio se conservaba en la cintas de *back-up* los datos que hubiesen permitido reconstruir como se producen los hechos que dieron lugar al litigio. Pese a constatarse la falta, el tribunal se mostró contrario a dar una instrucción de inferencia adversa o presunción en contrario porque Trepel no pudo adecuadamente aportar pruebas relevantes en relación a la pérdida de documentos, en su lugar el tribunal ordenó la restauración de ciertas cintas y el reconocimiento forense del disco duro del ordenador, todo a costa de la parte demandada, véase también en este mismo sentido *Hawaian Airlines Inc. v. Mesa Air Group Inc.* (Bkrtcy. SD. Haw., Jan. 22, 2008).[32]

## 7. **El deber de preservación**

El deber de diligencia en la conservación de la información obedece a la necesidad de garantizar la confianza creada en terceros por la información de la que somos de algún modo depositarios y de la que nos hemos valido en nuestras relaciones con aquellos. Este deber tiene en el derecho norteamericano un alcance distinto según del tipo de soporte de que se trate y su relación con el proceso. Así cabe distinguir un deber general de preservación de información, una carga de preservar la documentación en atención al hecho del litigio iniciado o que se presuma que va a iniciarse y una obligación concreta de preservación de información en virtud del acuerdo alcanzado por las partes conforme a la regla 26 FRPC u ordenado por el Tribunal a falta de éste, (preserve orders)

### 7.1. *Deber general de preservación*

Como hemos visto al principio de nuestra exposición la exteriorización de los datos contenidos en los documentos electrónicos determina que los estos últimos puedan llegar a tener la estabilidad que se predica de los verdaderos documentos. Adquiere así el documento una apariencia y crea una confianza hacia terceros que genera un deber de preservación como fundamento de las relaciones comerciales que han sido creadas al amparo de dicha información. Dicho deber puede tener un mayor o menor alcance dependiendo del carácter de la información que se contenga en aquél y el empleo que hayan sido objeto. Así por ejemplo, los datos que han servido para un informe contable o estadístico crean, en quien se ha servido de dicho informe, una

[32] *Hawaian Airlines Inc. v. Mesa Air Group Inc.* 2008, WL 185649, Robert. J. Faris, (Bkrtcy. SD. Haw., Jan. 22, 2008)

confianza de que aquellos son accesibles y pueden ser corroborados. Quien ha recibido un correo electrónico tiene que presumir que la parte contraria conserva un correo del mismo tenor, etc. Pese a ello, no existe, sin embargo, en el derecho norteamericano un deber general de preservar la información electrónicamente almacenada que este formulado taxativamente en una norma, pero el hecho cierto, es que la obligación de diligencia contenida en los artículos 26 FRCP y 502 de la FRE, de cara no sólo al proceso entablado sino el que existan visos que pueda llegarse a entablar, ha supuesto para las empresas la necesidad de organizar dentro de sus staffs departamentos que se dedican por entero a la labor de recopilación de todo tipo de información fundamentalmente correos electrónicos.

### 7.2. *Carga de preservación de la información en vistas de un proceso iniciado o de previsible iniciación.* (Litigation holds)

Esta obligación general de diligencia en la preservación de la información electrónicamente almacenada se concreta, cuando los interesados se encuentran de cara al proceso. En este sentido el magistrado David K. Isom,[33] ha explicado, como el deber de preservar las pruebas electrónicas existe sin necesidad de que se dicte una orden del tribunal en este sentido. En muchos casos esta orden de preservación dictada por el Tribunal, no es sino un modo auxiliar para concretar este deber, incrementando la probabilidad que los datos serán preservados, definiendo que datos deban de serlo y cuales puede ser destruidos, concretando la obligación de diligencia y aumentando la severidad de las sanciones, para el caso de que dichas pruebas no sean preservadas.

Se configura de este modo, una carga procesal para las partes en orden a asegurar la realización de la averiguación de los documentos electrónicos. De esta carga procesal se deriva, la exigencia de que las partes tan pronto tengan noticia de la existencia del proceso cesen en cualquier política de destrucción de documentos para asegurar que la información más relevante que deba de ser preservada en el juicio. La suspensión de la rutina de los documentos y las políticas de destrucción de datos telemáticos ayudarán a proteger a las compañías contra la reclamación por negligencia e intencional expoliación de pruebas. Sin embargo, tal acción por sí sola no será suficiente para proporcionar una completa protección, pues hay todavía mucha información electrónicamente almacenada que pudo ser perdida o suprimida. En tal sentido, la noticia de haberse entablado el proceso debería ser comunicada a todos los empleados que tengan información relevante, así como por terceras empresa, como proveedores de servicios TIC o detentadores de los pro-

[33] Isom, David K. "Electronic Discovery primer for Judges", fed, cts. L. Rev. I., 2005.

gramas de software de gestión quienes pueden ostentar la custodia directa de la organización de la información electrónicamente almacenada. Debe de advertirse a aquellos de la necesidad de preservar la información relevante para un eventual proceso, dar las directrices necesarias que deban de ser tenidos en cuenta para preservar las pruebas más relevantes e identificar a que personas dentro de la organización que sirvan como contacto si los empleados tienen alguna duda concerniente a sus deberes de preservación.

Dentro de este deber debemos de distinguir dos aspectos, la prohibición de destrucción de documentos y la obligación de conservar de forma accesible la información de interés para el resultado del pleito. El primer aspecto se liga a las consecuencias criminales implícitas al delito de obstrucción a la justicia, a la que anteriormente nos hemos referido con ocasión del caso Quattrone y de los procesos derivados de Enron y Andersen.

El otro aspecto es el relativo al momento a partir del cual existe una concreta obligación de tener localizada la información y sustraerla a la posible alteración que pueda verse envuelta por los procesos ordinarios de gestión del sistema informático. En este punto, no existe consenso por los tribunales norteamericanos. En un primer momento los tribunales estimaban que el deber de preservación no surge sino hasta que se tenga noticia del hecho cierto de la presentación de la demanda, *Computer Associates International Inc. v. American Fundware* (D CO 1990).[34] Sin embargo, esta postura conservadora, ha sido sistemáticamente desmontada por la jurisprudencia que surge tras el caso Zubulake, la cual ha anticipado este deber al momento mismo en que surge la controversia. A juicio de la juez Shira Schiendlin *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities*, (SDNY, Jan 2010)[35] tras un concienzudo examen de los antecedentes legales y jurisprudenciales de la cuestión, es bastante que se pruebe, que la intención del expoliador fue la de frustrar la acción ejercitada para estimar que se ha conculcado este deber de conservación. Recientemente el Juez Lee Rosental, en el asunto *Rimkus Consulting Group Inc. v. Nickie G. Cammarata (*S.D. Tex. Feb. 19, 2010*).*[36] refuerza esta línea jurisprudencial que se ha desarrollado a partir de Zubulake, y que se continúa en el asunto *Pension Committee*, afirmando la necesidad de preservar las pruebas desde el momento de activación de los eventos, "trigger event", justificando esta posición desde la perspectiva de una interpretación a sensu contrario de la excepción contenida en la Regla 37 (e) para el caso de expoliación.

---

[34] *Computer Associates International Inc. v. American Fundware* 133 FRD 166 (D CO 1990).

[35] *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities,* WL 184312, Shira Schiendlin, (SDNY, Jan 15)

[36] Rimkus Consulting Group Inc. v. Nickie G. Cammarata*,* 2010 WL 645253, Lee Roshental, (SD Tex. Feb. 19, 2010).

Respecto del contenido de dicho deber, la doctrina y la jurisprudencia han dado una serie de reglas a tener en cuenta para evitar la conculcación de este deber. Una de las más completas lista de sugerencias a las partes, respecto de las actuaciones que deben de realizar cuando comienza del deber de preservar, fue la indicada en Zubulake. El tribunal expuso entonces que hay ciertas cautelas que los administradores de las compañías deben de realizar para asegurar el cumplimiento de las obligaciones de preservación. En primer término, las partes deben anticipar las medidas oportunas tan pronto como sea previsible que el litigio tenga lugar, en segundo lugar los letrados de las partes deben de ponerse en contacto con los probables usuarios en litigio para asegurar que ellos están adecuadamente avisados de sus obligaciones de preservar las pruebas más relevantes y el tipo de pruebas que probablemente debe de llevarse a cabo durante las averiguaciones que tengan lugar en el proceso. En tercer lugar, los asesores deberán de trabajar con todos los empleados para saber las probabilidades que tengan en verse involucrados con las cuestiones en disputa e instruirles para generar copias de los archivos más relevantes, incluyendo e-mail, mensajes electrónicos y archivos. En cuarto lugar los administradores de la empresa deben de asegurarse que todos los soportes de back retenidos por la compañía están perfectamente identificados y se encuentran en un lugar seguro para evitar su pérdida.

Las partes y sus abogados deben también poner los medios necesarios para vigilar su cumplimiento de modo que todos los recursos de información averiguable estén identificados y localizados en todo momento.[37]

En particular ha sido discutido el deber de preservación de la información potencialmente peligrosa para el sistema, véase un correo electrónico decisivo para el curso del proceso que se vea afectado por un virus informático o produzca un prejuicio al sistema, cuestión ésta que ha dado lugar a una jurisprudencia muy casuística, sobre todo en los casos que se procedió a formatear los equipos para evitar mayores daños al sistema informático, (véase así *Johnson v. Wells Fargo, home mortage, Inc.* (DD Nev. May 16, 2008).[38]

### 7.3. *Orden de preservación de la información electrónicamente almacenada. (Preservation orders, stipulated agreements y preservation letters)*

Junto a este deber de diligencia general, cabe señalar la diligencia que en concreto deba de prestarse como consecuencia de una orden de preser-

---

[37] LANGE, Michele C.S. y NIMSGER, Kristin M. *Electronic Evidence and discovery...*, ibídem, p. 68

[38] *Wells Fargo, home mortage, Inc.,* 2008 WL 2142219, Robert A. Mcquaid, (DD Nev. May 16, 2008**).**

vación, (preservation Orders) dictada por el tribunal o acordada en el seno del proceso. La concreción de este deber de preservación de la información viene dada por la resolución judicial ordenando la preservación de la información y la determinación de la documentación que deba de ser aportada al proceso. Se ha de señalar, que las reglas federales del proceso civil contemplan tal tipo de resoluciones en última instancia como un remedio excepcional y subsidiario, que en todo caso no podrá suponer la paralización de los sistemas informáticos. Como señalan COHEN & LENDER,[39] aunque pueda pensarse que una orden de preservación es el instrumento más adecuado para asegurar la preservación de las pruebas electrónicas hay importantes inconvenientes prácticos y legales para asegurar que la misma tenga el efecto pretendido. De una parte, para que se pueda dictar una orden de este tipo las partes deben justificar claramente esta necesidad, como único mecanismo para prevenir la intencional o inadvertida destrucción de documentos. En tal sentido, no han faltado resoluciones, ordenando una preservación absoluta de la información electrónicamente almacenada pero en tales supuestos el ejercicio de la acción entablada se fundamentaba en algún tipo de lesión a bienes jurídicos especialmente protegidos que se encontraba más cercana al orden penal que al civil. Véase en tal sentido *Madden v. Wyeth* (ND Tex Apr. 16, 2003),[40] *Pepsi Cola Bottling Co. v. Caguill Inc. (D. Minn Oct. 20, 1995)*[41]; *Amstrong v. Bush, (D DC 1992)*[42]. En otros casos, fue el propio tribunal el que dio marcha atrás al comprobar los efectos devastadores de una resolución de este tipo. Así en el *Pueblo of Laguna v. United States* (Fed. Cl. 133, mar 19, 2004),[43] pese a la resolución inicial del Tribunal estimando la existencia de un importante riesgo de que las pruebas podrían ser pérdidas o destruidas, justificando en los antecedentes que se habían planteado en supuestos similares, posteriormente el tribunal modificó esta decisión al comprobar que la misma era excesivamente gravosa.

En todo caso, para el supuesto de que se llegue a acordar una orden de este tipo, es necesario que queden perfectamente acotados los soportes y formatos que serán objeto de la orden de preservación. En el caso *Computek Computer & Office Supplies inc. V. Walton*[44] se proporcionó además

[39] COHEN, Adam y LENDER, David. *Electronic Discovery law and practice,* Wolter Kluwers, 2009, p. 16

[40] *Madden v. Wyeth*, 2003 WL 21443404, Jeff Kaplan, (ND Tex Apr. 16, 2003).

[41] *Pepsi Cola Bottling Co. v. Caguill Inc.,* 1995, WL 783610, J. Briscoe, (ND Minn Oct. 20, 1995).

[42] *Amstrong v. Bush,* 807, F. Supp. 816, Charles R. Chilley, (DDc, 1992).

[43] *Pueblo of Laguna v. United States,* 60 n.º 0-24 L, Francis Allegra, (Fed. Cl. 133, mar 19, 2004).

[44] *Computek Computer & Office Supplies inc. V. Walton,* 2005, WL 352036, Moseley O'neill, (Tex App Feb. 15, 2005)

una aclaración de los criterios de razonabilidad que deben de ser tenidos en cuenta a la hora de proceder a la interrupción de los procesos informáticos para evitar la alteración de los soportes. En Computek el tribunal enjuiciador libró un mandato judicial que prohibía a los defensores suprimir o destruir cualesquiera archivos, o copias de archivos, incluyendo pero no limitando a los ordenadores o los archivos de los ordenadores del demandado. La defensa de los demandados argumentó que la decisión del tribunal era excesiva y que suponía una carga irracional para las actividades cotidianas de la empresa. El tribunal de apelación revocó la resolución dictada en la instancia y ordenó que el mandato judicial se aplicase sólo a algunos archivos o copias de archivos concretos, si bien incluyendo de forma ilimitada los archivos de los ordenadores de los demandados relacionados en la demanda.

Lo normal, sin embargo, es que las partes lleguen algún tipo de acuerdo en la comparecencia prevista en la regla 26 (f) y sólo cuando esto no sea posible, podrán obtener una resolución de este tipo. En tal caso, deberán de presentar inmediatamente después de dicha comparecencia un informe escrito al tribunal haciendo constar su resultado, las discrepancias de las partes y una propuesta en torno a las cuestiones planteadas. La orden de preservación que se dicte, sin embargo, servirá en la mayoría de los casos más que para que se ordene la intangibilidad de la información, como medio para racionalizar la averiguación y clarificar las obligaciones al inicio del proceso.

Estas resoluciones tienen por lo tanto un carácter limitado. Mayor importancia presenta la expedición de requerimientos frente a la parte contraria, *preservation letters*, que implican una alteración de la carga de la prueba en orden a valorar la diligencia en la expoliación de documentos. La finalidad de estos requerimientos, como señala CRAIG BALL,[45] se encuentra en la necesidad de recordar a la parte contraria que pruebas deben de preservar, sirviendo de fundamento de la consecuente reclamación para el caso de que se produzca una expoliación de información electrónicamente almacenada. Tales advertencias ayudan a establecer la mala fe y justificar la despreocupación de la parte contraria del deber de preservar las pruebas más relevantes. Como señala dicho autor, lo que hoy resulte aclarado, justifica que el día de mañana se pueda decir que ya entonces había quedado advertido. Cuanta más publicidad se dé a dicha notificación, y se compruebe que se ha entendido, incluyendo la metodología para la preservación y las consecuencias de la pérdida, más grande será la proba-

[45] BALL, Craig. "The perfect preservation letter", consultado en octubre de 2010, http://www.craigball.com/perfect%20preservation%20letter.pdf, p. 3

bilidad de que la parte contraria pueda ser penalizada por la destrucción de las evidencias.

## 8. **La divulgación por descuido o renuncia al privilegio, (inadvertent waiver o inadvertent dislosure)**

El derecho norteamericano parte del principio general de aportación de todos los medios de prueba y de no ocultación de información. Sin embargo, esta regla general cede en determinados supuestos, denominados en tal sentido privilegios (*privilege*), así el *attorney privilege* o secreto profesional, el *Work product protection privilege* o la *privacy* o derecho a la intimidad, (si bien este derecho no se encuentra tan desarrollado como en el derecho continental por carecer de una norma constitucional expresa que ampare este derecho). Sin embargo, tanto unos como otros pueden ser objeto de renuncia, la cual puede tener lugar con conocimiento de la parte o inadvertidamente como consecuencia del acceso fortuito a dicha información.

El problema que se presenta cuando tratamos de información electrónicamente almacenada, es que atendido el gran volumen de información que se contiene en los soportes electrónicos, la aportación indiscriminada al proceso de los soportes que contienen este tipo de información, pueden dar lugar a situaciones en que la parte que haga aportación de aquellos quede expuesta a verse sorprendida por revelaciones inesperadas o por información comprometida, situación que la dejaría manifiesta indefensión, no sólo por el hecho de la vulneración de los derechos que pueda implicar el acceso a ciertos contenidos, sino también por el carácter parcial de dicha información al extraerse de un contexto en el que la información no se encuentre perfectamente sistematizada. Todo esto puede dar lugar a una renuncia tácita de la parte a la situación privilegiada de la parte, cuyas consecuencias pueden ser decisivas en el curso del pleito.

Las normas procesales del proceso civil regula en su artículo 26(b)(5)(B) el modo en que deberá de procederse por las partes en tal caso.

> «Información aportada. Si la información aportada por la averiguación está sujeta a una solicitud de privilegio o de protección como material de preparación del juicio, la parte que presentó la reclamación puede notificar al resto de las partes haber presentado dicha reclamación y las bases que justifiquen su pretensión. Después de ser notificada, cada parte debe a la mayor brevedad devolver, secuestrar o destruir la información especificada y cualesquiera copias que tenga, no debiendo de utilizar o revelar la información hasta que la solicitud de protección esté resuelta y debiendo poner los medios necesarios para recuperar la información si se revelara su contenido antes de ser notificada, debiendo a la mayor brevedad presentar la información al tribunal debidamente precintada hasta que

> sea resuelto el incidente. La parte aportante debe de preservar la información para la que ha reclamado protección hasta que su solicitud quede resuelta.» [46]

Las Notas del Comité a la reforma de 2006, contiene una distinción fundamental en esta materia, según que la renuncia se produzca con carácter previo a la comparecencia preliminar o decisión que determine el alcance de la obligación de aportación de la información electrónicamente almacenada o se produzca después.

a) La renuncia al privilegio antes de la comparencia del art. 26 (f) (Schedule conference).

En el primero de los casos, la necesidad de aportación de dicha información es la genérica establecida en la regla 16.2(b) anteriormente comentada. Para facilitar el acceso a dicha información, el apartado f de la regla 26, regula con toda minuciosidad la comparecencia de ordenación del procedimiento, (*scheduling conference*) en la que se decidirá el modo en que dicha información debe de ser aportada, facilitando el acuerdo de las partes, sobre el formato, los costes, los plazos y los soportes en que deba de llevarse a cabo. A tal efecto se previene que las partes deberán de presentar un informe por escrito sobre el estado de la cuestión y una propuesta con anterioridad a la comparecencia previa. Por otra parte, deberán de someter a discusión las cautelas que deban de adoptarse para evitar el riesgo de renuncia. Tales previsiones pueden suponer para la parte que deba de facilitar esos materiales, substanciales costes, además de un retraso en la tramitación del pleito por el tiempo que se deba de emplear en la revisión de la información. Por tal razón la cuestión se encuentra íntimamente conectada con los aspectos relativos a doctrina de los costes y cargas de la aportación de información electrónicamente almacenada contenida en la sentencia Zubulake y a la misma nos remitimos. Se ha de señalar, únicamente que las partes pueden intentar minimizar estos costes y retrasos aceptando someterse a protocolos que minimicen los riesgos de renuncia, en este sentido, es fundamental el muestreo de la información, así suele resultar bastante común que la parte

---

[46] *Information Produced. If information produced in discovery is subject to a claim of privilege or of protection as trial preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.*

requerida proporcione los materiales solicitados para su examen inicial, sin renunciar a cualquier privilegio o protección, mediante su examen superficial, diligencia de averiguación abreviada conocida como "quick peek" (vistazo rápido).

b) La renuncia al privilegio luego de la comparencia del art. 26 (f) (Schedule conference).

Mayores son los problemas que se presentan en relación a las consecuencias que se producen como resultado de la desvelación inadvertida de información privilegiada con posterioridad a la comparecencia prevista en la regla 26 f). Lo normal en el derecho norteamericano, es que las partes lleguen a un acuerdo sobre el modo de acceso a la información. También puede darse la circunstancia de que las partes prevean para el supuesto de que se produjere la revelación inadvertida de información que pudiese afectar a sus intereses que la información así obtenida carezca de eficacia en juicio a estos efectos. Pues bien, tales acuerdos, acuerdos que son llamados muy expresivamente "claw back agreements" presentan siempre una base muy endeble en la medida que el consentimiento obtenido, viene viciado por el desconocimiento por la parte de todos los pormenores de la información electrónicamente almacenada que luego llegue a conocerse. Las situaciones que se producían dieron lugar a la reforma en el año 2009 del artículo 502 FRE. Antes de la publicación de la regla 502, los tribunales federales diferían notablemente en que supuestos la revelación inadvertida de información privilegiada podía ser objeto de renuncia. Algunos tribunales federales de forma estricta mantenían que cualquier divulgación, no importa lo inocente que fuese, suponía una renuncia al privilegio sobre todos los documentos que no constasen relacionados en un *claw arrengement* o por el contrario, suponía su exclusión si encontrasen comprendidos en aquel acuerdo, mientras que otros tribunales mantenían que una revelación privilegiada debía de tener carácter intencionado para constituir un supuesto de renuncia.

## 9. **La regla 502 de las Reglas Federales de Regulación de la Prueba**

### 9.1. *El origen de la regla*

La disparidad de pronunciamientos en relación a las consecuencias de la renuncia al privilegio de la información especialmente protegida, determinó que el Congreso de los Estados Unidos, en septiembre de 2008 promulgase la regla 502 de la Reglas Federales sobre la Prueba, (FRE) titulada: "*attorneys-client privilege and Work Products Limitations on Waiver*". La regla 502 tiene como objetivo incrementar la eficiencia y disminuir los riesgos y costes asociados a la aportación de documentos proporcionando protección

en los supuestos de divulgación inadvertida.[47] La regla fue propuesta por la conferencia judicial americana, (*Judicial Conference Rules Committees*), la cual se venía preocupando desde hacía bastante tiempo por los costes de los litigios, muchos de los cuales habían sido causados por las revisiones exigidas por la vigente ley procesal. La nueva redacción de la regla ha limitado los supuestos en los cuales revelación inadvertida de información puede tenerse por renunciada. La regla 502 FRE, pretende ante todo mitigar el miedo que la revelación inadvertida de algún documento pueda dar al traste con estrategia procesal de las partes (*smoking gun*). Debe de tenerse presente, que tal posicionamiento legal se ha adoptado desde la perspectiva de la reducción de los costes y los riesgos que implicaba la renuncia al privilegio, más que desde un principio de eficiencia procesal.

Se señala en dicha regla:

> Divulgaciones inadvertidas: Cuando en el curso de un proceso ante un tribunal federal, oficina federal o agencia, se produzca la revelación inadvertida de información, no tendrá la consideración de renuncia a la protección en el procedimiento, si se dan las circunstancias siguientes:
> – Que la revelación resulte ser inadvertida.
> – Que quien detenta el privilegio o protección haya adoptado los medios razonables para prevenir la revelación, y
> – Que el detentador de dicha información ha procedido de la manera más inmediata a rectificar el error, siguiendo los trámites previstos en la regla 26(b)(5(B) de las reglas federales del proceso civil.

A la luz de la manifiesta probabilidad de que información especialmente protegida sea divulgada de forma inadvertida, dado el enorme volumen de información que se maneja en los soportes electrónicos, la regla 502 FRE se decanta por una noción de justicia, por encima de las convenciones formales alcanzadas en el seno del proceso. Se atiende para ello a los criterios de diligencia e intencionalidad de las partes. Esto implica que el legislador ha optado por la vía de apartarse de la seguridad jurídica para atender a las pautas que vaya estableciendo la jurisprudencia para corregir los siempre discrecionales criterios culpabilísticos.

Se sigue con ello, la línea jurisprudencial que venía siendo mayoritaria. Así en el caso *Victor Stanley Inc. V. Creative Pipe, Inc.* (2008, DC. Md)[48]

---

[47] Lange, Michele C.S. y Nimsger, Kristin M. (2010); *Electronic Evidence and discovery...*, ibidem, p. 97.

[48] *Victor Stanley Inc. V. Creative Pipe, Inc*. 2008, WL 2221841, Paul W. Grimm (May 29, 2008 DC. Md)

resuelto por el Magistrado Paul Grimm, se analizó la inadvertida aportación de 165 documentos que tenían el carácter de especialmente protegidos, documentos que se deslizaron en el proceso por el acceso que se dio a la otra parte de una clave de búsqueda que le permitía reconocer los documentos privilegiados. El tribunal en este caso se centró sobre todo en el análisis de la razonabilidad de las precauciones adoptadas para prevenir la divulgación inadvertida de información privilegiada y estimó que la parte aportarte no había probado que se hubiesen adoptado al efecto las precauciones razonables. En concreto, se estimó que la parte aportante no había justificado que la elección de las contraseñas que condujeron a la información privilegiada, fuesen racionalmente seleccionadas, ni que el nivel de sofisticación de aquellas, ni la cualificación de las personas que realizaron la selección, fuese el adecuado y sin que por lo demás constase realizado un muestreo para asegurar la exactitud de los resultados de la selección de las contraseñas. El asunto también dio una pauta sobre que características debían de tener las contraseñas para que tuviese unas razonables garantías de seguridad conforme al criterio del justo medio, aspecto éste de gran interés pero que excedería del objeto del presente estudio.

### 9.2. *Eficacia procesal de los clawback* agreements

La regla 502 clarifica los efectos de las órdenes y los acuerdos de exclusión de la renuncia a la protección de la información privilegiada, (*clawback agreements*). Antes de que se dictase la regla 502, se percibía una clara tendencia a incrementar este tipo de acuerdos que impedían la renuncia al carácter protegido de los documentos durante el proceso de búsqueda de información electrónica. En virtud de estos acuerdos, la revelación inadvertida de documentos privilegiados no constituía una renuncia al carácter especialmente protegido de dicha información de modo que los documentos debían de ser inmediatamente devueltos y cualquier copia o nota de aquellos debería ser destruida. Algunos tribunales, llegaron más lejos sancionando este tipo de acuerdos al incluirlos entre las estipulaciones contenidas en las órdenes de protección. Sin embargo, esta práctica suponía una grave distorsión del proceso, por suponer una fuerte restricción de antemano de los medios de prueba, sobre la base de un perjuicio que *a priori* se desconocía y sin que en realidad se obtuviese garantía alguna frente a la utilización de dicha información una vez que se hubiese producido la divulgación. Por otra parte estos acuerdos, podrían dar lugar a un uso abusivo, que no se acomodase a la nueva situación que se crea en el proceso tras la nueva regulación de la diligencia de averiguación. La regla 502 reconoce la eficacia de dichos acuerdos, si bien la eficacia última de los mismos dependerá de las notas de eficiencia y diligencia, conceptos cuyos concretos *standards* dependerán del curso que tome la jurisprudencia en los próximos años, la cual deberá de fijar el alcance de los mismos.

### 9.3. *Extensión material*

Cuando se dictó la regla 502 FRE se solía considerar que la renuncia de la parte que hubiera renunciado al privilegio que ostentaba la información especialmente privilegiada, (tanto por razón del *attorney-client privilege* como el *work-product protection*) sólo se haría extensiva a las cuestiones relativas al tipo de privilegio renunciado o a cualquier información no divulgada fundamentada en dicho privilegio, pero no a otras materias aunque tuviesen el carácter de privilegiadas. De otra parte, tampoco existía un criterio uniforme por los tribunales norteamericanos acerca del carácter de la información o la trascendencia de dicha información como para ser considerada tal. Por ejemplo, la revelación inadvertida de un acuse de recibo de un abogado a un cliente, podría parecer que en principio carecería de entidad como para ser tutelada como una situación de privilegio, sin embargo la otra parte podría utilizar esta información para buscar todas las comunicaciones relativas a la referida carta en el periodo indicado, lo que de hecho vendría a dar lugar a una situación material semejante a la conculcación de información privilegiada. La extensión material de la renuncia ha sido siempre una de las cuestiones más controvertidas de las que se producen como consecuencia de la divulgación inadvertida de las comunicaciones privilegiadas. La nueve regla señala que las materias que puede renunciarse serán la excepción, cerrándose con ello la puerta a la eventual alegación genérica del carácter privilegiado de la información.

### 9.4. *Terceros*

Antes de que la FRE 502 entrase en vigor, los tribunales solían aprobar los acuerdos entre demandantes y demandados del tipo "*clawback*", siempre que la divulgación de los documentos protegidos no afectase al privilegio y exijan la devolución de los documentos inadvertidamente revelados. La jurisprudencia antes de publicarse la regla 502, venía entendiendo que los acuerdos de exclusión de la renuncia inadvertida negociados por las partes no les excusaban de adoptar las necesarias precauciones para evitar la revelación documentos especialmente protegidos, véase en este sentido *Hopson v. Mayor & Ctiy Council of Baltimore*; (DC. Md. November 22, 2005).[49] En otras palabras, como señalan LANGE & NIMSGER,[50] un acuerdo de exclusión debería de ser utilizado como una estrategia defensiva adicional, no como una primera línea de defensa. Sin embargo, tales acuerdos no protegían el privilegio con respecto a terceros que pudieran estar involucrados en un liti-

[49] *Hopson v. Mayor & Ctiy Council of Baltimore*; 232, FRD 228, Paul W. Grimm (DC. Md. November 22, 2005).

[50] LANGE, Michele C.S. y NIMSGER, Kristin M. *Electronic Evidence and discovery..*, *ibídem,* p. 101

gio posterior, ni impedía su empleo en las resoluciones dictadas por otros tribunales a instancia de las partes en procedimientos sucesivos. Sin embargo, tras la reforma del año 2009, conforme a la regla 502 (d) y (e), las resoluciones dictadas por los tribunales en relación a la información especialmente protegida es vinculante para todo el mundo incluyendo no sólo a los terceros sino también para el resto de tribunales estatales en cualesquiera otros procesos. [51]Se estimó entonces que la seguridad de conocer que las órdenes dictadas al amparo de la regla 502 (d), -que se aplicará ahora en todos los casos y en cualquier tribunal del país- permitirá que los abogados puedan llegar a acuerdos más libremente que hasta ahora. Mediante la concertación de estos acuerdos los abogados protegen enormemente sus documentos privilegiados y permiten disminuir la probabilidad de costosos incidentes de averiguación en relación a la renuncia al privilegio. De este modo, los tribunales federales pueden ordenar que las diligencias de búsqueda o averiguación de información electrónicamente almacenada no suponga una renuncia a la prohibición de divulgación de información especialmente protegida, tanto en los procesos judiciales ante el tribunal en el que la divulgación se renuncia como la de cualesquiera otros procedimientos ante tribunales federales o estatales. Debe de tenerse presente que tal previsión no se contiene respecto de cualquier otro acuerdo al que las partes puedan haber llegado y particularmente los que se alcancen en el curso de la comparecencia prevista en la regla 26 (f) de la FRCP. De este modo, un acuerdo sobre los efectos de la divulgación en un procedimiento ante los tribunales federales sólo será vinculante para terceros o para las partes en sucesivos procedimientos, si el mismo queda incorporado dentro de una orden de protección del Tribunal, no teniendo este carácter cualesquiera otros acuerdos adoptados por las partes y que no hayan sido confirmados por el Tribunal. Como señala, LANGE & NIMSGER,[52] resulta duro imaginar una situación en la cual un abogado no quisiera llevar a cabo este paso excepcional de obtener una orden de protección de la regla 502 (d), lo que hoy por hoy, es lo más común en los procesos civiles norteamericanos. La única atemperación vendrá determinada entonces por la necesidad de alegar, el carácter especialmente protegido en cada uno de los nuevos procedimientos, atendidas las circunstancias de cada caso, aspecto que ha sido objeto de críticas por la doctrina norteamericana y que se encuentra pendiente de desarrollo jurisprudencial.

---

[51] El apartado (e) de la regla 502, señala al efecto: Un acuerdo sobre los efectos de la divulgación en un procedimiento federal sólo es vinculante para las partes que lo hubiesen acordado, a menos que esté incorporado a una resolución judicial. An agreement on the effect of disclosure of a communication or information covered by the attorney-client privilege or work product protection is binding on the parties to the agreement, but not on other parties unless the agreement is incorporated into a court order

[52] LANGE, Michele C.S. y NIMSGER, Kristin M. (2010); *Electronic Evidence and discovery...*, *ibídem,* p. 100

### 9.5. *Interacción entre los tribunales federales y estatales conforme a la regla 502*

Con anterioridad a la publicación regla 502 se carecía de precedentes jurisprudenciales, en relación a la vinculación de los acuerdos dictados por los tribunales Federales respecto a los estatales en relación a la exclusión de la renuncia a la protección de la información privilegiada. La regla 502 (f) ha abordado esta cuestión, permitiendo que lo acordado por los Tribunales Federales, siempre que se encuentren insertos en una orden de protección, resulten vinculantes frente a los tribunales estatales. La norma va incluso más lejos, previniendo incluso, en el apartado (d) de la regla 502, que los tribunales federales deberán de respetar a su vez las determinación de los tribunales estatales en relación a la información especialmente protegida, cuando la aplicación de la ley estatal resulte más protectora frente la renuncia, tanto si lo es por aplicación de la regla 502 como si lo es por la ley del estado donde la revelación ha sucedido. Cabe destacar, sin embargo, que la regla 502 no permite que lo acordado por un tribunal estatal, en relación a estas cuestiones, resulte vinculante en otro estado. El efecto vinculante de las decisiones de los tribunales federales y estatales en relación a la información protegida es esencial para alcanzar la finalidad propuesta por el Congreso de reducir los costes asociados con la averiguación dentro de un marco completo de seguridad jurídica. Sólo mediante la eficacia, general de dichas decisiones podrán tener realmente efecto tales determinaciones, que de no ser así, resultarían ilusorias al quedar al albur de la aplicación que se haga de las diferentes legislaciones estatales en cada uno de los estados. Se permite así, dar una protección plena sin miedo a ser vulnerado este derecho por el amparo que a dicha divulgación se pueda dar fuera de la jurisdicción del tribunal que lo acuerda.

### 9.6. *Limitaciones a los acuerdos de* "claw back agreements"

La regla 502 ha revolucionado la regulación de la protección de la información privilegiada en los tribunales federales, proporcionando consistencia a la regulación procesal de estas cuestiones y permitiendo a los abogados predecir hasta cierto punto como se comportarán los tribunales en las cuestiones relativas a la información especialmente protegida en función de los *standards* jurisprudenciales que se vayan creando y que ahora se encuentran pendientes de desarrollo. De acuerdo, con esta disposición la regla debería de reducir la ansiedad que acompaña a la revisión de las ingentes cantidades de información electrónicamente almacenada que se aportan en los soportes informáticos por el riesgo de una revelación inadvertida. Lo cierto, es que pese a todos estos esfuerzos, exista o no renuncia, en el caso de que se produzca esta incidencia nada impedirá el conocimiento por la parte contraria de información potencialmente comprometedora, al que la parte contraria nunca hubiera podido acceder de otro modo. En tal

sentido, resulta especialmente relevante la diligente actuación de la defensa de los partes para percatarse cuanto antes de la transmisión inadvertida de este tipo de información, como la exigencia de responsabilidad a la contraria para que no se valga expresamente de la información obtenida de este modo.

Como se señala en el *Managing and litigating*,[53] pese a los mejores esfuerzos, debemos de asumir que en el curso de estas diligencias de búsqueda de información electrónicamente almacenada se seguirán aportando inadvertidamente documentos comprometedores. La reforma ha pretendido poner coto al enorme dispendio que estaba implicando las labores de revisión de documentos, pretendiendo reducir el *estrés* que implica el hecho de que en el curso de la averiguación pudiesen surgir alguno de estos documentos y consagrando así una jurisprudencia que viene reconociendo la legalidad de estos acuerdos. Ciertamente el art. 26 de la FRCP, ya reconocía el derecho de las partes para solicitar la recuperación de documentos (*claw back*) y sugería que las previsiones en orden a la recuperación de estos documentos podían ser incorporadas a la resolución de ordenación del procedimiento o a los acuerdos que las partes alcanzasen en el curso de la comparecencia preliminar del apartado (f) del propio art. 26. Estos acuerdos, resultaban beneficiosos para ambas partes y venían siendo reconocidos por la jurisprudencia. Ahora la nueva regla contenida en el art. 502 FRE ha querido matizar su alcance, supeditándolos a la noción de previsión y diligencia, evitando, que el proceso quede comprometido por lo inicialmente convenido, de modo que se pueda adaptar a las nuevas contingencias que se produzcan en el curso de la averiguación.

La nota de la Conferencia Judicial a la regla 502 FRE, establece que pese a la disminución de las exigencias requeridas para la preservación de la información especialmente protegida, el uso de avanzadas aplicaciones de software de análisis y herramientas lingüísticas en la detección de privilegio constituyen medios técnicos que en el futuro puedan prevenir la inadvertida divulgación de información. En tal sentido, una buena gestión de registros, que incluye el mapeo de datos (saber qué es lo que hay en los sistemas), los registros de los ciclos de retención (saber qué registros se mantienen por cada uno de los períodos establecidos) y la cadena de custodia (saber quién fue el responsable de recibir y mantener los registros) siguen siendo determinantes. En tal sentido, la Conferencia Judicial recomienda el desarrollo de protocolos de revisión, como el contenido en *Yelton guideline*, así como la conveniencia de que los abogados de las partes se reúnan y

[53] VVAA. *Managing and litigating, the complete sufery cases*. edit., Bruner, Phillip L. & Haley, Tracey L. 2nd edition, American Bar Asociation, 2008, p. 50.

acuerden lo procedente con la parte contraria tan pronto como se presente la ocasión.[54]

## 10. **Conclusiones**

El tratamiento de la cuestión de la preservación de la documentación electrónicamente almacenada, en las nuevas normas procesales civiles norteamericanas, ha implicado exacerbar las obligaciones de transparencia y diligencia a la hora de la conservación de la información electrónica. Este principio no sólo informa la práctica judicial, sino que además establece una carga sobre las personas y empresas de reordenar los sistemas informáticos, mediante el mantenimiento de forma racional de la información que periódicamente se incorporan a los sistemas de gestión. Se ha producido, por ello,

---

[54] En el ordenamiento jurídico español, la regulación de estos medios de prueba se contiene en el artículo 384, en la Sección VIII, del Capítulo VI, Libro II de la Ley de Enjuiciamiento Civil. En el mismo se previene que *los instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, que, por ser relevantes para el proceso, hayan sido admitidos como prueba, serán examinados por el tribunal por los medios que la parte proponente aporte o que el tribunal disponga utilizar, y de modo tal, que las demás partes del proceso puedan, con idéntico conocimiento que el tribunal, alegar y proponer lo que a su derecho convenga.* En estos casos, la parte que proponga este medio de prueba podrá aportar los dictámenes y medios de prueba instrumentales que considere convenientes para adverar su contenido, *pudiendo las demás partes aportar dictámenes y medios de prueba cuando cuestionen la autenticidad y exactitud de lo reproducido.* También se previene que la documentación en autos se hará del modo más apropiado a la naturaleza del instrumento, bajo la fe del Secretario Judicial, que en su caso, adoptará también las medidas de custodia que resulten necesarias. El tribunal valorará este tipo de soportes conforme a las reglas de sana crítica aplicables a aquéllos según su naturaleza. Donde estas diligencias, tiene una tradición ya consolida es en **materia mercantil**. El art. 327 de la LEC se remite con carácter general al Código de comercio, y únicamente contiene una previsión respecto a la inmediación de este tipo de pruebas de reconocimiento judicial *«De manera motivada, y con carácter excepcional, el tribunal podrá reclamar que se presenten ante él los libros o su soporte informático, siempre que se especifiquen los asientos que deben ser examinados»*. Esta previsión está en consonancia con la tradicional regulación contenida en las leyes mercantiles que parten del carácter secreto de la información mercantil y la excepcionalidad de la exhibición de su documentación. Así se previene que no será posible la comunicación o reconocimiento general de la documentación de los comerciantes, (art. 32.1), salvo en supuestos de sucesión universal, suspensión de pagos, quiebras, liquidaciones de sociedades o entidades mercantiles, expedientes de regulación de empleo, y cuando los socios o los representantes legales de los trabajadores tengan derecho a su examen directo (art. 32.2 Cco.). En cualquier otro caso, para que pueda decretarse la exhibición de los libros y documentos de los empresarios a instancia de parte o de oficio, cuando la persona a quien pertenezcan tenga interés o responsabilidad en el asunto en que proceda la exhibición. El reconocimiento se contraerá exclusivamente a los puntos que tengan relación con la cuestión de que se trate, (art. 33 Cco.).

una proliferación de empresas cuyo único cometido es el tratamiento y clasificación de los sistemas informáticos para adecuar los sistemas de gestión a las exigencias de la e-discovery. De este modo, las grandes multinacionales informáticas han encontrado un camino abonado para ampliar su base de negocio, respecto de lo cual, debemos de ser cautelosos. Por contra han surgido también quejas de cierto sector de la doctrina ante una situación desigualdad procesal entre las pequeñas y grandes empresas, en la medida que las primeras carecen de los recursos necesarios para el mantenimiento de un sistema de gestión documental. A esta reacción atiende la reforma de la regla 502 de las Leyes procesales civiles, que toma en cuenta el enorme gasto que supone la e-discovery, para mitigar sus efectos sobre la base del juicio de reproche culpabilístico el cual nunca debiera de haberse perdido como punto de referencia en esta materia.

***Tabla de jurisprudencia citada***

| *Tribunal, Sala y Fecha* | *Registro Judicial* | *Magistrado Ponente* | *Partes* |
|---|---|---|---|
| Tex. App. Jul. 3, 1991 | 813 S.W.2d.205, 206 | *Martha Jamison Hill* | Dempsey v. Pfizer; Inc. |
| *D. Minn., Oct. 20, 1995* | *1995, WL 783610,* | *J. Briscoe* | *Pepsi Cola Bottling Co. v. Caguill Inc.;* |
| USCA 4th Cir. 1995 | 71 E3d, 148, 1996 | *Victor Niemeyer* | Vodusek V. Bayiner Marine Corporation |
| *Mass. Super. Jun. 16, 1999* | *1999, WL 462015* | *Raymond J. Brassard* | *Linnen v. A.H. Robins Co.* |
| *D. DC 1992* | *807, F. Supp. 816* | *Charles R. Chilley* | *Amstrong v. Bush* |
| S.D. Ind. Jun. 7, 2000 | 194 FRD 639, 641 | *David F. Hamilton* | Simon Prop. Group L.P. v. Simon Inc. |
| E.D. Va. Nov. 9, 2001 | 204 FRD 277, 2001 | *Robert E. Payne* | Trigon Ins. Co. v. United States |
| E.D.Va. Aug. 9, 2002 | 215 F.Supp.2d 687 | *Robert E. Payne* | Trigon Ins. Co. v. United States |
| SD. NY, May 13, 2003 | 2003, WL 21087884 | Shira Sheindlin | Zubulake v. UBS Warburg |
| ND Tex, Apr. 16, 2003 | 2003, WL 21443404 | Jeff Kaplan | Madden v. Wyeth |
| S.D.N.Y. 2003 | 216 F.R.D. 280 | Shira Sheindlin | Zubulake v. UBS Warburg |
| DC SDNY, Oct. 22, 2003 | LLC 220, FRD 212, US Dis Lexis 18771 | Shira Sheindlin | Zubulake v. UBS Warburg |
| *D.D.C. January 9, 2003* | *U.S. Dist. LEXIS 172* | John M. Facciola | *McPeek v. Ashcroft,* |
| USCA 11th Cir. 2003 | 345, F.3d 1315 | James.L. Edmondson | In re Ford Motor Company |
| USCA 4th Cir., Mar. 10, 2004 | n.º 03-1597, 360 F.3d-446 | Michael Lutting | Hodge v. Wal Mart |
| Fed. Cl. 133, Mar. 19, 2004 | 60 n.º 0-24 L | Francis Allegra | Pueblo of Laguna v. United States, |
| SD. NY, July 20, 2004 | 2004, WL 1620866 | Shira Sheindlin | Zubulake v. UBS Warburg |
| Tex.App. Feb. 15, 2005 | 2005 WL 352036 | Moseley O'neill | Computek Computer & Office Supplies, Inc. v. Walton |

| *Tribunal, Sala y Fecha* | *Registro Judicial* | *Magistrado Ponente* | *Partes* |
|---|---|---|---|
| USCA 2005 | 374 f.3d 281. 544 U.S. 696, (2005) | Rehnquist | Arthur Andersen LLP v. United States |
| DC. Md. Nov. 22, 2005 | 232, FRD 228 | Paul W. Grimm | Hopson v. Mayor & Ctiy Council of Baltimore |
| USCA 2d Cir. Mar. 22, 2005 | 402, f.3d, 304 | S. Sotomayor | United States v. Quattrone |
| D. Kan. Mar. 24, 2006 | 2006, WL 763668 | Donald Bostwick | Balboa Threadworks., Inc. V. Stucky |
| USCA 2d Cir. Mar. 20, 2006 | 441, f.3d, 153 | Richard C. Wesley | United States v. Quattrone |
| C.D. Cal. May 29, 2007) (119) | 2007 WL 2080419 | Florence M. Cooper | Columbia Pictures Industries v. Bunnell |
| Bkrtcy. SD. Haw., Jan. 22, 2008 | 2008, WL 185649 | Robert. J. Faris | Hawaian Airlines Inc. v. Mesa Air Group Inc. |
| SD. Tex. Feb. 5, 2008 | 2008, WL 336382 | Nancy F. Atlas | Diabetes Centers of America, Inc. v. Healthpia America, Inc. |
| SD. NY, Apr. 2th, 2008 | 2008, WL 866594 | James C. Francis IV | Treppel V. Biovail Corp. |
| D. Nev., May 16, 2008 | 2008, WL2142219 | Robert A. McQuaid, | Johnson v. Wells Fargo, home mortage, Inc. |
| DC. Md. May 29, 2008 | 2008, WL 2221841 | P.W. Grimm | Victor Stanley Inc. V. Creative Pipe, Inc. |
| D. Minn. June 5, 2009 | 2009 WL 1606653 | Ann. D. Montgomey | In re Zurn Pex Plumbing Prods. Liab. Litig. |
| S.D. N.Y. 2009 | 256 F.R.D. 403 | Shira A. Scheindlin | Securities and exchange commission v. Collins & Aikman Corp. |
| D. Utah March 30, 2009 | 2009 WL 910801 | David Nuffer | Phillip Adams & Associates LLC v. Dell, Inc. |
| S.D. Tex. Feb. 19, 2010 | 2010 WL 645253 | Lee Roshental | Rimkus Consulting Group, Inc. v. Cammarata |
| S.D.N.Y. Jan. 15, 2010 | WL 184312 | Shira Scheindlin | *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC* |