Registro y confiscación de ordenadores y obtención de pruebas electrónicas en investigación criminal

Sección de Delitos Informáticos y Propiedad Intelectual
División de delitos
Ministerio de Justicia de Estados Unidos

Julio de 2002

ÍNDICE

[Índice]

PRÓLOGO

Esta publicación (el Manual) es una versión revisada de la edición de 2001 de "Registro y confiscación de ordenadores y obtención de pruebas electrónicas en investigaciones judiciales". Además de comentar la jurisprudencia reciente, el Manual incorpora los cambios más importantes que han experimentado las leyes que rigen las pruebas electrónicas, recogidos en la Ley USA PATRIOT de 2001, Pub. L. Nº 107-56, 115 Stat. 272 (2001) (la "Ley PATRIOT"). Estos cambios se debaten fundamentalmente en los capítulos 3 y 4.

Una gran parte de las disposiciones de la Ley PATRIOT relevantes a este respecto expirará el 31 de diciembre de 2005, a menos que se vuelvan a constituir en ley. Por consiguiente, se insta a los fiscales y agentes a informar a la Sección de Delitos Cibernéticos y Propiedad Intelectual, CCIPS (Computer Crime and Intellectual Property Section), en 202-514-1026, siempre que el uso de las nuevas autoridades demuestre ser útil en un caso penal. Esta información contribuirá a garantizar que el Congreso sea informado plenamente a la hora de decidir si volver a promulgar esta disposición.

Nathan Judish, de la CCIPS, es el principal responsable de las revisiones de este Manual, bajo la supervisión deMartha Stansell-Gamm, Directora de la Sección de Delitos Cibernéticos y Propiedad Intelectual. Los siguientes abogados de la CCIPS también prestaron su ayuda durante la edición (por orden alfabético): Richard Downing, Mark Eckenwiler, David Green, Patricia McGarry, Paul Ohm, Richard Salgado, Michael Sussmann y los becarios de verano Matthew Heintz, Andrew Ting, Arun Subramanian y Amalie Weber.

Asimismo, también aportaron valiosas sugerencias: Gregory Motta y Lynn Pierce de la Oficina del Consejo General del FBI y los coordinadores de ordenadores y telecomunicaciones (CTCs) Arif Alikhan, Mark Califano, Scott Christie y Steven Schroeder.

Esta edición tiene una tremenda deuda con Orin S. Kerr, el principal autor de la edición de 2001, quien dejó el Ministerio de Justicia en 2001 para impartir clases en la Facultad de Derecho de la George Washington University. La edición de 2001 reemplazaba las Directrices Federales de 1994 para el registro y confiscación de ordenadores y en ella quedó reflejada una inversión ingente de tiempo y reflexión por parte del Sr. Kerr y de numerosos abogados de la CCIPS, fiscales adjuntos y profesionales del FBI y otros organismos federales. En esta edición se ha conservado la organización y el análisis de la de 2001, no por inercia, sino porque ha demostrado ser sólida y perdurable.

Al igual que ocurre con la mayor parte de documentos de este tipo, el Manual pretende ofrecer asistencia, no imponer autoridad. Sus análisis y conclusiones reflejan las ideas actuales sobre áreas complejas del Derecho y no reflejan en modo alguno la postura oficial del Ministerio de Justicia ni de ningún otro organismo. No tiene ningún efecto normativo ni otorga derechos ni soluciones.

En la página web de la Sección de Delitos Cibernéticos y Propiedad Intelectual, http://www.cybercrime.gov./, están a su disposición copias electrónicas de este documento. La versión electrónica se actualizará periódicamente, por lo que se aconseja a los fiscales y agentes que comprueben la versión de la página web para estar al día de las últimas modificaciones. Si tiene cualquier duda, comentario o corrección, diríjase a Nathan Judish en el teléfono (202) 514-1026. Las solicitudes de copias en papel o correspondencia escrita solamente sea atenderán si provienen de oficiales de aplicación de la ley o de instituciones públicas. Dichas solicitudes se deben enviar a la siguiente dirección:

A/A: Manual de registro y confiscación
Sección de Delitos Cibernéticos y Propiedad Intelectual
10th & Constitution Ave., NW
John C. Keeney Bldg., Suite 600
Washington, DC 20530

[Índice]

INTRODUCCIÓN

Durante la última década, los ordenadores e Internet han adquirido un papel predominante en la vida estadounidense. Millones de ciudadanos de este país pasan varias horas al día frente a la pantalla de un ordenador, desde donde envían y reciben correos electrónicos, navegan por la red, mantienen bases de datos y participan en innumerables actividades.

Desgraciadamente, las personas que cometen delitos no se han mantenido al margen de la revolución de la informática. Cada vez son más los delincuentes que utilizan buscas, teléfonos móviles, ordenadores portátiles y servidores de red para perpetrar sus actividades delictivas. En algunos casos, incluso, los ordenadores son el medio que les permite cometerlas. Por ejemplo, Internet se puede utilizar para enviar una amenaza de muerte por correo electrónico; para lanzar ataques de hacker contra una red vulnerable de ordenadores; para divulgar virus informáticos o para transmitir imágenes de pornografía infantil. En otros casos, los ordenadores sirven simplemente como prácticos dispositivos de almacenamiento de pruebas de delitos. Por poner un ejemplo, un traficante de droga puede tener una lista de quién le debe dinero almacenada en un archivo de su ordenador, o en una operación de blanqueo de dinero se pueden conservar registros económicos falsos en un archivo de un servidor de red.

El espectacular aumento de los delitos relacionados con la informática hace que sea necesario que los fiscales y los agentes encargados de hacer cumplir la ley sean capaces de comprender cómo obtener pruebas electrónicas almacenadas en ordenadores. Registros electrónicos como diarios de redes informáticas, correos electrónicos, archivos de procesamiento de textos e imágenes "jpg" proporcionan al gobierno un número cada vez mayor de pruebas importantes (y en ocasiones, fundamentales) en casos delictivos. El objeto de esta publicación es proporcionar a los agentes federales encargados de hacer cumplir la ley y a los fiscales una orientación sistemática que les ayude a comprender los asuntos jurídicos que pueden surgir al buscar pruebas electrónicas en investigaciones judiciales.

La ley que rige las pruebas electrónicas en investigaciones judiciales tiene dos fuentes principales: la Cuarta Enmienda a la Constitución de Estados Unidos y las leyes sobre privacidad codificadas en 18 U.S.C. (Código de Estados Unidos, en adelante, U.S.C.) §§ 2510-22, 18 U.S.C. §§ 2701-12 y 18 U.S.C. §§ 3121-27. Si bien es cierto que en algunos casos se solapan asuntos constitucionales y jurídicos, en la mayor parte de las situaciones se presenta, bien un asunto constitucional sujeto a la Cuarta Enmienda, bien un asunto jurídico sujeto a estas tres leyes. Este manual refleja esta división: Los capítulos 1 y 2 se centran en la ley de la Cuarta Enmienda sobre registro y confiscación, mientras que los capítulos 3 y 4 lo hacen en los asuntos jurídicos, los cuales surgen mayoritariamente en casos relacionados con redes informáticas e Internet.

En el capítulo 1 se explican las restricciones que impone la Cuarta enmienda sobre el registro y confiscación injustificados de ordenadores y datos informáticos. El capítulo comienza explicando cómo aplican los tribunales la prueba de "expectativa razonable de privacidad" a los ordenadores, para continuar después con cómo se aplican las excepciones a los requisitos de justificación en los casos relacionados con ordenadores y concluye con una completa exposición de los asuntos más complejos de la Cuarta Enmienda que surgen a partir del registro de ordenadores sin justificación en lugares de trabajo. Entre las cuestiones que se tratan en este capítulo se incluyen: ¿Cuándo necesita el gobierno una orden de registro para analizar y confiscar el ordenador de un sospechoso? ¿Puede registrar un investigador sin orden de registro el busca de un sospechoso si se han encontrado incidentes para su detención? ¿Precisa el gobierno de una orden para registrar el ordenador de un empleado público situado en su oficina?

En el capítulo 2 se comenta la ley que rige el registro y confiscación de ordenadores con arreglo a las órdenes de registro. El capítulo arranca revisando los pasos que deben seguir los investigadores a la hora de planificar y ejecutar los registros para confiscar equipos y datos informáticos con una orden. Concretamente, el capítulo se centra en dos temas: En primer lugar, cómo deben planificar los investigadores la ejecución del registro informático y, a continuación, cómo deben redactar las órdenes

de registro propuestas y sus correspondientes declaraciones juradas. Por último, el capítulo concluye comentando lo que ocurre después de realizar el registro. Entre las cuestiones que se tratan en este capítulo se incluyen: ¿Cuándo deben prever los investigadores el registro informático in situ y cuándo deben llevarse los equipos y analizarlos posteriormente en otro lugar? ¿Cómo deben planificar los investigadores sus registros para evitar la responsabilidad civil en virtud de la Ley de Protección de la Privacidad, 42 U.S.C. § 2000aa? ¿Cómo deben redactar los fiscales las órdenes de registro para que cumplan los requisitos de particularidad de la Cuarta Enmienda y la Regla 41 de las Normas Federales de Procedimiento Penal? ¿Cuál es la ley que rige cuándo debe el gobierno registrar y devolver los ordenadores confiscados?

El tema principal del capítulo 3 es la parte de las comunicaciones guardadas de la Ley de Privacidad de las Comunicaciones Electrónicas, 18 U.S.C. §§ 2701-12 ("ECPA"). La ECPA describe el modo en el que los investigadores pueden obtener registros de cuenta almacenados y contenidos de proveedores de servicios de red, incluyendo los proveedores de servicios de Internet (PSI), de teléfono móvil y de satélite. Los problemas de la ECPA surgen con frecuencia en casos relacionados con Internet: cada vez que los investigadores buscan información almacenada relativa a cuentas de Internet de los proveedores de este servicio, deben cumplir con la ley. Este capítulo incluye las enmiendas a la ECPA especificadas por la Ley USA PATRIOT de 2001, Pub. L. Nº 107-56, 115 Stat. 272 (2001) (la "Ley PATRIOT"). La Ley PATRIOT aclaró y actualizó la ECPA a la luz de las nuevas tecnologías y, en algunos aspectos, relajó las restricciones sobre el acceso a las comunicaciones almacenadas para hacer cumplir la ley. Entre los temas que se abarcan en esta sección se incluyen: ¿Cómo puede obtener el gobierno correos electrónicos y registros de cuentas de red de los proveedores de servicios de Internet (ISP)? ¿Cuándo tiene el gobierno que obtener una orden de registro, frente a la 18 U.S.C. § 2703(d) solicitud o citación? ¿Cuándo pueden los proveedores revelar correos electrónicos y registros al gobierno de forma voluntaria? ¿Qué soluciones impondrá un tribunal si se ha infringido la ECPA?

El capítulo 4 analiza la estructura jurídica que rige la vigilancia electrónica, haciendo especial hincapié en cómo se aplican las leyes a la vigilancia de las redes de comunicaciones. Concretamente, el capítulo comenta el Título III en su versión modificada por la Ley de privacidad de las Comunicaciones Electrónicas, 18 U.S.C. §§ 2510-22 (a la que nos referiremos aquí como "Título III"),[(1)] así como la ley "Pen Register and Trap and Trace Devices" (Registro de llamadas y dispositivos de control y rastreo) 18 U.S.C. §§ 3121-27. Asimismo, este capítulo también incluye enmiendas a estas leyes especificadas mediante la Ley PATRIOT. Estas leyes estipulan cuándo y cómo puede realizar el gobierno una vigilancia en tiempo real, como el seguimiento de la actividad de un hacker informático cuando éste entre en una red gubernamental. Entre los asuntos que se tratan en este capítulo se incluyen: ¿Cuándo pueden las víctimas de delitos cibernéticos supervisar las intrusiones no autorizadas en sus redes y revelar esa información en aplicación de la ley? ¿Los banners de red pueden generar una autorización implícita a la supervisión? ¿Cómo puede obtener el gobierno una orden para el registro de llamadas o de control y rastreo que le permita recabar toda la información del encabezamiento de paquetes de las comunicaciones por Internet? ¿Qué soluciones impondrán los tribunales si se infringen las leyes de vigilancia electrónica?

Como es natural, los asuntos debatidos en los capítulos 1 a 4 pueden solaparse en los casos reales. Una investigación sobre el pirateo informático puede comenzar obteniendo los datos almacenados de un ISP de acuerdo con el capítulo 3, para pasar a continuación a una fase de vigilancia electrónica según el capítulo 4 y concluir, finalmente, con un registro de la residencia del sospechoso y la confiscación de sus ordenadores de acuerdo con los capítulos 1 y 2. En otros casos, los agentes y fiscales deben comprender los asuntos que pueden surgir en múltiples capítulos, no sólo en el mismo caso, sino de manera simultánea. Por ejemplo, una investigación acerca de una mala conducta en el lugar de trabajo por parte de un empleado del gobierno podría implicar los capítulos 1 a 4. Es posible que los investigadores deseen tener acceso a los correos electrónicos del empleado del servidor de red gubernamental (lo que también implicaría la ECPA, comentada en el capítulo 3); supervisar el uso por parte del empleado del teléfono o Internet en tiempo real (lo que traería a colación los problemas de vigilancia del capítulo 4); y, al mismo tiempo, podría ser necesario registrar el ordenador del empleado en su despacho para hallar pistas de su comportamiento inapropiado (problemas de registro y confiscación de los capítulos 1 y 2). Dado que los sistemas constitucional y jurídico se pueden solapar en determinados casos, es necesario que los agentes y fiscales comprendan no sólo los temas jurídicos

que se tratan en los capítulos 1 a 4, sino que deben tener clara la naturaleza exacta de la información que se debe recabar en estos casos concretos.

Después de los capítulos 1 a 4 aparece un quinto capítulo, de extensión breve, en el que se abordan los problemas relacionados con las pruebas que surgen a menudo en los casos relacionados con ordenadores. La publicación concluye con apéndices, en los que se ofrecen impresos de muestra e indicaciones sobre el lenguaje y las solicitudes.

Las investigaciones sobre delitos informáticos ponen sobre la mesa muchos problemas nuevos y los tribunales no han hecho más que comenzar a interpretar cómo aplicar la Cuarta Enmienda y las leyes federales a los casos relacionados con la informática. Aquellos agentes y fiscales que requieran un asesoramiento más detallado, pueden echar mano de varios recursos. Por distritos federales, todas y cada una de las Oficinas del Fiscal de Estados Unidos tiene al menos un abogado asistente de EE.UU. designado como Coordinador de ordenadores y telecomunicaciones ("CTC"). Los CTC reciben una formación completa en los delitos relacionados con la informática y tienen la responsabilidad de ofrecer su experiencia en los temas que se cubren en este manual dentro de su distrito. Se puede contactar con los CTC en su oficina de distrito. Asimismo, diversas secciones de la División de delitos del MInisterio estadounidense de Justicia de Washington DC cuentan con una amplia experiencia en el ámbito de la informática. La Oficina de Asuntos Internacionales ((202) 514-0000) ofrece asesoramiento en las múltiples investigaciones sobre delitos informáticos que pueden acarrear problemas internacionales. La Oficina de Operaciones de Seguridad ((202) 514-6809) ofrece asesoramiento jurídico sobre escuchas telefónicas y otras leyes sobre privacidad comentadas en los capítulos 3 y 4. Por otra parte, el Departamento de Explotación y Obscenidad Infantil ((202) 514-5780) asesora sobre casos relacionados con ordenadores que impliquen pornografía o explotación infantil.

Por último, siempre se agradece la aportación de agentes y fiscales que quieran ponerse en contacto con la Sección de Delitos Cibernéticos y Propiedad Intelectual ("CCIPS"), tanto si es para ofrecer asesoramiento en general como si es para un caso concreto. Durante las horas laborables hay al menos dos abogados de la CCIPS para responder dudas y ofrecer asistencia a agentes y fiscales acerca de los temas que se tratan en este documento, así como sobre otros asuntos que pueden surgir en casos relacionados con los delitos informáticos. El número principal de la CCIPS es el (202) 514-1026. Fuera del horario de oficina, puede contactar con la CCIPS por medio del Centro de Control de Justicia en el número de teléfono (202) 514-5000.

[Índice]

I. REGISTRO Y CONFISCACIÓN DE ORDENADORES SIN UNA ORDEN

A. Introducción

La Cuarta Enmienda limita la posibilidad de que los agentes gubernamentales realicen registros en busca de pruebas si no disponen de una orden. En este capítulo se explican los límites constitucionales de este tipo de registros en los casos relacionados con ordenadores.

La Cuarta Enmienda estipula:

El derecho de las personas a la seguridad en cuanto a su persona, hogar, documentos y efectos, contra registros y confiscaciones no razonables, no se infringirá y no se emitirán órdenes, excepto por causa probable, justificada por juramento o afirmación y, en particular, describiendo el lugar que se va a registrar y las personas u objetos que se detendrán o confiscarán.

Según el Tribunal Supremo, un registro sin orden no infringe la Cuarta Enmienda si se cumple una de estas dos condiciones. En primer lugar, si la conducta del gobierno no contraviene la "expectativa razonable de privacidad" de una persona, por lo que, desde el punto de vista formal, no constituye un

registro conforme a la Cuarta Enmienda y no se requiere una orden. Véase Illinois v. Andreas, 463 U.S. 765, 771 (1983). En segundo lugar, un registro sin orden que infrinja la expectativa razonable de privacidad de una persona será "razonable", no obstante, y por tanto constitucional, si constituye una excepción establecida al requisito de la orden. Véase Illinois v. Rodriguez, 497 U.S. 177, 185 (1990). Por consiguiente, los investigadores deben tener en cuenta dos preguntas a la hora de cuestionarse si un registro de un ordenador por parte del gobierno precisa una orden. Primeramente, ¿el registro infringe una expectativa razonable de privacidad? Y, si es el caso, ¿puede ser razonable aun así porque constituye una excepción al requisito de la orden?

[Índice]

B. La "expectativa razonable de privacidad" de la Cuarta Enmienda en casos relacionados con ordenadores

1. Principios generales

Un registro es constitucional si no contraviene la expectativa "razonable" o "legítima" de privacidad de una persona. Katz v. Estados Unidos, 389 U.S. 347, 362 (1967) (Harlan, J., concurrente). Esta cuestión abarca dos asuntos discretos: primero, si la conducta del individuo refleja una "expectativa real (subjetiva) de privacidad" y, en segundo lugar, si la sociedad está preparada para considerar dicha expectativa subjetiva de privacidad por parte de la persona como "razonable". Id. en 361. En la mayor parte de los casos, la dificultad de rebatir la expectativa subjetiva de privacidad por parte de un demandado centra el análisis sobre el aspecto objetivo de la prueba Katz, esto es, si dicha expectativa es razonable.

No hay una regla establecida que indique si una expectativa de privacidad es razonable desde el punto de vista constitucional. Véase O'Connor v. Ortega, 480 U.S. 709, 715 (1987). Por ejemplo, el Tribunal Supremo ha establecido que una persona tiene una expectativa razonable de privacidad en la propiedad situada dentro del hogar de una persona, véase Payton v. New York, 445 U.S. 573, 589-90 (1980); en "el calor relativo de las diversas estancias del hogar" revelado mediante el uso de un visor térmico, véase Kyllo v. Estados Unidos, 533 U.S. 27 (2001); en las conversaciones que se desarrollen dentro de una cabina telefónica cerrada, véase Katz, 389 U.S. en 358; y en el contenido de recipientes opacos, véase Estados Unidos v. Ross, 456 U.S. 798, 822-23 (1982). Por el contrario, una persona no tiene una expectativa razonable de privacidad en actividades que se desarrollen en campos abiertos, véase Oliver v. Estados Unidos, 466 U.S. 170, 177 (1984); en la basura depositada en los alrededores de la propiedad, véase California v. Greenwood, 486 U.S. 35, 40-41 (1988); o en la casa de una persona extraña en la que el individuo haya entrado sin la autorización del propietario con el fin de cometer un robo, véase Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978).

2. Expectativa razonable de privacidad en los ordenadores como dispositivos de almacenamiento

Para determinar si una persona tiene una expectativa razonable de privacidad en la información almacenada en un ordenador, puede resultar útil tratar el ordenador como un contenedor cerrado, al igual que un maletín o un archivador. Por lo general, la Cuarta Enmienda prohíbe para la aplicación de la ley el acceso y la observación de la información almacenada en un ordenador sin una orden si, en la misma situación, se prohibiría abrir un contenedor cerrado y examinar su contenido.

La pregunta más básica de la Cuarta Enmienda en los casos relacionados con los ordenadores cuestiona si un individuo disfruta de una expectativa razonable de privacidad en la información electrónica guardada en un ordenador (u otros dispositivos electrónicos de almacenamiento) bajo control del mismo. Por ejemplo, ¿tienen las personas una expectativa razonable de privacidad en el contenido de sus ordenadores portátiles, disquetes o buscas? Si la respuesta es afirmativa, el gobierno debe obtener una orden por el procedimiento habitual antes de acceder a dicha información.

Al abordar este asunto, los tribunales han comparado los dispositivos electrónicos de almacenamiento con contenedores cerrados y han deducido que acceder a la información almacenada en un dispositivo de este tipo es similar a abrir un contenedor cerrado. Dado que normalmente las personas muestran una expectativa razonable de privacidad en el contenido de los recipientes cerrados, véase Estados Unidos v. Ross, 456 U.S. 798, 822-23 (1982), hacen lo propio con los datos guardados en dispositivos electrónicos de almacenamiento. Por consiguiente, acceder a la información de un ordenador implicará por lo general la expectativa razonable de privacidad del propietario acerca de la misma. Véase Estados Unidos v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (se halló la expectativa razonable de privacidad en los archivos almacenados en el disco duro de un ordenador personal); Estados Unidos v. Reyes, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996) (se halló la expectativa razonable de privacidad en los datos guardados en un busca); Estados Unidos v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995) (igual); Estados Unidos v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (igual); Estados Unidos v. Blas, 1990 WL 265179, en *21 (E.D. Wis. 4 de diciembre de 1990) ("Una persona tiene la misma expectativa de privacidad en un busca, ordenador o cualquier otro dispositivo electrónico de almacenamiento o recuperación de datos que en un contenedor cerrado").

Si bien es cierto que los tribunales han coincidido al equiparar los dispositivos electrónicos de almacenamiento con contenedores cerrados, sus conclusiones difieren a la hora de considerar si cada archivo individual guardado en un ordenador o disco se debe tratar como un contenedor cerrado distinto. En dos casos el Quinto Circuito ha determinado que un disco de ordenador que contenga diversos archivos es un único contenedor en lo relativo a la finalidad de la Cuarta Enmienda. En primer lugar, en Estados Unidos v. Runyan, 275 F.3d 449, 464-65 (5º Cir. 2001), en el que partes privadas habían registrado determinados archivos y habían hallado pornografía infantil, el Quinto Circuito defendió que la policía no sobrepasó el alcance del registro privado al examinar otros archivos de otros discos que ya habían sido registrados parcialmente de manera privada. Equiparando un disco a un contenedor cerrado, el tribunal explicó que "la policía no excedió el registro privado al examinar más elementos de un contenedor cerrado de los que analizaron los investigadores privados". Id. en 464. En segundo lugar, en Estados Unidos v. Slanina, 283 F.3d 670, 680 (5º Cir. 2002), el tribunal sostuvo que el registro sin orden de parte de un ordenador y disco duro estaba justificado, el demandado ya no tenía ninguna expectativa razonable de privacidad en el contenido restante del ordenador y del disco y, por tanto, el registro exhaustivo por parte del personal de las fuerzas de seguridad no infringió la Cuarta Enmienda.

En contraste con el enfoque del Quinto Circuito, el Décimo Circuito ha rechazado autorizar registros tan exhaustivos de equipos informáticos en ausencia de una orden o de una excepción al requisito de la misma. Véase Estados Unidos v. Carey, 172 F.3d 1268, 1273-75 (10º Cir. 1999) (en la que el fallo estipulaba que un agente sobrepasó el margen de una orden para buscar pruebas de venta de drogas cuando "abandonó dicha búsqueda" y en lugar de ello se dedicó a buscar pornografía infantil durante cinco horas). Concretamente, el Décimo Circuito advirtió en un caso posterior de que "dado que un ordenador puede almacenar tanta información relativa a muchos ámbitos diferentes de la vida de una persona, existe un riesgo mayor de que se entremezclen documentos, lo que conlleva una invasión de la privacidad cuando la policía lleva a cabo una búsqueda de pruebas en un ordenador". Estados Unidos v. Walser, 275 F.3d 981, 986 (10º Cir. 2001).

Aunque las personas normalmente muestran una expectativa razonable de privacidad en los ordenadores que controlan, existen circunstancias especiales que pueden anular dicha expectativa. Por ejemplo, una persona no tendrá expectativa alguna de privacidad si ha hecho pública la información almacenada en el ordenador. En Estados Unidos v. David, 756 F. Supp. 1385 (D. Nev. 1991), los agentes obtuvieron la contraseña del demandado al mirar por encima del hombro de éste y verla en la pantalla cuando la tecleó en un ordenador portátil. El tribunal no halló indicios de infracción de la Cuarta Enmienda en la obtención de la contraseña, ya que el demandado no gozaba de una expectativa razonable de privacidad "en lo que aparecía en la pantalla". Id. En 1389. Véase también Katz v. Estados Unidos, 389 U.S. 347, 351 (1967) ("Aquello que una persona haga del dominio público, aunque lo haga desde su casa o despacho, no está sujeto a la protección de la Cuarta Enmienda").; Estados Unidos v. Gorshkov, 2001 WL 1024026, en *2 (W.D. Wash. 23 de mayo de 2001) (en la que se sostiene que el demandado no tenía ninguna expectativa razonable de privacidad en el uso de una red informática privada cuando los agentes secretos miraron por encima de su hombro, al no ser el propietario del ordenador que estaba

utilizando y al saber que el administrador del sistema podía vigilar lo que hacía). Asimismo, las personas tampoco pueden tener una expectativa razonable de privacidad en el contenido de un ordenador que hayan robado. Véase Estados Unidos v. Lyons, 992 F.2d 1029, 1031-32 (10º Cir. 1993).

3. Expectativa razonable de privacidad y posesión de terceras partes

Las personas que tengan una expectativa razonable de privacidad en información almacenada electrónicamente que esté bajo su control pueden perder la protección de la Cuarta Enmienda si ceden dicho control a terceras partes. Por ejemplo, una persona puede ofrecer un contenedor de información electrónica a una tercera parte al llevar un ordenador estropeado a una tienda para que se lo arreglen o al enviar un disquete a un amigo por correo. Por otra parte, un usuario puede transmitir información a terceras partes de manera electrónica al enviar datos por Internet. Si los agentes de la ley averiguan que terceras partes están en posesión de información que puede aportar pruebas de un delito, es probable que quieran analizarla. El hecho de que la Cuarta Enmienda exija que obtengan una orden antes de examinar la información depende primeramente de si la posesión de la tercera parte ha eliminado la expectativa razonable de privacidad de la persona.

A la hora de analizar los problemas derivados de la posesión de terceras partes ayuda realizar una distinción entre la posesión de un transportista en el transcurso de la transmisión al destinatario final y la posesión subsiguiente de dicho destinatario. Por ejemplo, si A contrata a B para llevar un paquete a C, la expectativa razonable de privacidad de A en el contenido del paquete durante el tiempo que tarde B en llevarlo a C puede ser diferente a la expectativa razonable de privacidad de A una vez que C haya recibido el paquete. Durante la transmisión, el contenido normalmente está sujeto a la protección de la Cuarta Enmienda. Por lo general, el gobierno no puede examinar el contenido de un paquete durante su transmisión sin una orden de registro. La intrusión del gobierno y el registro del contenido infringen la expectativa razonable de privacidad tanto del remitente como del destinatario. Véase Estados Unidos v. Villarreal, 963 F.2d 770, 774 (5º Cir. 1992); pero véase también Estados Unidos v. Walker, 20 F. Supp. 2d 971, 973-74 (S.D.W. Va. 1998) (en la que se concluye que el envío de paquetes a una persona escondida bajo un seudónimo siguiendo un esquema delictivo no respalda una expectativa razonable de privacidad). Esta norma se aplica independientemente de si el transportista es una sociedad pública o privada. Compárese Ex Parte Jackson, 96 U.S. (6 Otto) 727, 733 (1877) (transportista público) con Walter v. Estados Unidos, 447 U.S. 649, 651 (1980) (transportista privado).

El “registro” por parte del gobierno de una señal electrónica intangible durante su transmisión también puede atañer a la Cuarta Enmienda. Véase Berger v. New York, 388 U.S. 41, 58-60 (1967) (en la que se aplica la Cuarta Enmienda a una comunicación por teléfono en el contexto de una escucha telefónica). Sin embargo, los límites de la Cuarta Enmienda en estos casos siguen siendo confusos, ya que el Congreso abordó los problemas de la Cuarta Enmienda identificados en el caso Berger aprobando el Título III de la Ley General para el Control del Crimen y la Seguridad en las Calles de 1968 ("Título III"), 18 U.S.C. §§ 2510-2522. El Título III, el cual se comenta en profundidad en el capítulo 4, proporciona un completo andamiaje jurídico que regula la vigilancia en tiempo real de las comunicaciones por cable y electrónicas. Su alcance comprende y supera en muchos sentidos la protección que proporciona la Cuarta Enmienda. Véase Estados Unidos v. Torres, 751 F.2d 875, 884 (7º Cir. 1985); Chandler v. Ejército de Estados Unidos, 125 F.3d 1296, 1298 (9º Cir. 1997). Por tanto, desde el punto de vista práctico, la vigilancia de las comunicaciones por cable y electrónicas en el transcurso de la transmisión por lo general hace surgir muchas cuestiones legales, pero pocas constitucionales. Véase el capítulo 4.

Las personas pueden perder la protección de la Cuarta Enmienda sobre sus archivos informáticos si pierden el control de los mismos.

Una vez que el destinatario final ha recibido un archivo, la expectativa razonable de privacidad del remitente depende de si puede esperar razonablemente mantener el control sobre el archivo y su contenido. Cuando una persona deja un paquete a una tercera para que se lo guarde, por ejemplo, normalmente sí mantiene el control del paquete y, por tanto, mantiene una expectativa razonable de privacidad sobre su contenido. Véase por ejemplo Estados Unidos v. Most, 876 F.2d 191, 197-98 (D.C. Cir. 1989) (en la que se concluye que existe una expectativa razonable de privacidad en el contenido de

una bolsa de plástico que se dejó al cuidado del dependiente de una frutería); Estados Unidos v. Barry, 853 F.2d 1479, 1481-83 (8º Cir. 1988) (en la que se concluye que existe una expectativa razonable de privacidad sobre una maleta cerrada con llave almacenada en un mostrador de equipajes de un aeropuerto); Estados Unidos v. Presler, 610 F.2d 1206, 1213-14 (4° Cir. 1979) (en la que se concluye que existe una expectativa razonable de privacidad sobre unos maletines cerrados que el demandado dejó a un amigo para que se los cuidara). Véase también Estados Unidos v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (en la que se concluye que el demandado tiene una expectativa razonable de privacidad sobre los archivos informáticos guardados en el disco duro que dejó a un técnico con el objetivo limitado de reparar el ordenador).

No obstante, si el remitente no puede esperar de una manera razonable mantener el control sobre el elemento que está en posesión de la tercera parte, ya no puede tener una expectativa razonable de privacidad sobre su contenido. Por ejemplo, en Estados Unidos v. Horowitz, 806 F.2d 1222 (4° Cir. 1986), el demandado envió por correo electrónico información confidencial sobre precios perteneciente a su empleador a un competidor de éste. Cuando el FBI inspeccionó los ordenadores del competidor y halló la información sobre precios, el demandado aseguró que esta inspección contravenía sus derechos de la Cuarta Enmienda. El Cuarto Circuito se mostró en desacuerdo y sostuvo que el demandado cedió su interés y control sobre la información al enviarla al competidor para que éste la utilizara en el futuro. Véase id. en 1225-26. Véase también Estados Unidos v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (en la que se concluye que el demandado no mantiene una expectativa razonable de privacidad sobre el contenido de un mensaje de correo electrónico enviado a una sala de chat de America Online una vez que dicho mensaje ha sido recibido por los participantes en esa sala de chat) (se cita a Hoffa v. Estados Unidos, 385 U.S. 293, 302 (1966)). En algunos casos, el remitente puede conservar inicialmente el derecho a controlar la posesión de la tercera parte, aunque puede perder ese derecho con el paso del tiempo. La regla general es que los derechos de la Cuarta Enmienda que amparan al remitente se anulan a medida que disminuye el derecho de éste a controlar la posesión de la tercera parte. Por ejemplo, en Estados Unidos v. Poulsen, 41 F.3d 1330 (9° Cir. 1994), el pirata informático Kevin Poulsen dejó unas cintas de ordenador en un casillero situado en unas instalaciones de almacenamiento comercial pero descuidó el pago del alquiler del casillero. Después de un registro de las instalaciones realizado sin orden, el gobierno quiso utilizar las cintas contra Poulsen. El Noveno Circuito sostuvo que el registro no contravino la expectativa razonable de privacidad de Poulsen ya que, en virtud de las leyes del Estado, el hecho de que Poulsen no abonara el alquiler anuló su derecho a tener acceso a las cintas. Véase id. en 1337.

Una parte importante de los casos del Tribunal Supremo establece que las personas no pueden por lo general confiar en mantener el control sobre información revelada a terceras partes, incluso si los remitentes tienen la expectativa subjetiva de que las terceras partes mantendrán dicha información como confidencial. Por ejemplo, en Estados Unidos v. Miller, 425 U.S. 435, 443 (1976), el tribunal concluyó que la Cuarta Enmienda no protege información sobre cuentas bancarias si los titulares de las mismas la divulgan a sus bancos. Al poner la información bajo el control de una tercera parte, explica el tribunal, el tribunal de una cuenta asume el riesgo de que tal información sea revelada al gobierno, con lo cual, según el tribunal, "la Cuarta Enmienda no prohíbe la obtención de información revelada a una tercera parte y transmitida por ésta a autoridades gubernamentales, incluso si ésta se revela asumiendo que se utilizará únicamente con un objetivo limitado y que no se traicionará la confianza que se otorgó a la tercera parte". Id. (se cita a Hoffa v. Estados Unidos, 385 U.S. 293, 302 (1966)). Véase también Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (en la que no se encuentra ninguna expectativa razonable de privacidad en los números de teléfono marcados por el propietario de un teléfono ya que el hecho de marcar el número transmite efectivamente el número a la compañía telefónica); Couch v. Estados Unidos, 409 U.S. 322, 335 (1973) (en la que se sostiene que el gobierno puede citar a un contable para pedir información sobre un cliente que éste haya facilitado al primero, ya que un cliente no tiene una expectativa razonable de privacidad sobre la información que proporciona a un contable).

En vista de que los datos informáticos son "información", esta línea de casos sugiere que las personas que envían datos a través de redes de comunicaciones pueden perder la protección de la Cuarta Enmienda sobre los datos una vez que estos llegan al destinatario final. Véase Estados Unidos v. Meriwether, 917 F.2d 955, 959 (6° Cir. 1990) (en la que se sugiere que un mensaje electrónico enviado por medio de un busca es "información" según la línea de casos Smith/Miller); Charbonneau, 979 F.

Supp. en 1184 ("No se puede esperar que un mensaje de correo electrónico […] tenga una expectativa razonable de privacidad una vez que se haya recibido el mensaje"). Véase también no obstante C. Ryan Reetz, Nota, *Requisito de orden para registros de información computarizada*, 67 B.U. L. Rev. 179, 200-06 (1987) (en la que se aduce que determinados tipos de archivos informáticos almacenados de forma remota deben conservar la protección de la Cuarta Enmienda y en la que se intenta distinguir entre Estados Unidos v. Miller y Smith v. Maryland). Lógicamente, la ausencia de protección constitucional no implica necesariamente que el gobierno pueda acceder a los datos sin una orden o permiso del tribunal. Existen protecciones legales que protegen generalmente la privacidad de las comunicaciones electrónicas almacenadas de forma remota con los proveedores de servicios y que pueden brindar protección a los usuarios de Internet cuando la Cuarta Enmienda no lo hace. Véase 18 U.S.C. §§ 2701-2712 (comentada en el capítulo 3, más abajo).

En ocasiones, los demandados pueden apelar a la Cuarta Enmienda en cuanto a la adquisición de registros de cuentas e información sobre los abonados que poseen los proveedores de servicios de Internet mediante la utilización de procesos que implican menos que una orden de registro completa. Como se verá en un capítulo posterior, la Ley de Privacidad de las Comunicaciones Electrónicas permite al gobierno obtener registros sobre transacciones con una orden de tribunal de "hechos expresables" e información básica sobre los abonados por medio de una citación. Véase 18 U.S.C. §§ 2701-2712 (comentada en el capítulo 3, en adelante). Estos procedimientos jurídicos cumplen con la Cuarta Enmienda debido a que los clientes de los proveedores de servicios de Internet no tienen una expectativa razonable de privacidad sobre los registros de las cuentas de los clientes que se mantienen por y para la actividad comercial del proveedor. Véase Estados Unidos v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), declaración jurada, 225 F.3d 656 (4° Cir. 2000) (opinión no publicada) (en la que no se halla protección de la Cuarta Enmienda para la información básica de abonado del titular de una cuenta de red obtenida del proveedor de servicios de Internet); Estados Unidos v. Kennedy, 81 F. Supp. 2d 1103, 1110) (D. Kan. 2000) (igual). Esta regla coincide con casos anteriores que consideran el alcance de la protección de la Cuarta Enmienda en los registros de cuentas de cliente. Véase por ejemplo Estados Unidos v. Fregoso, 60 F.3d 1314, 1321 (8° Cir. 1995) (en la que se sostiene que el cliente de una compañía telefónica no tiene una expectativa razonable de privacidad sobre la información de cuenta revelada a dicha compañía); Procesos del Gran Jurado in re, 827 F.2d 301, 302-03 (8° Cir. 1987) (en la que se defiende que los registros de cuentas de cliente que mantiene y conserva Western Union no están sujetos a la protección de la Cuarta Enmienda).

4. Registros privados

La Cuarta Enmienda no se aplica a investigaciones llevadas a cabo por partes privadas que no actúen como agentes del gobierno.

La Cuarta Enmienda "es completamente inaplicable al registro o confiscación, incluso si no es razonable, realizado por un individuo privado que no actúe como agente del gobierno o con la participación o el conocimiento de un funcionario gubernamental". Estados Unidos v. Jacobsen, 466 U.S. 109, 113 (1984) (se omite cita interna). Como consecuencia de ello, si un individuo actúa por su cuenta, realiza un registro y pone los resultados del mismo a disposición de los agentes de la ley, no se infringe la Cuarta Enmienda. Véase id. por ejemplo, en Estados Unidos v. Hall, 142 F.3d 988 (7° Cir. 1998), el demandado llevó su ordenador a un especialista privado en informática para que se lo arreglara. Mientras se encontraba analizando el ordenador del demandado, la persona encargada de la reparación observó que muchos de los archivos que éste guardaba en él tenían nombres típicos de la pornografía infantil. Esta persona accedió a los archivos, comprobó que ciertamente contenían pornografía infantil y a continuación se puso en contacto con la policía del estado. Su indicación derivó en una orden, la detención del demandado y su condena por delitos de pornografía infantil. Durante la apelación, el Séptimo Circuito denegó la reclamación del demandado de que al haber registrado el ordenador sin una orden, el especialista había infringido la Cuarta Enmienda. Dado que el registro por parte del informático fue realizado por su cuenta, afirmó el tribunal, la Cuarta Enmienda no se aplicó a dicho registro ni a la posterior descripción de las pruebas a la policía del Estado. Véase id. en 993. Véase también Estados Unidos v. Kennedy, 81 F. Supp. 2d 1103, 1112 (D. Kan. 2000) (en la que se concluye que los registros del ordenador del demandado a través de Internet por parte de una persona

anónima y de empleados de una PSI privada no infringieron la Cuarta Enmienda ya que no se encontraron pruebas de que el gobierno estuviera implicado en los mismos).

En Estados Unidos v. Jacobsen, 466 U.S. 109 (1984), el Tribunal Supremo presentó el marco que debe guiar a los agentes que pretenden descubrir pruebas como consecuencia de un registro privado. Según Jacobsen, aquellos agentes que averigüen la existencia de pruebas a través de una búsqueda privada pueden recrear la búsqueda original sin violar ninguna expectativa razonable de privacidad. Lo que los agentes no pueden hacer sin una orden es "superar [] el alcance de la búsqueda privada". Id. en 115. Véase también Estados Unidos v. Miller, 152 F.3d 813, 815-16 (8° Cir. 1998); Estados Unidos v. Donnes, 947 F.2d 1430, 1434 (10° Cir. 1991). Sin embargo, véase Estados Unidos v. Allen, 106 F.3d 695, 699 (6° Cir. 1999) (sentencias) (en las que se estipula que Jacobsen no permite a los agentes de la ley recrear un registro privado de una casa o residencia privada). Esta norma exige que los agentes restrinjan su investigación al alcance del registro privado al investigar sin una orden y cuando se haya producido un registro privado con anterioridad. En tanto en cuanto los agentes se limiten al ámbito del registro privado, el registro que ellos realicen no infringirá la Cuarta Enmienda. Sin embargo, en cuanto los agentes sobrepasen el límite del registro privado realizado sin orden, todas las pruebas que se descubran pueden ser susceptibles de ser sometidas a una moción para que se excluyan.

En los casos relacionados con ordenadores, el uso por parte de las fuerzas de seguridad de la doctrina del registro privado dependerá en parte de si se considera que la inspección realizada por los cuerpos de seguridad de los archivos que no hayan sido examinados durante un registro anterior supera el alcance del registro privado realizado sin una orden. Véase Estados Unidos v. Runyan, 275 F.3d 449, 464-65 (5° Cir. 2001) (en la que se sostiene que la policía no excedió el alcance de un registro privado al examinar más archivos en los discos de los que se habían inspeccionado durante el registro privado). Según el enfoque adoptado por el Quinto Circuito en el caso Runyan, el registro de una tercera parte de un único archivo en un ordenador permite un registro sin necesidad de orden del contenido total del ordenador por parte de los cuerpos de seguridad. No obstante, otros tribunales pueden rechazar el enfoque del Quinto Circuito y establecer que los investigadores gubernamentales solamente pueden ver aquellos archivos cuyo contenido reveló el registro privado. Véase Estados Unidos v. Barth, 26 F. Supp. 2d 929, 937 (W.D. Tex. 1998) (en la que se sostiene, en un caso previo al de Runyan, que los agentes que inspeccionaron más archivos de los que vio la persona que realizó el registro privado superaron el alcance de dicho registro). Incluso en el caso de que los tribunales sigan el enfoque más restrictivo, la información obtenida del registro privado con frecuencia será útil para facilitar la causa probable necesaria para obtener una orden con vistas a un registro posterior.[(2)]

Si bien la mayoría de los asuntos relacionados con registros privados se producen cuando terceras partes examinan de forma intencionada una propiedad y ponen las pruebas de un delito a disposición de las fuerzas de seguridad, se aplica la misma estructura cuando terceras partes sacan a la luz involuntariamente pruebas de un delito. Por ejemplo, en Estados Unidos v. Procopio, 88 F.3d 21 (1° Cir. 1996), el demandado guardaba unos archivos que le incriminaban en la caja fuerte de su hermano. Posteriormente unos ladrones robaron la caja, la abrieron y la dejaron abandonada en un parque público. La policía encargada de investigar el robo de la caja halló los archivos desperdigados por el suelo alrededor de la misma, los recogió y posteriormente los utilizó contra el demandado en un caso que no guardaba relación con el primero. El Primer Circuito defendió que el uso de los archivos no infringía la Cuarta Enmienda, ya que los ladrones, con su registro privado, fueron los que sacaron los archivos a la luz pública. Véase id. en 26-27 (se cita a Jacobsen, 466 U.S. en 113).

Es muy importante destacar que el hecho de que la persona que realice un registro no sea un funcionario del gobierno no implica necesariamente que dicho registro sea "privado" en lo que respecta a la Cuarta Enmienda. Un registro realizado por una parte privada se considerará un registro gubernamental según la Cuarta Enmienda "si la parte privada actúa como instrumento o agente del gobierno". Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614 (1989). El Tribunal Supremo no ha contribuido demasiado a aclarar cuándo una conducta privada se puede atribuir al gobierno; el Tribunal se ha limitado a expresar que esta cuestión "depende necesariamente del grado de participación del gobierno en las actividades de la parte privada […], una cuestión que únicamente se puede resolver a la luz de todas las circunstancias". Id. en 614-15 (se cita Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)). A falta de una norma más precisa, los distintos tribunales federales de apelación han adoptado una serie

de enfoques para distinguir entre registros privados y realizados por el gobierno. Aproximadamente la mitad de los circuitos aplican un enfoque basado en "todas las circunstancias" que analiza tres factores: si el gobierno conoce o consiente la conducta intrusiva, si la parte que realiza el registro tiene como finalidad prestar su asistencia a las labores de las fuerzas de seguridad en el momento del registro y si el gobierno alienta, inicia o instiga positivamente la acción privada. Véase por ejemplo Estados Unidos v. Pervaz, 118 F.3d 1, 6 (1° Cir. 1997); Estados Unidos v. Smythe, 84 F.3d 1240, 1242-43 (10° Cir. 1996); Estados Unidos v. McAllister, 18 F.3d 1412, 1417-18 (7° Cir. 1994); Estados Unidos v. Malbrough, 922 F.2d 458, 462 (8° Cir. 1990). Otros circuitos han adoptado formulaciones más normativas que se centran solamente en dos de estos factores. Véase por ejemplo Estados Unidos v. Miller, 688 F.2d 652, 657 (9° Cir. 1982) (en la que se sentencia que la acción privada se considera conducta gubernamental si, en el momento del registro, el gobierno conoce o consiente la conducta invasiva y si la parte que realiza el registro tiene como objeto prestar su asistencia a las labores de las fuerzas de seguridad); Estados Unidos v. Paige, 136 F.3d 1012, 1017 (5° Cir. 1998) (igual); Estados Unidos v. Lambert, 771 F.2d 83, 89 (6° Cir. 1985) (en la que se defiende que un individuo privado es un agente del Estado según la Cuarta Enmienda si la policía ha instigado, fomentado o participado en el registro y si la persona se implicó en el mismo con la intención de ayudar a la policía en sus labores de investigación).

5.Uso de la tecnología para obtener información

El uso por parte del gobierno de tecnología innovadora para obtener información acerca de un objetivo puede atañer a la Cuarta Enmienda. Véase Kyllo v. Estados Unidos, 533 U.S. 27 (2001). En el caso Kyllo, el Tribunal Supremo sentenció que el uso sin orden previa de un visor térmico para averiguar la cantidad relativa de calor liberada de las distintas estancias del hogar del sospechoso constituyó un registro que infringió la Cuarta Enmienda. Concretamente, el tribunal sostuvo que cuando las fuerzas de seguridad "utilicen un dispositivo que quede fuera del alcance del público general para explorar detalles de la casa, que anteriormente habría sido imposible obtener sin una intrusión física, tal vigilancia constituye un "registro" y es presuntamente irrazonable sin una orden". Id. en 40. El uso por parte del gobierno de tecnología innovadora que quede fuera del alcance del público general para obtener información almacenada o transmitida a través de ordenadores o redes puede incumbir a esta sentencia de Kyllo y, consiguientemente, puede exigir la obtención de una orden. El hecho de si una tecnología entra dentro del alcance de la sentencia Kyllo depende de dos factores, al menos. En primer lugar, el uso de la tecnología no incumbe al caso Kyllo si dicha tecnología está al "alcance del público en general", véase id. en 34 & 39 n.6, aunque los tribunales aún no han definido la norma para determinar si una tecnología en concreto satisface este requisito. En segundo lugar, el Tribunal Supremo restringió sus conclusiones del caso Kyllo al uso de tecnología para revelar información sobre "el interior de una casa". Véase id. en 40 ("Hemos expresado que la Cuarta Enmienda traza una línea muy firme ante la entrada de la casa". (se omite cita interna)).

[Índice]

C. Excepciones al requisito de la orden en casos relacionados con ordenadores

Los registros que se realicen sin una orden y que contravengan una expectativa razonable de privacidad cumplirán con la Cuarta Enmienda si entran dentro de una excepción establecido a la exigencia de la orden. Los casos relacionados con la informática a menudo plantean cuestiones con respecto a cómo se aplican estas excepciones establecidas a las nuevas tecnologías.

1. Autorización

Los agentes pueden registrar un lugar u objeto sin una orden o sin ni siquiera una causa probable en el caso de que una persona con autoridad haya dado su consentimiento al registro de forma voluntaria. Véase Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973). Este consentimiento puede ser explícito o implícito. Véase Estados Unidos v. Milian-Rodriguez, 759 F.2d 1558, 1563-64 (11° Cir. 1985). El hecho de si la autorización se concedió de forma voluntaria es una cuestión que el tribunal deberá decidir teniendo en cuenta todas las circunstancias. Aunque es cierto que no hay ningún aspecto concreto que controle el resultado, el Tribunal Supremo ha identificado los siguientes factores

importantes: la edad, educación, inteligencia, estado físico y mental de la persona que concede la autorización, si la persona se encontraba detenida y si se había puesto en su conocimiento que le asistía el derecho de rechazar la autorización. Véase Schneckloth, 412 U.S. en 226. El gobierno es quien tiene que demostrar que el consentimiento fue voluntario. Véase Estados Unidos v. Matlock, 415 U.S. 164, 177 (1974); Estados Unidos v. Price, 599 F.2d 494, 503 (2° Cir. 1979).

En los casos relacionados con la informática son dos los problemas que surgen con más frecuencia acerca de la autorización. En primer lugar, ¿cuándo supera un registro la autorización expresada? Por ejemplo, si una persona autoriza el registro de una máquina, ¿hasta qué punto permite dicho consentimiento la recuperación de la información almacenada en la máquina? Por otra parte, ¿quién es la persona adecuada para dar su consentimiento para un registro? ¿Tienen autoridad compañeros de piso, amigos y padres para permitir el registro de los archivos informáticos de otra persona?[3]

a) Alcance de la autorización

"El alcance de una autorización para un registro se define generalmente por su finalidad expresada y está limitada por la amplitud del consentimiento concedido". Estados Unidos v. Pena, 143 F.3d 1363, 1368 (10° Cir. 1998) (se omite cita interna). La norma para medir el alcance de la autorización conforme a la Cuarta Enmienda es una razonabilidad objetiva: "¿Qué entendería una persona razonable con el intercambio entre el [agente] y la [persona que concede la autorización]?" Florida v. Jimeno, 500 U.S. 248, 251 (1991). Esto requiere una investigación intensiva sobre los hechos acerca de si para el agente fue razonable creer que el alcance de la autorización incluía los elementos registrados. Lógicamente, si se definen claramente los límites del consentimiento, ya sea antes o durante el registro, los agentes deben respetar dichos límites. Véase Vaughn v. Baldwin, 950 F.2d 331, 333 (6° Cir. 1991).

El alcance permitido de los registros autorizados depende de los hechos de cada caso.

Los casos relacionados con la informática suelen plantear la cuestión de si la autorización para registrar un lugar u objeto incluye de forma implícita la autorización para acceder a la memoria de los dispositivos electrónicos de almacenamiento que se puedan encontrar durante el registro. En casos así, los tribunales estudian si la situación particular de la solicitud de autorización por parte de los agentes ha limitado implícita o explícitamente el alcance del registro a un tipo, margen o duración concretos. Dado que, en última instancia, este enfoque depende de nociones de sentido común dependiendo de la situación, los resultados alcanzados en las opiniones publicadas se mueven entre distinciones muy sutiles, cuando no herméticas por completo. Compárese Estados Unidos v. Reyes, 922 F. Supp. 818, 834 (S.D.N.Y. 1996) (en la que se concluyó que la autorización para "registrar el interior" de un coche incluía el consentimiento para obtener los números guardados en los buscas que se encontraron en el asiento trasero del coche) con Estados Unidos v. Blas, 1990 WL 265179, en *20 (E.D. Wis. 4 de dic. de 1990) (en la que se concluyó que el consentimiento para "mirar en" un busca no incluía la autorización para activarlo y recuperar los números, ya que mirar en un busca se podía interpretar como ver "cómo es el dispositivo, qué tamaño tiene o de qué marca es"). Véase también Estados Unidos v. Carey, 172 F.3d 1268, 1274 (10° Cir. 1999) (en la que se expresa que la autorización por escrito era extremadamente limitada, de forma que el consentimiento para la confiscación de "cualquier propiedad" controlada por el demandado y para "realizar un registro completo de las instalaciones y propiedad" en la dirección del demandado permitía únicamente a los agentes confiscar el ordenador del demandado en su piso, no a registrarlo en otro lugar, puesto que entonces ya no estaría ubicado dentro de su casa). La parte demandante puede reforzar su argumento de que la autorización incluía el registro de dispositivos electrónicos de almacenamiento apelando a casos similares relacionados con contenedores cerrados. Véase, por ejemplo, Estados Unidos v. Galante, 1995 WL 507249, en *3 (S.D.N.Y. 25 de agosto de 1995) (en la que se sostiene que la autorización general para registrar un coche incluía la autorización para que el oficial accediera a la memoria del teléfono móvil que se halló dentro del mismo, apelando al circuito precedente relativo a contenedores cerrados); Reyes, 922 F. Supp. en 834.

Los agentes deben tener especial cuidado de no basarse en una autorización para registrar un ordenador si obtienen dicha autorización por una razón y desean realizar un registro por otro motivo. En dos casos recientes, los tribunales de apelación suprimieron imágenes de pornografía infantil que se hallaron en ordenadores porque los agentes obtuvieron la autorización del demandado para registrar sus propiedades

para encontrar otro tipo de indicios. En Estados Unidos v. Turner, 169 F.3d 84 (1° Cir. 1999), unos detectives que buscaban pruebas físicas de un intento de abuso sexual obtuvieron una autorización por escrito del vecino de la víctima para registrar la "propiedad" y los "efectos personales" del vecino. Antes de que éste hubiera firmado el impreso de autorización, los detectives descubrieron un cuchillo de gran tamaño y manchas de sangre en su piso y le explicaron que estaban buscando más pruebas de la agresión sexual que el sospechoso pudiera haber dejado. Véase id. en 86. Mientras unos agentes registraban en busca de pruebas físicas, otro analizó el contenido del ordenador personal del vecino y descubrió imágenes de pornografía infantil. Al vecino se le imputó la posesión de pornografía infantil. Durante la apelación interlocutoria, el Primer Circuito sentenció que el registro del ordenador excedía el alcance del consentimiento y anuló las pruebas. Según el tribunal, las declaraciones de los detectives en las que expresaban que estaban buscando señales de la agresión limitaban el alcance de la autorización al tipo de pruebas físicas que podría haber dejado tras de sí un intruso. Véase id. en 88. Al transformar la búsqueda de pruebas físicas en un registro de archivos informáticos, el detective sobrepasó los límites de la autorización. Véase id. Véase también Carey, 172 F.3d en 1277 (Baldock, J., concurrente) (en la que se concluyó que los agentes superaron la autorización registrando un ordenador después de que el demandado firmara un impreso de consentimiento con una redacción muy general, ya que los agentes le comunicaron que buscaban droga o elementos relacionados, no archivos informáticos que contuvieran pornografía infantil) (se cita a Turner).

Una buena práctica para los agentes consiste en utilizar modelos de autorización que expresen de forma explícita que el alcance de la misma incluye el registro de ordenadores y otros dispositivos electrónicos de almacenamiento.

Dado que las decisiones para evaluar el alcance del consentimiento para registrar ordenadores han alcanzado en ocasiones resultados impredecibles, los investigadores deben indicar el alcance del registro de forma explícita al obtener la autorización de un sospechoso para registrar un ordenador.

b) Consentimiento de terceras partes

i) Normas generales

Es muy común que varias personas utilicen o posean un mismo equipo informático. En tanto en cuanto una de esas personas dé su permiso para buscar datos, por lo general los agentes pueden confiar en dicha autorización, siempre y cuando la persona tenga autoridad sobre el ordenador. En estos casos, todos los usuarios han asumido el riesgo de que otra de las personas que utilizan el equipo pueda descubrir todo lo que hay en él y permitir también a las fuerzas de seguridad que registren esta "área común".

El caso que marcó un hito en este ámbito es Estados Unidos v. Matlock, 415 U.S. 164 (1974). En el caso Matlock, el Tribunal Supremo concluyó que una persona que tenga "autoridad común" sobre instalaciones u objetos puede autorizar un registro incluso aunque otro usuario ausente se oponga. Id. en 171. De acuerdo con el tribunal, la autoridad común que establece el derecho de autorización por terceras partes exige el uso mutuo de la propiedad por las personas que normalmente tengan un acceso o control conjunto para la mayoría de fines, de forma que es razonable reconocer que cualquiera de los co-habitantes tienen derecho a permitir la inspección en su propio derecho y que los demás han asumido el riesgo de que cualquiera de los otros puede autorizar el registro de lo que tienen en común.

Id. en 171 n.7.

Según el enfoque Matlock, una tercera parte privada puede autorizar el registro de una propiedad si está bajo el control o acceso conjunto de dicha tercera parte. Los agentes pueden acceder a lo que la tercera parte puede ver sin contravenir expectativa razonable de privacidad alguna, siempre y cuando restrinjan la inspección a la zona permitida de la autoridad común de la tercera parte. Véase Estados Unidos v. Jacobsen, 466 U.S. 109, 119 (1984) (en la que se destaca que no se infringe la Cuarta Enmienda cuando una tercera parte privada invita al gobierno a ver el contenido de un paquete que esté controlado por la tercera parte). Con frecuencia, esta norma exige que los agentes tengan que averiguar si la tercera parte

tiene derechos de acceso antes de iniciar un registro autorizado, así como poner límites para distinguir entre aquellas áreas que entran dentro de la autoridad común de la tercera parte y aquellas otras que quedan fuera de su control. Véase Estados Unidos v. Block, 590 F.2d 535, 541 (4° Cir. 1978) (en la que se concluye que una madre podía autorizar el registro general de la habitación de su hijo de 23 años, pero no podía permitir el registro de un cajón cerrado con llave que se encontró en la misma). Sin embargo, dado que la prueba de acceso común no exige unidad de intereses entre el sospechoso y la tercera parte, el caso Matlock permite la autorización de terceras partes incluso cuando el objetivo del registro esté presente y deniegue su autorización. Véase Estados Unidos v. Sumlin, 567 F.2d 684, 687-88 (6° Cir. 1977) (en la que se concluye que una mujer tenía autoridad para permitir el registro del piso que compartía con su novio, aunque éste no lo autorizaba).

Las personas que compartan el uso de un ordenador por lo general tendrán capacidad para autorizar el registro de sus archivos de acuerdo con el caso Matlock. Véase Estados Unidos v. Smith, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998) (en la que se concluye que una mujer podía permitir el registro del ordenador de su novio, situado en la casa de ambos, y en la que se destaca que el novio no había protegido sus archivos por medio de contraseñas). Sin embargo, si una persona protege sus archivos mediante contraseñas y no las pone en conocimiento de los demás usuarios del ordenador, el Cuarto Circuito defiende que la autoridad de los demás usuarios para consentir el registro del ordenador no será extensible a los archivos que estén protegidos por contraseña. Véase Trulock v. Freeh, 275 F.3d 391, 403-04 (4° Cir. 2001) (en la que se equiparan los archivos protegidos por contraseña con cajones cerrados con llave en una habitación, lo cual el tribunal había considerado previamente como fuera del alcance del consentimiento de autoridad común). Si, por el contrario, el sospechoso ha comunicado la contraseña a una de las personas con las que comparte el ordenador, ésta última probablemente tendrá la autoridad común necesaria para permitir el registro de los archivos conforme al caso Matlock. Véase Estados Unidos v. Murphy, 506 F.2d 529, 530 (9° Cir. 1974) (per curiam) (en la que se concluye que un empleado podía autorizar el registro de un almacén de su empleador por el hecho de que el primero estaba en posesión de la llave y se destaca la "especial significación" del hecho de que hubiera sido el propio empleador quien le había entregado la llave).

Desde el punto de vista práctico, es posible que los agentes tengan bastante difícil conocer los límites exactos de la autoridad común de una tercera parte al obtener su autorización para realizar un registro. Si se les pregunta al respecto, las terceras partes que conceden el permiso pueden asegurar que tienen autoridad común sobre la propiedad, sin que sea cierto. En el caso Illinois v. Rodriguez, 497 U.S. 177 (1990), el Tribunal Supremo defendió que la Cuarta Enmienda no exige automáticamente la supresión de las pruebas descubiertas durante un registro autorizado si después se averigua que la tercera parte que permitió el registro carecía de autoridad para hacerlo. Véase id. en 188-89. En lugar de ello, el tribunal concluyó que los agentes pueden fiarse de una declaración de autoridad para conceder el permiso si se basa en "los hechos de los que dispone el oficial en ese momento, […] si un hombre prudente […] creería que la parte que concedió la autorización tenía la autoridad" para permitir un registro del lugar. Id. (se omiten las citas internas) (se cita Terry v. Ohio, 392 U.S. 1, 21-22 (1968)). Si los agentes confían de una manera razonable en la autoridad aparente para conceder el consentimiento, el consiguiente registro no infringe la Cuarta Enmienda.

ii) Cónyuges y parejas

La mayor parte de registros autorizados por el cónyuge son válidos.

En ausencia de un documento que acredite que el cónyuge que va a conceder la autorización no tiene acceso a la propiedad que se va a registrar, los tribunales normalmente asumen que un cónyuge puede permitir el registro de todas las propiedades de su pareja. Véase por ejemplo Estados Unidos v. Duran, 957 F.2d 499, 504-05 (7° Cir. 1992) (en la que se concluye que la esposa podía permitir el registro de una cochera que ella no utilizaba porque su marido no le había denegado el derecho a entrar en ella); Estados Unidos v. Long, 524 F.2d 660, 661 (9° Cir. 1975) (en la que se concluye que la esposa que había abandonado a su marido podía autorizar el registro de su hogar en copropiedad, aunque el marido había cambiado la cerradura). Por ejemplo, en Estados Unidos v. Smith, 27 F. Supp. 2d 1111 (C.D. Ill. 1998), un hombre llamado Smith vivía con una mujer de nombre Ushman y sus dos hijas. Cuando se imputaron acusaciones contra Smith por acoso infantil, Ushman permitió el registro del ordenador de

éste, el cual estaba situado en la casa en una hornacina conectada al dormitorio principal. Si bien Ushman rara vez utilizaba el ordenador de Smith, el tribunal de distrito concluyó que sí podía autorizar su registro. El tribunal infirió que, dado que Ushman no tenía prohibido acceder a la hornacina y que Smith no había protegido el ordenador con contraseñas, ella tenía autoridad para permitir el registro. Véase id. en 1115-16. Además, el tribunal añadió que incluso en el caso de que careciera de autoridad real para autorizarlo, aparentemente sí tenía autoridad para hacerlo. Véase id. en 1116 (se cita Illinois v. Rodriguez).

iii) Padres

Los padres pueden autorizar el registro de las habitaciones de sus hijos si estos tienen menos de 18 años. Si tienen o superan esta edad, los padres pueden autorizarlo o no, en función de la situación.

En algunos casos de delitos cibernéticos, los autores son relativamente jóvenes y viven con sus padres. Si el autor es menor de edad, el consentimiento paternal para registrar la propiedad y el espacio vital del delincuente será válido en la mayoría de los casos. Véase 3 W. LaFave,Search and Seizure: A Treatise on the Fourth Amendment (Registro y confiscación: tratado sobre la Cuarta Enmienda) § 8.4(b) en 283 (2ª ed. 1987) (en el que se destaca que los tribunales han denegado incluso "intentos denodados por parte de niños menores para establecer un uso exclusivo").

No obstante, si lo hijos que viven con los padres son adultos desde el punto de vista legal, el asunto se vuelve más complicado. Según el caso Matlock, está claro que los padres pueden autorizar el registro de áreas comunes del hogar familiar, con independencia de la edad del sospechoso. Véase Estados Unidos v. Lavin, 1992 WL 373486, en *6 (S.D.N.Y. 30 de noviembre de 1992) (en la que se reconoce el derecho de los padres a permitir el registro de un sótano en el que su hijo guardaba su ordenador y archivos). La situación cambia, sin embargo, si los agentes quieren registrar la habitación u otras zonas privadas de un hijo adulto, ya que no pueden asumir que los padres tienen autoridad para conceder su permiso. Aunque es cierto que los tribunales han aportado enfoques divergentes, se ha prestado atención especialmente a tres factores: la edad del sospechoso, si paga renta y si ha tomado medidas para denegar a sus padres el acceso a su habitación o área privada. En los casos en los que los sospechosos son mayores, pagan una renta y/o deniegan el acceso a los padres, por lo general los tribunales deciden que los padres no pueden dar su autorización. Véase Estados Unidos v. Whitfield, 939 F.2d 1071, 1075 (D.C. Cir. 1991) (en la que se concluye que el "interrogatorio superficial" de la madre del sospechoso es insuficiente para determinar el derecho a autorizar el registro de la habitación de su hijo de 29 años); Estados Unidos v. Durham, 1998 WL 684241, en *4 (D. Kan. 11 de septiembre de 1998) (la madre no tenía autoridad ni aparente ni real para consentir el registro de la habitación de su hijo de 24 años, ya que éste había cambiado las cerraduras de la habitación sin comunicárselo a su madre y además pagaba una renta por la habitación). Por el contrario, habitualmente los padres pueden dar su autorización si sus hijos adultos no pagan renta, son bastante jóvenes y si no han tomado medidas para denegarles el acceso al espacio que se quiere registrar. Véase Estados Unidos v. Rith, 164 F.3d 1323, 1331 (10° Cir. 1999) (en el que se sugiere que se supone que los padres tienen autoridad para permitir el registro de la habitación de su hijo de 18 años por el hecho de que éste no pague alquiler); Estados Unidos v. Block, 590 F.2d 535, 541 (4° Cir. 1978) (la madre podía permitir a la policía registrar la habitación de su hijo de 23 años si él no pagaba renta).

iv) Administradores de sistemas

Los "administradores u operadores de sistemas" gestionan las redes informáticas. Su trabajo consiste en permitir que la red funcione sin problemas, supervisar la seguridad y reparar la red cuando surgen complicaciones. Los operadores de sistemas tienen un nivel de acceso completo a los sistemas que administran, lo cual les permite de manera efectiva tener la llave para abrir cualquier cuenta y leer cualquier archivo de los sistemas. Si los investigadores sospechan que una cuenta de red puede contener pruebas relevantes, es posible que busquen la autorización del administrador del sistema para analizar el contenido de dicha cuenta.

Desde el punto de vista práctico, la barrera fundamental para registrar una cuenta de red con arreglo a la autorización de un administrador de sistemas es legal, no constitucional. Los administradores de sistemas suelen funcionar como agentes de los "proveedores de servicios de comunicaciones electrónicas" con arreglo a la Ley de Privacidad de las Comunicaciones Electrónicas ("ECPA"), 18 U.S.C. §§ 2701-2712. La ECPA regula los esfuerzos de las fuerzas de seguridad para obtener la autorización de los administradores de sistemas para inspeccionar la cuenta de una persona. Véase 18 U.S.C. § 2702-2703. De acuerdo con ésta, cualquier pretensión de obtener el consentimiento de un administrador de sistemas para inspeccionar una cuenta debe cumplir con la ECPA. Véase el capítulo 3 en general "La Ley de Privacidad de las Comunicaciones Electrónicas", en adelante.

En la medida en la que la ECPA autorice a los administradores de sistema a permitir los registros, las consiguientes inspecciones autorizadas cumplirán en la mayor parte de los casos con la Cuarta Enmienda. Lo que es más importante, puede ser que las personas no tengan ninguna expectativa razonable de privacidad en los archivos almacenados de forma remota que contienen sus cuentas de red. Véase el capítulo I.B.3 en general, más arriba. Si una persona no tiene una expectativa razonable de privacidad sobre sus archivos almacenados de forma remota, ya no tendrá importancia si el administrador de sistema tiene el control conjunto necesario sobre la cuenta imprescindible para satisfacer la prueba Matlock, ya que en ese caso el registro consiguiente no infringirá la Cuarta Enmienda.

En el caso de que un tribunal concluyera que una persona sí posee una expectativa razonable de privacidad en sus archivos de cuenta almacenados remotamente, entonces el hecho de si la autorización del administrador del sistema satisface la prueba Matlock dependería de las circunstancias. Lo que sí está claro es que el acceso del administrador del sistema a todos los archivos de red no es suficiente en sí mismo para proporcionar la autoridad común que permite dar el consentimiento. En un caso anterior al de Matlock, Stoner v. California, 376 U.S. 483 (1964), el Tribunal Supremo sentenció que un empleado de hotel carecía de la autoridad para permitir el registro de una habitación del hotel. Aunque el empleado tenía permitido entrar en la habitación para llevar a cabo sus obligaciones y a pesar de que el huésped había entregado la llave de su habitación al empleado, el tribunal concluyó que éste no podía permitir el registro. Según el razonamiento del juez Stewart, si la protección de un huésped de hotel ante registros y confiscaciones no razonables "dependiera de la discreción sin restricciones de un empleado del hotel, dicha protección desaparecería". Id. en 490. Véase también Chapman v. Estados Unidos, 365 U.S. 610 (1961) (en el que se concluye que un arrendador carece de la autoridad para permitir el registro de las instalaciones utilizadas por el inquilino); Estados Unidos v. Most, 876 F.2d 191, 199-200 (D.C. Cir. 1989) (en el que se concluye que el empleado de una tienda no tiene autoridad para permitir el registro de unos paquetes que se habían dejado a su cuidado). En la medida en que el acceso de un operador de sistemas a una cuenta de red es similar al acceso de un empleado de hotel a una habitación, el argumento de que el primero puede autorizar el registro de archivos protegidos por la Cuarta Enmienda es débil. Cf. Barth, 26 F. Supp. 2d en 938 (en el que se concluye que el derecho de un técnico en reparaciones para acceder a los archivos con el objetivo limitado de arreglar el ordenador no le confería autoridad para permitir al gobierno examinar los archivos).

Lógicamente, la analogía con el empleado de hotel puede no ser adecuada en determinadas circunstancias. Por ejemplo, generalmente un empleado no tiene la misma relación con el administrador de sistema de la red de su empresa que la que puede tener un cliente de un PSI como AOL con el administrador de sistema del PSI. La empresa puede conceder al administrador de sistema de la red de la compañía plenos derechos para acceder a las cuentas de empleados por motivos relacionados con el trabajo y los empleados pueden saber que el administrador del sistema goza de este acceso. En circunstancias así, el administrador de sistema probablemente tendría suficiente autoridad común sobre las cuentas como para permitir un registro. Véase la nota, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication* (Mantener secretos en el ciberespacio: establecimiento de la protección de la Cuarta Enmienda para las comunicaciones por Internet), 110 Harv. L. Rev. 1591, 1602-03 (1997). Véase también Estados Unidos v. Clarke, 2 F.3d 81, 85 (4° Cir. 1993) (en el que se concluye que un correo de droga contratado para transportar una caja de herramientas del demandado cerrada con llave y que contenía drogas tenía la autoridad común conforme a Matlock para permitir un registro de la caja de herramientas guardada en el maletero del vehículo). Por otra parte, en el caso de una red gubernamental, las normas de la Cuarta Enmienda probablemente

diferirían en gran medida de las normas que se aplican a las redes privadas. Véase en general O'Connor v. Ortega, 480 U.S. 709 (1987) (en el que se describe cómo se aplica la Cuarta Enmienda en los lugares de trabajo del gobierno) (se comenta más abajo).

c) Consentimiento implícito

Es frecuente que las personas lleguen a acuerdos con el gobierno por los que renuncian a algunos de sus derechos de la Cuarta Enmienda. Por ejemplo, los funcionarios de prisiones pueden acceder a que se les registre en busca de drogas como condición para su empleo o los visitantes de los edificios gubernamentales pueden permitir que se les realice un registro limitado de su persona y propiedades para poder entrar. De igual manera, los usuarios de sistemas informáticos pueden renunciar a sus derechos de privacidad como condición para utilizar los sistemas. Por consiguiente, si se registra a un individuo que ha renunciado a sus derechos y posteriormente recurre el registro basándose en la Cuarta Enmienda, los tribunales se centran habitualmente en si la renuncia anuló la expectativa razonable de privacidad de la persona contra el registro. Véase por ejemplo, Sindicato estadounidense de trabajadores de correos, Columbus Area Local AFL-CIO v. Servicio de Correo de Estados Unidos, 871 F.2d 556, 56-61 (6° Cir. 1989) (en el que se concluye que los empleados de correos no tenían expectativa razonable de privacidad alguna sobre las taquillas del gobierno tras firmar la renuncia).

Algunos tribunales han abordado este mismo problema desde un sentido ligeramente distinto y se han cuestionado si la renuncia implicaba la autorización para el registro. Según la doctrina del consentimiento implícito, la autorización para un registro se puede inferir a partir del comportamiento de una persona. Por ejemplo, en Estados Unidos v. Ellis, 547 F.2d 863 (5° Cir. 1977), un civil que visitó una base naval aceptó colocar un pase de visitante en el parabrisas de su coche como condición para poder introducir el vehículo en la base. En el pase se expresaba que la "aceptación de este pase concede su autorización para registrar este vehículo al entrar, durante la visita o al salir de la base". Id. en 865 n.1. En el transcurso de la estancia del visitante, un investigador de la misma que tenía la sospecha de que el visitante tenía marihuana guardada en el coche se acercó al visitante y le preguntó si había leído lo que ponía en el pase. Tras admitir que sí lo había leído, el investigador registró el coche y halló 20 bolsitas de plástico con marihuana. El Quinto Circuito sentenció que estaba autorizado el registro del vehículo sin una orden, ya que el visitante había aceptado de forma implícita el registro al entrar consciente y voluntariamente en la base con pleno conocimiento de las condiciones del pase de visitante. Véase id. en 866-67.

A pesar del caso Ellis, es necesario destacar que varios circuitos se han mostrado críticos con la doctrina del consentimiento implícito en el contexto de la Cuarta Enmienda. A pesar de la interpretación tan amplia del Quinto Circuito, otros tribunales se han mostrado reticentes a aplicar esta doctrina en ausencia de pruebas de que el sospechoso supiera en realidad del registro y lo consintiera voluntariamente en el momento en que se produjo. Véase McGann v. Northeast Illinois Regional Commuter R.R. Corp., 8 F.3d 1174, 1180 (7° Cir. 1993) ("Los tribunales que han tenido que tratar declaraciones de consentimiento implícito han sido renuentes a confirmar un registro sin una orden basado simplemente en acciones tomadas a la luz de un aviso"); Empleados de las fuerzas de seguridad, Consejo de Distrito 82 v. Carey, 737 F.2d 187, 202 n.23 (2° Cir. 1984) (en el que se rechaza el argumento de que los funcionarios de prisiones consintieron de forma implícita el registro al aceptar su empleo en prisión, ya que dicha autorización era una condición para el mismo). En ausencia de pruebas, estos tribunales han optado por analizar las renuncias generales a los derechos de la Cuarta Enmienda únicamente con arreglo a la prueba de expectativa razonable de privacidad. Véase id.

2. Circunstancias apremiantes

En caso de una excepción al requisito de obtención de una orden por "situación apremiante", los agentes pueden realizar registros sin una orden si las circunstancias "a juicio de una persona razonable, hacen necesaria […] la entrada para evitar daños físicos a los oficiales o a otras personas, la destrucción de pruebas importantes, la huida del sospechoso u otras consecuencias que puedan frustrar los esfuerzos legítimos de las fuerzas de seguridad". Véase Estados Unidos v. McConney, 728 F.2d 1195, 1199 (9° Cir. 1984) (en banquillo). A la hora de determinar si se da una situación apremiante, los agentes deben tener en cuenta: (1) el grado de urgencia, (2) el tiempo necesario para obtener una orden, (3) si las

pruebas están a punto de ser eliminadas o destruidas, (4) la posibilidad de riesgos en el lugar, (5) si hay información que puedan indicar a los contrabandistas que la policía les sigue el rastro y (6) la destructibilidad de los objetos de contrabando. Véase Estados Unidos v. Reed, 935 F.2d 641, 642 (4° Cir. 1991).

En los casos relacionados con la informática, una de las circunstancias que hacen que una situación se haga apremiante es que los datos electrónicos no son indestructibles. Mediante un comando se pueden destruir datos en cuestión de segundos, al igual que puede ocurrir con la humedad, la temperatura, una mutilación física o campos magnéticos creados, por ejemplo, al pasar un imán potente por encima de un disco. En Estados Unidos v. David, 756 F. Supp. 1385 (D. Nev. 1991), por ejemplo, los agentes observaron cómo el demandado eliminaba archivos de su libro de notas del ordenador y lo confiscaron inmediatamente. El tribunal de distrito sentenció que no era necesario que los agentes obtuvieran una orden para requisar el libro de notas ya que las acciones del demandado habían creado una situación apremiante. Véase id. en 1392. De igual manera, en Estados Unidos v. Romero-Garcia, 991 F. Supp. 1223, 1225 (D. Or. 1997), afirmado sobre otros motivos 168 F.3d 502 (9° Cir. 1999), un tribunal de distrito concluyó que los agentes habían accedido convenientemente a la información de un busca electrónico que estaba en su posesión porque creyeron razonablemente que era necesario para evitar la destrucción de pruebas. Asimismo, el tribunal destacaba que la información almacenada en un busca se borra fácilmente: los mensajes entrantes pueden borrar la información guardada y las baterías se pueden descargar, haciendo que se borre la información. Por consiguiente, se justificó la actuación de los agentes al acceder al busca sin la obtención previa de una orden. Véase también Estados Unidos v. Gorshkov, 2001 WL 1024026, en *4 (W.D. Wash. 23 de mayo de 2001) (en el que se concluye que las circunstancias justificaban la descarga sin una orden de los datos de un ordenador en Rusia dado que era probable que dicho ordenador contuviera pruebas delictivas, ya que había buenas razones para temer que un retraso podría derivar en la destrucción o pérdida de acceso a las pruebas y porque el agente simplemente copió los datos y posteriormente obtuvo la orden de registro); Estados Unidos v. Ortiz, 84 F.3d 977, 984 (7° Cir. 1996) (al llevar a cabo un registro para proceder a una detención, se justificó el hecho de que los agentes recuperaran números de un busca porque la información de estos dispositivos se puede eliminar muy fácilmente).

Como es natural, en los casos relacionados con los ordenadores, al igual que en todos los demás, la existencia de circunstancias apremiantes está absolutamente ligada a los hechos. Compárese Romero-Garcia, 911 F. Supp. en 1225 con David, 756 F. Supp en 1392 n.2 (en el que se desestima como "insuficiente" el argumento del gobierno de que las circunstancias apremiantes justificaron el registro de un ordenador que funcionaba con batería porque el agente no sabía cuánto tiempo duraría ésta) y Estados Unidos v. Reyes, 922 F. Supp. 818, 835-36 (S.D.N.Y. 1996) (en el que se concluye que no hay ninguna circunstancia apremiante que justifique el registro de un busca porque el agente del gobierno creó de forma ilegítima la exigencia al encender el aparato).

Es decir, lo importante es que la existencia de una situación apremiante no permite a los agentes registrar o confiscar más allá de lo estrictamente necesario para evitar la destrucción de pruebas. El derecho a realizar registros sin orden termina en el mismo momento en el que desaparece la exigencia: la necesidad de adoptar determinadas medidas para evitar la destrucción de pruebas no autoriza a los agentes a tomar otras sin una orden. Véase Estados Unidos v. Doe, 61 F.3d 107, 110-11 (1° Cir. 1995). Consiguientemente, la confiscación de equipos informáticos para evitar la eliminación de la información que contenga normalmente no será pretexto para proceder a un registro posterior de la información sin una orden. Véase David, 756 F. Supp. en 1392.

3. Doctrina del "plain view" (a simple vista)

Las pruebas de un delito se pueden requisar sin una orden con arreglo a la excepción de "plain view" (a simple vista) al requisito de la orden. Para acogerse a esta excepción, el agente debe estar en una situación legal para observar y acceder a las pruebas y su carácter incriminatorio debe ser aparente de forma inmediata. Véase Horton v. California, 496 U.S. 128 (1990). Por ejemplo, si un agente realiza un registro válido de un disco duro y halla pruebas de un delito no relacionado mientras lo lleva a cabo, el agente puede requisar las pruebas con arreglo a la doctrina de la simple vista.

La doctrina de "plain view" (a simple vista) no autoriza a los agentes a abrir y ver el contenido de un archivo informático para cuya apertura e inspección no esté autorizado de otra manera.

Es importante destacar que la excepción de simple vista no puede justificar la violación de la expectativa razonable de privacidad de una persona. La excepción únicamente permite la confiscación de pruebas que un agente ya está autorizado a ver de acuerdo con la Cuarta Enmienda. En los casos relacionados con ordenadores, esto implica que el gobierno no puede apelar a la excepción de simple vista para justificar la apertura de un archivo informático cerrado que de otra forma no estaría autorizado a examinar.[(4)] El contenido de un archivo que se tenga que abrir para verlo no está a "simple vista". Véase Estados Unidos v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996). Esta norma concuerda con las decisiones para aplicar la excepción de simple vista a contenedores cerrados. Véase por ejemplo Estados Unidos v. Villarreal, 963 F.2d 770, 776 (5° Cir. 1992) (en el que se concluye que las etiquetas colocadas en unos tambores opacos de 55 galones no permiten ver el contenido de los mismos a simple vista) ("[Una] etiqueta colocada en un contenedor no constituye una invitación para registrarlo. Si el gobierno desea saber más de lo que revela la etiqueta abriendo el contenedor, por lo general deberá obtener una orden de registro").

Como ya se ha comentado anteriormente (véase el capítulo) I.B.2., los tribunales han llegado a conclusiones diferentes acerca de si cada archivo almacenado en un ordenador se debe considerar un contenedor individual y esta distinción tiene importantes repercusiones sobre el alcance de la excepción de simple vista. Estados Unidos v. Carey, 172 F.3d 1268, 1273 (10° Cir. 1999) supone un buen ejemplo del enfoque restrictivo. En el caso Carey, un detective de la policía que registraba un disco duro con una orden para buscar pruebas de tráfico de drogas abrió un archivo "jpg" y en lugar de este tipo de pruebas, halló pornografía infantil. Llegado a este punto, el detective pasó cinco horas accediendo y descargando varios cientos de archivos "jpg" en un registro cuya finalidad no era la de encontrar pruebas del tráfico de narcóticos para la que se le había autorizado a registrar e inspeccionar de acuerdo con la orden original, sino la de dar con más pornografía infantil. Cuando el demandado intentó excluir los archivos de pornografía infantil basándose en que se habían confiscado fuera del alcance de la orden, el gobierno adujo que el detective había obrado apropiadamente al confiscar los archivos "jpg" porque el contenido de los archivos de contrabando estaba a simple vista. El Décimo Circuito rechazó este argumento con respecto a todos los archivos salvo para la primera imagen "jpg" que recuperó el detective. Véase id. en 1273, 1273 n.4. Según se puede interpretar, la norma en el caso Carey parece ser que el detective podía confiscar la primera imagen "jpg" que se puso a simple vista mientras estaba realizando el registro con una orden, pero no podía acogerse a la excepción de simple vista para justificar el registro únicamente con el objetivo de buscar más archivos "jpg" con pornografía infantil en los ordenadores del demandado, ya que estas pruebas escapaban al alcance de la orden. Cf. Estados Unidos v. Walser, 275 F.3d 981, 986-87 (10° Cir. 2001) (en el que se concluye que no hay ninguna infracción de la Cuarta Enmienda porque un oficial con una orden para registrar en busca de registros electrónicos de transacciones de drogas abrió un único archivo informático que contenía pornografía infantil, suspendió la búsqueda y acudió al magistrado para solicitar una segunda orden para realizar otro registro en busca de pornografía infantil).

Al contrario del enfoque del Décimo Circuito en el caso Carey, la doctrina expuesta por el Quinto Circuito en Estados Unidos v. Runyan, 275 F.3d 449, 464-65 (5° Cir. 2001), y Estados Unidos v. Slanina, 283 F.3d 670, 680 (5°Cir. 2002) sugiere que la simple vista de un único archivo en un ordenador o dispositivo de almacenamiento podría servir de fundamento para realizar un registro más minucioso. En estos dos casos, el tribunal defendió que si el registro parcial de un ordenador o dispositivo de almacenamiento sin una orden se ha realizado de manera adecuada, el demandado ya no alberga expectativa razonable de privacidad alguna sobre el contenido restante de dichos equipos. Véase Slanina, 283 F.3d en 680; Runyan, 275 F.3d en 464-65. Por tanto, un registro más exhaustivo del ordenador o dispositivo de almacenamiento por parte de las fuerzas de seguridad no contraviene la Cuarta Enmienda. Este razonamiento también se puede aplicar si un archivo se ha puesto a simple vista.

4. Registro por una detención legítima

Si se produce una detención legítima, los agentes pueden llevar a cabo un "registro completo" de la persona arrestada y un registro más limitado de la zona circundante sin necesidad de una orden. Véase

Estados Unidos v. Robinson, 414 U.S. 218, 235 (1973); Chimel v. California, 395 U.S. 752, 762-63 (1969). Por ejemplo, en el caso Robinson, un oficial de policía que realizaba un cacheo a una persona arrestada por un delito de tráfico descubrió un paquete de cigarrillos arrugado en el bolsillo izquierdo del pecho del sospechoso. El oficial, que no sabía lo que contenía el paquete, lo abrió y descubrió catorce cápsulas de heroína. El Tribunal Supremo sentenció que el registro del paquete era permisible, aunque el oficial no tenía ninguna razón expresable para abrir el paquete. Véase id. en 234-35. En opinión del tribunal, la necesidad general de conservar las pruebas y evitar daños al oficial que lleva a cabo la detención hace que sea razonable en sí que el agente realice un "registro completo de la persona" con arreglo a una detención legítima. Id. en 235.

Dado el uso cada vez más extendido de ordenadores manuales y portátiles y de otros dispositivos electrónicos de almacenamiento, es frecuente que los agentes encuentren ordenadores al realizar registros tras una detención legítima. Al ser detenidos, los sospechosos pueden llevar consigo buscas, teléfonos móviles, asistentes digitales personales (como Palm Pilots) o incluso ordenadores portátiles. ¿La excepción del registro tras un arresto permite a un agente acceder a la memoria de un dispositivo electrónico de almacenamiento que lleve consigo el detenido durante un registro realizado sin una orden tras la detención? En el caso de buscas electrónicos, la respuesta es claramente afirmativa. Los tribunales, apelando al caso Robinson, han permitido de manera uniforme a los agentes acceder a los buscas electrónicos que lleven las personas detenidas en el momento de su arresto. Véase Estados Unidos v. Reyes, 922 F. Supp. 818, 833 (S.D.N.Y. 1996) (en el que se concluye que acceder a los números de un busca hallado en un bolso adosado a la silla de ruedas del demandado en el plazo de veinte minutos tras su detención entra dentro de la excepción del registro posterior al arresto); Estados Unidos v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993); Estados Unidos v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995); Yu v. Estados Unidos, 1997 WL 423070, en *2 (S.D.N.Y. 29 de julio de 1997); Estados Unidos v. Thomas, 114 F.3d 403, 404 n.2 (3° Cir. 1997) (sentencias). Véase también Estados Unidos v. Ortiz, 84 F.3d 977, 984 (7° Cir. 1996) (idéntica conclusión, pero basada en una teoría de exigencia).

Los tribunales aun no han abordado la cuestión de si el caso Robinson permitirá el registro sin orden de dispositivos electrónicos de almacenamiento que contengan más información que los buscas. En el ámbito del papel impreso, los casos han permitido ciertamente registros exhaustivos del material escrito descubierto tras detenciones legítimas. Por ejemplo, los tribunales han concluido de forma uniforme que los agentes pueden examinar completamente el contenido de la cartera de un sospechoso si la lleva encima. Véase por ejemplo Estados Unidos v. Castro, 596 F.2d 674, 676 (5° Cir. 1979); Estados Unidos v. Molinaro, 877 F.2d 1341, 1347 (7° Cir. 1989) (se citan casos). De igual forma, un tribunal concluyó que los agentes podían fotocopiar el contenido íntegro de una libreta de direcciones que el demandado lleva encima en el momento de su detención, véase Estados Unidos v. Rodriguez, 995 F.2d 776, 778 (7° Cir. 1993), mientras que otros han permitido el registro del maletín de un demandado que tenía a un lado cuando se le arrestó. Véase por ejemplo Estados Unidos v. Johnson, 846 F.2d 279, 283-84 (5° Cir. 1988); Estados Unidos v. Lam Muk Chiu, 522 F.2d 330, 332 (2° Cir. 1975). Si los agentes pueden analizar el contenido de carteras, libretas de direcciones y maletines, se podría argumentar que deberían tener la potestad de registrar también sus homólogos electrónicos, como organizadores electrónicos, disquetes y Palm Pilots. Cf. United v. Tank, 200 F.3d 627, 632 (9° Cir. 2000) (en el que se concluye que los agentes que realizaban el registro de un coche tras una detención legítima confiscaron correctamente un disco Zip que encontraron en el mismo, pero no se comenta si los agentes obtuvieron una orden antes de registrar el disco en busca de imágenes de pornografía infantil).

El límite para este argumento es que todo registro relacionado con una detención debe ser razonable. Véase Swain v. Spinney, 117 F.3d 1, 6 (1° Cir. 1997). Mientras que el registro en busca de artículos físicos en la persona del arrestado puede ser siempre razonable, una búsqueda más invasiva en situaciones diferentes pueden infringir la Cuarta Enmienda. Véase por ejemplo Mary Beth G. v. Ciudad de Chicago, 723 F.2d 1263, 1269-71 (7° Cir. 1983) (en el que se concluye que el caso Robinson no permite el registro al desnudo tras una detención ya que esto no es razonable en el contexto). Por ejemplo, la capacidad cada vez mayor de almacenamiento de los ordenadores manuales sugiere que la norma establecida de Robinson no es siempre aplicable en el caso de registros electrónicos. En caso de duda, los agentes deben considerar si es necesario obtener una orden de registro antes de examinar el

contenido de dispositivos electrónicos de almacenamiento que puedan contener gran cantidad de información. *5.* Registros de inventario

Los oficiales de las fuerzas de seguridad hacen inventarios habitualmente de los artículos confiscados. Estos "registros de inventario" son razonables, y por tanto entran dentro de la excepción al requisito de la orden, si se cumplen dos condiciones. En primer lugar, el registro debe obedecer a una finalidad legítima y no relacionada con ninguna investigación (por ejemplo, para proteger la propiedad de una persona mientras permanezca en custodia, para asegurarse frente a demandas de pérdida, robo o vandalismo sobre la propiedad o para proteger a la policía de posibles riesgos) que tenga más peso que la intrusión sobre los derechos que la Cuarta Enmienda otorga a la persona. Véase Illinois v. Lafayette, 462 U.S. 640, 644 (1983); South Dakota v. Opperman, 428 U.S. 364, 369-70 (1976). En segundo lugar, el registro debe seguir un procedimiento normalizado. Véase Colorado v. Bertine, 479 U.S. 367, 374 n.6 (1987); Florida v. Wells, 495 U.S. 1, 4-5 (1990).

Es poco probable que la excepción del registro de inventario al requisito de la orden respaldara un registro de archivos informáticos confiscados. Véase Estados Unidos v. O'Razvi, 1998 WL 405048, en *6-7 (S.D.N.Y. 17 de julio de 1998) (en el que se destacan las dificultades para aplicar los requisitos del registro de inventario a los discos de ordenador); véase también Estados Unidos v. Flores, 122 F. Supp. 2d 491, 493-95 (S.D.N.Y. 2000) (en el que se cataloga el registro de un teléfono móvil como "meramente de investigación", con lo que no se considera un registro de inventario legítimo). Aun asumiendo que los procedimientos estándar autorizaran un registro así, los propósitos legítimos de los registros de inventario en el mundo físico no se adaptan bien al ámbito de lo intangible. Por lo general no es necesario revisar la información para protegerla y tampoco supone un riesgo ni peligro físico. Si bien es cierto que una persona podría asegurar que sus archivos informáticos han sido modificados o eliminados mientras han estado bajo custodia de la policía, no es menos cierto que inspeccionar su contenido no ofrecería protección alguna contra la manipulación. Por lo tanto, generalmente es necesario que los agentes obtengan una orden de registro para examinar archivos informáticos confiscados que estén bajo su custodia.

6. Registros fronterizos

En aras de proteger la capacidad gubernamental para vigilar el contrabando y otras propiedades que puedan entrar o salir de Estados Unidos de forma ilegal, el Tribunal Supremo ha reconocido una excepción especial al requisito de la orden para aquellos registros que se lleven a cabo en las fronteras de Estados Unidos. Según el tribunal, los "registros habituales" en la frontera o su equivalente funcional no requieren una orden, causa probable o incluso una sospecha razonable de que el registro permita descubrir contrabando o pruebas. Estados Unidos v. Montoya De Hernandez, 473 U.S. 531, 538 (1985). Sin embargo, los registros que sean especialmente minuciosos exigen que haya al menos una sospecha razonable. Véase id. en 541. Estas normas se aplican a personas y propiedades que entren o salgan de Estados Unidos. Véase Estados Unidos v. Oriakhi, 57 F.3d 1290, 1297 (4° Cir. 1995).

En al menos un caso los tribunales han abordado la cuestión de si la excepción del registro fronterizo permite una inspección sin orden de un disco de ordenador en busca de archivos informáticos sobre contrabando. En Estados Unidos v. Roberts, 86 F. Supp. 2d 678 (S.D. Tex. 2000), afirmado sobre otros motivos, 274 F.3d 1007 (5° Cir. 2001), los agentes de aduanas de Estados Unidos averiguaron que William Roberts, sospechoso del que se creía que llevaba imágenes informatizadas de pornografía infantil, tenía programado un vuelo de Houston, Texas a París, Francia en una fecha concreta. El día del vuelo, los agentes establecieron una zona de inspección en el puente de acceso del aeropuerto de Houston con el único propósito de registrar a Roberts. Roberts llegó a la zona de inspección y los agentes le comunicaron que estaban buscando "divisas" y "alta tecnología u otros datos" que no se pudieran exportar de forma legal. Id. en 681. Una vez que los agentes registraron las propiedades de Roberts y encontraron un ordenador portátil y seis discos Zip, Roberts aceptó firmar un impreso de autorización para permitir a los agentes inspeccionar su propiedad. El registro posterior reveló varios miles de imágenes de pornografía infantil. Véase id. en 682.

El tribunal de distrito rechazó la petición del demandado de desestimar los archivos informáticos, alegando que el registro del equipaje de Roberts haba sido "rutinario", para lo cual no se requería

ninguna sospecha, a pesar de que la justificación que ofrecieron los agentes para el registro no había sido más que un pretexto. Véase id. en 686, 688 (se cita Whren v. Estados Unidos, 517 U.S. 806 (1996)). El tribunal concluyó también que la autorización de Roberts justificaba el análisis del portátil y los discos e indicó que incluso en el caso de que no hubiera permitido el registro, "la exploración del ordenador y los discos habría tenido un carácter habitual sobre la exportación, válido con arreglo a la Cuarta Enmienda". Véase Roberts, 98 F. Supp. 2d en 688. Durante la apelación, el Quinto Circuito corroboró el rechazo del tribunal de distrito a desestimar las pruebas a causa de que el registro inicial en el puente de acceso que se le realizó a Roberts estaba justificado por la sospecha razonable de que éste poseía pornografía infantil y que la inspección y confiscación posterior del equipo informático estaban justificadas por causa probable. Véase id. en 1017. El tribunal no abordó el asunto de si la confiscación del equipo informático de Roberts se podía considerar rutinaria.

Cabe destacar que los agentes y fiscales no deben interpretar que Roberts permitió la interceptación de los datos transmitidos electrónicamente desde y hasta Estados Unidos. Toda interceptación en tiempo real de datos transmitidos electrónicamente en Estados Unidos debe observar estrictamente los requisitos del Título III 18 U.S.C. §§ 2510-2522, o la ley de registro y de control de llamadas, 18 U.S.C. §§ 3121-3127. Véase el capítulo 4. Asimismo, una vez que los datos transmitidos electrónicamente desde fuera de Estados Unidos llegan a su destino dentro del país, el gobierno no puede generalmente acogerse a la excepción del registro fronterizo para registrar y confiscar los datos ya que éstos no se encuentran en la frontera o en su equivalente funcional. Cf. Almeida-Sanchez v. Estados Unidos, 413 U.S. 266, 273-74 (1973) (en el que se concluye que un registro realizado a 25 millas de la frontera de Estados Unidos no puede considerarse susceptible de acogerse a la excepción del registro fronterizo, aun siendo el caso de que se produjo en una autopista conocida por ser la ruta común de inmigrantes ilegales, ya que no se produjo en la frontera o equivalente funcional).

7. Asuntos internacionales

Cada vez con más frecuencia las pruebas electrónicas necesarias para evitar, investigar o perseguir un delito pueden estar situadas fuera de las fronteras estadounidenses. Esto puede ocurrir por varias razones. Los delincuentes pueden utilizar Internet para perpetrar o facilitar sus actos delictivos de forma remota, como cuando un hacker ruso roba dinero de un banco de Nueva York o si la persona que ha secuestrado a un ciudadano estadounidense envía por correo electrónico sus exigencias para poner en libertad al secuestrado. Las comunicaciones también se pueden "lavar" por medio de terceros países, como puede ocurrir si un delincuente situado en Brooklyn utiliza Internet para transmitir una comunicación a través de Tokio, Tel Aviv y Johannesburgo antes de llegar a su destinatario en Manhattan, un modo muy similar a como se blanquean capitales mediante bancos de distintos países para ocultar su procedencia. Por otra parte, el proveedor de la arquitectura puede enviar o almacenar las comunicaciones en el país en el que está domiciliado, independientemente de la ubicación de sus usuarios.

Si las autoridades de Estados Unidos que están investigando un delito creen que puede haber pruebas electrónicas almacenadas por un proveedor de servicios de Internet o en un ordenador situado en el extranjero (en el "País A"), por lo general las fuerzas de seguridad de Estados Unidos deberán solicitar la asistencia de las fuerzas de seguridad del País A. Dado que normalmente los oficiales de las fuerzas de seguridad ejercen sus funciones en el territorio de otro país con el consentimiento de dicho país, el personal de Estados Unidos solamente tiene que contactar directamente con un PSI localizado en el País A con (1) la autorización previa del gobierno extranjero; (2) la aprobación de la Oficina de Asuntos Internacionales ("OAI") del Departamento de Justicia (el cual conocerá cuáles pueden ser los ámbitos especialmente delicados y/o las prácticas aceptadas); o (3) otros indicios claros de que dicha práctica no sea censurable en el País A. (Existe el consenso general de que el acceso a materiales que están a disposición del público en general en el País A, como los que se ofrecen en una página web pública, y el acceso a los materiales en el País A con la autorización de el propietario o persona al cargo de los mismos es permisible sin necesidad de realizar consultas previas).

En determinadas circunstancias, las autoridades extranjeras responsables de las fuerzas de seguridad pueden poner en común pruebas de manera informal con sus homólogos estadounidenses. Sin embargo, dar con el oficial adecuado en el País A con el que explorar esta forma de cooperación es, como

mínimo, una ciencia inexacta. Entre las posibles vías para entablar contacto con las fuerzas de seguridad de otro país se incluyen: (1) el experto designado que participa en la red del G8 de puntos de contacto internacionales sobre delitos relacionados con la alta tecnología (se comenta más abajo); (2) contactos de las fuerzas de seguridad mantenidos por la OAI; (3) representantes de los órganos de las fuerzas de seguridad de Estados Unidos emplazados en la embajada Americana correspondiente (como por ejemplo agregados legales del FBI y agentes del Servicio Secreto y del Servicio de Aduanas de Estados Unidos) y (4) el Funcionario de Seguridad Regional (del Servicio de Seguridad Diplomático) de la embajada estadounidense (que puede tener buenos contactos dentro las fuerzas de seguridad en el país). El teléfono de contacto de la OAI es el 202-514-0000.

En los casos en los que el País A no pueda ofrecer asistencia informal, las solicitudes de pruebas se realizarán normalmente con arreglo a los Tratados de Asistencia Legal Mutua (MLAT, por sus siglas en inglés) o a los Acuerdos de Asistencia legal Mutua existentes o bien a través del proceso de comisión rogatoria. Véase 28 U.S.C. § 1781-1782. Estas solicitudes oficiales de asistencia se realizan desde la OAI a la "Autoridad Central" designada del País A o, en ausencia de un MLAT, a las autoridades correspondientes. (Las Autoridades Centrales normalmente se encuentran integradas en el Ministerio de Justicia o en otro ministerio u oficina del País A que tenga autoridad sobre las fuerzas de seguridad). La OAI tiene abogados que se ocupan de todos los países y regiones del mundo. Teniendo en cuenta que las solicitudes oficiales de este tipo requieren documentos y procedimientos específicos y pueden tardar un tiempo en arrojar resultados, las fuerzas de seguridad deben ponerse en contacto con la OAI en cuanto la solicitud de asistencia legal internacional se convierta en una posibilidad.

Si las fuerzas de seguridad de Estados Unidos tienen motivos para creer que existen pruebas electrónicas en un ordenador o red informática extranjeros y prevé un periodo de demora antes de que se puedan obtener dichas pruebas en el País A, es necesario presentar lo antes posible una solicitud a las fuerzas de seguridad del otro país para la conservación de las pruebas. Dicha solicitud, similar a la expresada con arreglo a 18 U.S.C. § 2703(f) a un proveedor estadounidense (véase capítulo 3.G.1, pág. 101), será más o menos satisfactoria dependiendo de varios factores, siendo el más importante de ellos si el País A cuenta con una ley de conservación de datos o no y si Estados Unidos tiene los suficientes contactos con las fuerzas de seguridad del País A como para garantizar una rápida ejecución de la solicitud. El Convenio sobre Ciberdelincuencia del Consejo de Europa, firmado en 2001, obliga a todas las partes contratantes a tener la capacidad para atender las solicitudes de conservación transfronterizas y la disponibilidad de esta forma esencial de asistencia, por lo que se espera que aumente en gran medida en un futuro próximo.

Para garantizar la conservación, o en emergencias en las que se necesita asistencia internacional inmediata, la red internacional de puntos de contacto de 24 horas creada por el Subgrupo de países del G8 para la delincuencia de alta tecnología puede proporcionar su asistencia. Esta red, creada en 1997, está compuesta de aproximadamente veintisiete países miembros y sigue creciendo todos los años.[(5)] Los países participantes cuentan con un experto dedicado a la delincuencia cibernética y con un medio para ponerse en contacto con dicho organismo o persona veinticuatro horas al día. Véase Michael A. Sussmann, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium* (Los desafíos más importantes de la delincuencia internacional relacionada con la alta tecnología y la informática en el milenio), 9 Duke J. Comp. & Int'l L. 451, 484 (1999). La CCIPS es el punto de contacto para Estados Unidos y se puede contactar con este organismo a través del número de teléfono 202-514-1026 en horas normales de oficina o fuera de este horario por medio del Centro de Control del Departamento de Justicia en el número de teléfono 202-514-5000. El Convenio sobre Ciberdelincuencia del Consejo de Europa obliga a todos los países contratantes a tener un punto de contacto las 24 horas del día para casos de delitos informáticos, por lo que se espera que aumente la capacidad para responder internacionalmente en menos de 24 horas. Asimismo, la CCIPS cuenta con contactos de las fuerzas de seguridad de alta tecnología en numerosos países que no forman parte de la red del G8 ni del Consejo de Europa; los agentes y fiscales deben solicitar asistencia a la CCIPS.

En el caso de que las fuerzas de seguridad de Estados Unidos accedan de forma involuntaria a un ordenador situado en otro país, es necesario consultar inmediatamente a la CCIPS, OAI o a la autoridad competente que corresponda, ya que es posible que se vean implicados asuntos como la soberanía y el respeto mutuo. De la misma manera, si una situación de urgencia como puede ser una amenaza

terrorista hace que aumente la posibilidad de que las fuerzas de seguridad de Estados Unidos accedan directamente a un ordenador situado en el extranjero, se debe consultar a las autoridades estadounidenses competentes de manera inmediata.

El registro, la confiscación u otras formas de obtener pruebas electrónicas situadas fuera de Estados Unidos pueden conllevar cuestiones complejas tanto en relación con el Derecho como con la política. Por ejemplo, la Cuarta Enmienda es aplicable en determinadas circunstancias, pero no en otras. Véase Estados Unidos v. Verdugo-Urquidez, 494 U.S. 259 (1990) (en la que se considera hasta qué punto se aplica la Cuarta Enmienda en registros fuera de Estados Unidos). El presente manual no pretende ofrecer una orientación detallada sobre cómo resolver los difíciles problemas internacionales que pueden surgir en los casos relacionados con pruebas electrónicas situadas fuera de nuestras fronteras. Los investigadores y fiscales deben solicitar asistencia a la CCIPS u OAI en casos concretos.

[índice]

D. Un caso especial: registro de los lugares de trabajo

Con frecuencia se producen registros sin orden en lugares de trabajo en casos relacionados con la informática, registros que conllevan problemas jurídicos inusualmente complicados. El punto de partida para este análisis es la compleja decisión del Tribunal Supremo en O'Connor v. Ortega, 480 U.S. 709 (1987). Con arreglo a O'Connor, la legalidad de un registro sin orden realizado en un lugar de trabajo depende a menudo de distinciones objetivas muy sutiles, como por ejemplo el hecho de si el lugar de trabajo corresponde a un sector público o privado, si existen políticas de empleo que autoricen el registro y si éste está relacionado con el trabajo.

Cualquier registro de este tipo se debe evaluar minuciosamente basándose en los hechos. Por lo general, no obstante, los oficiales de las fuerzas de seguridad pueden llevar a cabo un registro sin orden de lugares de trabajo privados, es decir, no gubernamentales, únicamente en el caso de obtener bien la autorización del empresario o bien de otro empleado con autoridad común sobre la zona que se vaya a examinar. En los lugares públicos de trabajo (gubernamentales), los oficiales no se pueden acoger a la autorización del empleador, aunque sí pueden realizar registros si existen políticas de empleo o prácticas de oficina por escrito que expresen que los empleados del gobierno que sean objeto de la inspección no pueden esperar una expectativa razonable de privacidad en su puesto de trabajo. Por otra parte, los empleadores y supervisores del gobierno pueden llevar a cabo inspecciones razonables relacionadas con el trabajo en los puestos de un empleado sin necesidad de una orden, incluso si éstas contravienen la expectativa razonable de privacidad del empleado.

En este punto se recomienda cautela. En esta parte se evalúa la legalidad de un registro sin orden de ordenadores en el lugar de trabajo con arreglo a la Cuarta Enmienda. En muchos casos, sin embargo, estos registros afectan a las leyes federales de privacidad además de la Cuarta Enmienda. Por ejemplo, los esfuerzos para obtener los archivos y correos electrónicos del servidor de red de un empleador plantean problemas relacionados con la Ley de Privacidad de las Comunicaciones Electrónicas, 18 U.S.C. §§ 2701-2712 (se comenta en el capítulo 3), mientras que la vigilancia del uso que hace un empleado de Internet en el puesto de trabajo afecta al Título III, 18 U.S.C. §§ 2510-2522 (se comenta en el capítulo 4). Antes de realizar una inspección en el lugar de trabajo, los investigadores deben asegurarse de que ello no infringirá ni la Cuarta Enmienda ni las leyes federales de privacidad relevantes. Los investigadores se deben poner en contacto con la CCIPS en el número de teléfono (202) 514-1026 o con el CTC de su distrito (véase la introducción, p. ix) para solicitar asistencia.

1. Registros en lugares de trabajo del sector privado

Las normas para realizar registros y confiscaciones sin una orden en lugares de trabajo del sector privado suelen ser similares a las normas para este tipo de inspecciones en viviendas y otras residencias personales. Los empleados de compañías privadas normalmente mantienen una expectativa razonable de privacidad en sus puestos de trabajo. Como consecuencia de ello, para que las fuerzas de seguridad

puedan registrar un lugar de trabajo privado necesitarán una orden, a menos que los agentes obtengan la autorización del empresario o de un compañero de trabajo que tenga autoridad común.

a) Expectativa razonable de privacidad en lugares de trabajo del sector privado

Por lo general, los empleados del sector privado mantienen una expectativa razonable de privacidad sobre su área dentro de la oficina. En Mancusi v. DeForte, 392 U.S. 364 (1968), unos oficiales de policía llevaron a cabo una inspección sin una orden de una oficina en la sede de un sindicato local que el demandado Frank DeForte compartía con otros oficiales del sindicato. Al argumento de DeForte de que este registro contravenía los derechos que le otorga la Cuarta Enmienda los oficiales de la policía respondieron que el uso conjunto del espacio con los compañeros de trabajo de DeForte hacía que su expectativa razonable de privacidad no estuviera fundada. El tribunal no estuvo de acuerdo con esta afirmación, asegurando que DeForte "aún podía haber confiado razonablemente en que solamente entrarían en su despacho [sus compañeros de oficina] y sus invitados personales o de trabajo y que, por tanto, no se verían modificados los archivos a menos que fuera con su autorización o la de sus superiores dentro del sindicato". Id. en 369. Dado que sólo un grupo concreto de personas gozaban realmente del acceso y el uso conjunto del despacho de DeForte, la presencia de los oficiales infringió la expectativa razonable de privacidad de éste. Véase id. Véase también Estados Unidos v. Most, 876 F.2d 191, 198 (D.C. Cir. 1989) ("No es necesario que una persona se aísle del mundo para conservar los derechos que le otorga la Cuarta Enmienda. Puede invitar a sus amigos a su casa pero excluir a la policía; puede compartir su despacho con sus compañeros sin por ello autorizar un registro oficial. Estados Unidos v. Lyons, 706 F.2d 321, 325 (D.C. Cir. 1983) ("Una persona puede admitir libremente a invitados de su propia elección, o verse obligado legalmente a admitir a personas específicas, sin sacrificar su derecho a confiar en que el espacio se mantenga seguro frente a todos los demás"). Por lo tanto, desde el punto de vista práctico, los empleados de una empresa privada normalmente conservarán una expectativa razonable de privacidad en su puesto de trabajo a menos que ese espacio esté "abierto para todo el mundo". Id. en 326.

b) Autorización en lugares de trabajo del sector privado

Si bien es cierto que la mayoría de los lugares de trabajo no gubernamentales respaldarían una expectativa razonable de privacidad ante un registro de las fuerzas de seguridad, los agentes pueden anular esta expectativa si obtienen la autorización de una tercera parte que ejerza una autoridad común sobre el área que se vaya a inspeccionar. Véase Matlock, 415 U.S. en 171. En la práctica, esto implica que con frecuencia los agentes pueden superar el requisito de la orden consiguiendo el consentimiento del empleador o de un supervisor de la persona en cuestión. Dependiendo de la situación, puede ser suficiente incluso con el consentimiento de un compañero de trabajo.

Los empleados y supervisores del sector privado normalmente gozan de una autoridad mayor a la hora de permitir registros en el lugar de trabajo. Por ejemplo, en Estados Unidos v. Gargiso, 456 F.2d 584 (2° Cir. 1972), un caso anterior al de Matlock, unos agentes que estaban realizando una investigación criminal de un empleado de una compañía privada solicitaron el acceso a una zona restringida y desconectada del sótano de la empresa. Explicaron sus necesidades al vicepresidente de la compañía, quien acompañó en persona a los agentes hasta el sótano y abrió la puerta con su llave. Posteriormente el empleado intentó invalidar las pruebas que los agentes descubrieron allí, pero el tribunal sentenció que la autorización del vicepresidente era efectiva. Según su razonamiento, dado que el vicepresidente compartía el poder de supervisión sobre esta zona con el empleado, tenía potestad para permitir el registro de la misma por parte de los agentes. Véase id. en 586-87. Véase también Estados Unidos v. Bilanzich, 771 F.2d 292, 296-97 (7° Cir. 1985) (en el que se concluye que el propietario de un hotel podía autorizar la inspección de una habitación cerrada que utilizaba un empleado para guardar archivos, a pesar de que el primero no tenía la llave, ya que el empleado trabajaba a su servicio); J.L. Foti Constr. Co. v. Donovan, 786 F.2d 714, 716-17 (6° Cir. 1986) (per curiam) (en el que se concluye que el encargado de un contratista general podía autorizar la inspección de todas las obras, incluyendo la zona de trabajo del subcontratista). En un caso similar, una política de empleados o un banner en una red informática mediante los que se exprese el derecho del empleador a autorizar un registro del lugar de trabajo puede contribuir a fijar la autoridad común del empleador para dar su consentimiento con arreglo al caso Matlock. Véase el Apéndice A.

Los agentes deben mostrarse cautos a la hora de acogerse a la autorización de un compañero de trabajo para realizar una inspección en el lugar de trabajo. Un superior normalmente conserva el derecho de acceder al puesto de sus empleados, mientras que una persona de rango similar puede o puede que no, dependiendo de la situación. No obstante, si un compañero sí ejerce la autoridad común sobre un lugar de trabajo, los investigadores pueden fiarse por completo de su autorización para examinar dicho lugar. Por ejemplo, en Estados Unidos v. Buettner-Janusch, 646 F.2d 759 (2° Cir. 1981), un profesor y un asistente universitario de investigación permitieron el registro de un laboratorio de la NYU, el cual estaba gestionado por un segundo profesor del que se sospechaba que lo utilizaba para producir LSD y otras drogas. Aunque el registro implicó la apertura de viales y diversos contenedores cerrados, el Segundo Circuito convino que el caso Matlock permitía la inspección puesto que los dos compañeros de trabajo que la habían consentido tenían autorización para utilizar plenamente el laboratorio para sus investigaciones. Véase id. en 765-66. Véase también Estados Unidos v. Jenkins, 46 F.3d 447, 455-58 (5° Cir. 1995) (en el que se permite que un empleado autorice un registro de la propiedad de su empleador); Estados Unidos v. Murphy, 506 F.2d 529, 530 (9° Cir. 1974) (per curiam) (igual); Estados Unidos v. Longo, 70 F. Supp. 2d 225, 256 (W.D.N.Y. 1999) (en el que se permite a una secretaria autorizar una inspección del ordenador de su empleador). Por el contrario, véase Estados Unidos v. Buitrago Pelaez, 961 F. Supp. 64, 67-68 (S.D.N.Y. 1997) (en el que se concluye que un recepcionista podía autorizar la exploración general del despacho, pero no así de una caja fuerte cerrada cuya combinación desconocía).

c) Registros del empleador en lugares de trabajo del sector privado

No es habitual que un registro sin orden del lugar de trabajo por parte de empleadores privados infrinja la Cuarta Enmienda. Siempre y cuando el empleador no actúe como instrumento o agente del gobierno en el momento de llevarlo a cabo, el registro se considera privado, por lo que no es aplicable la Cuarta Enmienda. Véase Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614 (1989).

2. Registros en lugares de trabajo del sector público

Aunque la inspección de un ordenador sin una orden en lugares de trabajo del sector privado sigue unas normas similares a la Cuarta Enmienda, la aplicación de ésta a los registros de ordenadores en los lugares de trabajo del sector público plantea un asunto diferente. En O'Connor v. Ortega, 480 U.S. 709 (1987), el Tribunal Supremo presentó un marco distinto para evaluar los registros realizados en entornos laborales del gobierno sin una orden, un marco aplicable a la inspección de ordenadores. Según el caso O'Connor, un empleado gubernamental puede gozar de una expectativa razonable de privacidad en su puesto. Véase id. en 717 (O'Connor, J., opinión de pluralidad); id. en 721 (Scalia, J., concurrente). Sin embargo, la expectativa razonable de privacidad se vuelve irrazonable si "las prácticas y procedimientos reales de oficina o […] la regulación legítima" permiten al supervisor de los empleados, a sus compañeros o al público entrar en el lugar de trabajo del empleado. Id. en 717 (O'Connor, J., opinión de pluralidad). Asimismo, los empresarios pueden realizar registros "razonables" sin una orden incluso en el caso de que estos contravengan la expectativa razonable de privacidad de un empleado. Dichas inspecciones incluyen las intrusiones relacionadas con el trabajo y sin ánimo de investigación (por ejemplo, entrar en la oficina cerrada de un empleado para coger un archivo) e inspecciones razonables sobre una conducta inadecuada en el trabajo. Véase id. en 725-26 (O'Connor, J., opinión de pluralidad); id. en 732 (Scalia, J., concurrente).

a) Expectativa razonable de privacidad en lugares de trabajo públicos

La prueba de la expectativa razonable de privacidad formulada por la pluralidad de O'Connor plantea la cuestión de si el lugar de trabajo de un funcionario del gobierno está "tan abierto a sus compañeros o al público que no cabe albergar una expectativa razonable de privacidad". O'Connor, 480 U.S. en 718 (opinión de pluralidad). Esta norma difiere de forma significativa del análisis estándar que se aplica en los entornos laborales privados. Mientras que los empleados del sector privado gozan de una expectativa razonable de privacidad en su puesto de trabajo, a menos que éste esté "abierto para todo el mundo", Lyons, 706 F.2d en 326, los funcionarios gubernamentales solamente pueden albergar una expectativa razonable de privacidad en su entorno laboral si en una investigación caso por caso de las "prácticas y procedimientos reales de oficina" los resultados arrojan que es razonable que los empleados

esperen que los demás no penetren en su espacio. Véase O'Connor, 480 U.S. en 717 (opinión de pluralidad); Rossi v. Town of Pelham, 35 F. Supp. 2d. 58, 63-64 (D.N.H. 1997). Véase también O'Connor, 480 U.S. en 730-31 (Scalia, J., concurrente) (en el que se destaca la diferencia entre el análisis de la expectativa de privacidad ofrecido por la pluralidad de O'Connor y el que se aplica tradicionalmente en los registros en un entorno laboral del sector privado). Por lo tanto, desde un punto de vista práctico, es menos probable que los empleados públicos conserven una expectativa razonable de privacidad frente a registros del gobierno en el trabajo que los empleados del sector privado.

Los tribunales que evalúan la expectativa razonable de privacidad de los empleados públicos en la estela del caso O'Connor han tenido en cuenta los siguientes factores: si el área de trabajo en cuestión está asignada únicamente al empleado; si los demás tienen acceso a dicho espacio; si la naturaleza del empleo exige una relación laboral estrecha con los demás; si el reglamento de la oficina advierte a los empleados de que determinadas zonas son susceptibles de ser registradas y si la propiedad examinada es pública o privada. Véase Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 179-80 (1° Cir. 1997) (resumen de casos); Estados Unidos v. Mancini, 8 F.3d 104, 109 (1° Cir. 1993). Por lo general, los tribunales han rechazado las reivindicaciones de expectativa de privacidad en las oficinas en las que los empleados supieran o deberían haber sabido que otras personas podían acceder a su entorno laboral. Véase por ejemplo Sheppard v. Beerman, 18 F.3d 147, 152 (2° Cir. 1994) (en el que se concluye que la inspección realizada por un juez en el escritorio y los armarios de archivos de su secretario judicial no infringió la expectativa razonable de privacidad de éste a causa de la estrecha relación laboral del secretario con el juez; Schowengerdt v. Estados Unidos, 944 F.2d 483, 488 (9° Cir. 1991) (en el que se concluye que un ingeniero civil contratado por la Marina, el cual trabajaba con documentos clasificados en una planta de armamento, no tenía ninguna expectativa razonable de privacidad en su despacho porque de todo el mundo era sabido que las oficinas de los empleados eran registradas con regularidad en busca de pruebas de conducta inadecuada). Sin embargo, véase Estados Unidos v. Taketa, 923 F.2d 665, 673 (9° Cir. 1991) (en el que se concluye en las sentencias que un empleado público tenía una expectativa razonable de privacidad en su despacho, a pesar de compartirlo con varios compañeros). Por el contrario, los tribunales han sentenciado que un registro contraviene la expectativa razonable de privacidad de un empleado público cuando éste no tiene motivos para esperar que otras personas accedan a la zona inspeccionada. Véase O'Connor, 480 U.S. en 718-19 (pluralidad) (en el que se concluye que un médico del hospital del estado tenía una expectativa razonable de privacidad sobre su escritorio y los armarios archivadores al no ser previsible que otros empleados pudieran entrar en su despacho y acceder a su contenido); Rossi, 35 F. Supp. 2d en 64 (en el que se concluye que un secretario municipal tenía una expectativa razonable de privacidad en su despacho de 8' x 8' en el que el público no podía entrar y otros empleados del ayuntamiento no entraban).

Mientras que los agentes deben valorar si un empleado público tiene una expectativa razonable de privacidad sobre su entorno laboral caso por caso, las políticas oficiales de empleo expresadas por escrito pueden simplificar la labor de manera espectacular. Véase O'Connor, 480 U.S. en 717 (pluralidad) (en el que se destaca que la "regulación legítima" del lugar de trabajo puede disminuir las protecciones de los empleados públicos otorgadas por la Cuarta Enmienda). Los tribunales han respetado de manera uniforme las políticas oficiales de los empleadores públicos que autorizan expresamente el acceso al lugar de trabajo de los empleados y se han acogido a dichas políticas a la hora de concluir que un empleado no puede tener una expectativa razonable de privacidad en su entorno laboral. Véase Sindicato estadounidense de trabajadores de correos, Columbus Area Local AFL-CIO v. Servicio de Correo de Estados Unidos, 871 F.2d 556, 56-61 (6° Cir. 1989) (en el que se concluye que los empleados de correos no tenían expectativa razonable de privacidad alguna sobre el contenido de las taquillas del gobierno tras firmar una renuncia expresando que éstas eran susceptibles de ser inspeccionadas en cualquier momento, aunque en el interior hubiera objetos personales), Estados Unidos v. Bunkers, 521 F.2d 1217, 1219-1221 (9° Cir. 1975) (igual, en el que se destaca el lenguaje del manual de correos que establece que una taquilla es "susceptible de ser registrada por supervisores e inspectores postales"). No es necesario decir que si una política concreta elimina una expectativa razonable de privacidad o no es una cuestión objetiva. Las políticas de empleo que no abordan de forma explícita la privacidad del empleado pueden resultar insuficientes para eliminar la protección de la Cuarta Enmienda. Véase por ejemplo, Taketa, 923 F.2d en 672-73 (en el que se concluye que el reglamento que exige que los empleados de la DEA "mantenga ordenado su escritorio" no contraviene

la expectativa razonable de privacidad de un empleado no relacionado con la DEA destinado en la oficina de la DEA).

A la hora de planificar el registro de un ordenador del gobierno en un lugar de trabajo gubernamental, los agentes deben buscar políticas de empleo oficiales o "banners" que puedan eliminar una expectativa razonable de privacidad sobre dicho ordenador.

Estas políticas de empleo y "banners" expresados por escrito cobran particular importancia en casos en los que se considera si los funcionarios gubernamentales tienen una expectativa razonable de privacidad sobre los ordenadores del gobierno. Los banners son avisos escritos que se muestran a los usuarios al registrarse en un ordenador o red informática y mediante los que se les puede informar de los derechos de privacidad que tienen o no al usar dicho equipo o red. Véase el Apéndice A.

En general, los funcionarios del gobierno que reciben la notificación de que sus superiores tienen derecho a acceder o analizar la información almacenada en sus ordenadores no pueden albergar expectativa razonable de privacidad alguna sobre la información guardada en ellos. Por ejemplo, en Estados Unidos v. Simons, 206 F.3d 392 (4° Cir. 2000), varios expertos en informática de un departamento de la CIA averiguaron que un empleado llamado Mark Simons había utilizado su ordenador del trabajo para obtener pornografía de Internet, infringiendo así la política de la CIA. Los expertos informáticos accedieron al ordenador de Simona de manera remota y sin una orden e hicieron copias de más de mil archivos de imágenes que Simons había almacenado en el disco duro. En muchos casos estos archivos contenían pornografía infantil, los cuales se entregaron a las fuerzas de seguridad. Cuando Simona presentó una moción para anular los resultados de este registro remoto de su disco duro, el Cuarto Circuito concluyó que la política oficial de uso de Internet del departamento de la CIA eliminaba cualquier expectativa razonable de privacidad que Simona pudiera haber tenido sobre los archivos copiados. Véase id. en 398. Esta política establecía que el departamento de la CIA podía "revisar, inspeccionar y/o supervisar periódicamente el acceso a Internet de [cada] usuario según lo considerara oportuno", así como que dicha inspección se llevaría a cabo con el fin de "permitir la detección, interrupción y persecución de cualquier actividad no autorizada". Id. en 395-96. Simons no negó conocer esta política. Véase id. en 398 n.8. Teniendo en cuenta esta política, el Cuarto Circuito concluyó que Simona no tenía ninguna expectativa razonable de privacidad "con respecto a los resultados del uso que el hacía de Internet", incluyendo los archivos que había descargado. Id. en 398.

Otros tribunales se han mostrado de acuerdo con el enfoque expresado en el caso Simona y han sentenciado que los banners y las políticas eliminan por lo general toda expectativa razonable de privacidad sobre los contenidos almacenados en una cuenta de red de un funcionario del gobierno. Véase Estados Unidos v. Angevine, 281 F.3d 1130, 1134-35 (10° Cir. 2002) (en el que se concluye que un banner y la política informática anulaba la expectativa razonable de privacidad de un empleado público sobre los datos descargados de Internet); Wasson v. Sonoma County Junior College, 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997) (en el que se concluye que la política informática del empleador público, por la que se concede a éste "el derecho a acceder a toda la información almacenada en los ordenadores [del empleador]" anula la expectativa razonable de privacidad de un empleado acerca de los archivos guardados en los ordenadores del empleador); Bohach v. Ciudad de Reno, 932 F. Supp. 1232, 1235 (D. Nev. 1996) (en el que se concluye que unos oficiales de policía no tenían expectativa razonable de privacidad sobre el uso de un sistema de busca, en parte porque el Jefe de Policía había emitido una orden mediante la que anunciaba que los mensajes se iban a registrar); Estados Unidos v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (en el que se concluye que un sargento de la Fuerza Aérea no tenía una expectativa razonable de privacidad sobre su cuenta de correo electrónico del gobierno ya que el uso del correo electrónico estaba reservado para asuntos oficiales y el banner de red informaba a cada usuario al registrarse a la red de que su uso estaba sujeto a vigilancia). Sin embargo, véase DeMaine v. Samuels, 2000 WL 1658586, en *7 (D. Conn. 25 de septiembre de 2000) (en el que se sugiere que la existencia de un manual de empleo que autoriza explícitamente los registros "tiene mucho peso" a la hora de determiner si un empleado del gobierno tiene una expectativa razonable de privacidad en el trabajo, pero que "no liquida la cuestión en sí misma"). Por el contrario, un tribunal puede destacar la ausencia de un banner o política informática al concluir que un empleado alberga una expectativa razonable de privacidad sobre el uso de su ordenador. Véase Estados Unidos v. Slanina, 283 F.3d 670, 676-77 (5° Cir. 2002).

No es necesario decir que si una política concreta elimina una expectativa razonable de privacidad o no es una cuestión objetiva. Los agentes y fiscales deben considerar si una política concreta es lo suficientemente amplia como para contemplar razonablemente que se lleve a cabo el registro. Si no lo es tanto, puede que no anule la expectativa razonable de privacidad del funcionario del gobierno frente a la inspección que éste planea ejecutar. Por ejemplo, en el caso Simons, el Cuarto Circuito concluyó que a pesar de que la política de uso de Internet del departamento de la CIA eliminaba la expectativa razonable de privacidad de Simons sobre los resultados del uso que hacía de Internet, *no* eliminaba su expectativa razonable de privacidad sobre los límites físicos de su despacho. Véase Simons, 206 F.3d en 399 n.10. Por consiguiente, la política propiamente dicha no era suficiente para justificar el acceso físico al despacho de Simon. Véase id. en 399. Véase también Taketa, 923 F.2d en 672-73 (en el que se concluye que el reglamento que exige que los empleados de la DEA "mantenga ordenado su escritorio" no contraviene la expectativa razonable de privacidad de un empleado no relacionado con la DEA destinado en la oficina de la DEA). En el Apéndice A se incluyen banners de muestra.

b) Registros "razonables" del lugar de trabajo con arreglo al caso O'Connor v. Ortega

Los empleadores gubernamentales y sus agentes pueden llevar a cabo inspecciones "razonables" relacionadas con el trabajo aunque éstas contravengan la expectativa razonable de privacidad de un empleado.

En la mayoría de situaciones es necesario obtener una orden antes de que un agente del gobierno pueda realizar un registro que infrinja la expectativa razonable de privacidad de un individuo. Sin embargo, en el contexto del empleo del gobierno, el papel de éste como empleador, frente a su función como agente encargado de hacer cumplir la ley, supone un caso especial. En el caso O'Connor, el Tribunal Supremo concluyó que un empleador público o su agente pueden realizar una inspección del lugar de trabajo que infrinja la expectativa razonable de privacidad de un empleado público en tanto en cuanto dicha inspección sea "razonable". Véase O'Connor, 480 U.S. en 722-23 (pluralidad); Id. en 732 (Scalia, J., concurrente). La decisión del tribunal incorpora los registros por parte de los empleadores en los entornos laborales públicos a la lista de excepciones por "necesidades especiales" al requisito de la orden. Las excepciones por "necesidades especiales" permiten al gobierno dispensar el requisito habitual de la orden cuando sus oficiales contravienen derechos de privacidad protegidos en el transcurso de su actuación en una capacidad no relacionada con las fuerzas de seguridad. Véase por ejemplo, New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurrente) (en el que se aplica la excepción por "necesidades especiales" para permitir a unos funcionarios de un colegio público que registren las propiedades de un alumno sin una orden en un intento por mantener la disciplina y el orden en las escuelas públicas); Sindicato de Empleados del Tesoro v. Von Raab, 489 U.S. 656, 677 (1989) (en el que se aplica la excepción por "necesidades especiales" para permitir la realización de una prueba de drogas sin una orden a los empleados de Aduanas que desean ascender a puestos en los que gestionarían información confidencial). En estos casos, el Tribunal ha concluido que la necesidad de los oficiales del gobierno de perseguir objetivos legítimos no relacionados con las fuerzas de seguridad justifica una relajación del requisito de la orden debido a que "la carga de obtener una orden hace que aumente la probabilidad de que se frustre el fin gubernamental [no relacionado con las fuerzas de seguridad] que constituye el objetivo del registro". O'Connor, 480 U.S. en 720 (se cita Camara v. Tribunal Municipal, 387 U.S. 523, 533 (1967)).

Según el caso O'Connor, un registro sin orden debe satisfacer al menos dos requisitos para ser considerado "razonable". En primer lugar, el empleador o sus agentes deben tomar parte en el registro por un motivo relacionado con el trabajo, en lugar de limitarse a obtener pruebas para su uso en procedimientos penales. Por otra parte, la inspección debe estar justificada desde el inicio y debe ser permisible en su alcance.

i) El registro debe estar relacionado con el trabajo

El primer elemento de la prueba del carácter razonable del caso O'Connor exige que el empleador o sus agentes tomen parte en el registro por un motivo relacionado con el trabajo, en lugar de limitarse a obtener pruebas para su uso en procedimientos penales. Véase O'Connor, 480 U.S. en 721. Este elemento restringe la excepción O'Connor a situaciones en las que los agentes del gobierno que lleven a

cabo la inspección actúen en calidad de empleadores, en lugar de como agentes de las fuerzas de seguridad. El tribunal de O'Connor especificó dos circunstancias de esta índole. Primeramente, el tribunal concluyó que los empleadores públicos pueden realizar intrusiones razonables relacionadas con el trabajo y sin fines de investigación, como entrar en el despacho de un empleado para coger un archivo o informe mientras éste está fuera. Véase id. en 721-22 (pluralidad); Id. en 732 (Scalia, J., concurrente). En segundo lugar, el tribunal concluyó que los empleadores pueden llevar a cabo investigaciones razonables sobre una conducta inadecuada de un empleado en el trabajo, como entrar en el despacho de un empleado para investigar la infidencia de éste que pueda poner en peligro el funcionamiento eficiente y adecuado de la oficina. Véase id. en 724 (pluralidad); Id. en 732 (Scalia, J., concurrente).

La línea divisoria entre un registro legítimo relacionado con el trabajo y uno ilegítimo para buscar pruebas penales está clara en teoría, pero en la práctica a menudo es difusa. Los empleadores públicos que se enteren de una conducta inadecuada en el trabajo pueden investigarla con dos motivaciones: pueden buscar pruebas para acabar de raíz con la "ineficiencia, incompetencia, mala administración u otra infidencia relacionada con el trabajo", id. en 724 o también para buscar pruebas con el fin de iniciar un proceso penal. En realidad, las dos categorías se pueden combinar. Por ejemplo, los oficiales del gobierno que tengan investigadores penales bajo su mando pueden responder a las alegaciones de mala conducta laboral dirigiéndolos a registrar el despacho de un empleado para buscar pruebas de un delito.

Los tribunales han adoptado interpretaciones bastante generosas del caso O'Connor cuando han tenido que abordar registros con motivaciones mezcladas. En general, la presencia e implicación de oficiales de las fuerzas de seguridad no tiene por qué invalidar el registro en tanto en cuanto el empleador o su agente participen en el mismo por razones legítimas asociadas al trabajo. Véase por ejemplo Estados Unidos v. Slanina, 283 F.3d 670, 678 (5° Cir. 2002) (en el que se autoriza un registro por parte de un oficial a cargo de los departamentos de bomberos y policía y se establece que "no se debe frustrar el objetivo de O'Connor de garantizar un entorno laboral eficiente por el simple hecho de que la misma conducta inadecuada que infringe una política de un empleador gubernamental resultar ser también ilegal"); Gossmeyer v. McDonald, 128 F.3d 481, 492 (7° Cir. 1997) (en el que se concluye que la presencia de oficiales de las fuerzas de seguridad en un equipo de inspección dedicado a la búsqueda de pruebas de comportamientos inadecuados en el trabajo no transforma dicha inspección en un registro ilegítimo de las fuerzas de seguridad); Taketa, 923 F.2d en 674 (en el que se concluye que la inspección del espacio de las oficinas de la DEA por agentes propios de ésta que investigaban las alegaciones de escuchas telefónicas ilegales "constituye una investigación interna dirigida a descubrir comportamientos inapropiados de los empleados en su trabajo"). Shields v. Burge, 874 F.2d 1201, 1202-05 (7° Cir. 1989) (en el que se aplica la excepción de O'Connor en una investigación de asuntos internos de un sargento de policía que realizó una investigación penal en paralelo); Ross v. Hinton, 740 F. Supp. 451, 458 (S.D. Ohio 1990) (en el que se concluye que las conversaciones de un empleador público con un oficial de las fuerzas de seguridad en relación con una presunta conducta penal de uno de los empleados, las cuales culminaron con el consejo del oficial de "asegurar" los archivos del empleado, no convirtieron la posterior inspección del despacho del éste por parte del empleador en un registro de las fuerzas de seguridad).

Si bien la presencia de oficiales de las fuerzas de seguridad normalmente no invalida una inspección relacionada con el trabajo, es cierto que varios tribunales han indicado que el hecho de que se aplique O'Connor o no depende tanto de la identidad del personal que lleve a cabo el registro como de que la finalidad del mismo esté asociada al trabajo. Por ejemplo, en Estados Unidos v. Simons, 206 F.3d 392, 400 (4° Cir. 2000), el Cuarto Circuito concluyó que O'Connor autorizaba la inspección del despacho de un funcionario del gobierno por parte de su supervisor, a pesar de que el objetivo predominante para llevarla a cabo era descubrir pruebas de un delito. A juicio del tribunal, este registro entraba dentro de los márgenes de O'Connor al ser realizado por el supervisor del empleado. Véase id. ("[El empleador] no perdió sus necesidades especiales de un funcionamiento eficiente y adecuado del lugar de trabajo simplemente porque las pruebas obtenidas correspondieran a un delito"). (se omiten las citas internas). Por el contrario, un tribunal de distrito sentenció que la excepción O'Connor no era aplicable en un caso en el que un empleador público envió a un oficial uniformado de la policía al despacho de un empleado, a pesar de que el objeto de su presencia estaba completamente relacionado con el trabajo. Véase Rossi v. Town of Pelham, 35 F. Supp. 2d 58, 65-66 (D.N.H. 1997) (acción civil en virtud de 42 U.S.C.

§ 1983) (en el que se concluye que la excepción O'Connor no era de aplicación cuando unos oficiales municipales enviaron a un solo oficial de policía a la oficina de una secretaria del ayuntamiento para vigilar que éste no eliminar registros públicos de su despacho antes de que se produjera una inspección programada; el registro resultante fue una "intrusión policial" en lugar de una "intrusión del empleador".

Lógicamente, los tribunales invalidarán todos aquellos registros realizados sin una orden en un lugar de trabajo cuando los hechos determinen que las fuerzas de seguridad fueron los impulsores reales de la inspección y que ésta contraviene la expectativa razonable de privacidad de un empleado. Véase Estados Unidos v. Hagarty, 388 F.2d 713, 717 (7° Cir. 1968) (en el que se concluye que la vigilancia instalada por investigadores penales infringía la Cuarta Enmienda, ya que la finalidad de dicha vigilancia consistía en "detector actividades delictivas", en lugar de "supervisar e investigar" a un funcionario del gobierno); Estados Unidos v. Kahan, 350 F. Supp. 784, 791 (S.D.N.Y. 1972) (por el que se invalida un registro realizado sin una orden en la papelera de un empleado del INS por parte de un investigador penal del propio INS con el objetivo de encontrar pruebas de un delito que se realizaba todos los días tras el trabajo con el consentimiento del empleador), revelado parcialmente por otros motivos, 479 F.2d 290 (2° Cir. 1973), revelado con instrucciones de reintegrar la sentencia del tribunal de distrito, 415 U.S. 239 (1974).

ii) El registro debe estar justificado desde el inicio y ser permisible en su alcance

Para que sea "razonable" conforme a la Cuarta Enmienda, un registro relacionado con el trabajo por parte del empleador, del tipo refrendado en O'Connor, también debe estar justificado desde el inicio y debe ser permisible en su alcance. O'Connor, 480 U.S. en 726 (pluralidad). Una inspección estará justificada desde el inicio "siempre y cuando haya motivos fundados para sospechar que gracias a ella se hallarán pruebas de que el empleado es culpable de mala conducta en el trabajo o que dicha inspección sea necesaria para una finalidad asociada al trabajo pero no de investigación". Id. Véase por ejemplo Simons, 206 F.3d en 401 (en el que se concluye que el acceso al despacho de un empleado para requisar su ordenador estaba justificado desde el inicio debido a que el empleador sabía que el empleado había utilizado el ordenador para descargar pornografía infantil); Gossmeyer, 128 F.3d en 491 (en el que se concluye que las legaciones específicas de un compañero de trabajo acerca de una grave conducta inadecuada justificaron desde el principio el registro del escritorio y los armarios archivadores cerrados del Investigador de Protección de los Niños por parte del Sheriff); Taketa, 923 F.2d en 674 (en el que se concluye que un informe de comportamiento inapropiado justificó el registro inicial de la oficina del empleado); Shields, 874 F.2d en 1204 (en el que se sugiere en las sentencias que la inspección del escritorio de un oficial de policía en busca de narcóticos conforme a una investigación interna podría ser razonable si obedeciera a una pista anónima); DeMaine v. Samuels, 2000 WL 1658586, en * 10 (D. Conn. 25 de septiembre de 2000) (en el que se concluye que la inspección de una agenda diaria del oficial de policía estaba justificada por la información de dos fuentes fidedignas que indicaban que esta persona mantenía unas notadas detalladas sobre asistencia relevantes para una investigación sobre horas extra que incumbían a otros oficiales); Williams v. Philadelphia Housing Auth., 826 F. Supp. 952, 954 (E.D. Pa. 1993) (en el que se concluye que el registro del despacho de un empleado para buscar un disco de ordenador estaba justificado desde el inicio porque el empleador necesitaba el contenido del disco con fines oficiales). Compárese Ortega v. O'Connor, 146 F.3d 1149, 1162 (9° Cir. 1998) (en el que se concluye que unas quejas imprecisas y no corroboradas de comportamiento inapropiado no justifican una decisión para inspeccionar el despacho de un empleado).

Una inspección será "permisible en su alcance" cuando "las medidas adoptadas estén prudentemente relacionadas con los objetivos de la misma y no [sean] excesivamente invasivas en función del tipo de conducta inadecuada. O'Connor, 480 U.S. en 726 (pluralidad) (se omiten las citas internas). Esta norma exige que los empleadores y sus agentes adapten los registros relacionados con el trabajo a la presunta infidencia. Véase por ejemplo Leventhal v. Knapek, 266 F.3d 64, 75-77 (2° Cir. 2001) (en el que se concluye que el registro para comprobar la presencia de software no autorizado por el organismo en el ordenador de un empleado no era excesivamente invasivo porque los oficiales exploraron únicamente los nombres de los archivos al principio y después registraron sólo los directorios sospechosos en posteriores visitas); Simons, 206 F.3d en 401 (en el que se concluye que el registro en busca de pornografía infantil que se creía almacenada en el ordenador de un empleado era permisible en su

alcance porque la persona que lo llevó a cabo "se limitó a cruzar el despacho [del demandado], cambió los discos duros y salió"); Gossmeyer, 128 F.3d en 491 (en el que se concluye que el registro de un lugar de trabajo en busca de imágenes de pornografía infantil era permisible en su alcance porque se limitó a aquellos lugares donde era más probable que estuvieran almacenadas estas imágenes); Samuels, 2000 WL 1658586, en *10 (en el que se concluye que la inspección de la agenda diaria de un oficial de policía era razonable porque los investigadores de asuntos internos tenían motivos para creer que en ella había información relevante para una investigación sobre el abuso de horas extra). Si los empleadores realizan una exploración que exceda de forma no razonable el alcance necesario para perseguir los objetivos legítimos del empleador en relación con el trabajo, dicha exploración se considerará "irrazonable" e infringirá la Cuarta Enmienda. Véase O'Connor, 146 F.3d en 1163 (en el que se concluye que una inspección "general e ilimitada" del escritorio, los armarios y documentos personales de un empleado no era permisible en su alcance en tanto en cuanto el equipo de inspección no intentó limitar su investigación a las pruebas de la presunta conducta inadecuada).

b) Autorización en lugares de trabajo del sector público

Aun teniendo en cuenta que los empleadores públicos pueden registrar el entorno laboral de los empleados sin necesidad de una orden por motivos asociados con el trabajo, estos lugares públicos suponen un entorno más restrictivo en un aspecto. En los lugares de trabajo del gobierno, los empleadores que actúan en calidad oficial normalmente no pueden autorizar un registro de las oficinas de sus empleados por parte de las fuerzas de seguridad. Véase Estados Unidos v. Blok, 188 F.2d 1019, 1021 (D.C. Cir. 1951) (en el que se concluye que un supervisor gubernamental no puede permitir un registro de las fuerzas de seguridad del escritorio de un funcionario del gobierno); Taketa, 923 F.2d en 673; Kahan, 350 F. Supp. en 791. Los motivos para este resultado es que la Cuarta Enmienda no puede autorizar a un oficial del gobierno que permita un registro por parte de otro. Véase Blok, 188 F.2d en 1021 ("El funcionamiento de un organismo gubernamental y el cumplimiento de una ley penal no se unen para dar derecho a un registro que supere el alcance de cualquiera de los dos"). Por consiguiente, todo registro de las fuerzas de seguridad ejecutado en virtud de la autorización de un empleador público se debe valorar con arreglo a O'Connor, en lugar de las normas de autorización de terceras partes de Matlock. La cuestión en estos casos no es si el empleador público tenía autoridad común para permitir el registro, sino más bien si el registro combinado de las fuerzas de seguridad y del empleador observó las normas de la Cuarta Enmienda de O'Connor v. Ortega.

[Índice]

II. REGISTRO Y CONFISCACIÓN DE ORDENADORES CON UNA ORDEN

A. Introducción

El marco legal para registrar y confiscar ordenadores con una orden es similar en gran medida al de otros registros y confiscaciones. Al igual que cualquier tipo de inspección en virtud de una orden, las fuerzas de seguridad deben determinar una "causa probable, acreditada mediante juramento o declaración" y "describir concretamente el lugar que se va a registrar y las personas u objetos que se vayan a detener o requisar". Constitución de Estados Unidos, Cuarta Enmienda.

A pesar del marco legal común, los registros informáticos son diferentes a los demás debido a que la tecnología de la informática con frecuencia obliga a los agentes a llevarlos a cabo de formas no tradicionales. Pensemos por un momento en el caso tradicional de una orden para confiscar un coche robado de un aparcamiento privado. Por lo general, los agentes asumen que el aparcamiento seguirá existiendo en su emplazamiento anterior cuando vayan a ejecutar el registro, así como que podrán identificar el coche robado basándose en el modelo, versión, matrícula o en el número de identificación del vehículo. Como consecuencia de ello, el proceso de redacción de una orden y de ejecución del registro es relativamente simple. Una vez que los agentes determinan la causa probable y describen el coche y el aparcamiento al magistrado, éste puede emitir la orden por la que autoriza a los agentes a acudir al aparcamiento y recuperar el coche.

El registro de archivos informáticos suele ser más complicado. Dado que un archivo informático está formado de impulsos eléctricos que caben en la cabeza de un alfiler y pueden dar la vuelta al mundo en un instante, es posible que los agentes no sepan el lugar en el que están almacenados los archivos o en qué manera. Pueden estar almacenados en un disquete, en un directorio oculto en el ordenador portátil del sospechoso o en un servidor remoto situado a miles de kilómetros. Pueden estar codificados, pueden llevar un título que induzca a error, pueden estar almacenados en formatos de archivo poco comunes o mezclados con miles de archivos que no guarden ninguna relación, inofensivos o que gocen incluso de protección jurídica. Estas incertidumbres provocan que los agentes no puedan simplemente determinar la causa probable, describir los archivos que necesitan y posteriormente "ir a recuperar" los datos. En lugar de ello, deben comprender las limitaciones técnicas de las distintas prácticas de registro, planificar la inspección minuciosamente y por último redactar la orden de tal manera que autorice a los agentes a adoptar las medidas necesarias para obtener las pruebas que precisan.

El registro y confiscación de ordenadores con una orden es tanto un arte como una ciencia. Sin embargo, los agentes y fiscales se han dado cuenta de que generalmente pueden aumentar al máximo las probabilidades de éxito de un registro y confiscación siguiendo estos cuatro pasos:

1) Reunir a un equipo formado por el agente del caso, la parte demandante y un experto en tecnología con la mayor antelación posible al registro.

Es cierto que el agente principal que lleva la investigación es la figura central en la mayor parte de las inspecciones, pero en los registros informáticos se necesita un equipo con tres participantes importantes: el agente, la parte demandante y un especialista en tecnología con experiencia en ordenadores e investigación científica relacionada con la informática. En la mayoría de los registros de ordenadores, el agente encargado del caso organiza y dirige el registro, averigua todo lo posible acerca de los equipos que se van a analizar y elabora una declaración jurada mediante la que determina la causa probable. El especialista en tecnología explica al agente y a la parte demandante las limitaciones técnicas que determinan el registro, crea el plan para llevarlo a cabo y en numerosas ocasiones adopta el papel principal a la hora de ejecutar el registro propiamente dicho. Por último, el fiscal revisa la declaración jurada y la orden y comprueba que todo el proceso cumpla con la Cuarta Enmienda y la Norma 41 de las Normas Federales de Procedimiento Penal. No hace falta decir que todos y cada uno de los miembros del equipo deben colaborar con el resto para garantizar un registro eficaz.

Existen muchas fuentes de expertos técnicos en el gobierno federal. Casi todos los organismos que cuentan con investigadores de las fuerzas de seguridad tienen también especialistas en tecnología que han recibido formación en investigación científica relacionada con la informática. Por ejemplo, el FBI cuenta con los inspectores del Computer Analysis Response Team (Equipo de Respuesta de Análisis Informático, CART), el servicio de Hacienda tiene a su disposición a los especialistas del Seized Computer Evidence Recovery (Recuperación de Pruebas Informáticas Confiscadas, SCER) y el Servicio Secreto, por su parte, tiene el Electronic Crime Special Agent Program (Programa Especial de Agentes para Delitos Electrónicos, ECSAP). Los agentes encargados de la investigación deben ponerse en contacto con los expertos en tecnología de su propio organismo. Por otra parte, también hay organismos que proporcionan a sus agentes la suficiente formación técnica como para que puedan actuar también como especialistas. En estos casos los agentes no suelen necesitar consultar a los expertos y hacen las veces de especialistas en tecnología y de agentes de forma simultánea.

2) Averiguar todo lo posible acerca del sistema informático que se va a registrar antes de elaborar una estrategia para la inspección o de redactar la orden.

Una vez reunido el equipo, el agente encargado del caso debe recabar tanta información como le sea posible acerca del sistema informático objetivo del registro. Es difícil exagerar la importancia de este paso. En su mayor parte, la necesidad de información detallada y precisa sobre el ordenador de destino es el resultado de consideraciones prácticas. Hasta que el agente no averigua que tipo de ordenador y sistema operativo utiliza el sospechoso es imposible saber cómo se puede recuperar la información que guarda el sistema o incluso dónde se puede localizar la información. Cada ordenador y red informática es diferente y cualquier diferencia, por sutil que sea, en el hardware, el software, los sistemas operativos o la configuración del sistema puede hacer que el planteamiento de registro cambie radicalmente. Por

ejemplo, una estrategia concreta de inspección puede funcionar bien si una red considerada como objetivo funciona con el sistema operativo Linux y no funcionar bien en absoluto si en cambio tiene instalado Windows NT.

Estas consideraciones cobran especial relevancia si los registros se van a realizar sobre redes informáticas complejas (frente a ordenadores individuales). Por ejemplo, el mero hecho de que una empresa utilice ordenadores en sus oficinas no implica que los dispositivos que allí se encuentran contengan información útil. Las empresas pueden contratar proveedores de servicios de red que almacenan su información en servidores de red remotos situados a kilómetros de distancia, posiblemente miles. Es debido a esto que un especialista en tecnología no puede asesorar al agente encargado del caso acerca de los aspectos prácticos de las distintas estrategias de registro sin conocer la naturaleza del sistema informático que se va a registrar. Es necesario que los agentes averigüen todo lo posible sobre el ordenador declarado como objetivo antes de redactar la orden, incluyendo, si es posible, el hardware, el software, el sistema operativo y la configuración de la red.

Por otra parte, la obtención de información detallada y precisa sobre el ordenador también tiene importantes consecuencias jurídicas. Por poner un ejemplo, la confiscación adicional de materiales conforme a la Primera Enmienda como borradores de boletines o páginas web puede afectar a la Ley de Protección de la Privacidad ("PPA"), 42 U.S.C. § 2000aa, mientras que la confiscación adicional y posterior registro de cuentas de red puede generar problemas de acuerdo con la Ley de Privacidad de las Comunicaciones Electrónicas ("ECPA"), 18 U.S.C. §§ 2701-2712 (véanse las partes B.2 y B.3, más abajo). Con el fin de reducir al mínimo la responsabilidad con respecto a estas leyes, los agentes deben llevar a cabo una investigación minuciosa sobre dónde y si pueden estar almacenados materiales y cuentas de red con respecto a la Primera Enmienda en el sistema informático objetivo del registro. Al menos un tribunal ha sugerido la posibilidad de que la no realización de esta investigación puede privar al gobierno de una defensa de buena fe frente a la responsabilidad relacionada con estas leyes. Véase Steve Jackson Games, Inc. v. Servicio Secreto de Estados Unidos, 816 F. Supp. 432 (W.D. Tex. 1993), afirmado, 36 F.3d 457 (5° Cir. 1994).

Desde un punto de vista práctico, los agentes pueden adoptar varios enfoques para averiguar datos acerca de la red informática declarada como objetivo. En algunos casos, los agentes pueden entrevistar al administrador de sistema de dicha red (en ocasiones, ocultando su posición) y obtener así toda o la mayor parte de la información que precisa el especialista en tecnología para planificar y ejecutar la inspección. Si esto es imposible o peligroso, es posible que resulten eficaces otras estrategias menos sistemáticas. Por ejemplo, algunas veces los agentes llevan a cabo visitas de campo, a menudo en secreto, que revelan cuando menos algunos elementos del equipo material en cuestión. Una fuente de información muy útil para las redes conectadas a Internet es Internet en sí. Con frecuencia es posible que el público pueda hacer uso de preguntas de red para determinar el sistema operativo, las máquinas y la disposición general de una red en concreto conectada a Internet, aunque puede disparar las alarmas en la red en cuestión.

3) Formular una estrategia para llevar a cabo la inspección (incluyendo un plan secundario) basándose en la información conocida sobre el sistema informático que constituya el objetivo.

Una vez reunido el equipo y con el registro del sistema en cuestión, el siguiente paso consiste en formular una estrategia para realizar la inspección. Por ejemplo, ¿los agentes inspeccionarán todos los ordenadores en las instalaciones o simplemente accederán a las mismas y se llevarán todos los equipos? ¿Deberán hacer copias de archivos sueltos o harán copias exactas de los discos duros completos? ¿Qué harán los agentes si fracasa su plan original o si los equipos informáticos o el software resultan ser distintos de lo previsto? Estas decisiones se mueven en una serie de consideraciones prácticas y jurídicas. En la mayor parte de los casos, el equipo de registro debe decidir una estrategia principal de inspección para a continuación planificar una serie de estrategias secundarias por si la primera no resulta ser práctica.

En muchos casos los agentes no podrán averiguar lo suficiente sobre el sistema informático que se va a examinar como para desarrollar una estrategia única o exhaustiva de inspección. La consecuencia es que los agentes deben reconocer cómo pueden influir sobre la estrategia de inspección aquellos aspectos del

sistema que *no* conocen. Incluso en los casos en los que se tiene una cantidad considerable de información sobre un sistema es frecuente que los agentes y técnicos que realizan una revisión de los datos tengan que hacer uso de distintas técnicas con el fin de analizar minuciosamente un ordenador y sus medios de almacenamiento. En ocasiones no se pueden copiar, revisar o analizar datos o configuraciones aparentemente corrientes por medio de un programa o protocolo de búsqueda, por lo que es necesario probar con otro o con varios distintos. Puede ocurrir que no sea posible realizar búsquedas por palabras clave hasta que no se haya ejecutado un análisis minucioso de una parte de los archivos; por otra parte, una inspección atenta de los datos puede poner de manifiesto otros aspectos, por lo demás ocultos, sobre cómo se ha utilizado el sistema y se generaron, accedieron, transmitieron y guardaron los datos. Es muy importante que los agentes tengan presentes estas posibilidades y que las tengan en cuenta a la hora de formular su estrategia.

Los asuntos que se deben considerar a la hora de desarrollar una estrategia para registrar y confiscar un ordenador se comentan con más detalle en el apartado B de este capítulo. No obstante, por lo general estos asuntos se resumen en cuatro preguntas: Primero, ¿cuál es la estrategia de inspección más efectiva que cumpla con la Norma 41 de la Cuarta Enmienda? En segundo lugar, ¿es necesario modificar dicha estrategia para reducir al mínimo la posibilidad de infringir la PPA o la ECPA? Tercero, ¿la inspección requerirá varias órdenes? Y cuarta y última, ¿deben los agentes pedir un permiso especial para realizar un registro sorpresa o rápido y tentativo?

4) Redactar la orden prestando especial atención para describir la finalidad del registro y de la propiedad que se va a requisar de una forma precisa y concreta, así como explicar las posibles estrategias de inspección (además de los asuntos prácticos y jurídicos que han contribuido a darles forma) en la declaración jurada acreditativa.

Los ingredientes esenciales para elaborar una orden de registro satisfactorio se ven en el apartado C, mientras que en el Apéndice F se puede consultar una guía práctica para redactar órdenes y declaraciones juradas. Por lo general, sin embargo, las claves para redactar órdenes de registros informáticos eficaces consisten en describir minuciosa y concretamente en primer lugar la finalidad de la orden de la que los investigadores tienen la causa probable para confiscar y, en segundo lugar, explicar de una forma adecuada la estrategia de inspección en la declaración jurada acreditativa. Desde un punto de vista práctico, estos pasos contribuyen a centrar y a orientar a los investigadores a medida que realizan la inspección. En el plano legal, el primero de ellos sirve para superar retos de la particularidad, mientras que el objetivo del segundo consiste en desbaratar las posibles afirmaciones de que los agentes llevaron a cabo el registro con una "indiferencia flagrante" hacia la orden.

[Índice]

B. Planificación del registro

1. Estrategias básicas para llevar a cabo inspecciones de equipos informáticos

Los registros de ordenadores se pueden realizar de diversas maneras. En general hay cuatro posibilidades:

- Analizar el ordenador e imprimir una copia en papel de los archivos concretos en ese mismo momento;
- Analizar el ordenador y realizar una copia electrónica de los archivos concretos en ese mismo momento;
- Crear una copia electrónica duplicada de todo el dispositivo de almacenamiento in situ y posteriormente recrear una copia operativa del dispositivo en otro lugar para su revisión;[(6)] y
- Confiscar el equipo, trasladarlo fuera del lugar en el que esté instalado y analizar su contenido en otro sitio.

La mejor opción para cada registro concreto dependerá de múltiples factores. El más importante de ellos es el papel desempeñado por el equipo material en el delito. Es conveniente destacar que la primera opción, imprimir copias en papel de archivos concretos, no suele ser una buena opción. Puede desembocar en una pérdida importante de información, incluyendo la fecha del archivo y los sellos de tiempo, el nombre de la ruta del archivo, el historial de "deshacer", comentarios y muchas otras cosas.

A pesar de que todas las inspecciones de ordenadores son diferentes, las estrategias de inspección dependen frecuentemente del papel desempeñado por el equipo en el delito. Si el equipo en sí es una prueba, un instrumento, contrabando o el resultado de un delito, lo habitual es que los agentes se planteen confiscarlo y analizar su contenido en otro lugar. Si por el contrario el equipo es simplemente un dispositivo de almacenamiento de pruebas, los agentes se limitarán por lo general a confiscarlo únicamente en el caso de que no sean viables otras alternativas menos problemáticas.

Comúnmente, un equipo informático puede tener una o dos funciones en un caso delictivo. La primera de ellas es que sea un dispositivo de almacenamiento de pruebas de un delito. Si un sospechoso guarda pruebas de sus planes de fraude en su ordenador personal, por ejemplo, el equipo material no es más que un contenedor de pruebas. La finalidad del registro del ordenador del sospechoso será recuperar las pruebas que éste contenga.

En otros casos, sin embargo, el propio equipo físico puede ser en sí mismo contrabando, prueba, un instrumento o el resultado de un delito. Por ejemplo, un ordenador utilizado para transmitir pornografía infantil es un instrumento de delito, mientras que un ordenador robado es el fruto de un delito. En estos casos la Norma Federal de Procedimiento Penal Nº 41 otorga a los agentes el derecho a requisar el ordenador en sí, independientemente de los materiales que contenga el soporte físico. Véase el Apéndice F (en el que se explica el alcance de los materiales que se pueden confiscar en virtud de la Norma 41). Dado que la Norma 41 autoriza a los agentes a requisar un ordenador en el último caso pero no en el primero, la estrategia de registro para un ordenador en concreto gira primero en torno al papel desempeñado por el mismo en el delito.[(7)]

a) Cuando el equipo físico es en sí mismo contrabando, prueba, un instrumento o el resultado de un delito

Conforme a la Norma Federal de Procedimiento Penal Nº 41 (b), los agentes pueden obtener órdenes de registro para confiscar equipos informáticos si el soporte físico es contrabando, prueba, un instrumento o el resultado de un delito. Véase Norma 41(b); Apéndice F. En aquellos casos en los que se pueda requisar el equipo propiamente dicho de acuerdo con la Norma 41, los agentes normalmente realizan el registro confiscando el ordenador y analizándolo en otro lugar. Por ejemplo, un ordenador personal utilizado para guardar y transmitir imágenes de contrabando es en sí mismo un instrumento del delito. Véase Davis v. Gracey, 111 F.3d 1472, 1480 (10° Cir. 1997) (ordenador utilizado para almacenar imágenes obscenas); Estados Unidos v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) (ordenador utilizado para almacenar pornografía infantil). Por consiguiente, la Norma 41 permite a los agentes obtener una orden que les autorice a confiscar el soporte físico del ordenador. En la mayor parte de los casos, los investigadores se limitan a obtener una orden para confiscar el ordenador, requisan el soporte físico durante el registro y posteriormente inspeccionan el ordenador del demandado para buscar archivos de contrabando, una vez ya en la comisaría de policía o en el laboratorio de investigación científica relacionad con la informática. En estos casos, los agentes deben explicar claramente en la declaración jurada acreditativa que tienen previsto registrar el ordenador en busca de pruebas y/o contrabando una vez haya sido confiscado y trasladado desde el lugar del registro.

En particular, se producen excepciones en aquellos casos en los que los agentes no van a confiscar los equipos informáticos a pesar de que se hayan utilizado como instrumentos, pruebas, contrabando o sean el resultado de un delito. Cuando el "ordenador" en cuestión no es un PC único sino que forma parte de una red compleja, los daños colaterales y los dolores de cabeza que pueden surgir de la confiscación de toda la red a menudo desaconsejan requisar todo el lote. Por ejemplo, si un administrador de sistemas de una red informática guarda información protegida en algún lugar de la red, ésta se convierte en un

instrumento del delito del administrador de sistemas. Desde el punto de vista técnico, es posible que los agentes pudieran obtener una orden para requisar toda la red. Sin embargo, llevarse la red entera puede paralizar una empresa legítima y en funcionamiento, trastocando así la vida de cientos de personas, además de que podría someter al gobierno a denuncias civiles en virtud de la Ley de Protección de la Privacidad, 42 U.S.C. § 2000aa y la Ley de Privacidad de las Comunicaciones Electrónicas, 18 U.S.C. §§ 2701-2712. Véase Jackson Games, Inc. v. Servicio Secreto, 816 F. Supp. 432, 440, 443 (W.D. Tex. 1993) (se comenta más abajo). Cuando se dan circunstancias de este tipo, es aconsejable que los agentes realicen un enfoque más matizado para obtener las pruebas que necesitan. Por otro lado, si la red es propiedad de una empresa criminal que se ocupa de administrarla, es adecuado confiscar la red para detener la actividad delictiva y evitar pérdidas mayores a las víctimas. Para realizar una confiscación así se necesitará un compromiso importante de los recursos y una planificación anticipada. Los agentes que tienen que afrontar una situación de esta índole pueden ponerse en contacto con la Sección de Delitos Cibernéticos y Propiedad Intelectual a través del número de teléfono (202) 514-1026 o con el Fiscal Adjunto de Estados Unidos designado como Coordinador de ordenadores y telecomunicaciones (CTC) de su distrito (véase introducción, pág. ix) si se desea una orientación más específica.

b) Cuando el equipo físico es simplemente un dispositivo de almacenamiento de pruebas del delito

La estrategia para realizar un registro informático cambia de manera significativa si el equipo es simplemente un dispositivo de almacenamiento de pruebas del delito. En este caso, la Norma 41(b) autoriza a los agentes a obtener una orden para requisar las pruebas electrónicas, aunque posiblemente no les autorice de forma directa a confiscar el hardware que realmente contiene dichas pruebas. Estados Unidos v. Tamura, 694 F.2d 591, 595 (9° Cir. 1982) (en el que se destaca que la causa probable para confiscar archivos concretos en papel enumerados en una orden permite técnicamente confiscar también archivos inofensivos que estén mezclados con ellos). El equipo es un mero contenedor de almacenamiento de pruebas, no la prueba propiamente dicha, lo cual no significa que el gobierno no pueda requisar el equipo: más bien significa que en general no debería hacerlo a menos que no sea viable una alternativa menos invasiva que permita la recuperación efectiva de las pruebas en la situación concreta del caso. Cf. id. en 596.

Desde el punto de vista práctico, con frecuencia la situación obligará a los investigadores a requisar el equipo y analizar su contenido en otro lugar. En primer lugar, puede llevar días o incluso semanas encontrar la información específica descrita en la orden, ya que los dispositivos informáticos de almacenamiento pueden contener cantidades ingentes de información. No es razonable esperar que los agentes dediquen más de unas cuantas horas a registrar los materiales in situ y en algunas circunstancias puede que incluso unas cuantas horas no sea un tiempo razonable, como al registrar la casa de un sospechoso. Véase Estados Unidos v. Santarelli, 778 F.2d 609, 615-16 (11° Cir. 1985). Teniendo en cuenta que los ordenadores personales vendidos en 2002 pueden almacenar aproximadamente el equivalente a treinta millones de páginas de información y que las redes pueden guardar esa cantidad multiplicada por cientos de veces (esta capacidad prácticamente se duplica todos los años), es casi imposible que los agentes lleven a cabo en el lugar un registro rápido de un ordenador en busca de datos específicos, de un archivo concreto o de una serie de archivos. Aun suponiendo que los agentes conozcan información específica de los archivos que buscan, puede que los datos tengan nombres engañosos o que estén codificados, guardados en directorios ocultos o incluido en "puntos ciegos" que un simple listado de archivos pasará por alto. Recuperar las pruebas puede exigir un análisis meticuloso por parte de un experto en el entorno controlado de un laboratorio científico.

El intentar buscar los archivos in situ puede incluso conllevar el riesgo de dañar las pruebas en determinados casos. Puede ocurrir que los agentes que realicen un registro no averigüen hasta llegar al lugar en cuestión que el ordenador utiliza un sistema operativo poco común que el especialista en tecnología desplazado hasta allí no llegue a comprender del todo. Dado que un enfoque poco elaborado a la hora de realizar un registro puede tener como consecuencia la destrucción de pruebas, la mejor estrategia puede ser trasladar el equipo físico de forma que una persona del gobierno experta en dicho sistema operativo en particular pueda analizar el ordenador posteriormente. Los registros en otro lugar también pueden resultar necesarios si los agentes tienen motivos para pensar que el ordenador puede haber sido trucado por un delincuente espabilado. Un usuario hábil técnicamente puede saber cómo trampear su ordenador con programas de autodestrucción que borren pruebas vitales si el sistema es

examinado por una persona que no sea experta. Por ejemplo, un delincuente puede desarrollar un programa muy corto que haga que el ordenador pida una contraseña periódicamente y si no se introduce la contraseña correcta en el plazo de diez segundos, se active la destrucción automática de los archivos del ordenador. En estos casos resulta más aconsejable confiscar el equipo y permitir que un experto en otro lugar desactive el programa antes de proceder al registro.

En vista de estas circunstancias, los agentes suelen plantearse intentar realizar la inspección in situ, con la idea de que si las circunstancias que allí descubran hacen que su plan sea inviable, confiscarán el equipo. Una vez en el lugar en cuestión para llevar a cabo la inspección, los agentes evalúan el hardware, el software y los recursos disponibles para determinar si es posible hacer el registro en el lugar. La estrategia de exploración dependerá en muchos casos de la sensibilidad del entorno en el que se produzca el registro. Es decir, los agentes que deseen obtener la información almacenada en la red informática de una empresa operativa intentarán en la mayoría de situaciones hacer todo lo posible por conseguirla sin tener que confiscar los ordenadores de la misma. En casos así, lo más apropiado suele ser una estrategia escalonada de registro diseñada para utilizar el enfoque menos invasivo mediante el que recuperar la información. En el Apéndice F se comentan estos enfoques. En cualquier caso, sea cual sea la estrategia elegida, se debe explicar detalladamente en la declaración jurada que acredite la solicitud de una orden.

En ocasiones, sin embargo, sí será posible realizar un registro in situ. Si se da con un empleado o un administrador de sistemas amable, puede ser que se muestre de acuerdo en localizar con exactitud un archivo o registro o incluso que disponga de una copia de seguridad reciente, lo que permitiría a los agentes obtener una copia de los archivos que buscan mientras están en el lugar. Véase por ejemplo Estados Unidos v. Longo, 70 F. Supp. 2d 225 (W.D.N.Y. 1999) (en el que se confirma la búsqueda con la asistencia del secretario del sospechoso de dos archivos informáticos específicos). Por otra parte, los agentes pueden localizar la serie de archivos en cuestión y realizar copias electrónicas o realizar una réplica de una parte del disco de almacenamiento basándose en el conocimiento de que la información está en dicha parte. Lógicamente, estas estrategias a menudo resultan insuficientes. Son relativamente pocos los casos que piden una serie limitada de archivos conocidos, ya que los registros en busca de pruebas de un delito concreto suelen ser más abiertos. Si los agentes no pueden averiguar dónde está guardada la información o por razones técnicas no son capaces de crear una réplica que funcione, al final puede que no quede otra opción que confiscar el ordenador y trasladarlo. Dado que los ordenadores personales se pueden trasladar fácilmente y registrar de una manera efectiva en otro lugar por medio de herramientas científicas especiales, es especialmente probable que los agentes confisquen este tipo de equipos en ausencia de circunstancias inusuales.

La estrategia general consiste en buscar la forma de registro más rápida y directa y menos invasiva que sea compatible con la obtención de las pruebas descritas en la orden. Esta estrategia permitirá a los agentes realizar el registro in situ en algunos casos, mientras que en otros podrán confiscar los ordenadores para analizarlos en otro lugar. La flexibilidad es la clave.

2. La Ley de Protección de la Privacidad

Si los agentes tienen motivos para creer que un registro puede desembocar en una confiscación de los materiales en relación con actividades de la Primera Enmienda, como la publicación de materiales en Internet, deben tener en cuenta la influencia de la Ley de Protección de la Privacidad ("PPA"), 42 U.S.C. § 2000aa. Todo registro informático federal que afecte a la PPA debe ser aprobado por el Departamento (Ministerio) de Justicia coordinado a través de la CCIPS en el teléfono (202) 514-1026.

En virtud de la Ley de Protección de la Privacidad ("PPA"), 42 U.S.C. § 2000aa, las fuerzas de seguridad deben adoptar medidas especiales a la hora de planificar una inspección de la que tengan razones para creer que puede derivar en la confiscación de determinados materiales conforme a la Primera Enmienda. Los registros de las fuerzas de seguridad federales que afecten a la PPA deben ser aprobadas con autoridad por un Abogado Adjunto Asistente General de la División Penal. La Sección

de Delitos Cibernéticos y Propiedad Intelectual sirve como punto de contacto para este tipo de registros relacionados con ordenadores y se debe contactar con ella directamente en el teléfono (202) 514-1026.

a) Breve historia de la Ley de Protección de la Privacidad

Antes de la sentencia del Tribunal Supremo en Warden v. Hayden, 387 U.S. 294, 309 (1967), los oficiales de las fuerzas de seguridad no podían obtener órdenes de registro para buscar y confiscar "pruebas" de un delito. Éstas sólo se permitían para confiscar contrabando, instrumentos o los frutos de la actividad delictiva. Véase Boyd v. Estados Unidos, 116 U.S. 616 (1886). En el caso Hayden, el tribunal invirtió el rumbo y concluyó que la Cuarta Enmienda permitía al gobierno obtener órdenes de registro para confiscar pruebas. Esta sentencia creó el marco para una colisión entre las fuerzas de seguridad y la prensa. Dado que los periodistas y reporteros a menudo recogen pruebas de actividades criminales al desarrollar la historia de las noticias, con frecuencia poseen pruebas de delitos que pueden resultar útiles para las investigaciones. Al liberar la Cuarta Enmienda del régimen tan restrictivo de Boyd, Hayden creó la posibilidad de que las fuerzas de seguridad pudieran utilizar las órdenes de registro para dirigirlas a la prensa con respecto a las pruebas de delitos que recogieran durante sus investigaciones y al informar de las noticias.

No tuvo que pasar mucho tiempo hasta que se produjo el primer registro de este tipo. El 12 de abril de 1971, la Oficina del Fiscal de Distrito del condado de Santa Clara, en California, obtuvo una orden para registrar las oficinas del Stanford Daily, un periódico realizado por estudiantes de la Stanford University. La oficina de la DA se encontraba investigando un choque muy violento que se había producido entre la policía y manifestantes en el Hospital de la Stanford University tres días antes. El Stanford Daily había cubierto el incidente, publicando posteriormente una edición especial en la que aparecían fotografías del altercado. La policía, creyendo que era probable que el periódico tuviera más fotografías del incidente que pudieran ayudarles a identificar a los manifestantes, obtuvo una orden y envió a cuatro oficiales de policía a registrar las oficinas del periódico en busca de más pruebas que pudieran ser de utilidad en la investigación. Los oficiales no encontraron nada. Sin embargo, un mes más tarde el Stanford Daily y sus editores interpusieron una demanda contra la policía asegurando que el registro había vulnerado los derechos que les concedían la Primera y la Cuarta Enmienda. En última instancia el caso llegó al Tribunal Supremo y en Zurcher v. Stanford Daily, 436 U.S. 547 (1978), el tribunal rechazó la demanda del periódico. Aunque el tribunal destacó que "la Cuarta Enmienda no previene ni aconseja en contra de acciones legislativas o ejecutivas para establecer protecciones no constitucionales" con respecto a registros de la prensa, concluyó que ni la Cuarta ni la Primera Enmienda prohibían dichos registros. Id. en 567.

El Congreso aprobó la PPA en 1980 en respuesta al caso del Stanford Daily. De acuerdo con el informe del Senado, la PPA protegía "a la prensa y a otras personas no sospechosas de haber cometido un crimen por medio de determinadas protecciones que no ofrecía actualmente la Cuarta Enmienda". S. Rep. N° 96-874, en 4 (1980), reimpreso en 1980 U.S.C.C.A.N. 3950. La finalidad de esta ley consistía en garantizar a los editores ciertos derechos legales para disuadir a los oficiales de las fuerzas de seguridad de que fijaran su objetivo en estos por el mero hecho de que con frecuencia recogían "pruebas" de delitos. Tal y como indica la historia de la legislación, el objeto de esta ley es restringir los registros en busca de materiales en posesión de personas implicadas en actividades de acuerdo con la Primera Enmienda pero que no sean sospechosas de participar en la actividad delictiva de la que se buscan materiales, no para limitar la potestad de los oficiales de las fuerzas de seguridad para buscar y confiscar materiales en posesión de los sospechosos de haber cometido el delito que se está investigando.

Id. en 11.

b) Condiciones de la Ley de Protección de la Privacidad

La PPA, aunque con algunas excepciones, hace que sea ilegal que un oficial del gobierno "registre o confisque" materiales siempre y cuando:

(a) dichos materiales sean "producto del trabajo" preparados, generados, redactados o creados "antes de comunicarlos al público", 42 U.S.C. § 2000aa-7(b)(1);

(b) los materiales incluyan "impresiones mentales, conclusiones o teorías" de su creador, 42 U.S.C. § 2000aa-7(b)(3); y

(c) la finalidad de los materiales sea hacerlos públicos y estén en posesión de una persona "de la que se crea razonablemente que tiene el objetivo de comunicar al público" algún tipo de "comunicado público", 42 U.S.C. §§ 2000aa-7(b)(3), 2000aa(a);

o

(a) los materiales sean "de carácter documental" y contengan información",

42 U.S.C. § 2000aa-7(a); y

(b) los materiales estén en posesión de una persona "relacionada con el objetivo de comunicar al público" algún tipo de "comunicación pública". 42 U.S.C. §§ 2000aa(b), 2000aa-7(a).

Aunque lo dictado por la PPA sea de carácter bastante general, la ley incluye varias excepciones. Un registro no infringirá la PPA si:

1) los únicos materiales registrados o confiscados son contrabando, instrumentos o el resultado de un delito, véase 42 U.S.C. § 2000aa-7(a),(b);

2) hay motivos para pensar que es necesaria la confiscación inmediata de dichos materiales para evitar muertes o lesiones personales graves, véase 42 U.S.C. §§ 2000aa(a)(2), 2000aa(b)(2);

3) hay causa probable para creer que la persona que está en posesión de dichos materiales ha cometido o está cometiendo el delito penal con el que están relacionados los materiales (excepción que, a su vez, está sujeta a varias excepciones), véase 42 U.S.C. §§ 2000aa(a)(1), 2000aa(b)(1); y

4) en una búsqueda o confiscación de "material documental" tal y como se define en § 2000aa-7(a), ha resultado inadecuada una citación o existen razones para pensar que tal citación no daría como resultado la entrega del material, véase 42 U.S.C. § 2000aa(b)(3)-(4).

La contravención de la PPA no dará como resultado la anulación de las pruebas, véase 42 U.S.C. § 2000aa-6(d), aunque sí puede derivar en daños civiles contra la soberanía por parte de los oficiales o empleados que realicen el registro. Véase § 2000aa-6(a), (e); Davis v. Gracey, 111 F.3d 1472, 1482 (10° Cir. 1997) (en el que se rechaza una demanda basada en la PPA contra oficiales municipales en calidad personal, ya que dichas demandas se deben interponer contra la "entidad gubernamental" a menos que ésta no haya renunciado a la inmunidad soberana). Si oficiales o empleados del Estado infringen la PPA y el Estado no renuncia a su inmunidad soberana y, por consiguiente, no es inmune ante una demanda, véase Barnes v. Estado de Missouri, 960 F.2d 63, 65 (8° Cir. 1992), se podrá imputar la responsabilidad a los oficiales o empleados del estado de manera individual por actos que entran dentro del ámbito de su empleo sujetos a una defensa razonable de buena fe. Véase § 2000aa-6(a)(2),(b).

c) Aplicación de la PPA a registros y confiscaciones de ordenadores

En los casos relacionados con la informática surgen con frecuencia problemas con la PPA y esto se debe a dos razones que el Congreso no podría haber previsto en 1980. En primer lugar, el uso de ordenadores personales para publicar en Internet ha ampliado exponencialmente el alcance de quién está "implicado en actividades relacionadas con la Primera Enmienda". Actualmente, cualquier persona que tenga un ordenador y acceso a Internet puede convertirse en un editor en posesión de materiales protegidos por la PPA en su ordenador.

La segunda razón para que se planteen problemas con la PPA a menudo en casos relacionados con la informática es que la redacción de la ley no excluye explícitamente la responsabilidad tras confiscaciones *secundarias* de material protegido por la PPA y dichas confiscaciones pueden producirse si los agentes registran y requisan productos de contrabando o pruebas de delitos almacenadas en un ordenador y que estén mezclados con materiales protegidos por la PPA. Por ejemplo, investigaciones de empresas ilegales que publican imágenes de pornografía infantil por Internet han revelado que dichas empresas a menudo tienen otros materiales de publicación (como pornografía para adultos) que pueden estar protegidos por la PPA. La confiscación de un ordenador para buscar elementos de contrabando tiene como consecuencia lógica la confiscación de material protegido por la PPA, ya que en los ordenadores de las empresas el contrabando está mezclado con materiales protegidos por esta ley. Si se interpretara la PPA para prohibir estas confiscaciones, no sólo impediría que las fuerzas de seguridad fijaran como objetivo editores inocentes por las pruebas que pudieran tener, sino que además obstaculizaría el registro y la confiscación del ordenador de un sospechoso de delito si el equipo incluye materiales protegidos por la PPA, aunque sea de forma secundaria.

La historia de la legislación y el texto de la PPA indican que la finalidad del Congreso fuera probablemente que esta ley se aplicara solamente cuando las fuerzas de seguridad se fijaran como objetivo de forma intencionada material de la Primera Enmienda relacionado con un delito, como en el caso del Stanford Daily. Por ejemplo, la denominada "excepción del sospechoso" anula la obligación de la PPA si "existe causa probable para pensar que la persona que está en posesión de estos materiales ha cometido o está cometiendo el delito penal *con el que están relacionados los materiales*" 42 U.S.C. § 2000aa(a)(1), § 2000aa(b)(1) (se hace hincapié en este punto). Este texto indica que el Congreso creía que el material protegido por la PPA estaría relacionado necesariamente con un delito penal, como cuando los investigadores se centran en los materiales como prueba. Sin embargo, si los agentes confiscan accidentalmente materiales protegidos por la PPA porque están mezclados en un ordenador con otros materiales que son un objetivo adecuado de las fuerzas de seguridad, los primeros no tienen por qué estar relacionados con ningún delito. Por ejemplo, estos materiales protegidos pueden ser artículos de un boletín de horticultura que simplemente resulten estar en el mismo disco duro que imágenes de pornografía infantil o registros de un plan fraudulento.

El Sexto Circuito ha sentenciado de forma explícita que la confiscación accidental de material protegido por la PPA que esté mezclado en el ordenador de un sospechoso con pruebas de un delito no da lugar a la obligación de la PPA. Guest v. Leis, 255 F.3d 325 (6° Cir. 2001), en el que se vieron envueltas dos demandas interpuestas contra el Departamento del Sheriff en el Condado de Hamilton, Ohio. Las demandas se produjeron como consecuencia de la confiscación de dos servidores que se habían utilizado para alojar dos sistemas de boletines sospechosos de albergar pruebas y elementos de contrabando relacionados con obscenidades, escuchas telefónicas, pornografía infantil, robo de tarjetas de crédito y piratería de software. El Sexto Circuito destacó que "cuando la policía ejecuta una orden de registro para buscar documentos en un ordenador, a menudo será difícil o imposible (especialmente si el propietario no coopera) separar en el ordenador los materiales constitutivos de delito de los "inocentes" en el lugar donde se realice el registro. Id. en 341-42. Teniendo en cuenta estas cuestiones pragmáticas, el tribunal negó hallar responsabilidad de la PPA por confiscaciones secundarias; una interpretación de la PPA en otro sentido "evitaría en muchos casos que la policía pudiera confiscar pruebas en un ordenador". Id. en 342. En lugar de ello, el tribunal sentenció que "cuando los materiales protegidos estén mezclados en el ordenador del sospechoso de delito con pruebas penales no protegidas por la ley, no hallaremos responsabilidad con arreglo a la PPA por la confiscación de material protegido por ésta". Id. Sin embargo, el tribunal invitado advirtió de que a pesar de que la confiscación accidental de materiales de trabajo y documentales relacionados con la PPA no infringe la ley, el análisis posterior de estos materiales probablemente esté prohibido. Id.

La decisión del Sexto Circuito en calidad de invitado corrobora que la excepción del sospechoso funciona tal y como pretendía la legislación: limitando el alcance de la protección de la PPA "a la prensa y a otras personas no sospechosas de haber cometido un delito". S. Rep. N° 96-874, en 4 (1980), reimpreso en 1980 U.S.C.C.A.N. 3950. Hay al menos otro tribunal que ha llegado a esta conclusión mediante la interpretación más general de la frase de la excepción del sospechoso "con el que están relacionados los materiales" cuando se produce una confiscación involuntaria de material mezclado. Véase Estados Unidos v. Hunter, 13 F. Supp. 2d 574, 582 (D. Vt. 1998) (en el que se concluye que el

material de un boletín semanal legal publicado por el demandado desde su despacho de abogados "estaba vinculado" con la presunta implicación del demandado en los delitos de su cliente relacionados con las drogas cuando al primero se le confiscó involuntariamente material en un registro en busca de pruebas sobre su cliente). Véase también Carpa v. Smith, 208 F.3d 220, 2000 WL 189678, en *1 (9° Cir. Feb. 8, 2000) (sin publicar) ("La Ley de Protección de la Privacidad […] no es aplicable a sospechosos de delincuencia").

La decisión del Sexto Circuito en calidad de invitado no aborda la cuestión de la mezcla de elementos si el propietario del ordenador confiscado no es sospechoso. En la única resolución publicada hasta la fecha en la que se toca este tema, un tribunal de distrito declaró responsable al Servicio Secreto de Estados Unidos por la confiscación involuntaria de material protegido por la PPA. Véase Steve Jackson Games, Inc. v. Servicio Secreto, 816 F. Supp. 432 (W.D. Tex. 1993), afirmado sobre otros motivos, 36 F.3d 457 (5° Cir. 1994).[(8)] Steve Jackson Games, Inc. ("SJG") era fundamentalmente un editor de juegos de role-play, pero también administraba una red de trece ordenadores que ofrecía a sus clientes servicio de correo electrónico, información publicada sobre los productos de SJG y los borradores de las próximas publicaciones. El Servicio Secreto, con la convicción de que el administrador del sistema de los ordenadores de SJG tenía almacenadas pruebas de delitos, obtuvo una orden y confiscó dos de los trece ordenadores conectados a la red de SJG, además de otros materiales. El Servicio Secreto no supo que los ordenadores de SJG contenían material de publicaciones hasta el día después del registro. A pesar de ello, el Servicio Secreto no devolvió los ordenadores confiscados hasta unos meses más tarde. En ningún momento sospechó que SJG estuviera implicada en el delito que se estaba investigando.

El tribunal de distrito sentenció en el caso Steve Jackson Games que el Servicio Secreto había infringido la PPA; por desgracia, es difícil discernir los matices exactos del razonamiento del tribunal. Por ejemplo, el tribunal no explicó con exactitud qué materiales confiscados por el Servicio Secreto estaban cubiertos por la PPA; en lugar de ello se limitó a enumera las propiedades que se habían requisado y concluyó que se habían obtenido algunos materiales protegidos por la PPA durante el registro. Id. en 440. Asimismo, el tribunal indicó que el registro de SJG y la confiscación inicial de su propiedad no había contravenido la PPA, pero que la retención continuada por parte del Servicio Secreto de la propiedad de SJG tras averiguar la situación de SJG como editor, y a pesar de una solicitud de SJG para que le fueran devueltas sus propiedades, constituía el origen de la vulneración de la PPA, algo que la ley propiamente dicha no parece contemplar. Véase id. en 441. El tribunal sugirió por otra parte que la sentencia podría haber sido distinta si el Servicio Secreto hubiera realizado "copias de toda la información confiscada" y hubiera devuelto los equipos tan pronto como le hubiera resultado posible, aunque no respondió a la cuestión de si habría alcanzado un resultado distinto en tal caso. Id.

La confiscación accidental de materiales protegidos por la PPA en un ordenador perteneciente a una persona no sospechosa sigue siendo un área con lagunas en la legislación, en parte porque no son frecuentes los litigios por problemas relacionados con esta ley. Desde un punto de vista práctico, los agentes pueden evitar a menudo la confiscación de materiales protegidos por la PPA del ordenador de una persona no considerada sospechosa mediante el uso de una citación en virtud de la ECPA para solicitar a dicha persona que les facilite la información deseada, tal y como se describe en el capítulo 3. Hasta la fecha, ningún otro tribunal ha optado por el enfoque sobre la PPA del caso Steve Jackson Games. Véase por ejemplo State v. One (1) Pioneer CD-ROM Changer, 891 P.2d 600, 607 (Okla. App. 1995) (en el que se cuestiona la premisa aparente de Steve Jackson Games de que la confiscación de equipos informáticos podría vulnerar la PPA por el mero hecho de que el equipo "también contenía o se utilizaba para difundir "materiales potencialmente documentales"). Por otra parte, aunque los tribunales rechazaran restringir la PPA a casos en los que las fuerzas de seguridad confisquen de manera intencionada material relacionado con la Primera Enmienda que sea prueba de un delito, también pueden concluir que otras excepciones a la PPA, como la de "contrabando o resultado de un delito", se deben interpretar de una forma tan general como hizo el tribunal invitado con la excepción del sospechoso.

Los pocos tribunales federales restantes que han resuelto pleitos civiles interpuestos con arreglo a la PPA han resuelto en contra de los demandantes sin apenas aportar análisis significativos. Véase por ejemplo Davis v. Gracey, 111 F.3d 1472, 1482 (10° Cir. 1997) (en el que se rechaza por falta de jurisdicción un pleito por la PPA interpuesto inadecuadamente contra funcionarios municipales de

forma personal); Berglund v. Ciudad de Maplewood, 173 F. Supp. 2d 935, 949-50 (D. Minn. 2001) (en el que se concluye que la confiscación por parte de la policía de una cinta de vídeo del demandado entraba dentro de las excepciones de "sospechoso criminal" y "destrucción de pruebas" a la PPA dado que la cinta podría haber contenido pruebas documentales de la conducta desordenada del demandado); DePugh v. Sutton, 917 F. Supp. 690, 696-97 (W.D. Mo. 1996) (en el que se rechaza per se una objeción con arreglo a la PPA a la confiscación de materiales relacionados con pornografía infantil ya que existía causa probable para creer que la persona que estaba en posesión de dichos materiales cometió el delito penal con el que estaban vinculados los materiales), afirmado, 104 F.3d 363 (8° Cir. 1996); Powell v. Tordoff, 911 F. Supp. 1184, 1189-90 (N.D. Iowa 1995) (en el que se rechaza una demanda en virtud de la PPA debido a que el demandante no estaba en situación de oponerse al registro y confiscación con arreglo a la Cuarta Enmienda). Véase también Lambert v. Polk County, 723 F. Supp. 128, 132 (S.D. Iowa 1989) (en el que se rechaza una demanda en virtud de la PPA tras la confiscación de una cinta de vídeo por parte de la policía, ya que los oficiales no podían pensar desde un punto de vista razonable que el dueño de la cinta tuviera el propósito de poner el material a disposición del público).

Los agentes y fiscales que tengan motivos para creer que el registro de un ordenador puede entrar en el ámbito de la PPA deben ponerse en contacto con la Sección de Delitos Cibernéticos y Propiedad Intelectual a través del teléfono (202) 514-1026 o con el CTC de su distrito (véase la introducción, pág. ix) si desea orientación específica.

3. Responsabilidad civil con arreglo a la Ley de Privacidad de las Comunicaciones Electrónicas

En aquellos casos en los que un registro pueda derivar en la confiscación accidental de cuentas de red pertenecientes a terceras partes inocentes, los agentes deben adoptar todas las medidas necesarias para proteger la integridad de las cuentas de terceros y evitar así una posible responsabilidad por la ECPA.

Cuando las fuerzas de seguridad realizan un registro de un proveedor de servicios de Internet y confisca las cuentas de clientes y abonados, estos pueden emprender acciones legales alegando que el registro contraviene la Ley de Privacidad de las Comunicaciones Electrónicas (ECPA). La ECPA rige el acceso de las fuerzas de seguridad a los contenidos de comunicaciones electrónicas almacenadas por proveedores de servicios de terceros. Véase 18 U.S.C. § 2703; capítulo 3, más abajo (en el que se comenta la Ley de Privacidad de las Comunicaciones Electrónicas). Asimismo, la ECPA incorpora una disposición penal que prohíbe el acceso no autorizado a comunicaciones electrónicas o por cable en forma de "almacenamiento electrónico". Véase 18 U.S.C. § 2701; capítulo 3, más abajo (en el que se comenta la definición de "almacenamiento electrónico").

La preocupación porque un registro ejecutado en virtud de una orden válida pueda infringir la ECPA se deriva del caso Steve Jackson Games, Inc. v. Servicio Secreto, 816 F. Supp. 432 (W.D. Tex. 1993), comentado en el apartado B.2.c más arriba. En Steve Jackson Games, el tribunal de distrito declare responsable al Servicio Secreto conforma a la ECPA tras confiscar, analizar y (en algunos casos) eliminar comunicaciones electrónicas guardadas que se habían confiscado de acuerdo con una orden de registro válida. Véase id. en 442-43. La conclusión del tribunal parece tener su origen en la falsa creencia de que la ECPA exige que las órdenes de registro cumplan también con la 18 U.S.C. § 2703(d) y los diversos requisitos de aviso de § 2703. Véase id. De hecho, la ECPA deja bien claro que § 2703(d) y los requisitos de aviso § 2703 se ven afectados únicamente si las fuerzas de seguridad no obtienen una orden de registro. Compárese 18 U.S.C. § 2703(b)(1)(A) con 18 U.S.C. § 2703(b)(1)(B). Véase el capítulo 3 en general, más abajo. En realidad, el texto de la ECPA no parece contemplar la responsabilidad civil para registros y confiscaciones autorizados por órdenes de registro válidos conforme a la Norma 41. La ECPA autoriza expresamente al gobierno a acceder a comunicaciones almacenadas en virtud de una orden emitida conforme a las Normas Federales de Procedimiento Penal, véase 18 U.S.C. § 2703(a), (b), (c)(1)(A); Davis v. Gracey, 111 F.3d 1472, 1483 (10° Cir. 1997) y la prohibición penal de § 2701 no es aplicable si el acceso está autorizado de acuerdo con § 2703. Véase 18 U.S.C. § 2701(c)(3).[(9)] Por otra parte, la confianza objetivamente razonable de buena fe en una orden, nota judicial o autorización legal constituye una protección completa ante una infracción de la

ECPA. Véase 18 U.S.C. § 2707(e); Gracey, 111 F.3d en 1484 (en el que se aplica la protección de buena fe dado que la confiscación de comunicaciones almacenadas de forma accidental durante un registro válido fue objetivamente razonable). Compárese Steve Jackson Games, 816 F. Supp. en 443 (en el que se expresa sin explicación alguna que el tribunal "niega hallar esta protección").

La mejor forma de conciliar el resultado de Steve Jackson Games con la redacción simple de la ECPA es andar con la máxima precaución cuando los agentes tengan que llevar a cabo registros de proveedores de servicios de Internet y otras terceras partes que posean comunicaciones por cable o electrónicas almacenadas. En la mayor parte de los casos los investigadores preferirán evitar un registro y confiscación completos de los ordenadores del proveedor. Si no les queda otra opción que realizar el registro, por ejemplo si se da el caso de que se sospeche que la entidad propietaria del sistema está muy implicada en la conducta delictiva, deberán tener especial cuidado. Por ejemplo, si los agentes tienen motivos para creer que pueden requisar cuentas de cliente que pertenezcan a personas inocentes pero no tienen razones para pensar que no estén almacenadas en ellas las pruebas que buscan, deberán informar al magistrado en la declaración jurada de la orden de que no registrarán dichas cuentas y deberán adoptar las medidas necesarias para garantizar la confidencialidad de las mismas en vista de las inquietudes por la privacidad expresadas por 18 U.S.C. § 2703. La salvaguarda de las cuentas de personas inocentes en ausencia de razones específicas para pensar que en ellas puede haber pruebas almacenadas satisfará las inquietudes expresadas por Steve Jackson Games. Compárese Steve Jackson Games, 816 F. Supp. en 441 (en el que se declara la responsabilidad con respecto a la ECPA debido a que los agentes leyeron comunicaciones privadas de clientes que no estaban implicados en el delito "y posteriormente eliminaron o destruyeron algunas de ellas, intencionada o accidentalmente") con Gracey, 111 F.3d en 1483 (en el que se rechaza la responsabilidad con respecto a la ECPA en la confiscación ya que los "demandantes no alegaron que los oficiales intentaron acceder o leer los correos electrónicos confiscados y los oficiales negaron cualquier interés en hacerlo").

En el caso de que los agentes crean que es posible que un hacker o administrador de sistemas haya ocultado pruebas de un delito en la cuenta de un cliente o abonado inocente, deberán actuar con cautela. Los agentes deberán informar al magistrado por medio de la declaración jurada de la necesidad de registrar la cuenta e intentarán obtener la autorización del cliente o abonado en caso de ser viable. En estos casos, los agentes deben ponerse en contacto con la Sección de Delitos Cibernéticos y Propiedad Intelectual a través del teléfono (202) 514-1026 o con el CTC de su distrito (véase la introducción, pág. ix) si desean una orientación más específica.

4. Consideración de la necesidad de varias órdenes en registros de redes

Los agentes deberán obtener varias órdenes si tienen motivos para creer que al registrar una red recuperarán datos almacenados en múltiples lugares.

La Norma Federal de Procedimiento Penal 41(a) establece que un magistrado destinado en un distrito judicial puede emitir una orden para "registrar propiedades […] dentro de su distrito" o para "registrar propiedades […] fuera de su distrito si éstas […] estaban dentro del mismo cuando se solicitó la orden pero han sido trasladadas a otro lugar antes de ejecutar la orden". El Tribunal Supremo ha concluido que "propiedad", según se describe en la Norma 41, incluye propiedades intangibles como pueden ser los datos informáticos. Véase Estados Unidos v. New York Tel. Co., 434 U.S. 159, 170 (1977). A pesar de que los tribunales no han abordado el asunto directamente, la redacción de la Norma 41 combinada con la interpretación del Tribunal Supremo del concepto de "propiedad" puede limitar los registros de datos informáticos situados en el distrito en el que se emitió la orden.[(10)] Cf. Estados Unidos v. Walters, 558 F. Supp. 726, 730 (D. Md. 1980) (en el que se sugiere tal limitación en un caso relacionado con registros telefónicos).

La limitación territorial a los registros de datos informáticos plantea muchos problemas a las fuerzas de seguridad, ya que los datos almacenados en una red informática pueden estar en cualquier parte del mundo. Por ejemplo, si un agente se dispone a registrar una oficina en Manhattan en virtud de una orden

del Distrito Sur de Nueva York, es posible que se siente delante de un terminal y acceda a información almacenada de forma remota en un ordenador situado en Nueva Jersey, California o incluso en otro país. Un único archivo descrito por la orden podría estar en cualquier lugar del planeta o dividido en varios sitios en distintos distritos o países. O lo que es peor, podría resultar imposible que los agentes supieran a la hora de ejecutar el registro si los datos que van a confiscar se han almacenado dentro o fuera del distrito. En algunos casos los agentes son capaces de averiguar dónde están los datos antes del registro, pero en otros no podrán saber el lugar de almacenamiento hasta que no hayan terminado el registro.

En el caso de que los agentes averigüen antes del registro que algunos o todos los datos descritos en la orden están almacenados en un emplazamiento diferente a aquél en el que van a realizar la inspección, la mejor medida dependerá de dónde estén guardados los datos remotos. Si los datos están en dos o más lugares dentro de Estados Unidos y sus territorios, los agentes deberán obtener órdenes adicionales para cada uno de ellos a fin de garantizar el cumplimiento de una interpretación estricta de la Norma 41(a). Por ejemplo, si los datos están almacenados en dos distritos, los agentes se verán obligados a obtener órdenes individuales de cada uno de ellos. Asimismo, deberán incluir una explicación minuciosa de la ubicación de los datos y los medios propuestos para realizar el registro en las declaraciones juradas que acompañan a las órdenes.

La cosa se complica más si se averigua antes de un registro que parte o todos los datos están almacenados remotamente fuera de Estados Unidos. Es posible que Estados Unidos tenga que emprender diversas acciones que pueden ir desde una notificación informal hasta una solicitud formal de asistencia al país en cuestión. Asimismo, algunos países pueden poner trabas a los intentos de las fuerzas de seguridad de Estados Unidos de acceder a ordenadores situados dentro de sus fronteras. Aunque para un oficial estadounidense que realice el registro dentro de Estados Unidos en virtud de una orden le pueda parecer que se trata de un asunto nacional, otros países pueden tener otra perspectiva. Los agentes y fiscales deben ponerse en contacto con la Oficina de Asuntos Internacionales por medio del teléfono (202) 514-0000 para solicitar asistencia con estas difíciles cuestiones.

Si los agentes no saben o ni siquiera pueden saber que los datos registrados desde un distrito están en realidad fuera de éste, el hecho de que las pruebas se confisquen de forma remota en otro distrito normalmente no debería dar como resultado la anulación de dichas pruebas. Hay dos motivos para esto. En primer lugar, los tribunales pueden sentenciar que los agentes situados en un distrito que registran un ordenador de dicho distrito y provocan involuntariamente que se envíe información intangible a otro distrito cumplen con la Norma 41(a). Cf. Estados Unidos v. Ramirez, 112 F.3d 849, 852 (7° Cir. 1997) (Posner, C.J.) (por el que se adopta una interpretación permisiva de las disposiciones de territorialidad del Título III); Estados Unidos v. Denman, 100 F.3d 399, 402 (5° Cir. 1996) (igual); Estados Unidos v. Rodriguez, 968 F.2d 130, 135-36 (2° Cir. 1992) (igual).

En segundo lugar, aun en el caso de que los tribunales concluyan que el registro viola la Norma 41(a), dicha infracción no derivará en la anulación de las pruebas a menos que los agentes hayan hecho caso omiso voluntaria y deliberadamente de la Norma o que la infracción ocasione un "prejuicio" en el sentido de que, en caso de haber observado la Norma, no se habría producido el registro o no habría sido tan "brusco". Véase Estados Unidos v. Burke, 517 F.2d 377, 386 (2° Cir. 1975) (Friendly, J.); Estados Unidos v. Martinez-Zayas, 857 F.2d 122, 136 (3° Cir. 1988) (se citan casos). Con arreglo a la prueba de Burke, que goza de una gran aceptación, los tribunales normalmente deniegan las demandas de anulación cuando los agentes encargados de realizar la inspección no pueden saber si ésta infringe la Norma 41 desde el punto de vista jurídico o de los hechos. Véase Martinez-Zayas, 857 F.2d en 136 (en el que se concluye que un registro pasó la prueba de Burke "debido a la situación incierta de la ley" con respecto a si la conducta infringía la Norma 41(a)). Por consiguiente, las pruebas recogidas en el registro de una red mediante el que se haya accedido a datos almacenados en varios distritos no debe ocasionar su anulación a menos que los agentes hayan hecho caso omiso de la Norma 41(a) de forma voluntaria y deliberada o que se haya generado un prejuicio. Véase Estados Unidos v. Trost, 152 F.3d 715, 722 (7° Cir. 1998) ("Resulta difícil prever una infracción de la Norma 41, un tipo de fallo que también contravenga la cláusula de la orden de la Cuarta Enmienda y que diera como resultado la anulación").

5. Órdenes para registros sorpresa

Por regla general, los agentes están obligados a anunciar su presencia y autoridad antes de ejecutar una orden de registro. Véase Wilson v. Arkansas, 514 U.S. 927, 934 (1995); 18 U.S.C. § 3109. Esta norma de "llamar para anunciarse" reduce el riesgo de violencia y destrucción de las propiedades cuando los agente lleven a cabo una inspección. Sin embargo, la norma no es absoluta. En Richards v. Wisconsin, 520 U.S. 385 (1997), el Tribunal Supremo concluyó que los agentes pueden pasar por alto este requisito si tienen una sospecha razonable de que, en una situación concreta, llamar para anunciar su presencia sería peligroso o inútil, o de que ello obstaculizaría la investigación eficaz del delito al permitir, por ejemplo, la destrucción de pruebas.

Id. en 394. El tribunal estableció que esta actuación "no es imprescindible, pero la policía deberá realizarla cuando se pueda cuestionar lo razonable de una entrada por sorpresa". Id. en 394-95. Dicha actuación cumple tanto la Cuarta Enmienda como la norma legal de llamar y anunciarse 18 U.S.C. § 3109. Véase Estados Unidos v. Ramirez, 523 U.S. 65, 71-73 (1998).

Es posible que en ocasiones los agentes tengan que realizar registros por sorpresa en casos de delitos cibernéticos, ya que un sospechoso hábil puede "trampear" su ordenador en un intento por destruir pruebas". Por ejemplo, se han conocido casos de piratas muy hábiles desde el punto de vista técnico que han utilizado "teclas de acceso rápido", programas informáticos que destruyen pruebas si se pulsa un botón especial. Si los agentes llaman a la puerta para anunciar el registro, el sospechoso no tiene más que pulsar el botón y activar el programa para destruir las pruebas.

Si los agentes tienen motivos para pensar que anunciar su presencia permitiría la destrucción de pruebas, sería peligroso o inútil, pueden solicitar al juez que emita una orden para realizar un registro sorpresa. Sin embargo, la ausencia de una autorización judicial para pasar por alto la norma de llamar y anunciarse no impide que los agentes no puedan llevar a cabo una inspección por sorpresa. Puede ocurrir que a los agentes se les olvide solicitar una orden de este tipo o simplemente puede ocurrir que no tengan una sospecha razonable de que se vayan a destruir pruebas hasta el momento de realizar el registro. En Richards, el Tribunal Supremo aclaró que "el carácter razonable de la decisión del oficial [de pasar por alto la norma de llamar y anunciarse] […] se debe evaluar en el momento de la entrada" en el lugar que se vaya a examinar. Richards, 520 U.S. en 395. Por lo tanto, los agentes pueden "ejercer su juicio independiente" y resolver llevar a cabo una inspección por sorpresa en el momento de ejecutarla, a pesar de no haber solicitado tal autoridad al juez o aunque el magistrado haya rechazado específicamente autorizar un registro por sorpresa. Id. en 396 n.7. La cuestión en estos casos es si los agentes albergaban "una sospecha razonable de que anunciar su presencia llamando a la puerta, en una situación particular, sería peligroso o inútil o que obstaculizaría la investigación eficaz del delito al permitir, por ejemplo, la destrucción de pruebas". Id. en 394.

6. Registros rápidos y tentativos

Si se cumplen determinadas condiciones, un tribunal puede autorizar las denominadas "órdenes de entrada subrepticia" o "rápida y tentativa" que eximen a los agentes de la obligación de notificar a las personas cuyas instalaciones se van a registrar en el momento de hacerlo. En virtud de 18 U.S.C. § 3103a, en la versión enmendada por la Ley USA PATRIOT de 2001 § 213, Pub. L. N° 107-56, 115 Stat. 272 (2001), un tribunal puede conceder la demora de notificación en relación con la ejecución de una orden de registro si halla "causa razonable" para creer que la comunicación de la ejecución de la orden puede ocasionar alguna de las consecuencias adversas enumeradas en 18 U.S.C. § 2705: que se ponga en peligro la vida o la integridad física de una persona, huída del proceso judicial, manipulación de pruebas, intimidación de testigos o cualquier otra situación que pueda poner en peligro una investigación o demorar indebidamente un juicio. Esta norma puede reducir algunas de las incoherencias entre jurisdicciones en las normas que rigen las órdenes rápidas y tentativas que existían antes de la Ley PATRIOT. Compárese Estados Unidos v. Simons, 206 F.3d 392, 403 (4° Cir. 2000) (la demora de 45 días en notificar la ejecución de la orden no hace que el registro sea inconstitucional) con Estados Unidos v. Freitas, 800 F.2d 1451, 1456 (9° Cir. 1986) (orden irregular desde el punto de vista constitucional por no prever explícitamente la notificación dentro de un "plazo de tiempo razonable, pero breve").

Asimismo, conforme a la sección 3103a, las autoridades de las fuerzas de seguridad deben realizar la notificación retrasada dentro de un "plazo razonable" tras la ejecución de una orden, si bien el tribunal puede demorarla aún más por una causa justificada. La expresión "un plazo razonable" es una norma flexible para cumplir las circunstancias de cada caso. Cf. Estados Unidos v. Villegas, 899 F.2d 1324, 1337 (2° Cir. 1990) (en el que se destacada antes de la enmienda de la sección 3103a que "lo que constituye un plazo razonable dependerá de la situación de cada caso concreto"). Los tribunales que resolvieron acerca de este asunto antes de la enmienda de la ley emitieron sentencias diferentes sobre qué periodo de demora es "razonable". Estados Unidos v. Simons, 206 F.3d 392, 403 (4° Cir. 2000) (la demora de 45 días en notificar la ejecución de la orden no hace que el registro sea inconstitucional); Villegas, 899 F.2d en 1337 (el retraso inicial de siete días es razonable, con posibilidad de prórroga); Estados Unidos v. Freitas, 800 F.2d 1451, 1456 (9° Cir. 1986) ("Dicho plazo no deberá ser superior a siete días excepto en caso de que una razón extraordinaria así lo justifique").

La disposición distingue entre el retraso en la notificación de un *registro* y en la de una *confiscación*. En realidad, a menos que el tribunal considere una "necesidad razonable" para una confiscación, las órdenes emitidas en virtud de esta sección deben prohibir requisar toda propiedad tangible, comunicación por cable o electrónica o información telefónica o electrónica almacenada (excepto en los casos expresados en el capítulo 121). El Congreso pretendió que si los investigadores tenían la intención de realizar copias furtivas de la información almacenada en el ordenador de un sospechoso, estos tuvieran que obtener la autorización previa del tribunal.

Los fiscales deben ser discretos y obtener la aprobación de un oficial de supervisión de su oficina antes de solicitar órdenes de notificación demorada. Asimismo, se deben adoptar todas las medidas necesarias para garantizar que el período de demora sea lo más breve posible, dentro de lo razonable. Por otra parte, se deberá notificar a la Oficina Ejecutiva de Fiscales de Estados Unidos acerca de dichas órdenes. Para más información con respecto a esta disposición, los fiscales e investigadores deben ponerse en contacto con la Oficina de Operaciones de Seguridad, División Criminal, a través de los teléfonos (202) 514-0746 ó (202) 514-3684.

7. Documentos con privilegios

Los agentes deberán extremar las precauciones a la hora de planificar un registro informático que pueda derivar en la confiscación de documentos que gocen de privilegios jurídicos, como pueden ser registros médicos o comunicaciones entre un abogado y sus clientes. Hay que tener en cuenta dos factores: en primer lugar, los agentes deben asegurarse de que el registro no infrinja los reglamentos del Fiscal General relativos a la obtención de información confidencial de terceras partes neutrales. A continuación, deben desarrollar una estrategia para analizar los archivos informáticos requisados después del registro de forma que no se infrinjan los privilegios.

a) Reglamentos del Fiscal General en relación con registros de abogados, médicos y religiosos neutrales

Los agentes deben tener especial cuidado si se plantean registrar el despacho de un médico, de un abogado o de un religioso que no esté implicado en el delito que se esté investigando. Siguiendo las instrucciones del Congreso, el Fiscal General ha publicado unas pautas para aquellos oficiales federales que deseen obtener material documental de este tipo de terceras partes. Véase 42 U.S.C. § 2000aa-11(a); 28 C.F.R. § 59.4(b). Conforme a estas normas, los oficiales federales de las fuerzas de seguridad no deberán utilizar una orden de registro para obtener materiales documentales que se crean en posesión privada de un médico, abogado o religioso neutral si el material buscado o que probablemente se vaya a analizar durante la ejecución de la orden contiene información sobre pacientes, clientes o feligreses. 28 C.F.R. § 59.4(b). La normativa incluye una excepción muy limitada. Se puede utilizar una orden de registro si el uso de medios menos invasivos puede poner seriamente en peligro la disponibilidad o utilidad de los materiales que se van a buscar, si el acceso a los materiales documentales es muy importante para la investigación y si la solicitud de la orden es una recomendación del Fiscal General de Estados Unidos y ha sido aprobada por el Fiscal Adjunto Asistente General que corresponda. Véase 28 C.F.R. § 59.4(b)(1) y (2).

Al planificar el registro del despacho de un abogado que esté siendo investigado, los agentes deben seguir las pautas descritas en el Manual de Fiscal General de Estados Unidos, así como consultar a la Oficina de Operaciones de Seguridad por medio del número de teléfono (202) 514-3684. Véase el Manual de Fiscal General de Estados Unidos, § 9-13.420 (1997).

b) Estrategias para el análisis de archivos informáticos que gocen de privilegios

Los agentes que estén considerando realizar una inspección que pueda dar como resultado la confiscación de archivos informáticos protegidos por privilegios jurídicos deben desarrollar una estrategia post-confiscación para aislar dichos archivos, estrategia que habrán de describir en la declaración jurada.

Si los agentes requisan un ordenador que contenga archivos protegidos por privilegios, una tercera parte que sea digna de confianza deberá filtrar los archivos para separar los que entran dentro del alcance de la orden de aquellos otros que contengan material protegido. Una vez revisados los archivos, la tercera parte facilitará los que entren en el primer grupo al equipo encargado del proceso penal. Las prácticas más adecuadas para determinar quién filtrará los archivos varían entre los distintos tribunales. No obstante, por lo general existen tres opciones: en primer lugar, el propio tribunal puede revisar los archivos en privado. En segundo lugar, el juez principal puede designar a una tercera parte neutral que recibe el nombre de "maestro especial" para que lleve a cabo la labor de revisión de los archivos. Por último, se puede formar un "equipo objetivo o de privilegio" con fiscales o agentes que no estén trabajando en el caso para que ayuden a ejecutar el registro y revisen los archivos posteriormente. El equipo objetivo fijarán la denominada "muralla china" entre las pruebas y el equipo encargado del proceso judicial y solamente permitirán que pasen la muralla los archivos que no estén protegidos por privilegios y que entren dentro del alcance de la orden.

Teniendo en cuenta que un solo ordenador puede guardar millones de archivos, rara vez optarán los jueces por acometer la revisión de los archivos informáticos en privado. Véase Black v. Estados Unidos, 172 F.R.D. 511, 516-17 (S.D. Fla. 1997) (en el que se acepta la revisión en privado en situaciones inusuales); Estados Unidos v. Skeddle, 989 F. Supp. 890, 893 (N.D. Ohio 1997) (en el que se rechaza la revisión en privado). En lugar de ello, la opción más habitual es la de utilizar un equipo objetivo y un maestro especial. Si el tribunal lo autoriza, la mayoría de los fiscales prefieren la primera de las opciones. Normalmente, un equipo objetivo puede filtrar los archivos informáticos confiscados muy rápidamente, mientras que a los maestros especiales con frecuencia les lleva años concluir su revisión. Véase Black, 172 F.R.D. en 514 n.4. Por el contrario, hay algunos tribunales que se han mostrado en desacuerdo con estos equipos. Véase Estados Unidos v. Neill, 952 F. Supp. 834, 841 (D.D.C. 1997); Estados Unidos v. Hunter, 13 F. Supp. 2d 574, 583 n.2 (D. Vt. 1998) (en el que se expresa que "puede ser preferible" la revisión por parte de un magistrado o maestro especial antes que delegar esta labor en un equipo objetivo) (se cita la orden de registro In re, 153 F.R.D. 55, 59 (S.D.N.Y. 1994)).

A pesar de que no se ha fijado una norma, los tribunales han indicado por lo general que las pruebas aisladas por un equipo objetivo serán admisibles solamente si el gobierno demuestra que sus procedimientos han protegido convenientemente los derechos del demandado y no se ha generado prejuicio. Véase por ejemplo Neill, 952 F. Supp. en 840-42; Hunter, 13 F. Supp. 2d en 583. Un posible enfoque para limitar la cantidad de material en disputa potencialmente protegido por privilegios es pedir al consejo de la defensa que revise el resultado del equipo objetivo para que identifique aquellos documentos para los que pretenda presentar una demanda de privilegio. De esta manera no se tendrán que litigar los archivos identificados por este método y que no parezcan relevantes para la investigación. A pesar de que este enfoque puede no ser adecuado en todos los casos, los magistrados pueden apreciar el hecho de que se le ha dado la oportunidad al consejo de la defensa de identificar posibles demandas antes de que el tribunal resuelva qué debe proporcionar al equipo encargado del proceso judicial.

En situaciones especiales, el tribunal puede concluir que no sería adecuado un equipo objetivo y designar en cambio a un maestro especial para que inspeccione los archivos. Véase por ejemplo Estados Unidos v. Abbell, 914 F. Supp. 519 (S.D. Fla. 1995); DeMassa v. Nunez, 747 F.2d 1283 (9° Cir. 1984). En todo caso, la autoridad que se ocupe del análisis necesitará casi con toda seguridad la ayuda de un

experto técnico neutral para la clasificación, identificación y análisis de las pruebas digitales para el proceso de revisión.

[Índice]

C. Redacción de la orden y de la declaración jurada

Los oficiales de las fuerzas de seguridad deben redactar dos documentos para obtener una orden de registro de un magistrado. El primero de ellos es una declaración jurada en la que se explique (conforme a determinados mínimos) el motivo que el deponente cree que justifica el registro por causa probable. El segundo es la orden propuesta propiamente dicha. La orden propuesta suele ser un impreso de una página, más los documentos que se adjunten como referencia, en el que se describe el lugar que se va a registrar y las personas u objetos que se van a detener o confiscar. El magistrado firmará la orden si está de acuerdo en que la declaración establece una causa probable y que las descripciones que aparecen en la orden propuesta acerca del lugar que se va a registrar y de los objetos que se van a requisar son convenientemente concretas. Con arreglo a las Normas Federales de Procedimiento Penal, los oficiales deben ejecutar la orden en el plazo de diez días a partir de que se firme. Véase la Norma Federal de Procedimiento Penal 41(b).

En general, la elaboración de la orden y de la declaración jurada implica tres pasos. Primeramente, la orden (y/o los documentos que se vayan a adjuntar) deben describir de forma precisa y concreta la propiedad que se va a confiscar. A continuación, la declaración debe establecer la causa probable. Por último, en la declaración se incluirá una explicación de la estrategia de inspección. A continuación se comentan estos tres componentes.

Paso 1: Descripción precisa y concreta de la propiedad que se va a confiscar en la orden y/o en los documentos anexos a la misma

a. General

Los agentes deben prestar especial atención a la hora de describir los archivos informáticos o los equipos que se van a confiscar, ya sea en la propia orden o, lo más probable, en un documento adjunto a la orden como referencia. La Cuarta Enmienda exige que toda orden debe "describir concretamente […] los […] objetos que se vayan a confiscar". Constitución de Estados Unidos, IV Enmienda. El requisito de la concreción evita que las fuerzas de seguridad redacten "órdenes generales" que permitan "hurgar con afán de investigación" entre las pertenencias de una persona en busca de pruebas de un delito. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

Este requisito comprende dos elementos distintos. Véase Estados Unidos v. Upham, 168 F.3d 532, 535 (1° Cir. 1999). En primer lugar, la orden debe describir los objetos que se van a confiscar con un lenguaje lo suficientemente preciso como para que indique a los oficiales cómo separar convenientemente los artículos susceptibles de ser confiscados de los irrelevantes. Véase Marron v. Estados Unidos, 275 U.S. 192, 296 (1925) ("En lo referente a lo que se va a requisar, no se deja nada al criterio del oficial que ejecute la orden"); Davis v. Gracey, 111 F.3d 1472, 1478 (10° Cir. 1997). En segundo lugar, la descripción de los objetos no debe ser tan amplia que incluya artículos que no se deban requisar. Véase Upham, 168 F.3d en 535. Dicho de otra manera, la descripción de los objetos que se vayan a confiscar que figure en la orden se ha de limitar el alcance de la causa probable establecida en la orden. Véase Investigación In re del Gran Jurado en Relación con Solid State Devices, 130 F.3d 853, 857 (9° Cir. 1997). En su conjunto, estos elementos prohíben a los agentes obtener "órdenes generales" y les obliga en cambio a realizar confiscaciones restringidas cuya finalidad es "reducir al mínimo las intrusiones de la privacidad sin una orden". Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

b. Órdenes para confiscar equipos frente a órdenes para confiscar información

Si el equipo informático es un objeto de contrabando, prueba, resultado o instrumento de un delito, en la orden se deberá describir el equipo en sí. Si la causa probable sólo atañe a la información, en cambio, la orden tendrá que describir la información, en lugar de los dispositivos físicos de almacenamiento en los que pueda estar almacenada.

La decisión más importante que deben tomar los agentes a la hora de describir la propiedad en la orden es si la propiedad confiscable conforme a la Norma 41 es el equipo informático en sí o simplemente la información que contiene. Si el equipo informático es un objeto de contrabando, el instrumento o la prueba de un delito, la orden se deberá centrar en el propio equipo y no en la información que contenga. En ella se describirá el hardware y se indicará que éste va a ser confiscado. Véase por ejemplo Davis v. Gracey, 111 F.3d 1472, 1480 (10° Cir. 1997) (la confiscación de un "equipo" informático utilizado para guardar pornografía obscena fue correcta dado que el ordenador era un instrumento). Sin embargo, si la causa probable está relacionada total o parcialmente con la información almacenada en el ordenador, la orden deberá centrarse en el contenido de los archivos correspondientes en lugar de en los dispositivos de almacenamiento que los contengan. Véase por ejemplo Estados Unidos v. Gawrysiak, 972 F. Supp. 853, 860 (D.N.J. 1997), afirmado, 178 F.3d 1281 (3° Cir. 1999) (en el que se confirma la confiscación de "registros entre los que se incluye información y/o datos almacenados en forma de codificación magnética o electrónica en medios informáticos […] que constituyen pruebas" de los delitos federales mencionados). La orden debe describir la información en función de su contenido (por ejemplo, prueba de un fraude) y a continuación solicitar a la autoridad que requise la información independientemente de la forma en la que esté almacenada. Para determinar si la orden tiene que describir el equipo físico o la información que contiene, los agentes han de consultar el Apéndice F y definir si el hardware propiamente dicho constituye una prueba, un elemento de contrabando o un instrumento que pueda ser confiscable de acuerdo con la Norma 41(a).

A la hora de realizar una búsqueda de información, los agentes han de pararse a considerar qué información precisan exactamente. La información puede ser muy limitada (un archivo o informe específico, por ejemplo) o bastante amplia (todos los registros relacionados con un plan elaborado de fraude). Cada orden se tiene que adaptar a las necesidades de cada registro. La orden debe describir la información que se va a confiscar y a continuación solicitar a la autoridad que requise la información independientemente de la forma en la que esté almacenada (ya sea electrónica o no).

Los agentes deben tener especial cautela cuando soliciten autoridad para confiscar una amplia gama de información. Esto ocurre con frecuencia cuando planean inspeccionar los ordenadores de una empresa. Véase por ejemplo Estados Unidos v. Leary, 846 F.2d 592, 600-04 (10° Cir. 1988). No pueden simplemente solicitar permiso para confiscar "todos los registros" de una empresa operativa a menos que tengan una causa probable para pensar que la actividad delictiva que se está investigando se desarrolle en toda la compañía. Véase Estados Unidos v. Ford, 184 F.3d 566, 576 (6° Cir. 1999) (se citan casos); Investigación In re del Gran Jurado en Relación con Solid State Devices, 130 F.3d 853, 857 (9° Cir. 1997). En lugar de ello, la descripción de los archivos que se vayan a confiscar deberá incluir frases restrictivas que puedan modificar y limitar la inspección de "todos los archivos". Por ejemplo, los agentes pueden especificar el delito que se está investigando, el objetivo de la investigación, si se conoce, y el marco temporal de los archivos relacionados. Véase por ejemplo Estados Unidos v. Kow, 58 F.3d 423, 427 (9° Cir. 1995) (en el que se invalida una orden por no definir el delito o limitar la confiscación a los documentos redactados durante el marco temporal que se estaba investigando); Ford, 184 F.3d en 576 ("No limitar términos descriptivos amplios en fechas relevantes, cuando la policía disponga de dichas fechas, hará que una orden sea demasiado general"); En el caso de la solicitud de la Lafayette Academy, 610 F.2d 1, 3-4, 4 n.4 (1° Cir. 1979); Estados Unidos v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (en el que se concluye que la orden para requisar "todos los ordenadores" no es lo suficientemente concreta, puesto que la descripción "no indicaba los delitos específicos por los que se buscaba el ordenador, ni se incorporaban como referencia declaraciones acreditativas ni las restricciones incluidas en las instrucciones de registro").

A la vista de estos casos, los agentes deben limitar los registros "de todos los archivos" con lenguaje restrictivo cuando sea necesario y procedente. Un enfoque eficaz consiste en comenzar con una descripción "de todos los archivos": añadir lenguaje restrictivo describiendo el delito, los sospechosos y

el período de tiempo en cuestión si procede, incluir ejemplos concretos de los archivos que se vayan a confiscar y a continuación indicar que estos se pueden requisar en cualquier formato, sea electrónico o no. Si se va a redactar una orden para registrar un ordenador en una empresa para buscar pruebas de un delito de tráfico de drogas, por ejemplo, los agentes pueden describir la propiedad que se va a confiscar del modo siguiente:

Todos los registros relacionados con la infracción de 21 U.S.C. § 841(a) (tráfico de estupefacientes) y/o 21 U.S.C. § 846 (conspiración para el tráfico de estupefacientes) que impliquen [al sospechoso] desde el 1 de enero de 1996, incluyendo listas de clientes e información identificativa relacionada; tipos, cantidades y precios de drogas con las que se haya traficado, así como fechas, lugares y cantidades de transacciones específicas; toda información relativa al origen de los estupefacientes (incluyendo nombres, direcciones, números de teléfono y cualquier otra información identificativa); toda información que dé cuenta de las actividades o los viajes [del sospechoso] desde 1995 hasta la actualidad; todos los registros bancarios, cheques, liquidaciones de tarjetas de crédito, información de cuentas y otros registros financieros.

Los términos "registros" e "información" incluyen todos los elementos anteriores de pruebas estén en el formato que estén e independientemente del medio mediante el cual se hayan creado o almacenado, incluyendo cualquier forma eléctrica, electrónica o magnética (como información en un dispositivo de almacenamiento electrónico o magnético, incluyendo disquetes, discos duros, discos Zip, CD-ROM, discos ópticos, cintas de seguridad, memoria de impresora, tarjetas inteligentes, dispositivos de almacenamiento USB, calculadoras de memoria, buscas, asistentes digitales personales como ordenadores Palm Pilot, así como impresiones y lecturas de cualquier dispositivo de almacenamiento magnético); cualquier formato manual (como escritura, dibujo o pintura); cualquier forma mecánica (como impresión o mecanografiado) y cualquier forma fotográfica (como en microfilm, impresiones, diapositivas, negativos, cintas de vídeo, películas o fotocopias).

Esta redacción describe el tipo general de información que se va a confiscar ("todos los registros"), lo restringe en la medida de lo posible (sólo aquellos registros relacionados con las actividades de tráfico de estupefacientes del demandado desde 1995), ofrece ejemplos de los tipos de registros buscados (como listas de clientes y datos bancarios) y por último explica los distintos formatos en que pueden estar los registros (incluyendo electrónicos y no electrónicos).

Lógicamente, no es necesario que los agentes sigan este enfoque en todos los casos; la revisión judicial de las órdenes de registro obedece al "sentido común" y es de "carácter práctico", más que "demasiado técnica". Estados Unidos v. Ventresca, 380 U.S. 102, 108 (1965). Si los agentes no pueden saber la forma exacta en la que estarán los registros antes de realizar la inspección, deberá bastar con una descripción genérica. Véase Estados Unidos v. Logan, 250 F.3d 350, 365 (6° Cir. 2001) (en el que se aprueba una orden con una redacción muy general y se destaca que "la naturaleza general de la misma" era apropiada teniendo en cuenta las circunstancias de la investigación); Davis v. Gracey, 111 F.3d 1472, 1478 (10° Cir. 1997) ("Incluso una orden en la que se describan los artículos que se van a confiscar mediante términos amplios o genéricos puede ser válida si la descripción es tan específica como lo permitan las circunstancias y el tipo de actividad que se esté investigando"). (se omiten las citas internas); Estados Unidos v. Lacy, 119 F.3d 742, 746-47 (9° Cir. 1997) (en el que se concluye que la descripción general del equipo informático que se va a confiscar era suficiente al no haber "modo alguno de especificar qué hardware o software había que requisar para recuperar las imágenes de forma precisa"); Estados Unidos v. London, 66 F.3d 1227, 1238 (1° Cir. 1995) (en el que se destaca que si el demandado "gestionaba una compleja empresa criminal en la que mezclaba documentos "inocentes" con otros inocentes en apariencia que, en realidad, registraban transacciones ilegales [...], habría sido muy difícil que el magistrado utilizara un lenguaje más restrictivo al redactar la orden y que los oficiales encargados de ejecutarla hubieran sido más selectivos a la hora de definir lo que se debía requisar"); Estados Unidos v. Sharfman, 448 F.2d 1352, 1354-55 (2° Cir. 1971); Gawrysiak, 972 F. Supp. en 861. En ocasiones, las órdenes autorizan la confiscación de todos los registros en relación con un delito concreto. Véase London, 66 F.3d en 1238 (en el que se confirma la inspección en busca de "libros y registros […] y cualquier otro documento […] que aluda a las apuestas ilegales"); Estados Unidos v. Riley, 906 F.2d 841, 844-45 (2° Cir. 1990) (en el que se confirma la confiscación de objetos que constituyen una prueba de los delitos de conspiración para distribuir sustancias controladas"); Estados

Unidos v. Wayne, 903 F.2d 1188, 1195 (8° Cir. 1990) (en el que se confirma una inspección en busca de "documentos y materiales que puedan estar asociados al […] contrabando [narcóticos]"). En determinadas circunstancias puede incluso ser apropiada una inspección "de todos los registros". Véase también Estados Unidos v. Hargus, 128 F.3d 1358, 1362-63 (10° Cir. 1997) (en el que se confirma la confiscación de "todo registro relacionado con la empresa" que se está investigando por fraude postal y blanqueo de capitales).

c. Defensa de las órdenes de registro informático frente a recursos fundados en la descripción de los "objetos confiscables"

Las órdenes de registro pueden verse expuestas a un recurso si la descripción de los "objetos confiscables" no cumple plenamente con las prácticas mencionadas anteriormente. Hay dos tipos de recursos que se producen con especial frecuencia con respecto al alcance de las órdenes. En el primero de ellos, el demandado puede reivindicar que una orden no es lo suficientemente concreta si autoriza la confiscación de hardware aunque la declaración jurada solamente establezca causa probable para requisar información. En segundo lugar, puede alegar que los agentes se extralimitaron con respecto al alcance de la orden al requisar equipos informáticos si en ésta no se expresa de forma explícita que la información que se va a confiscar puede estar en formato electrónico. En el primero de los recursos se aduce que la descripción de la propiedad confiscable era demasiado general, mientras que en el segundo la alegación consiste en decir que no lo era lo suficiente.

1) La orden autoriza a requisar hardware pero en la declaración jurada únicamente se establece causa probable para confiscar información

En ocasiones puede ocurrir que una orden de registro informático autorice la confiscación de hardware si la causa probable de la declaración jurada está relacionada solamente con los archivos que contenga dicho hardware. Por poner un ejemplo, un grupo de agentes puede tener una causa probable para creer que un sospechoso está en posesión de pruebas de un fraude y, por tanto, puede redactar la orden que les autorice a requisar el equipo informático del demandado en lugar de los datos almacenados en el mismo. Desde una perspectiva práctica, una descripción así tiene sentido en tanto en cuanto describe de manera precisa lo que van a hacer los agentes en el momento de ejecutar la orden, esto es, confiscar el equipo. No obstante, desde un punto de vista jurídico, la descripción no es tan ideal: es posible argüir que el equipo *propiamente dicho* no constituye una prueba del delito, un instrumento o un artículo de contrabando que pueda ser requisado de conformidad con la Norma 41(a). Véase Apéndice F; cf. Citación Duces Tecum In re del Gran Jurado, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (en la que se concluye que una citación que solicitaba la entrega de hardware informático en lugar de la información que contenía era irrazonablemente general conforme a la Norma Federal de Procedimiento Penal 17(c)). El equipo físico simplemente guarda la información de la que los agentes tienen causa probable para confiscar. A pesar de que puede ser necesario que los agentes tengan que confiscar el equipo a fin de obtener los archivos que contiene y que es posible que estos archivos no existan separadamente de un medio de almacenamiento, la mejor práctica consiste en describir la información en lugar del equipo en la orden. Si los agentes obtienen una orden que les autorice a requisar el equipo, el demandado puede alegar que la descripción de la propiedad confiscable es demasiado general. Véase por ejemplo Davis v. Gracey, 111 F.3d 1472, 1479 (10° Cir. 1997).[(11)]

Hasta la fecha, los tribunales han adoptado una postura indulgente al hacer frente a esta alegación. Por lo general han concluido que las descripciones de equipos pueden satisfacer el requisito de la concreción en tanto en cuanto exista la probabilidad razonable de que el análisis posterior del equipo incautado ofrezca pruebas de un delito. Véase por ejemplo Estados Unidos v. Hay, 231 F.3d 630, 634 (9° Cir. 2000) (en el que se confirma la confiscación de "hardware informático" en busca de material que contenga pornografía infantil); Estados Unidos v. Campos, 221 F.3d 1143, 1147 (10° Cir. 2000) (en el que se confirma la confiscación de "equipos informáticos que sean o puedan ser utilizados para mostrar visualmente pornografía infantil" y se destaca que en la declaración adjunta que acompaña a la orden se explica por qué sería necesario confiscar los equipos y analizarlos en otro lugar debido a las imágenes que contenían); Estados Unidos v. Upham, 168 F.3d 532, 535 (1° Cir. 1999) (en el que se confirma la confiscación de "todo software y hardware informático, […] discos de ordenador, unidades de disco" en un caso de investigación de pornografía infantil ya que "desde un punto de vista práctico,

la confiscación y análisis posterior en otro lugar del ordenador y de todos los discos disponibles era prácticamente el registro y confiscación más restringido que se podía definir y que tuviera una probabilidad razonable de obtener las imágenes [que se estaban buscando]"); Estados Unidos v. Lacy, 119 F.3d 742, 746 (9° Cir. 1997) (una orden que permitía la confiscación indiscriminada de equipos informáticos del piso del demandado no era lo suficientemente concreta si había causa probable para pensar que el ordenador contenía pruebas de delitos relacionados con pornografía infantil); Estados Unidos v. Henson, 848 F.2d 1374, 1382-83 (6° Cir. 1988) (en el que se permite la confiscación de "ordenador[es], terminales informáticos, […] cables, impresoras, discos, disquetes [y] cintas" que puedan alojar pruebas del delito de manipulación de un cuentakilómetros por parte del demandado, ya que este lenguaje "está dirigido a artículos que puedan ofrecer información sobre la implicación [del demandado] en el […] delito, por lo que no autorizaba a los oficiales a requisar más de lo que fuera razonable con arreglo a las circunstancias"); Estados Unidos v. Albert, 195 F. Supp. 2d 267, 275-76 (D. Mass. 2002) (en el que se confirma una orden para confiscar un equipo informático y todo el software y dispositivos de almacenamiento relacionados debido a que una inspección tan general es "el único modo práctico" de obtener imágenes de pornografía infantil). Cf. Estados Unidos v. Lamb, 945 F. Supp. 441, 458-59 (N.D.N.Y. 1996) (no lo suficientemente general como para solicitar "todos los archivos almacenados" en una cuenta de red AOL al inspeccionar la cuenta en busca de pornografía obscena ya que, desde un punto de vista práctico, es necesario revisar todos los archivos para determinar cuáles de ellos contienen pornografía).

A pesar de estas resoluciones, los agentes deben observar las prescripciones técnicas de la Norma 41 a la hora de describir la "propiedad que se va a confiscar" en una orden de registro. Si tal propiedad es información, en la orden se habrá de describir la información que se va a requisar, en lugar del dispositivo donde esté almacenada. Lógicamente, la confiscación de equipos informáticos no tiene por qué ser necesariamente inadecuada. Por ejemplo, si la información que se va a requisar es contrabando (como en el caso de pornografía infantil), el contenedor en sí se puede confiscar como un instrumento. Véase Gracey, 111 F.3d en 1480 (la confiscación de "equipamiento" informático fue adecuada en un caso relacionado con obscenidad porque el hardware era un instrumento del delito).

2) Los agentes se incautan de datos y equipos informáticos pero la orden no autoriza expresamente su confiscación

En ocasiones las órdenes no mencionan que la información descrita en ellas puede aparecer en formato electrónico. Por ejemplo, una orden en busca de "todos los registros" relativos a un delito puede enumerar documentos en papel pero olvidar hacer mención al hecho de que los registros pueden estar almacenados en un ordenador. Los oficiales que ejecuten el registro y encuentren equipos informáticos pueden no saber si la orden les autoriza a confiscar los ordenadores. Si optan por hacerlo, el consejo de la defensa puede interponer una demanda para anular las pruebas alegando que los ordenadores requisados quedaban fuera del alcance de la orden.

Normalmente los tribunales han permitido a los agentes incautarse de equipos informáticos siempre y cuando tuvieran motivos razonables para creer que los archivos mencionados en la orden pudieran estar almacenados en ellos, independientemente de si la orden expresa explícitamente que la información puede estar almacenada en formato electrónico. Véase por ejemplo Estados Unidos v. Musson, 650 F. Supp. 525, 532 (D. Colo. 1986). Tal y como lo expuso el Décimo Circuito en Estados Unidos v. Reyes, 798 F.2d 380, 383 (10° Cir. 1986), "en la era de la tecnología moderna y de la disponibilidad comercial de diversas formas de artículos, no se puede esperar que se describa con exactitud la forma precisa que adoptarán los registros". Por consiguiente, lo importante es la esencia de la prueba, no su forma, y los tribunales respetarán una interpretación razonable del oficial que ejecute la orden acerca de qué propiedades se deben confiscar para obtener las pruebas descritas en la misma. Véase Estados Unidos v. Hill, 19 F.3d 984, 987-89 (5° Cir. 1994); Hessel v. O'Hearn, 977 F.2d 299 (7° Cir. 1992); Estados Unidos v. Word, 806 F.2d 658, 661 (6° Cir. 1986); Estados Unidos v. Gomez-Soto, 723 F.2d 649, 655 (9° Cir. 1984) ("El hecho de que en la orden no se prevea el contenedor concreto en el que se puede encontrar el material buscado no es definitivo"). Véase también Estados Unidos v. Abbell, 963 F. Supp. 1178, 1997 (S.D. Fla. 1997) (en el que se destaca que los agentes pueden confiscar de manera legítima "documentos que entren dentro del alcance de la orden, aun en el caso de que no se hayan identificado específicamente").

3) Medidas generales de defensa ante recursos contra órdenes de registros informáticos basados en la descripción de los "objetos confiscables"

Aquellos fiscales que se enfrenten a alegaciones con respecto a la concreción de una orden de registro informático, tienen a su disposición numerosos argumentos adicionales que pueden salvar órdenes mal redactadas. En primer lugar, pueden aducir que los agentes que ejecutaron la orden creían objetivamente y de forma razonable que la orden era lo suficientemente concreta. Véase Estados Unidos v. Leon, 468 U.S. 897, 922 (1984); Massachusetts v. Shepard, 468 U.S. 981, 990-91 (1984). Si esto es cierto, el tribunal no ordenará la anulación de las pruebas. Véase por ejemplo Estados Unidos v. Hunter, 13 F. Supp. 2d 574, 584-85 (D. Vt. 1998) (en el que se concluye que es aplicable la excepción de buena fe a pesar de que la orden de registro informático no era lo bastante concreta). Por otra parte, los fiscales pueden alegar que la descripción general de la orden se debe interpretar en combinación con la descripción más concreta que figura en la declaración jurada acreditativa. A pesar de que los estándares jurídicos varían en gran medida entre los circuitos, véase Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment (Registro y confiscación: tratado sobre la Cuarta Enmienda) § 4.6(a) (1994), la mayoría de los circuitos permiten interpretar la orden remitiéndose a la declaración jurada a fin de satisfacer el requisito de concreción en determinadas circunstancias. Por último, son varios los circuitos que han concluido que los tribunales pueden redactar con un lenguaje general y admitir pruebas procedentes de una confiscación general si éstas se han requisado en virtud de una redacción lo suficientemente concreta. Véase Estados Unidos v. Christine, 687 F.2d 749, 759 (3° Cir. 1982); Gomez-Soto, 723 F.2d en 654.

Paso 2: Establecer la causa probable en la declaración adjunta

El segundo paso a la hora de preparar una orden para registrar y confiscar un ordenador consiste en redactar una declaración adjunta en la que se establezca la causa probable para creer que en el lugar que se va a registrar existe contrabando, pruebas, resultados o instrumentos de un delito. Véase la Cuarta Enmienda de la Constitución de Estados Unidos ("no se emitirá ninguna orden a menos que se base en una causa probable, respaldada por juramento o afirmación"); Norma Federal de Procedimiento Penal 41(b),(c). De acuerdo con el Tribunal Supremo, la declaración debe establecer "una probabilidad objetiva de que en un lugar concreto se hallará contrabando o pruebas de un delito". Illinois v. Gates, 462 U.S. 213, 238 (1983). Esto exige una determinación práctica de sentido común basada en la situación en su conjunto. Véase id. Lógicamente, no existirá causa probable si el agente solamente puede indicar una "mera sospecha" de que en el lugar que se va a inspeccionar se encontrarán pruebas de un delito. Véase Brinegar v. Estados Unidos, 338 U.S. 160, 175 (1949). Una vez que un magistrado halle causa probable y emita la orden, a la determinación del magistrado de que existe causa probable se le debe "gran deferencia", Gates, 462 U.S. en 236, y se confirmará en tanto en cuanto haya "un fundamento sólido para concluir que existió causa probable". Id. en 238-39 (se omiten citas internas).

Cabe destacar que el requisito de causa probable no exige que los agentes sean adivinos en cuanto a la forma precisa de las pruebas o contrabando que habrá en el lugar que se va a registrar. Por ejemplo, los agentes no necesitan una causa probable para creer que las pruebas que buscan se encontrarán en formato informático (como contraposición al papel). Véase Estados Unidos v. Reyes, 798 F.2d 380, 382 (10° Cir. 1986) (en el que se destaca que "en la era de la tecnología moderna […] no se puede esperar que en la orden se describa con exactitud la forma precisa que adoptarán los registros"). De igual manera, no es necesario que los agentes sepan exactamente qué infracción jurídica contribuirán a revelar las pruebas, véase Estados Unidos v. Prandy-Binett, 995 F.2d 1069, 1073 (D.C. Cir. 1993), ni tampoco que sepan a quién pertenece la propiedad que se va a registrar o confiscar, véase Estados Unidos v. McNally, 473 F.2d 934, 942 (3° Cir. 1973). La norma de la causa probable simplemente exige que los agentes establezcan la probabilidad objetiva de que en el lugar concreto que se va a inspeccionar se encontrarán elementos de contrabando o pruebas de un delito. Véase Gates, 462 U.S. en 238. Como es natural, aquellos oficiales que conozcan concretamente la forma de las pruebas o el contrabando que exista en el lugar que se va a registrar deberán describir minuciosamente lo que sepan en la declaración jurada.

Los recursos por causa probable frente a órdenes de registros informáticos se producen especialmente a menudo en casos relacionados con la posesión o transmisión de imágenes de pornografía infantil. [(12)]

Por ejemplo, los demandados suelen alegar que el periodo de tiempo transcurrido entre la solicitud de la orden y el momento en el que se produjeron los hechos incriminatorios mencionados en la declaración jurada desposee al magistrado de motivos suficientes para creer que se encontrarían imágenes de pornografía infantil en el ordenador del demandado. Por lo general, los tribunales no han admitido estos argumentos de "caducidad", en parte porque han tomado conocimiento judicial del hecho de que las personas que acumulan pornografía infantil no suelen deshacerse del material. Véase por ejemplo Estados Unidos v. Hay, 231 F.3d 630, 636 (9° Cir. 2000); Estados Unidos v. Horn, 187 F.3d 781, 786-87 (8° Cir. 1999); Estados Unidos v. Lacy, 119 F.3d 742, 745-46 (9° Cir. 1997); Estados Unidos v. Sassani, 139 F.3d 895, 1998 WL 89875, en *4-5 (4° Cir. 4 de marzo de 1998) (sin publicar) (se citan casos). Por el contrario, véase Estados Unidos v. Zimmerman, 277 F.3d 426, 433-34 (3d Cir. 2002) (en el que se diferencia entre la tenencia de pornografía adulta y la de pornografía infantil y se concluye que había expirado la prueba de que la primera estaba en el ordenador desde al menos seis meses antes de que se emitiera la orden). Los tribunales también han destacado que los avances en el análisis científico de la informática permiten a los investigadores recuperar archivos incluso después de que hayan sido eliminados, lo que arroja aún más dudas sobre la validez de los argumentos de "caducidad". Véase Hay, 231 F.3d en 636; Estados Unidos v. Cox, 190 F. Supp. 2° 330, 334 (N.D.N.Y. 2002).

Asimismo, también pueden surgir alegaciones contra la causa probable si la prueba acreditativa de una declaración jurada se deriva en gran medida de los registros de una cuenta particular de Internet o de una dirección de protocolo de Internet ("IP"). La naturaleza del problema es práctica: desde un punto de vista general, el hecho de que una cuenta o dirección se haya utilizado no fija de forma definitiva la identidad o ubicación de la persona concreta que la usara. La consecuencia es que toda declaración fundada profundamente en los registros de una cuenta o dirección IP deberá demostrar una relación suficiente entre tales registros y el lugar que se vaya a registrar, con el fin de establecer "una probabilidad objetiva de que en dicho lugar se hallará contrabando o pruebas de un delito". Gates, 462 U.S. en 238. Véase por ejemplo Estados Unidos v. Cervini, 2001 WL 863559 (10° Cir. Jul. 31, 2001) (sin publicar) (en el que se confirma la conclusión de causa probable para registrar una casa basándose en la prueba de que se utilizó una dirección IP particular para transmitir pornografía infantil en un momento concreto, que la dirección IP y la fecha de la transmisión estaban relacionadas con la cuenta que el sospechoso tenía con un proveedor de servicios de Internet, y que el sospechoso tenía dos líneas telefónicas activas conectadas a esta casa); Estados Unidos v. Hay, 231 F.3d 630, 634 (9° Cir. 2000) (la prueba de que se habían enviado imágenes de pornografía infantil a una dirección IP vinculada con el domicilio del demandado, en conjunción con otras pruebas del interés del demandado por los niños pequeños, estableció la causa probable para registrar el piso del demandado en busca de pornografía infantil); Estados Unidos v. Grant, 218 F.3d 72, 76 (1° Cir. 2000) (la prueba de que una cuenta de Internet perteneciente al demandado había estado implicada en actividades delictivas en varias ocasiones, así como que el coche del demandado estuviera implicado en su residencia al menos en una de esas ocasiones, estableció la causa probable para registrar el domicilio del demandado).

Paso 3: En la declaración jurada anexa a la orden, incluir una explicación de la estrategia de registro (como puede ser la necesidad de realizar un registro fuera del lugar) así como las consideraciones prácticas y jurídicas a las que estará sujeta la ejecución de la inspección

El tercer paso en la redacción de una orden satisfactoria para un registro informático consiste en explicar en la declaración jurada tanto la estrategia de la inspección como las consideraciones prácticas subyacentes a la misma. Por ejemplo, si los agentes prevén que puede resultar necesario confiscar un ordenador personal y analizarlo en otro lugar para recuperar las pruebas relevantes, la declaración deberá explicar al magistrado esta previsión y sus fundamentos. La declaración jurada debe informar al tribunal de las restricciones prácticas de llevar a cabo un registro in situ, así como describir minuciosamente el plan para trasladar el ordenador completo del lugar si fuera necesario. Por otra parte, en la declaración también se debe explicar qué técnicas piensan utilizar los agentes para analizar el ordenador en busca de los archivos específicos que representan la prueba de un delito y que pueden estar mezclados con otros documentos totalmente inofensivos. Si la estrategia de inspección se ha visto influida por consideraciones jurídicas, como puede ser la posible responsabilidad con arreglo a la PPA, la declaración jurada deberá reflejar cómo y por qué. En el caso de que los agentes gocen de autoridad para requisar equipos debido a que estos sean en sí una prueba, contrabando o instrumento de un crimen, la declaración deberá explicar si los agentes pretenden registrar los equipos después de

requisarlos y, en caso afirmativo, para qué. En conclusión, la declaración jurada debe abordar todos los asuntos prácticos y jurídicos relevantes que hayan tenido en cuenta los agentes durante la planificación del registro, así como explicar la línea de conducta que seguirán estos como consecuencia de ello. Si bien no se pide un estilo de redacción concreto, en el Apéndice F se ofrecen muestras que pueden resultar útiles a los agentes en numerosas situaciones. Por ultimo, si la estrategia de registro es compleja o si la declaración jurada lleva sello, los agentes pueden considerar la posibilidad de reproducir la explicación de la estrategia incluida en la declaración como un anexo a la propia orden.

Los motivos para describir la estrategia de inspección en la declaración son tanto prácticos como jurídicos. Desde un punto de vista práctico, explicar la estrategia en la declaración da lugar a un documento que pueden leer y consultar el tribunal y los agentes a modo de pauta para la ejecución del registro. Véase Nat'l City Trading Corp. v. Estados Unidos, 635 F.2d 1020, 1026 (2° Cir. 1980) ("Constatamos con aprobación la cautela empleada por el gobierno en este registro en cuestión. […] Esta cautela autorrestrictiva [al ejecutar una orden] supone una conducta extraordinariamente adecuada para el gobierno"). De igual forma, si la explicación de la estrategia de inspección se reproduce como documento anexo a la orden y se entrega a la persona objeto de la misma como se estipula en la Norma 41(d), ello permite al dueño de la propiedad registrada comprobar durante el proceso que la conducta de los agentes se ciña al alcance de la orden. Véase Michigan v. Tyler, 436 U.S. 499, 508 (1978) (en el que se destaca que "una de las principales funciones de una orden es facilitar la suficiente información al dueño de la propiedad como para garantizarle la legalidad de la actuación"). Por último, desde el punto de vista jurídico, explicar la estrategia de registro en la declaración ayuda a contrarrestar las demandas del consejo de la defensa para anularlo basándose en la presunta "indiferencia flagrante" de los agentes con respecto a la orden durante la ejecución de la inspección. Sin embargo, los agentes también deben tener cuidado de no expresar una estrategia de registro demasiado limitada o restrictiva: el consejo de la defensa puede alegar también indiferencia flagrante de una orden si los oficiales transgreden la estrategia descrita en la orden.

Para comprender las demandas de anulación basadas en la norma de la "indiferencia flagrante", los agentes y fiscales deben recordar las limitaciones sobre registros y confiscaciones impuestas por la Norma 41 y por la Cuarta Enmienda. En general, la Cuarta Enmienda y la Norma 41 limitan a los agentes para que busquen y confisquen la propiedad descrita en la orden que sea en sí misma prueba, contrabando, resultado o instrumento de un delito. Véase Estados Unidos v. Tamura, 694 F.2d 591, 595 (9° Cir. 1982); véase también el Apéndice F (en el que se describe la propiedad que se va a requisar conforme a la Norma 41). Si los agentes ejecutan una orden y requisan propiedades adicionales que no figuren en la misma, el consejo de la defensa puede interponer una demanda de anulación de las pruebas adicionales. Este tipo de demandas no son comunes ya que, en caso de que sean concedidas, el único resultado sería la supresión de la propiedad que no se menciona en la orden. Véase Estados Unidos v. Hargus, 128 F.3d 1358, 1363 (10° Cir. 1997).

Por otra parte, el consejo de la defensa intentará utilizar a menudo la confiscación de propiedad adicional como base para una demanda de anulación de todas las pruebas recogidas en el registro. Para tener derecho a la solución extrema de la anulación general, el demandado deberá establecer que la confiscación de material adicional demuestra que los agentes ejecutaron la orden con "indiferencia flagrante" hacia sus condiciones. Véase por ejemplo Estados Unidos v. Le, 173 F.3d 1258, 1269 (10° Cir. 1999); Estados Unidos v. Matias, 836 F.2d 744, 747-48 (2° Cir. 1988) (se citan casos). Un registro se lleva a cabo con "indiferencia flagrante" hacia sus condiciones cuando los oficiales excedan de tal manera el alcance de la orden durante la ejecución del registro que la inspección autorizada parezca un simple pretexto para "ir de pesca" a la propiedad privada de la persona declarada como objetivo. Véase por ejemplo Estados Unidos v. Liu, 239 F.3d 138 (2° Cir. 2000); Estados Unidos v. Foster, 100 F.3d 846, 851 (10° Cir. 1996); Estados Unidos v. Young, 877 F.2d 1099, 1105-06 (1° Cir. 1989).

Las demandas de anulación alegando "indiferencia flagrante" son habituales en los registros informáticos debido a que, por razones prácticas y técnicas, los agentes que los llevan a cabo se ven obligados con frecuencia a confiscar equipos o archivos que no se describen en la orden. Por ejemplo, como se acaba de mencionar, los agentes que tengan causa probable para pensar que hay pruebas de un fraude perpetrado por el demandado en el ordenador de su casa pueden tener que confiscar el equipo completo y registrarlo en otro lugar. Los abogados de la defensa suelen aducir que al requisar más que

los archivos informáticos concretos indicados en la orden, los agentes "hicieron caso omiso de manera flagrante" de la autorización de confiscación otorgada por la orden. Véase por ejemplo Estados Unidos v. Henson, 848 F.2d 1374, 1383 (6° Cir. 1988); Estados Unidos v. Hunter, 13 F. Supp. 2d 574, 585 (D. Vt. 1998); Estados Unidos v. Gawryisiak, 972 F. Supp. 853, 865 (D.N.J. 1997), afirmado, 178 F.3d 1281 (3° Cir. 1999); Estados Unidos v. Schwimmer, 692 F. Supp. 119, 127 (E.D.N.Y. 1988).

La mejor forma que tienen los fiscales de responder a las demandas de "indiferencia flagrante" es hacer ver que la confiscación de propiedad no mencionada en la orden obedeció a una respuesta de buena fe ante las dificultades prácticas inherentes, más que a un deseo de llevar a cabo una inspección general de la propiedad del demandado disfrazada bajo la forma de una orden limitada. Los tribunales han reconocido las dificultades prácticas a las que tienen que hacer frente los agentes al acometer registros informáticos en busca de archivos concretos y han autorizado inspecciones en otro lugar a pesar de la confiscación de propiedad adicional. Véase por ejemplo Davis v. Gracey, 111 F.3d 1472, 1280 (10° Cir. 1997) (en el que se destacan "las dificultades obvias que comporta la separación de los contenidos de un dispositivos electrónico [que se busque como prueba] del equipo informático [requisado] en el transcurso de una inspección"); Estados Unidos v. Schandl, 947 F.2d 462, 465-466 (11° Cir. 1991) (en el que se destaca que un registro in situ "podría haber sido mucho más negativo" que el registro en otro lugar que finalmente se realizó); Henson, 848 F.2d en 1383-84 ("No creemos que hubiera sido razonable exigir a los oficiales que filtraran la ingente cantidad de documentos y archivos informáticos hallados en la oficina [del demandado] a fin de separar los pocos papeles que escapaban al alcance de la orden"); Estados Unidos v. Scott-Emuakpor, 2000 WL 288443, en *7 (W.D. Mich. 25 de junio de 2000) (en el que se destacan "los problemas específicos asociados con la ejecución de un registro en busca de registros informáticos" que justifique una inspección en otro lugar); Gawrysiak, 972 F. Supp. en 866 ("El requisito de razonabilidad expresado por la Cuarta Enmienda no exige que el agente pase días y días sin moverse del sitio revisando la pantalla del ordenador para determinar concretamente qué documentos se pueden copiar en virtud de la orden"); Estados Unidos v. Sissler, 1991 WL 239000, en *4 (W.D. Mich. 25 de enero de 1991) ("La policía […] no estaba obligada a analizar el ordenador y los discos en el […] domicilio porque a menudo se utilizan contraseñas y otros dispositivos de seguridad para proteger la información almacenada en ellos. Como es natural, se permitió a la policía trasladarlos del […] domicilio a fin de que un experto en informática pudiera intentar superar estas medidas de seguridad, un proceso que lleva tiempo y trabajo. Al igual que la confiscación de documentos, la de hardware y software informático estuvo motivada por consideraciones de conveniencia. Por consiguiente, la presunta confiscación por carta blanca no constituyó una "indiferencia flagrante" hacia las limitaciones de una orden de registro"). Véase también Estados Unidos v. Upham, 168 F.3d 532, 535 (1° Cir. 1999) ("No es tarea fácil inspeccionar un disco duro bien cargado analizando toda la información que contiene […] El acta muestra que la mecánica del registro en busca de imágenes que se realizó posteriormente [en otro lugar] no se podría haber llevado a cabo fácilmente in situ"); Estados Unidos v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) ("Si algunos de los archivos de imágenes están almacenados en el disco duro interno del ordenador, es muy probable que la única forma práctica de examinar su contenido sea trasladar el ordenador a una oficina o laboratorio del FBI").

Las decisiones de permitir registros informáticos en otro lugar se ven reforzadas por casos análogos del ámbito físico que han autorizado a los agentes a trasladar armarios archivadores y cajas de documentos en papel de forma que estos pudieran inspeccionar su contenido en otro lugar en busca de los documentos mencionados en la orden. Véase por ejemplo Estados Unidos v. Hargus, 128 F.3d 1358, 1363 (10° Cir. 1997) (en el que se concluye que la "confiscación completa de armarios archivadores y documentos varios" no constituyó indiferencia flagrante porque "estuvo motivada por la imposibilidad de realizar una clasificación in situ y por la limitación temporal de ejecutar una orden de registro de día"); Crooker v. Mulligan, 788 F.2d 809, 812 (1° Cir. 1986) (en el que se destacan casos "que confirman la confiscación de documentos, tanto incriminatorios como inofensivos, que no están especificados en una orden pero que aparecen mezclados en un solo conjunto con documentos relevantes"); Estados Unidos v. Tamura, 694 F.2d 591, 596 (9° Cir. 1982) (en el que se sentencia que el tribunal de distrito denegó correctamente la demanda de anulación "en vista de que las confiscaciones generales del gobierno estaban motivadas por consideraciones de carácter práctico más que por un deseo de "pescar" de manera indiscriminada"; Estados Unidos v. Hillyard, 677 F.2d 1336, 1340 (9° Cir. 1982) ("Si la

mezcla evita la inspección in situ y no existe otra alternativa viable, la propiedad entera puede ser confiscable, al menos de forma temporal").

Explicar en la declaración jurada la estrategia de registro de los agentes y los aspectos prácticos subyacentes a la misma puede contribuir a garantizar que la ejecución de la inspección no se considerará en "indiferencia flagrante" hacia la orden. Cf. Estados Unidos v. Hay, 231 F.3d 630, 634 (9° Cir. 2000) (en el que se sugiere que la autorización de un registro concedida por un magistrado y acompañada de una declaración en la que se explicaba la necesidad de una inspección en otro lugar constituía "la autorización del magistrado" para llevar a cabo el registro en otro sitio); Estados Unidos v. Campos, 221 F.3d 1143, 1147 (10° Cir. 2000) (en el que se acoge a la explicación de la estrategia de registro incluida en la declaración jurada para concluir que no se había excedido una orden de registro informático). Una explicación minuciosa de la estrategia de inspección pone de manifiesto la buena fe y la atención del agente, expresa las consideraciones prácticas que impulsan el registro y permite al juez autorizar la estrategia descrita en la declaración. Todo registro que cumpla con la estrategia explicada en la declaración acreditativa no estará en indiferencia flagrante de la orden. Véase por ejemplo Estados Unidos v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997) (en el que se destaca que la observación por parte de los agentes del plan de registro incluido en la declaración daba fe de una atención adecuada y razonable a la hora de ejecutar la inspección autorizada).

A pesar de que explicar la estrategia de registro aporta beneficios significativos, también es importante que los agentes no se vean limitados por una estrategia ineficaz o demasiado restrictiva. Por ejemplo, no suele resultar muy prudente limitar una estrategia únicamente a registros por palabras clave. No es frecuente saber con certeza que la información buscada contendrá las palabras clave especificadas y que en el medio de almacenamiento se podrán realizar tales búsquedas. Los bufetes de abogados y compañías de inversión, por no hablar de las personas implicadas en actividades delictivas, suelen utilizar palabras en código para identificar a entidades, individuos y acuerdos comerciales específicos en documentos y comunicaciones; en ocasiones es posible que no se aprecie la importancia de estos términos hasta que no se haya iniciado una revisión meticulosa archivo por archivo. Debería ser suficiente con decir que los agentes adoptarán "estrategias de inspección como pueden ser búsquedas por palabras clave" para hallar la información descrita en la orden. Además, es posible que los datos esenciales de un ordenador se encuentren en los recovecos y ranuras más sorprendentes. Por ejemplo, una estrategia sólida de registro debería permitir a los agentes buscar archivos eliminados en puntos ciegos. Una estrategia de inspección debe ser lo bastante amplia para permitir que los agentes no se vean en la necesidad de extralimitarse en la estrategia para dar con los elementos identificados en la orden. Una buena práctica consiste en referir una serie de estrategias posibles.

Si los agentes prevén que los archivos descritos en la orden pueden estar mezclados con otros inocentes que queden fuera del alcance de la misma, es aconsejable, si es posible desde el punto de vista técnico, explicar en la declaración jurada cómo planean los agentes registrar el ordenador en busca de los archivos en cuestión.

Si los agentes realizan un registro de archivos informáticos y otras pruebas electrónicas almacenadas en un disco duro u otro dispositivo de almacenamiento, las pruebas pueden estar entremezcladas con otros datos y archivos que no guarden relación con el delito que se esté investigando. Intuir la mejor manera de localizar y recuperar las pruebas entre todos los datos no relacionados es más un arte que una ciencia y a menudo exige una importante experiencia técnica y una atención minuciosa a los hechos. Como consecuencia, los agentes pueden saber o no en el momento de obtener la orden cómo se registrará el dispositivo de almacenamiento y, al iniciar la inspección, pueden saber o no si será posible localizar las pruebas sin llevar a cabo un análisis completo de los archivos no relacionados.

En el caso de que los agentes tengan una base objetiva para pensar que pueden localizar las pruebas por medio de una serie concreta de técnicas, en la declaración jurada se tendrán que explicar las técnicas que planean utilizar los agentes para distinguir los documentos incriminatorios de los que simplemente aparecen mezclados. Dependiendo de las circunstancias, puede resultar útil consultar a expertos en el campo del análisis científico informático para determinar qué tipo de registro se puede llevar a cabo para localizar los archivos concretos descritos en la orden. Puede ser que en algunos casos sea posible realizar una búsqueda por "palabras clave" o utilizar otro enfoque quirúrgico similar. Cabe destacar que

la Cuarta Enmienda no exige por lo general un enfoque de este tipo. Véase Estados Unidos v. Habershaw, 2001 WL 1867803, en *7 (D. Mass. 13 de mayo de 2001) (en el que se rechaza el argumento de que un registro sector por sector infringe la Cuarta Enmienda, ya que se podría haber utilizado una búsqueda por palabras clave); Estados Unidos v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) ("Las inspecciones de archivos informáticos no son menos constitucionales que las de archivos físicos, en las que se pueden analizar documentos inocuos para determinar su relevancia"); Estados Unidos v. Lloyd, 1998 WL 846822, en *3 (E.D.N.Y. 5 de octubre de 1998). No obstante, en sentencias amplias, el Décimo Circuito ha indicado que fomenta un enfoque más limitado porque reduce al mínimo la posibilidad de que el gobierno pueda utilizar una orden restrictiva para justificar un registro más amplio. Véase Estados Unidos v. Carey, 172 F.3d 1268, 1275-76, 1275 n.8. (10° Cir. 1999) (en el que se cita a Raphael Winick, *Searches and Seizures of Computers and Computer Data* (Registros y confiscaciones de ordenadores y datos informáticos), 8 Harv. J. L. &. Tech. 75, 108 (1994)); Campos, 221 F.3d en 1148. Véase también Gawrysiak, 972 F. Supp. en 866 (en el que se sugiere en sentencias que los agentes que ejecutan un registro en busca de archivos informáticos "podían haber comprobado al menos la fecha en la que se creó cada archivo y así haber evitado copiar aquellos que se hubieran creado antes del periodo de tiempo cubierto por la orden").

Lógicamente, serán muchos los casos en los que un enfoque limitado sea técnicamente imposible. Los archivos buscados pueden tener denominaciones engañosas, estar ocultos, configurados de forma extraña, escritos con palabras codificadas para impedir su detección, cifrados o sencillamente puede que resulte imposible su localización mediante una técnica tan simple como una búsqueda "por palabras clave". La experiencia ha demostrado que las personas implicadas en diversos tipos de conductas delictivas utilizan estas técnicas para confundir las pruebas electrónicas incriminatorias. Dado que es posible que algunos jueces no aprecien estas dificultades técnicas, una buena práctica consiste en que los agentes comenten estos problemas en la declaración jurada. En muchos casos será necesario un análisis más amplio entre archivos inocentes para determinar qué archivos entran dentro del alcance de la orden. La mejor solución es con frecuencia presentar la estructura y tomar como muestra parte del contenido del dispositivo de almacenamiento confiscado para adaptarlo a las mejores técnicas de registro. No obstante, durante el análisis preliminar del medio de almacenamiento pueden surgir dificultades técnicas imprevistas, en cuyo caso la descripción de la declaración deberá advertir al magistrado de la necesidad de permitir el desarrollo de estrategias de registro flexibles y cambiantes. Si se exponen estas necesidades prácticas en la declaración, esto puede servir para dejar claro desde el inicio por qué un registro amplio no supondría "indiferencia flagrante" hacia la orden y por qué tal registro cumple plenamente con los principios tradicionales de la Cuarta Enmienda. Véase Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("Se asume que en registros de documentos en papel se examinarán documentos inocentes, aunque sea someramente, a fin de determinar si entran dentro de los confiscables conforme a la autorización concedida"); Estados Unidos v. Riley, 906 F.2d 841, 845 (2° Cir. 1990) (en el que se destaca que las inspecciones de registros permiten a los agentes buscar entre muchos papeles porque "no hay mucha gente que guarde los documentos de sus transacciones ilegales en una carpeta en la que ponga "Archivos [del delito]"); Estados Unidos v. Gray, 78 F. Supp. 2d 524, 530 (E.D. Va. 1999) (en el que se destaca que a los agentes que ejecutan un registro de archivos informáticos "no se les exige que acepten como exacto un nombre de archivo o sufijo y que limiten la búsqueda en consecuencia", ya que los delincuentes pueden "darle un nombre erróneo de forma intencionada a los archivos o intentar camuflar documentos incriminatorios entre directorios de nombres inocuos"); Hunter, 13 F. Supp. 2d en 584; Estados Unidos v. Sissler, 1991 WL 239000, en *4 (W.D. Mich. 25 de enero de 1991) ("La policía no estaba obligada a otorgar credibilidad a las etiquetas descriptivas colocadas en los discos por [el demandado]. En caso contrario, sería extremadamente sencillo proteger registros de actividades ilícitas con adjudicar simplemente un nombre inocuo al disco informático que los contenga.

Si los agentes obtienen una orden para confiscar equipos que sean en sí pruebas, contrabando o instrumentos de un delito, deberán explicar en la declaración adjunta si registrarán los equipos tras la confiscación y cómo se plantean hacerlo.

Si los agentes tienen causa probable para confiscar hardware porque éste sea una prueba, contrabando o un instrumento de un delito, en la orden se describirá normalmente el hardware propiamente dicho como la propiedad que se va a requisar. Sin embargo, en muchos de estos casos los agentes se

plantearán inspeccionar el equipo después de confiscarlo para buscar datos electrónicos almacenados en el mismo que puedan constituir también una prueba o contrabando. Siempre es aconsejable que los agentes informen al magistrado acerca de este plan en la declaración acreditativa. Si bien es cierto que hay tribunales que han confirmado estos registros a pesar de que los agentes no explicaran esta previsión en la declaración, véase por ejemplo Estados Unidos v. Simpson, 152 F.3d 1241, 1248 (10° Cir. 1998) (se comenta más abajo), lo más aconsejable es informar al magistrado en la declaración acerca del plan de los agentes de registrar los equipos tras requisarlos.

[Índice]

D. Problemas que pueden surgir tras la confiscación

En muchos casos, los equipos informáticos confiscados se envían a un laboratorio para proceder a su análisis forense. El periodo de tiempo que puede transcurrir antes de que un especialista técnico finalice dicho análisis varía mucho, en función del propio equipo, de las pruebas buscadas y de la urgencia del registro. En cualquier caso, sin embargo, este periodo suele abarcar varios meses. Durante el plazo posterior a la confiscación pueden surgir diversos problemas legales relativos al derecho del gobierno a retener y registrar los ordenadores que estén bajo su custodia.

1. Exploración de ordenadores que ya se encuentren bajo la custodia de las fuerzas de seguridad

Para registrar un ordenador confiscado en virtud de una orden válida, los agentes, por lo general, deberán obtener una segunda orden si la propiedad fijada como objetivo del registro propuesto es diferente de la indicada en la primera orden.

Ocurre con frecuencia que los agentes requisen un ordenador conforme a una orden y después pregunten si necesitan una segunda orden para examinarlo. Esto dependerá del objeto de la inspección. Si los agentes desean registrar el equipo en busca de la información que era el objetivo de la confiscación original, no es necesaria otra orden. Por ejemplo, en Estados Unidos v. Simpson, 152 F.3d 1241 (10° Cir. 1998), los investigadores obtuvieron una orden para confiscar los "disquetes […] y el ordenador del demandado" basada en la causa probable para pensar que contenía pornografía infantil. Los investigadores requisaron el ordenador y después lo examinaron bajo la custodia de la policía, hallando imágenes de pornografía infantil. En la apelación tras la condena, el demandado expuso que los investigadores carecían de la autoridad para *registrar* el ordenador puesto que la orden solamente autorizaba la *confiscación* del equipo. El Décimo Circuito desestimó este argumento, concluyendo que una orden para confiscar un equipo informático autoriza a los agentes a registrar dicho equipo. Véase id. en 1248. Véase también Estados Unidos v. Gray, 78 F. Supp. 2d 524, 530-31 (E.D. Va. 1999) (en el que se concluye que la orden inicial que permitía el registro en busca de pruebas de piratería informática justificaba una búsqueda posterior de dichas pruebas, a pesar de que durante la ejecución del registro los agentes descubrieron pruebas incriminatorios que escapaban al alcance de la orden).

Sin embargo, si los investigadores confiscan equipos informáticos por las pruebas que contienen y posteriormente deciden registrarlos para buscar otras pruebas, quizá sea más seguro solicitar una segunda orden. En Estados Unidos v. Carey, 172 F.3d 1268 (10° Cir. 1999), los detectives obtuvieron una orden para examinar el ordenador del demandado en busca de registros de ventas de narcóticos. Durante la inspección del ordenador en la comisaría de policía, un detective descubrió imágenes de pornografía infantil. En ese momento el detective "dejó a un lado la búsqueda de pruebas relacionadas con drogas" y en lugar de ello se dedicó a examinar el disco duro entero para buscar pruebas de pornografía infantil. Id. en 1277-78. El Décimo Circuito anuló la pornografía infantil basándose en que el registro posterior de este tipo de imágenes superaba el alcance de la orden original. Véase id. en 1276. Compárese Carey con Estados Unidos v. Walser, 275 F.3d 981, 986-87 (10° Cir. 2001) (en el que se confirma una inspección en la que un oficial que tenía una orden para buscar registros de transacciones de drogas descubrió pornografía infantil en el ordenador, suspendió el registro y volvió a solicitar una segunda orden al magistrado para buscar pornografía infantil); Gray, 78 F. Supp. 2d en 530-31 (en el que se confirma un registro en el que un agente descubrió pornografía infantil durante la

búsqueda de pruebas de piratería informática en virtud de una orden y que posteriormente obtuvo otra antes de inspeccionar el ordenador en busca de pornografía infantil).

Véase en particular CareySee, por ejemplo, Whren v. Estados Unidos, 517 U.S. 806, 813 (1996); Horton v. California, 496 U.S. 128, 138 (1990). Basándose en estos precedentes, son varios los tribunales que han indicado que el propósito subjetivo de un agente durante la ejecución de una orden ya no determina si el registro excede el alcance de la orden e infringe la Cuarta Enmienda. Véase Estados Unidos v. Van Dreel, 155 F.3d 902, 905 (7° Cir. 1998) ("Conforme a Whren, […] una vez que existe causa probable y que se ha emitido una orden válida, la intención subjetiva del oficial a la hora de llevar a cabo el registro es irrelevante"); Estados Unidos v. Ewain, 88 F.3d 689, 694 (9° Cir. 1996) ("La utilización de un criterio subjetivo no sería coherente con respecto a Horton y haría que la anulación dependiese demasiado de cómo contara su versión la policía, en lugar de lo que ocurrió en realidad"). De acuerdo con estos casos, la cuestión es si, desde una perspectiva objetiva, el registro que los agentes llevaron a cabo en realidad fue coherente con la orden obtenida. Véase Ewain, 88 F.3d en 694. La intención subjetiva del agente es o bien "irrelevante", Van Dreel, 155 F.3d en 905, o bien un factor más en la determinación general de "si la policía limitó el registro a lo que permitía la orden". Ewain, 88 F.3d en 694.

2. Plazo de tiempo admisible para inspeccionar los ordenadores confiscados

Ni la Norma 41 ni la Cuarta Enmienda expresan límites de tiempo específicos sobre el examen forense de los ordenadores confiscados realizado por el gobierno. Sin embargo, algunos magistrados sí imponen restricciones.

A pesar de los esfuerzos del gobierno por analizar rápidamente los ordenadores confiscados, el examen forense de estos con frecuencia lleva meses hasta que se finaliza, ya que los equipos pueden almacenar cantidades ingentes de datos. Como consecuencia de ello, los sospechosos a los que se les hayan confiscado ordenadores pueden verse privados de sus equipos durante largos periodos de tiempo. Ni la Norma 41 ni la Cuarta Enmienda imponen límites específicos sobre el periodo de tiempo para el examen forense del gobierno. Lo normal es que el gobierno pueda retener el ordenador confiscado y examinar su contenido de forma minuciosa y deliberada sin restricciones legales, sujeto únicamente a la autorización de la Norma 41(e), según la cual una "persona afectada" por la confiscación de una propiedad puede interponer una petición para la devolución de la misma (véase "Peticiones conforme a la Norma 41(e) para la devolución de la propiedad", más abajo).[(13)]

Sin embargo, algunos magistrados han adoptado una perspectiva diferente. Varios de ellos han rechazado firmar órdenes de registro que autoricen la confiscación de ordenadores a menos que el gobierno lleve a cabo el examen forense en un espacio corto de tiempo, como en treinta días. Algunos magistrados han llegado a imponer límites temporales de hasta siete días y otros han impuesto límites específicos cuando los agentes solicitan una orden para confiscar ordenadores de empresas que están operativas. Para justificar estas restricciones, algunos magistrados han mostrado su inquietud de que es probable que desde el punto de vista constitucional y de acuerdo con la Cuarta Enmienda no sea razonable que el gobierno prive de sus ordenadores a estas personas durante más de un periodo corto de tiempo. Otros magistrados han sugerido que el requisito de la Norma 41, conforme al cual los agentes deben ejecutar el "registro" en los 10 días posteriores a la obtención de la norma, puede ser de aplicación al análisis forense del ordenador, así como al registro y la confiscación iniciales. Véase la Norma Federal de Procedimiento Penal 41(c)(1).

La ley no autoriza expresamente a los magistrados a emitir órdenes que impongan restricciones temporales al análisis de las pruebas incautadas por parte de las fuerzas de seguridad. Aunque la jurisprudencia relevante es escasa, ésta sugiere que los magistrados carecen de autoridad legal para negarse a emitir órdenes de registro basándose en la creencia de que los agentes pueden ejecutar las órdenes en el futuro de manera inconstitucional. Véase Abraham S. Goldstein, *The Search Warrant, the Magistrate, and Judicial Review* (La orden de registro, el magistrado y la revisión judicial), 62 N.Y.U. L. Rev. 1173, 1196 (1987) ("Los pocos casos que tratan acerca de [si un magistrado puede negarse a emitir una orden basándose en que la inspección se puede llevar a cabo de manera inconstitucional]

sostienen que un juez tiene la obligación "ministerial" de emitir una orden una vez se haya establecido "causa probable"); Inspección In re del entorno laboral de Quality Products, Inc., 592 F.2d 611, 613 (1° Cir. 1979) (en la que se destaca la función limitada de los magistrados en la emisión de órdenes). Como sugirió el Tribunal Supremo en un caso temprano, la línea de acción correcta es que el magistrado emita la orden mientras siga existiendo causa probable y que después permita a las partes litigar los asuntos constitucionales. Véase Ex Parte Estados Unidos, 287 U.S. 241, 250 (1932) ("La denegación de un tribunal de primera instancia a emitir una orden […] constituye, en realidad y consecuencia, una negativa a permitir que el caso llegue a una vista por cuestiones de ley u objetivas y está muy cerca de ser una negativa a permitir que se haga cumplir la ley").

Por otra parte, los fiscales también deben estar dispuestos a explicar a los magistrados por qué no es necesario que la inspección forense de los archivos almacenados en un ordenador confiscado se produzca en los 10 siguientes a la obtención de la orden. La norma 41(c)(1) exige que los agentes obtengan una orden deben "registrar, dentro de un periodo de tiempo concreto que no puede superar los 10 días, a la persona o el lugar mencionado en cuanto a la propiedad o la persona especificados". Esta norma insta a los agentes a inspeccionar el lugar mencionado en la orden y a confiscar la propiedad en cuestión en dicho plazo a fin de evitar que la orden "caduque" antes de ser ejecutada. Véase Estados Unidos v. Sanchez, 689 F.2d 508, 512 n.5 (5° Cir. 1982). No obstante, esta norma no es aplicable al análisis forense de las pruebas que ya se hayan confiscado, incluso si dicho análisis implica un "registro" conforme a la Cuarta Enmienda en algunos casos, ya que claramente no se produce "en el lugar […] mencionado" en la orden. Véase Estados Unidos v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (en el que se expone que la Norma 41 no "prevé un límite de tiempo concreto durante el cual se puede someter a un ordenador a un examen forense por parte del gobierno después de haber sido confiscado en virtud de una orden de registro"); Estados Unidos v. Habershaw, 2001 WL 1867803, en *8 (D. Mass. 13 de mayo de 2001) (en el que se destaca que "un nuevo análisis forense de la imagen del disco duro confiscado no constituye una segunda ejecución de la orden").

Puede que resulte útil establecer una analogía con documentos en papel. Una orden conforme a la Norma 41 que autorice la confiscación de un libro exige que el libro sea requisado en el lugar descrito en la orden y en el plazo de 10 días. Sin embargo, ni la orden ni la Norma 41 exigen que las fuerzas de seguridad examinen el libro y finalicen los análisis forenses de sus páginas dentro del mismo periodo de 10 días. Cf. Commonwealth v. Ellis, 10 Mass. L. Rptr. 429, 1999 WL 815818, en *8-9 (Mass. Super. 27 de agosto de 1999) (en el que se interpreta una disposición legal estatal análoga y se expone que "el registro continuo de la memoria del ordenador no tendría por qué haberse finalizado dentro del […] plazo exigido para la devolución de la orden").

Aunque la base legal para imponer restricciones de tiempo al análisis forense sigue sin estar clara, el hecho de que un magistrado se oponga a emitir una orden de registro informático sin que ésta lleve aparejada una limitación temporal puede dar muchos dolores de cabeza a los fiscales. En la práctica, los fiscales no tienen más opción que acatar los deseos del magistrado. La negación de un juez a firmar una orden de registro suele ser una orden final inapelable, por lo que el único recurso del fiscal es acudir a otro juez. Véase Estados Unidos v. Savides, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987) (en el que se destaca que al segundo juez se le debe comunicar que otro antes se ha negado a firmar la orden, afirmado en la parte relevante sub nom. Estados Unidos v. Pace, 898 F.2d 1218, 1230 (7° Cir. 1990). Por lo tanto, lo único que pueden hacer los fiscales es intentar convencer al juez de que no imponga una limitación de tiempo y, en caso de no conseguirlo, solicitar prórrogas cuando se compruebe que es imposible observar el plazo concedido.

Al menos un tribunal ha adoptado la postura extrema de declarar apropiada la anulación cuando el gobierno incumpla los plazos impuestos por el tribunal para analizar los ordenadores confiscados. En Estados Unidos v. Brunette, 76 F. Supp. 2d 30 (D. Me. 1999), un magistrado permitió a los agentes requisar los ordenadores de un sospechoso de posesión de pornografía infantil con la condición de que los inspeccionaran en busca de pruebas "en un plazo de 30 días". Los agentes ejecutaron el registro cinco días más tarde y confiscaron varios equipos. Varios días antes de que venciera el plazo de treinta días, el gobierno solicitó y obtuvo una prórroga de treinta días para la inspección. En este plazo los agentes revisaron todos los ordenadores confiscados menos uno, encontrando cientos de imágenes de pornografía infantil. Sin embargo, no empezaron a revisar el último hasta dos días después del

vencimiento del período de extensión. El demandado solicitó entonces la anulación de las imágenes de pornografía infantil que se encontraron en el último ordenador basándose en que el registro fuera del plazo de sesenta días contravenía las condiciones de la orden y de la prórroga posterior. El tribunal se mostró de acuerdo y sentenció que "dado que el gobierno no ha seguido las condiciones de la orden de registro y de la ampliación posterior, […] quedan anuladas todas las pruebas recabadas en el ordenador". Id. en 42.

El resultado de Brunette no tiene mucho sentido en relación con la Norma 41 ni con la Cuarta Enmienda. Aun asumiendo que un magistrado tiene la autoridad suficiente como para imponer restricciones de tiempo a los análisis forenses, parece incongruente declarar la anulación por la contravención de estas condiciones cuando otras infracciones análogas de la propia Norma 41 no tendrían esa consecuencia. Compárese Brunette con Estados Unidos v. Veintidós mil doscientos ochenta y siete dólares (22.287,00 $), moneda estadounidense, 709 F.2d 442, 448 (6° Cir. 1983) (en el que se rechaza la anulación porque los agentes comenzaran el registro "poco después de las" 22:00 h. a pesar de que la estricta Norma 41 establece que todos los registros se deben efectuar entre las 6:00 y las 22:00 h.). Esto es especialmente aplicable cuando el hardware que se va a registrar contienen pornografía infantil de contrabando, por lo que es en sí mismo un instrumento del delito no susceptible de devolución.

3. Solicitudes de devolución de la propiedad conforme a la Norma 41(e)

La Norma 41(e) establece que

Una persona afectada por un registro o confiscación ilegales o por la privación de propiedad puede solicitar al tribunal de distrito del distrito en el que se confiscó la propiedad que le sea devuelta la misma sobre la base de que dicha persona tiene derecho a la posesión legal de la propiedad. El tribunal recibirá pruebas sobre cualquier asunto objetivo que pueda ser necesario para tomar una resolución al respecto. De concederse la solicitud, la propiedad se devolverá al solicitante, aunque se pueden imponer condiciones razonables para salvaguardar el acceso y el uso de la misma en procesos posteriores. Si se realiza una solicitud de devolución de propiedad o se atiende en audiencia en el distrito judicial después de que se presente una acusación o información, ésta se considerará también una solicitud de anulación en virtud de la Norma 12.

Norma Federal de Procedimiento Penal 41(e).

La Norma 41(e) es de particular relevancia en los casos de registros informáticos porque permite a los propietarios de los equipos confiscados solicitar la devolución de los mismos antes de que se presenten los cargos. Los demandados presentan estas solicitudes en algunos casos porque creen que la confiscación de sus equipos infringió la Cuarta Enmienda. Si están en lo cierto, se deberá devolver su propiedad. Véase por ejemplo Investigación In re del Gran Jurado en Relación con Solid State Devices, Inc., 130 F.3d 853, 855-56 (9° Cir. 1997). La Norma 41(e) también permite a los propietarios solicitar la devolución de su propiedad en el caso de que la confiscación fuera legal pero el solicitante se vea "afectado por la posesión continua por parte del gobierno de la propiedad requisada". Id. en 856. La funcionalidad múltiple de los ordenadores lleva a veces a solicitudes basadas en este hecho conforme a la Norma 41(e). Por ejemplo, un sospechoso que esté siendo investigado por piratería informática puede presentar una solicitud en la que exponga que necesita que le devuelvan el ordenador para calcular sus impuestos o comprobar su correo electrónico. De igual manera, una empresa sospechosa de fraude puede presentar una solicitud para que se le devuelvan sus equipos argumentando que necesitan que se los devuelvan o la compañía se resentirá.

Los propietarios de equipos informáticos confiscados deben superar varios obstáculos importantes antes de que un tribunal ordene al gobierno que les sean devueltos. En primer lugar, el propietario debe convencer al tribunal de que debe ejercer una jurisdicción equitativa sobre su solicitud. Véase Floyd v. Estados Unidos, 860 F.2d 999, 1003 (10° Cir. 1988) ("La jurisdicción de la Norma 41(e) se debe ejercer con cautela y comedimiento"). A pesar de que las normas jurisdiccionales varían enormemente entre los distintos tribunales, la mayoría de ellos afirmarán la jurisdicción de una solicitud conforme a la Norma

41(e) solamente si el solicitante establece: 1) la privación de la posesión de la propiedad le provoca "perjuicios irreparables" y 2) que de otra manera el solicitante se quede sin solución alguna ante la ley. Véase el caso In re del registro de Kitty's East, 905 F.2d 1367, 1370-71 (10° Cir. 1990). Cf. Ramsden v. Estados Unidos, 2 F.3d 322, 325 (9° Cir. 1993) (en el que se expresa una prueba jurisdiccional de cuatro factores de la versión de la Norma 41(e) anterior a 1989). Si el solicitante establece estos elementos, el tribunal atenderá los méritos de la demanda. Teniendo estos en cuenta, la propiedad confiscada se devolverá únicamente si la posesión continuada del gobierno no es razonable. Véase Ramsden, 2 F.3d en 326. Esta prueba requiere que el tribunal sopese el interés del gobierno en la posesión continuada de la propiedad frente al interés del dueño en la devolución de la misma. Véase Estados Unidos v. Instalaciones Conocidas como 608 Taylor Ave., 584 F.2d 1297, 1304 (3° Cir. 1978). Concretamente, si Estados Unidos precisa la propiedad para una investigación o proceso judicial, la retención de la misma será generalmente razonable. Por el contrario, si los intereses legítimos de Estados Unidos se pueden satisfacer aun devolviendo la propiedad, la retención continuada de ésta sería irrazonable.

Notas del Comité Consultivo de la Enmienda de 1989 de la Norma 41(e) (se cita en Ramsden, 2 F.3d en 326).

Son raras las ocasiones en las que se resuelven afirmativamente las solicitudes de devolución de equipos informáticos confiscados correctamente que se presentan conforme a la Norma 41(e). En primer lugar, los tribunales normalmente rechazan ejercer jurisdicción sobre la solicitud si el gobierno ha facilitado una copia electrónica de los archivos informáticos requisados al dueño de la propiedad. Véase Orden de Registro In re ejecutada el 1 de febrero de 1995, 1995 WL 406276, en *2 (S.D.N.Y. 7 de julio de 1995) (en la que se concluye que el dueño de un ordenador portátil confiscado no hizo mención alguna a perjuicios irreparables cuando el gobierno le ofreció la posibilidad de copiar los archivos que contenía); Estados Unidos v. East Side Ophthalmology, 1996 WL 384891, en *4 (S.D.N.Y. 9 de julio de 1996). Véase también Standard Drywall, Inc. v. Estados Unidos, 668 F.2d 156, 157 n.2. (2° Cir. 1982) ("Ponemos seriamente en duda el hecho de que, en ausencia de confiscación de propiedades exclusivas o documentos que gocen de privilegios, una parte pueda llegar a demostrar perjuicios irreparables [que justifiquen la jurisdicción] cuando el gobierno o bien proporciona copias de los artículos confiscados a la parte o bien le devuelve los originales y presenta las copias al jurado").

En segundo lugar, los tribunales que alcanzan los méritos normalmente concluyen que el interés del gobierno en el equipo informático es mayor que el del demandado en tanto en cuanto se esté llevando a cabo un proceso judicial penal o de confiscación. Véase Estados Unidos v. Stowe, 1996 WL 467238, en *1-3 (N.D. Ill. 15 de agosto de 1996) (la retención continuada de equipos informáticos es razonable tras 18 meses si el gobierno alega que la investigación estaba en curso y el demandado no expresó motivos convincentes para la devolución del equipo; En el Asunto de la Orden de Registro de K-Sports Imports, Inc., 163 F.R.D. 594, 597 (C.D. Cal. 1995) (en el que se deniega la solicitud de devolución de registros informáticos relativos a procesos de confiscación pendientes); Véase también Johnson v. Estados Unidos, 971 F. Supp. 862, 868 (D.N.J. 1997) (en el que se deniega una solicitud conforme a la Norma 41(e) de devolución de las cintas de ordenador de un banco porque éste ya no era una empresa operativa). Si el gobierno, por el contrario, no tiene previsto utilizar los ordenadores en procesos posteriores, estos deberán ser devueltos. Véase Estados Unidos v. Moore, 188 F.3d 516, 1999 WL 650568, en *6 (9° Cir. 15 de julio de 1999) (sin publicar) (en el que se ordena la devolución de un ordenador en vista de que "la necesidad de retención del ordenador por parte del gobierno para su utilización en otro proceso parece […] remota"); K-Sports Imports, Inc., 163 F.R.D. en 597. Asimismo, un tribunal puede conceder una solicitud conforme a la Norma 41(e) si el demandado no puede gestionar su empresa sin el equipo informático confiscado y si el gobierno puede trabajar igualmente a partir de una copia de los archivos confiscados. Véase Estados Unidos v. Bryant, 1995 WL 555700, en *3 (S.D.N.Y. 18 de septiembre de 1995) (en el que se hace referencia a una sentencia anterior del magistrado no publicada que decreta la devolución de un equipo informático y expone que "el magistrado concluyó que el demandado precisaba este equipo para gestionar su empresa").

[índice]

III. LA LEY DE PRIVACIDAD DE LAS COMUNICACIONES ELECTRÓNICAS

A. Introducción

La ECPA regula la forma en la que el gobierno puede obtener información de cuentas almacenada de proveedores de servicios de red, como los PSI. Siempre que un agente o fiscal investigue correos electrónicos guardados, registros de cuentas o información de un abonado de un proveedor de servicios de red, deberán observar la ECPA. Para entender mejor las clasificaciones de la ECPA, utilice la gráfica que aparece en la Sección F de este capítulo

La parte relativa a las comunicaciones electrónicas de la Ley de Privacidad de las Comunicaciones Electrónicas ("ECPA"), 18 U.S.C. §§ 2701-2712, otorga derechos de privacidad jurídicos a los clientes y abonados de proveedores de servicios de redes informáticas.

En un sentido amplio, la ECPA "rellena las lagunas" que deja la aplicación incierta de las protecciones de la Cuarta Enmienda en relación con el ciberespacio. Para comprender estas lagunas, pensemos en las protecciones jurídicas de las que gozamos en nuestra casa. La Cuarta Enmienda protege claramente nuestras casas en el ámbito físico: excepto en caso de que se den circunstancias especiales, el gobierno debe obtener una orden antes de poder registrarlas. Al utilizar una red informática como Internet, sin embargo, no tenemos una "casa" física. En lugar de ello, normalmente tenemos una cuenta de red que consta de un bloque de almacenamiento informático propiedad de un proveedor de servicios de red como America Online. Si los investigadores de las fuerzas de seguridad desean obtener el contenido de una cuenta de red o información sobre su uso, no necesitan acudir al usuario para acceder a dicha información. El gobierno puede obtenerla directamente del proveedor.

Aunque la Cuarta Enmienda normalmente exige que el gobierno obtenga una orden antes de registrar una casa, no ocurre lo mismo a la hora de inspeccionar el contenido guardado de una cuenta de red. En cambio, la Cuarta Enmienda permite que el gobierno emita una citación a un proveedor de red ordenándole que divulgue el contenido de una cuenta.[(14)] La ECPA aborda este desequilibrio ofreciendo a los titulares de cuentas de red una serie de derechos jurídicos de privacidad contra el acceso a la información de cuenta almacenada en posesión de los proveedores de servicios de red.

Teniendo en cuenta que la ECPA es una ley inusualmente compleja, a la hora de acercarse a ella resulta útil comprender la intención de las personas que la redactaron. La estructura de esta ley refleja una serie de clasificaciones que indican las opiniones de sus promulgadores acerca de qué tipos de información implican intereses de privacidad mayores o menores. Por poner un ejemplo, estos creyeron que tenían un mayor interés de privacidad los correos electrónicos almacenados que la información de cuenta de los abonados. De igual manera, los servicios informáticos disponibles "para el público" requerían a su juicio una normativa más estricta que aquellos otros servicios que no lo estuvieran. (Quizá este juicio refleje la idea de que no es probable que los proveedores disponibles para el público mantengan una relación estrecha con sus clientes, por lo que pueden tener menos incentivos para proteger la privacidad de estos). Para proteger el abanico de intereses de privacidad identificado por sus promulgadores, la ECPA ofrece diversos grados de protección jurídica en función de la importancia que se perciba en los intereses de privacidad en cuestión. En algunos casos es posible obtener determinada información con una simple citación. Otros tipos de información requieren una orden especial de un tribunal o incluso una orden de registro. En general, cuanto mayor sea el interés de privacidad, mayor será la protección de la privacidad.

Los agentes y fiscales deben aplicar las diversas clasificaciones concebidas por los promulgadores de la ECPA a cada situación concreta para averiguar el procedimiento adecuado para obtener la información deseada. Primero han de clasificar al proveedor de servicios de red; por ejemplo, si el proveedor ofrece "servicios de comunicación electrónica", "servicios informáticos remotos" o ninguna de las dos opciones. A continuación tienen que clasificar la información que buscan, por ejemplo, si la información está en forma de "almacenamiento electrónico", si se encuentra en un servicio informático remoto, si es "un registro […] correspondiente a un abonado" u otra información mencionada por la ECPA. En tercer lugar, deben considerar si lo que buscan es forzar su revelación o aceptar la

información revelada voluntariamente por el proveedor. En el primer caso, será necesario que determinen si precisan una orden de registro, una orden de tribunal 2703(d) o una citación para obligar a la revelación. Si la opción deseada es que se haga de forma voluntaria, deberán determinar si la ley permite la revelación. En la gráfica de la Sección F de este capítulo se muestra un método de utilidad para aplicar estas distinciones en la práctica.

La organización de este capítulo seguirá las diversas clasificaciones de la ECPA. La Sección B explica la estructura de clasificación de la ECPA que distingue entre proveedores de "servicios de comunicaciones electrónicas" y proveedores de "servicios informáticos remotos". En la Sección C se explican los distintos tipos de información que pueden divulgar los proveedores, como pueden ser contenidos "almacenados en formato electrónico" y "registros […] correspondientes a un abonado". La Sección D describe el proceso jurídico que deben seguir los agentes y fiscales para obligar a un proveedor a que revele la información. La Sección E se centra en la otra cara del problema y explica cuándo pueden los proveedores revelar informaciones de cuentas de manera voluntaria. En la Sección F aparece una gráfica resumida, mientras que el capítulo termina con dos secciones adicionales. En la Sección G se tratan tres problemas importantes que pueden surgir cuando los agentes obtienen registros de proveedores de red: medidas para conservar las pruebas, medidas para evitar la revelación a los sujetos y problemas de la Ley sobre Comunicaciones por Cable ("Cable Act"). Por último, en la Sección H se comentan las soluciones que pueden imponer los tribunales en caso de contravención de la ECPA.

Este capítulo incluye las enmiendas a la ECPA especificados por la Ley USA PATRIOT de 2001, Pub. L. Nº 107-56, 115 Stat. 272 (2001) (la "Ley PATRIOT"). La Ley PATRIOT aclaró y actualizó la ECPA a la luz de las nuevas tecnologías y, en algunos aspectos, relajó las restricciones sobre el acceso a las comunicaciones almacenadas para hacer cumplir la ley. Algunas de estas enmiendas, como se destaca aquí, está previsto que queden derogadas el 31 de diciembre de 2005. Véase Ley PATRIOT § 224, 115 Stat. 272, 295. Al personal de las fuerzas de seguridad que utilice disposiciones jurídicas cuya derogación ya esté programada se le recomienda encarecidamente que informen de sus experiencias a la Sección de Delitos Cibernéticos y Propiedad Intelectual a través del teléfono (202) 514-1026. La CCIPS puede trasladar esta información al Congreso, el cual decidirá si los cambios introducidos por la Ley PATRIOT deben convertirse en permanentes.

[índice]

B. Proveedores de servicios de comunicaciones electrónicas frente a proveedores de servicios informáticos remotos

La ECPA distingue a los proveedores cubiertos por la ley entre "proveedores de servicios de comunicaciones electrónicas" y "proveedores de servicios informáticos remotos". Para comprender estas condiciones resulta útil recordar la época en la que se redactó la ECPA, una ley de 1986. En aquel momento, los titulares de cuentas de red utilizaban normalmente proveedores de servicios de red de terceras partes por dos motivos. El primero de ellos es que los titulares de cuentas las utilizaban para enviar y recibir comunicaciones como correos electrónicos. El uso de redes informáticas para comunicarse provocó inquietudes en cuanto a la privacidad, ya que durante el envío y la recuperación de mensajes era común que estos se copiaran y almacenaran de manera temporal en varios ordenadores. Las copias creadas por estos proveedores de "servicios de comunicaciones electrónicas" y "almacenadas temporalmente de forma electrónica" durante la transmisión podían permanecer hasta varios meses en el ordenador del proveedor. Véase H.R. Rep. N° 99-647, en 22 (1986).

El segundo motivo por el que los titulares de cuenta recurrían a los proveedores de servicios de red era para subcontratar labores informáticas. Por ejemplo, los usuarios pagaban por almacenar archivos secundarios en ordenadores remotos o por procesar grandes cantidades de datos. Al contratar estos "servicios informáticos remotos" comerciales para que hicieran trabajos en su lugar, los usuarios enviaban una copia de su información privada a una tercera parte encargada de los servicios, que conservaba estos datos por si los necesitaba en el futuro. Los servicios informáticos remotos hicieron surgir inquietudes relacionadas con la privacidad, ya que los proveedores de los servicios conservaban

con frecuencia copias de los archivos de sus clientes. Véase S. Rep. N° 99-541 (1986), reimpreso en 1986 U.S.C.C.A.N. 3555, 3557.

La ECPA protege las comunicaciones conservadas por los proveedores de servicios de comunicaciones electrónicas si dichas comunicaciones se encuentran "almacenadas electrónicamente", así como las comunicaciones conservadas por proveedores de servicios informáticos remotos. Con este fin, la ley define "servicio de comunicaciones electrónicas", "almacenamiento electrónico" y "servicio informático remoto" como sigue:

"Servicio de comunicaciones electrónicas"

Un servicio de comunicaciones electrónicas "SCE" es "aquel servicio que proporciona al usuario de los mismos la capacidad para enviar o recibir comunicaciones por cable o electrónicas". 18 U.S.C. § 2510(15). (Si se desea consultar las definiciones de comunicación por cable y electrónica, véase el capítulo 4.C.2, más abajo). Por ejemplo, "las compañías telefónicas y compañías de correo electrónico" actúan generalmente como proveedores de servicios de comunicaciones electrónicas. Véase S. Rep. N° 99-541 (1986), reimpreso en 1986 U.S.C.C.A.N. 3555, 3568; véase también FTC v. Netscape Communications Corp., 196 F.R.D. 559, 560 (N.D. Cal. 2000) (en el que se destaca que Netscape, un proveedor de cuentas de correo electrónico a través de netscape.net, es un proveedor de SCE).

La historia legislativa y la jurisprudencia indican que el asunto clave a la hora de determinar si una empresa ofrece SCE es el papel de la misma al ofrecer la capacidad para enviar o recibir las comunicaciones precisas en cuestión, independientemente del objeto comercial principal de la compañía. Véase H.R. Rep. N° 99-647, en 65 (1986). Toda compañía o entidad gubernamental que proporcione a terceros los medios para comunicarse de manera electrónica puede ser un "proveedor de servicios de comunicaciones electrónicas" en relación con las comunicaciones que provea, aun en el caso de que la facilitación de estos servicios sea meramente secundaria con respecto a la finalidad principal del proveedor. Véase Bohach v. Ciudad de Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (una ciudad que proporcionaba un servicio de busca a sus oficiales de policía puede ser un proveedor de servicios de comunicaciones electrónicas); Estados Unidos v. Mullins, 992 F.2d 1472, 1478 (9° Cir. 1993) (una compañía aérea que ofrece a sus agencias de viajes un sistema de reservas informático al que se puede acceder a través de terminales individuales puede ser un proveedor de servicios de comunicaciones electrónicas).

Por el contrario, un servicio no puede proporcionar SCE con respecto a una comunicación si no ofrece la posibilidad de enviar o recibir dicha comunicación. Véase Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923, 930-31 (N.D. Cal. 1996) (un fabricante de videojuegos que accedió al correo electrónico privado almacenado en el sistema de boletines de otra empresa con el fin de sacar a la luz la infracción de derechos de propiedad intelectual no era un proveedor de servicios de comunicaciones electrónicas); State Wide Photocopy v. Tokai Fin. Servs. Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (una compañía financiera que utilizaba faxes y ordenadores pero que no ofrecía la capacidad de enviar o recibir comunicaciones no era un proveedor de servicios de comunicaciones electrónicas).

Es significativo que un simple usuario de SCE facilitados por otro no es un SCE. Por ejemplo, una página web no es un proveedor de servicios de comunicaciones electrónicas, a pesar de que puede enviar y recibir comunicaciones electrónicas de los clientes. En Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001), el demandante arguyó que Amazon.com (a quien él envió su nombre, número de tarjeta de crédito y otros datos identificativos) era un proveedor de servicios de comunicaciones electrónicas porque "sin receptores como Amazon.com, los usuarios no tendrían la posibilidad de enviar información electrónica". El tribunal rechazó esta argumentación y concluyó que Amazon estaba clasificado adecuadamente como usuario en lugar de como proveedor de SCE. Véase id.

"Almacenamiento electrónico"

En 18 U.S.C. § 2510(17) se define "almacenamiento electrónico" como "el almacenamiento temporal o intermedio de una comunicación por cable o electrónica secundario a la transmisión electrónica de la

misma" o, de otra manera, como "el almacenamiento de dicha comunicación por un servicio de comunicaciones electrónicas con el fin de conservar una copia de seguridad". La diferencia entre el significado cotidiano de "almacenamiento electrónico" y su limitada definición jurídica ha generado no poca confusión. Es fundamental recordar que "almacenamiento electrónico" hace referencia únicamente al almacenamiento temporal, realizado durante la transmisión por un proveedor de servicios de comunicaciones electrónicas. Por ejemplo, en la Litigación In re sobre privacidad de Doubleclick Inc., 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001), el tribunal concluyó que las cookies, que son información que guardan las páginas web en el ordenador del usuario y que se reenvían a la página web al acceder de nuevo a la misma, no entran en la definición de "almacenamiento electrónico" y, por tanto, tampoco de la ECPA a causa de "su prolongada conservación en los discos duros del demandante".

Para determinar si una comunicación está en "almacenamiento electrónico", resulta útil delimitar el destino final de la misma. Una copia de una comunicación se encuentra en "almacenamiento electrónico" solamente si se trata de una copia creada en un punto intermedio generada para enviarse a su destino final. Por ejemplo, un correo electrónico que haya sido recibido por el proveedor de servicios del receptor pero al que todavía éste no haya accedido está en "almacenamiento electrónico". Véase Steve Jackson Games, Inc. v. Servicio Secreto de Estados Unidos, 36 F.3d 457, 461 (5° Cir. 1994). En esta fase, la copia de la comunicación almacenada existe sólo como medida temporal e intermedia, a la espera de que el receptor la recupere del proveedor del servicio. Sin embargo, una vez que el receptor recupera el correo electrónico, la comunicación llega a su destino final. Si el receptor opta por conservar una copia de la comunicación a la que haya accedido en el sistema del proveedor, la copia almacenada en la red ya no estará en "almacenamiento electrónico" ya que ésta ya no estará en "almacenamiento temporal e intermedio […] secundario para […] la transmisión electrónica". 18 U.S.C. § 2510(17). En realidad, puesto que el proceso de transmisión hacia el receptor de destino ya ha concluido, la copia no es más que un archivo almacenado de forma remota. Véase Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635-38 (E.D. Pa. 2001) (en el que se concluye que dado que se obtuvo un correo electrónico desde su almacenamiento posterior a la transmisión, éste no estaba en "almacenamiento electrónico" y su obtención no estaba prohibida conforme a la ECPA); H.R. Rep. N° 99-647, en 64-65 (1986) (en el que se destaca la intención del Congreso de que los correos electrónicos y de voz consultados que se dejen en el sistema de un proveedor queden cubiertos por las disposiciones relativas a los servicios informáticos remotos, en lugar de las relativas a los servicios que conservan las comunicaciones en "almacenamiento electrónico").

En la práctica, del hecho de si un proveedor guarda una comunicación en "almacenamiento electrónico" o no depende si la empresa proporciona SCE con respecto a la comunicación. Los dos conceptos son similares: una empresa ofrece SCE con respecto a una comunicación solamente si el servicio guarda dicha comunicación en almacenamiento electrónico. De ello se infiere que si una comunicación no está en almacenamiento temporal e intermedio secundario para su transmisión electrónica, la empresa no puede proporcionar SCE para esa comunicación. En lugar de ello, la empresa proporcionará o bien "servicios informáticos remotos", también conocidos como SIR (se comentan más abajo) o bien ni SCE ni SIR. Véase el comentario a continuación.

"Servicios informáticos remotos"

El término "servicio informático remoto" ("SIR") se define en 18 U.S.C. § 2711(2) como "prestación pública de servicios de almacenamiento o procesamiento informáticos por medio de un sistema de comunicaciones electrónicas". Un "sistema de comunicaciones electrónicas" es "toda instalación telefónica, de radio, electromagnética, fotoóptica o fotoeléctrica utilizada para la transmisión de comunicaciones telefónicas o electrónicas, así como cualquier instalación informática o equipos electrónicos asociados que se usen para el almacenamiento electrónico de dichas comunicaciones". 18 U.S.C. § 2510(14).

Dicho de otra forma, un servicio informático remoto se presta desde un ordenador situado en otro lugar que almacena o procesa datos de un cliente. Véase S. Rep. N° 99-541 (1986), reimpreso en 1986 U.S.C.C.A.N. 3555, 3564-65. Por ejemplo, un proveedor de servicios que procese datos en régimen de tiempo compartido presta SIR. Véase H.R. Rep. N° 99-647, en 23 (1986). Un ordenador central en el

que se almacenen datos para su recuperación en el futuro también proporciona SIR. Véase Steve Jackson Games, Inc. v. Servicio Secreto de Estados Unidos, 816 F. Supp. 432, 443 (W.D. Tex. 1993) (en el que se concluye que el proveedor de servicios de boletines electrónicos era una empresa de servicios informáticos remotos). En contraposición a un proveedor de SCE, uno de SIR no almacena archivos de los clientes en su camino hacia el destino final, sino que el proveedor los almacena o procesa para comodidad del titular de la cuenta. En consecuencia, los archivos almacenados por un proveedor que actúe como SIR no pueden estar en "almacenamiento electrónico de acuerdo con § 2510(17).

En virtud de la definición establecida por § 2711(2), un servicio solamente puede ser un "servicio informático remoto" si está disponible "para el público". Los servicios son públicos si están a disposición de cualquier persona que cumpla con los procedimientos requeridos y que pague las cuotas correspondientes, si procede. Por ejemplo, America Online es un proveedor público: cualquier persona puede obtener una cuenta de AOL. (Al principio puede resultar extraño que se pueda cobrar una cuota por un servicio y que aún así se considere "público", pero esto no hace otra cosa que reflejar las relaciones comerciales del mundo físico. Por ejemplo, las salas de cine están abiertas "al público" puesto que cualquiera puede comprar una entrada y ver una película, a pesar de que las entradas no son gratuitas). Por el contrario, aquellos proveedores cuyos servicios solamente estén disponibles para las personas que tengan una relación especial con ellos no están disponibles para el público. Por ejemplo, los empresarios pueden ofrecer cuentas de red únicamente a sus empleados. Véase Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (en el que se interpreta la cláusula "que preste […] al público" de § 2702(a) para excluir un sistema interno de correo electrónico que se puso a disposición de un contratista pero no de "cualquier miembro de la comunidad en general"). Estos proveedores no pueden prestar servicios informáticos remotos porque sus servicios de red no están disponibles para el público.

El hecho de si una entidad es un proveedor de "servicios de comunicaciones electrónicas", de "servicios informáticos remotos" o de ninguno de ellos depende de la naturaleza de la comunicación concreta. Por ejemplo, un único proveedor puede prestar de forma simultánea "servicios de comunicaciones electrónicas" con respecto a una comunicación y "servicios informáticos remotos" en relación con otra.

Vamos a ilustrar con un ejemplo cómo funcionan estos principios en la práctica. Imaginemos que Joe envía un correo electrónico desde su cuenta del trabajo ("joe@goodcompany.com") a la cuenta personal de su amiga Jane ("jane@localisp.com"). El correo electrónico atravesará Internet hasta llegar a los servidores del proveedor de servicios de Internet, en este caso el ficticio LocalISP. Cuando el mensaje llega por primera vez a LocalISP, éste es un proveedor de SCE con respecto a este mensaje. Mientras Jane no acceda a LocalISP y consulte el mensaje, el correo electrónico de Joe se encuentra en "almacenamiento electrónico". Véase Steve Jackson Games, Inc. v. Servicio Secreto de Estados Unidos, 36 F.3d 457, 461 (5° Cir. 1994). Una vez que Jane recupere el correo de Joe, puede optar por borrar el mensaje del servidor de LocalISP o dejarlo almacenado ahí. Si decide guardar el correo electrónico en LocalISP, LocalISP se convierte en un proveedor de SIR (y no de SCE) en relación con el correo electrónico enviado por Joe. La función de LocalISP ha cambiado de transmisor del correo de Joe a un servicio de almacenamiento para un archivo guardado de manera remota en beneficio de Jane por un proveedor de SIR. Véase H.R. Rep. N° 99-647, en 64-65 (1986) (en el que se expone la intención del Congreso de tratar el correo electrónico abierto que esté almacenado en un servidor con arreglo a las disposiciones relativas a los servicios informáticos remotos, en lugar de servicios que guardan las comunicaciones en "almacenamiento electrónico").

Ahora imaginemos que Jane responde al correo electrónico de Joe. Su correo de respuesta atravesará de nuevo Internet hasta los servidores de la empresa de Joe, Good Company. Hasta que Joe recupere el correo de los servidores de Good Company, Good Company es un proveedor de SCE con respecto al mensaje de Jane (al igual que lo era LocalISP en relación con el correo electrónico original de Joe antes de que Jane lo leyera). Una vez que Joe acceda al mensaje de Jane y que la comunicación llegue a su destino (Joe), Good Company dejará de ser un proveedor de SCE con respecto a ese correo (de igual forma que LocalISP dejó de serlo en relación con el correo electrónico original de Joe cuando Jane lo leyó). Sin embargo, a diferencia de LocalISP, Good Company no se convierte en un proveedor de SIR si

Joe opta por almacenar el correo abierto en su servidor. En realidad, en lo que a este mensaje concreto respecta, Good Company no es proveedor de SCE ni de SIR. Good Company no presta SIR porque no ofrece servicios al público. Véase 18 U.S.C. § 2711(2) ("El término "servicio informático remoto" implica la prestación de servicios de almacenamiento o procesamiento informáticos al público por medio de un sistema de comunicaciones electrónicas"). (Se hace hincapié en este punto); Andersen Consulting, 991 F. Supp. en 1043. Teniendo en cuenta que Good Company no presta SCE ni SIR en relación con el correo electrónico abierto que se encuentra en la cuenta de Joe, el acceso a este mensaje ya no está sujeto a la ECPA, sino exclusivamente por la Cuarta Enmienda. Dicho en términos prácticos, el correo electrónico abierto de la cuenta de Joe queda fuera de la ECPA.

Por último, veamos el estatus de otras copias en esta situación: Jane ha descargado una copia del correo de Joe del servidor de LocalISP al ordenador personal de su casa, mientras que Joe ha descargado una copia del correo electrónico de Jane del servidor de Good Company a su ordenador de sobremesa del trabajo. Ninguno de los dos casos está sujeto a la ECPA. Aunque estos ordenadores contienen copias de correos electrónicos, éstas no se encuentran en el servidor de un proveedor de terceras partes o de SIR o SCE, por lo que la ECPA no es aplicable. El acceso a las copias de las comunicaciones almacenadas en el ordenador personal de Jane y en el ordenador del trabajo de Joe está regido única y exclusivamente por la Cuarta Enmienda. Véanse los capítulos 1 y 2.

Como ilustra este ejemplo, un solo proveedor puede prestar simultáneamente SCE con respecto a determinadas comunicaciones y SIR en relación con otras, o prestar SCE para ciertas comunicaciones y no prestar ni SCE ni SIR para otras. En la práctica, no obstante, en la mayor parte de los casos los agentes no tienen que lidiar con estas dificultades. En realidad, pueden redactar simplemente la orden adecuada en función de la información que busquen. Por ejemplo, si la policía sospecha que Jane y Joe han conspirado para cometer un delito, puede solicitar una orden o citación mediante la que obligue a LocalIsp a divulgar todos los archivos de la cuenta de Jane salvo aquellos que estén en "almacenamiento electrónico". En otras palabras, esto equivale a solicitar todos los correos electrónicos abiertos y archivos almacenados de Jane. Por otro lado, la policía puede solicitar una orden que fuerce a Good Company a revelar todos los archivos que se encuentren en "almacenamiento electrónico en la cuenta de Joe. Es decir, puede solicitar los correos electrónicos sin abrir de la cuenta de Joe. En la Sección F encontrará una gráfica aclaratoria. En los Apéndices B, E y F se ofrecen muestras del tipo de redacción que se puede utilizar.

[Índice]

C. Clasificación de los tipos de información en poder de los proveedores de servicios

Los proveedores de servicios de red pueden almacenar distintos tipos de información en relación con un cliente o abonado. Retomemos el intercambio de correos electrónicos entre Joe y Jane mencionado anteriormente. Es probable que el proveedor de servicios de Jane, LocalISP, tenga acceso a un conjunto de información sobre Jane y su cuenta. Por ejemplo, LocalISP puede tener correos abiertos y sin abrir, registros de cuenta que indiquen cuándo se ha conectado y desconectado Jane de LocalISP, información de la tarjeta de crédito de Jane para cobros y el nombre y la dirección de Jane. Si un agente o fiscal desea obtener estos registros, deben poder clasificar estos tipos de información utilizando el lenguaje de la ECPA. La ECPA subdivide la información en tres categorías: la información básica sobre los abonados mencionada en 18 U.S.C. § 2703(c)(2); "registros u otros datos correspondientes a un abonado o cliente del servicio" y "contenido". Véase 18 U.S.C. §§ 2510(8), 2703(c)(1).

1. Información básica de abonados mencionada en el 18 U.S.C. § 2703(c)(2)

En 18 U.S.C. § 2703(c)(2) se enumeran las categorías de la información básica sobre los abonados:

(A) nombre; (B) dirección; (C) registros sobre conexiones telefónicas locales y de larga distancia o sobre hora y duración de las sesiones; (D) antigüedad en el servicio (incluyendo la fecha de inicio) y

tipos de servicios utilizados; (E) número de teléfono o de cualquier otro aparato u otro número o identidad de abonado, incluyendo direcciones de red asignadas de forma temporal y (F) medios y origen del pago de dicho servicio (incluyendo número de tarjetas de crédito y cuentas bancarias)[.]

En general, los elementos de esta lista son relativos a la identidad de un abonado, su relación con su proveedor de servicios y los registros básicos de conexión en cada sesión. Esta lista no incluye otros registros más amplios relativos a transacciones, como información de entradas en el sistema que contenga las direcciones de correo electrónico de las personas con las que un cliente ha mantenido comunicación durante una sesión anterior. La Ley PATRIOT aumentó las categorías de la información básica sobre abonados en tres aspectos. Véase Ley PATRIOT § 210, 115 Stat. 272, 283 (2001). Agregó a 18 U.S.C. § 2703(c)(2) "registros de horas y duración de las sesiones" y "direcciones de red asignadas de forma temporal". En el marco de Internet, estos registros incluyen la dirección IP asignada por un proveedor de servicios de Internet a un cliente para una sesión concreta. También incluye otros datos relativos al acceso a la cuenta, como el número de teléfono utilizado para el acceso a Internet por marcación o la dirección IP de un usuario que accede a una cuenta por Internet. Asimismo, la PATRIOT Act añadió a esta lista de información de abonados los "medios y el origen de los pagos" que utiliza un cliente para pagar una cuenta "incluyendo números de tarjetas de crédito y cuentas bancarias".

2. Registros u otros datos correspondientes al cliente o abonado

18 U.S.C. § 2703(c)(1) cubre un segundo tipo de información: "un registro u otros datos correspondientes a un abonado o cliente del servicio (sin incluir el contenido de las comunicaciones)". Se trata de una categoría que abarca todos los registros que no sean contenido, incluyendo información básica de los abonados.

Entre los ejemplos más típicos de "registros […] correspondientes a un abonado" se incluyen los relativos a transacciones, como registros de cuenta que consignan el uso de la misma, datos de configuración para llamadas de teléfonos móviles y direcciones de correo electrónico de otras personas con la que el titular de la cuenta haya mantenido comunicación. Véase H.R. Rep. N° 103-827, en 10, 17, 31 (1994), reimpresos en 1994 U.S.C.C.A.N. 3489, 3490, 3497, 3511; Estados Unidos v. Allen, 53 M.J. 402, 409 (C.A.A.F. 2000) (en el que se concluye que "un registro que identifique la fecha, la hora, el usuario y la dirección detallada de Internet de las páginas web a las que haya accedido" un usuario constituyen "un registro u otros datos correspondientes a un abonado o cliente de dicho servicio" conforme a la ECPA). Véase también Hill v. MCI Worldcom, 120 F. Supp. 2d 1194, 1195-96 (S.D. Iowa 2000) (en el que se concluye que los "nombres, direcciones y números de teléfono de las partes […] a las que se llamó" constituyen "un registro u otra información correspondiente a un abonado o cliente de dicho servicio" para una cuenta de teléfono). Según la historia legislativa de las enmiendas de 1994 de § 2703(c), el objeto de separar la información básica de los abonados de otros registros no relacionados con el contenido era distinguir la primera de otros datos más reveladores sobre transacciones que pudieran contener el "perfil completo de las actividades en línea de una persona". H.R. Rep. N° 103-827 (1994), reimpreso en 1994 U.S.C.C.A.N. 3489, 3497, 3511.

3. Contenido

El contenido de una cuenta de red son los archivos que están almacenados en la misma. Véase 18 U.S.C. § 2510(8) ("el término "contenidos", cuando se utilice con respecto a la comunicación por cable, oral o electrónica incluye toda información relativa a la sustancia, el sentido o el significado de dicha comunicación"). Por ejemplo, los correos electrónicos o de voz almacenados son "contenidos", al igual que los archivos de procesamiento de textos guardados en las cuentas de red de los empleados. La línea del asunto en los correos electrónicos también se considera contenido. Cf. Brown v. Waddell, 50 F.3d 285, 292 (4° Cir. 1995) (en el que se destaca que los mensajes numéricos de busca suponen una "serie ilimitada de mensajes sustantivos codificados con números" al mantener que la interceptación de mensajes de busca exige el cumplimiento del Título III).

Los contenidos se pueden dividir a su vez en tres subcategorías: contenidos guardados en "almacenamiento electrónico" por proveedores de servicios de comunicaciones electrónicas, contenidos

almacenados por proveedores de servicios informáticos remotos y contenidos que no están almacenados por ninguno de estos dos tipos de proveedores. Las diferencias entre estos tipos de contenido se comentan en la Sección B, más arriba.

[índice]

D. Revelación forzosa con arreglo a la ECPA

En 18 U.S.C. § 2703 se exponen las medidas que debe adoptar el gobierno para forzar a los proveedores a revelar los contenidos de comunicaciones por cable o electrónicas almacenadas (incluyendo correo electrónico y de voz), así como otros datos como registros de cuentas e información básica de los abonados.

La sección 2703 ofrece cinco mecanismos de los que puede hacer uso una "entidad gubernamental" para obligar a un proveedor a revelar determinados tipos de información. Los cinco mecanismos, en orden ascendente según la actuación requerida, son los siguientes:

1) Citación;

2) Citación con aviso previo al abonado o cliente;

3) Orden judicial conforme a § 2703(d);

4) Orden judicial conforme a § 2703(d) con aviso previo al abonado o cliente y

5) Orden de registro.

Una de las características de las disposiciones de revelación forzosa de la ECPA es que cada proceso de un paso superior incluye por lo general el acceso a información que se puede obtener con un proceso de los niveles inferiores. Así, una orden judicial conforme a § 2703(d) puede obligar a todo lo que puede forzar una citación (más información adicional), mientras que una orden de registro puede obligar a la entrega de todo lo que pueda conseguirse con una orden conforme a § 2703(d) (y más). Como consecuencia de ello, el trabajo adicional necesario para satisfacer un umbral más alto se verá justificado con frecuencia, por una parte porque puede autorizar una revelación mayor y, por otra, porque perseguir un umbral más alto ofrece una seguridad adicional de que el proceso cumple plenamente la ley. Nótese, sin embargo, que el requisito del aviso se debe considerar una carga separada conforme a este análisis: una citación con aviso al abonado se puede utilizar para forzar la revelación de información a la que no se pueda acceder mediante una orden conforme a § 2703(d) sin aviso al abonado. (Existe una categoría pequeña de información cuya revelación se puede forzar conforme a la ECPA sin una citación. Al investigar el fraude en televentas, las fuerzas de seguridad pueden enviar una solicitud por escrito a un proveedor de servicios pidiendo el nombre, la dirección y el emplazamiento comercial de un abonado o cliente que se dedique a la televenta. Véase 18 U.S.C. § 2703(c)(1)(D)).

1. Citación

Los investigadores pueden emitir una citación para revelar información básica de abonados.

La ECPA permite al gobierno forzar la revelación de dos tipos de datos por medio de una citación. El primero de ellos es la información básica de abonados (se ha comentado anteriormente en la sección C.1) mencionado en 18 U.S.C. § 2703(c)(2):

(A) nombre; (B) dirección; (C) registros sobre conexiones telefónicas locales y de larga distancia o sobre hora y duración de las sesiones; (D) antigüedad en el servicio (incluyendo la fecha de inicio) y tipos de servicios utilizados; (E) número de teléfono o de cualquier otro aparato u otro número o

identidad de abonado, incluyendo direcciones de red asignadas de forma temporal y (F) medios y origen del pago de dicho servicio (incluyendo número de tarjetas de crédito y cuentas bancarias)[.]

18 U.S.C. § 2703(c)(2).

Asimismo, los agentes también pueden utilizar una citación para obtener información que quede fuera del alcance de la ECPA. El intercambio hipotético de correos entre Jane y Joe mencionado en la sección B de este capítulo nos viene muy bien como ejemplo: Good Company no prestaba "servicios informáticos remotos" ni "servicios de comunicaciones electrónicas" con respecto a los correos electrónicos abiertos que estaban en el servidor de Good Company. Véase sección B, más arriba. Por consiguiente, § 2703 no impone ningún requisito sobre su revelación y los investigadores pueden emitir una citación obligando a Good Company a divulgar la comunicación como lo harían de no existir la ECPA. De igual manera, la información relativa o perteneciente a una persona que no sea "cliente" ni "abonado" no está protegida por la ECPA y se puede obtener mediante una citación por la misma razón. Cf. Organización JD Ltda. v. Departamento de Justicia de Estados Unidos, 124 F.3d 354, 359-61 (2° Cir. 1997) (en el que se comenta el ámbito de la palabra "cliente" según se utiliza en la ECPA).

El límite legal para emitir una citación es bajo. Véase Estados Unidos v. Morton Salt Co., 338 U.S. 632, 642-43 (1950). No es necesario decir que las pruebas obtenidas como respuesta a una citación federal del gran jurado se deben proteger para evitar su divulgación conforme a la Norma Federal de Procedimiento Penal 6(e). Aparte de las citaciones federales del gran jurado se pueden utilizar otro tipo de citaciones para obtener la información de acuerdo con 18 U.S.C. § 2703(c)(2): bastará cualquier citación federal, estatal de gran jurado o judicial, así como una citación administrativa autorizada por una ley federal o estatal. Véase 18 U.S.C. § 2703(c)(2). Por ejemplo, se pueden utilizar las citaciones autorizadas por § 6(a)(4) de la Ley General de Inspectores. Véase 5 U.S.C. app. No obstante, hay al menos un tribunal que ha sentenciado que una citación de revelación emitida en un caso civil con arreglo a la Norma Federal de Procedimiento Penal 45 es inadecuada. Véase FTC v. Netscape Communications Corp., 196 F.R.D. 559 (N.D. Cal. 2000) (en el que se concluye que la citación de revelación no entraba dentro del significado "citación judicial"). En el Apéndice E se ofrece una muestra del tipo de lenguaje utilizado en las citaciones.

2. Citación con aviso previo al abonado o cliente

Los investigadores pueden emitir una citación para la revelación de correo electrónico abierto por parte del proveedor si cumplen con las disposiciones relativas a los avisos de §§ 2703(b)(1)(B) y 2705.

Los agentes que obtengan una citación y que den aviso previo al abonado o que cumplan con las disposiciones de aviso demorado de § 2705(a) pueden obtener:

1) todo lo que se puede obtener mediante una citación sin aviso;

2) "el contenido de cualquier comunicación por cable o electrónica" en posesión de un proveedor de servicios informáticos remotos "en representación de […] un abonado o cliente de dichos servicios". 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2); y

3) "el contenido de una comunicación por cable o electrónica que haya estado en almacenamiento electrónico en un sistema de comunicaciones electrónicas durante más de ciento ochenta días". 18 U.S.C. § 2703(a).

En la práctica, esto implica que los agentes pueden obtener el acceso al correo electrónico abierto (y a otras comunicaciones electrónicas o por cable almacenadas[(15)] "en almacenamiento electrónico" durante más de 180 días) a través de una citación, en tanto en cuanto cumplan con las disposiciones relativas a los avisos de la ECPA. Véase H.R. Rep. N° 99-647, en 64-65 (1986).

Estas disposiciones se pueden cumplir dando al cliente o abonado "aviso previo" de la revelación. Véase 18 U.S.C. § 2703(b)(1)(B). Sin embargo, 18 U.S.C. § 2705(a)(1)(B) y § 2705(a)(4) permiten demorar el aviso durante noventa días "en virtud de la ejecución de una certificación expresada por escrito de un oficial supervisor en la que se exponga que hay motivos para creer que la notificación de la existencia de la citación puede tener consecuencias adversas". 18 U.S.C. § 2705(a)(1)(B). Tanto "oficial supervisor" como "consecuencias adversas" son términos con una definición específica para la finalidad de la demora del aviso. Véase 2705(a)(2) (definición de "consecuencias adversas"); § 2705(a)(6) (definición de "oficial supervisor"). Esta disposición de la ECPA ofrece a los agentes un modo aceptable de demorar el aviso cuando éste pueda suponer una amenaza para una investigación pendiente o poner en peligro la vida o la integridad física de una persona. Una vez vencido el plazo de aviso demorado,[(16)] la ley exige que el gobierno envíe al cliente o abonado una copia de la solicitud o proceso junto con una carta en la que se explique la razón para la demora del aviso. Véase 18 U.S.C. § 2705(a)(5).

La disposición de la ECPA que permite obtener acceso al correo electrónico abierto mediante una citación combinada con el aviso previo al abonado deriva aparentemente de la interpretación de la jurisprudencia de la Cuarta y Quinta Enmiendas por parte del Tribunal Supremo. Véase Clifford S. Fishman & Anne T. McKenna, Wiretapping and Eavesdropping (*Escuchas telefónicas e interceptación de señales electrónicas*) § 26:9, en 26-12 (2ª ed. 1995). Si un individuo da unos documentos en papel a una tercera persona, un contable, por ejemplo, el gobierno puede emitir una citación para que esa tercera parte entregue los documentos sin infringir la Cuarta ni la Quinta Enmienda. Véase Estados Unidos v. Couch, 409 U.S. 322 (1973) (en el que se rechazan las alegaciones conforme a la Cuarta y la Quinta Enmiendas frente a la citación entregada al contable del demandado para la entrega de los datos comerciales que obraban en poder del primero). Al permitir que el gobierno emita una citación para acceder a correos electrónicos consultados, "el Congreso parece concluir que al "alquilar" espacio de almacenamiento informático mediante un servicio informático remoto, el cliente está en la misma situación que una persona que entrega datos comerciales a un cliente o abogado". Fishman & McKenna, §26:9, en 26-13.

3. Orden judicial conforme al artículo 2703(d)

Los agentes necesitan una orden judicial conforme a § 2703(d) para obtener la mayoría de los diarios de cuenta y de los registros sobre transacciones.

Los agentes que obtengan una orden judicial en virtud de 18 U.S.C. § 2703(d) pueden obtener:

- 1) todo lo que se puede obtener mediante una citación sin aviso; y
- 2) todos los "registros u otros datos correspondientes a un abonado o cliente de dicho servicio (sin incluir el contenido de las comunicaciones [en poder de los proveedores de servicios de comunicaciones electrónicas y de servicios informáticos remotos])". 18 U.S.C. § 2703(c)(1).

Una orden judicial autorizada en virtud de 18 U.S.C. § 2703(d) puede ser emitida por cualquier magistrado federal, tribunal de distrito o juez de un tribunal estatal equivalente. Véase 18 U.S.C. §§ 2703(d), 2711(3). Para la obtención de una orden de este tipo, conocida como orden judicial de "hechos expresables" o, simplemente, una orden "d", la entidad gubernamental debe exponer hechos específicos y expresables que demuestren que existen motivos razonables para creer que el contenido de una comunicación electrónica, los registros o los datos que se persigan son relevantes para una investigación penal que se esté llevando a cabo.

Id.

Esta norma no permite que las fuerzas de seguridad se limiten a certificar que tiene datos específicos y expresables que justificarían tal actuación. En lugar de ello, el gobierno debe ofrecer esos datos al tribunal en el momento de solicitar la orden. Véase Estados Unidos v. Kennedy, 81 F. Supp. 2d 1103,

1109-11 (D. Kan. 2000) (en el que se decide que una solicitud concluyente de una orden en virtud de § 2703(d) "no satisfacía los requisitos de la ley"). El Informe de la Cámara que acompañaba la enmienda de 1994 a § 2703(d) incluía el siguiente análisis:

Esta sección impone una norma intermedia para proteger los registros de transacciones en línea. Se trata de una norma superior a una citación, pero no a una orden con causa probable. El objeto de endurecer la norma para el acceso a los datos sobre transacciones es evitar que las fuerzas de seguridad puedan "ir de pesca". Con arreglo a esta norma intermedia, el tribunal debe concluir, basándose en la provisión de los datos por parte de las fuerzas de seguridad, que existen motivos específicos y expresables para creer que los registros son relevantes e importantes para una investigación criminal en curso.

H.R. Rep. N° 102-827, en 31 (1994), reimpreso en 1994 U.S.C.C.A.N. 3489, 3511 (se cita íntegramente en Kennedy, 81 F. Supp. 2° en 1109 n.8). En la práctica, para satisfacer este cliente debería ser suficiente con presentar un breve resumen de los hechos de la investigación y del papel que desempeñarán los registros para adelantar en la misma. En casos especialmente complejos es posible que se necesite una explicación más en profundidad. En el Apéndice B puede encontrar una solicitud y una orden de muestra conforme a § 2703(d).

Las órdenes conforme a 2703(d) emitidas por tribunales federales tienen efecto fuera del distrito del tribunal que las haya emitido. La ECPA permite a un juez emitir una orden conforme a § 2703(d) mediante la que se obligue a los proveedores a facilitar información aun en el caso de que el juez no esté designado en el distrito en el que esté almacenada la información. Véase 18 U.S.C. § 2703(d) (en la que se establece que "todo tribunal competente en materia de jurisdicción" puede emitir una orden en virtud de § 2703(d)) (se hace hincapié en este punto); 18 U.S.C. § 2711(3) (en la que se expone que un "tribunal con jurisdicción competente" tiene las implicaciones asignadas por la sección 3127 e incluye a cualquier tribunal federal que entre dentro de dicha definición, sin restricciones geográficas")[(17)]; 18 U.S.C. § 3127(2) (en el que se define "tribunal con jurisdicción competente").

Los tribunales estatales también pueden emitir órdenes en virtud de la sección 2703(d). Véase 18 U.S.C. §§ 2711(3), 3127(2)(B) (se define "tribunal con jurisdicción competente" para incluir "un tribunal con jurisdicción penal general de un Estado autorizado por la ley de dicho Estado para emitir órdenes que autoricen el uso de un dispositivo de registro de llamadas o de control y rastreo"). Sin embargo, la ley no confiere validez extraterritorial a las órdenes conforme a § 2703(d) emitidas por tribunales estatales. Véase 18 U.S.C. §§ 2711(3).

4. Orden conforme al § 2703(d) con aviso previo al abonado o cliente

Los investigadores pueden obtener todo lo que haya en una cuenta, salvo los correos electrónicos o de voz que no hayan sido abiertos, a través de un proveedor que lo haya sido durante 180 días o menos mediante una orden judicial conforme a § 2703(d) que cumpla con las directrices de aviso de § 2705.

Los agentes que obtengan una orden judicial en virtud de 18 U.S.C. § 2703(d) y que den aviso previo al abonado o que cumplan con las disposiciones de aviso demorado de § 2705(a) pueden obtener:

- 1) todo lo que se puede obtener mediante una orden judicial conforme a § 2703(d) sin aviso;
- 2) "el contenido de cualquier comunicación por cable o electrónica" en posesión de un proveedor de servicios informáticos remotos "en representación de […] un abonado o cliente de dichos servicios". 18 U.S.C. § 2703(b)(1)(B)(ii), § 2703(b)(2); y
- 3) "el contenido de una comunicación por cable o electrónica que haya estado en almacenamiento electrónico en un sistema de comunicaciones electrónicas durante más de ciento ochenta días". 18 U.S.C. § 2703(a).

Desde el punto de vista práctico, esto implica que el gobierno puede obtener el contenido íntegro de la cuenta de un abonado, excepto el correo electrónico y de voz no abierto (que haya estado en "almacenamiento electrónico" durante 180 días o menos), mediante una orden en virtud de § 2703(d) que cumpla con las directrices de aviso previo de § 2703(b)(1)(B).[(18)]

Como alternativa a dar el aviso previo, los agentes pueden obtener una orden para demorar la notificación hasta noventa días cuando ésta pueda poner en peligro la investigación. Véase 18 U.S.C. § 2705(a). En casos así, los agentes podrán obtener la orden por lo general incluyendo una solicitud adecuada en la solicitud 2703(d) de los agentes y en la orden propuesta; en el Apéndice B se ofrece una muestra. Los agentes también pueden solicitar al tribunal ampliaciones de la demora. Véase 18 U.S.C. § 2705(a)(1)(A), § 2705(a)(4). Las normas jurídicas para obtener una orden judicial para demorar el aviso reflejan las normas de la certificación del aviso demorado por parte de un oficial supervisor. Véase la sección D.2., más arriba. El solicitante debe convencer al tribunal de "que existen motivos para creer que la notificación de la existencia de la orden judicial puede […] poner en peligro la vida o la integridad física de una persona, [provocar] la huida del proceso judicial, [provocar] la destrucción o manipulación de pruebas, [provocar] la intimidación de testigos potenciales o […] poner en grave peligro una investigación o retrasar indebidamente un juicio". 18 U.S.C. § 2705(a)(1)(A), § 2705(a)(2). Cabe destacar que el solicitante debe satisfacer este requisito cada vez que pida una prórroga del aviso demorado.

5. Orden de registro

Una orden de registro permitirá a los investigadores obtener el contenido íntegro de una cuenta. La ECPA no exige que el gobierno notifique al cliente o abonado si se obtiene la información de un proveedor mediante una orden de registro.

Los agentes que obtengan una orden de registro conforme a la Norma 41 de las Normas Federales de Procedimiento Penal o una orden estatal equivalente pueden obtener:

- 1) todo lo que se puede obtener mediante una orden judicial conforme a § 2703(d) con aviso y
- 2) "el contenido de una comunicación por cable o electrónica que lleve en almacenamiento electrónico en un sistema de comunicaciones electrónicas durante ciento ochenta días o menos". 18 U.S.C. § 2703(a).
- En otras palabras, los agentes pueden obtener todos los registros y todo el contenido de una cuenta si consiguen una orden de registro basada en causa probable y de acuerdo con la Norma Federal de Procedimiento Penal.[(21)] La orden de registro puede ejecutarse ante el proveedor de servicios, obligando a éste a facilitar a las fuerzas de seguridad la información descrita en la misma. Es importante destacar que la obtención de una orden de registro permite pasar por alto la necesidad de advertir al abonado. Véase 18 U.S.C. § 2703(b)(1)(A). Es más, dado que la orden es emitida por un magistrado neutral basada en causa probable, la obtención de una orden de este tipo aísla el proceso de manera efectiva frente a alegaciones conforme a la Cuarta Enmienda.

Si bien la mayoría de las órdenes de registro obtenidas en virtud de la Norma 41 se limitan a "un registro de la propiedad […] en el distrito" correspondiente al magistrado que lo autoriza, es posible conseguir órdenes de registro conforme a § 2703(a) emitidas por "un tribunal federal con jurisdicción sobre el delito que se esté investigando", incluso para registros que se lleven a cabo en otro distrito.[(22)] 18 U.S.C. § 2703(a). (Asimismo, los tribunales estatales también pueden emitir órdenes conforme a § 2703(a), aunque la ley no concede efecto a estas órdenes fuera de los límites de la jurisdicción territorial del tribunal. Véase id.) Por lo demás, en la práctica, las órdenes de registro en virtud de § 2703(a) se obtienen de igual manera que las que se hacen conforme a la Norma 41. Al igual que con una orden habitual conforme a la Norma 41, los investigadores deben redactar una declaración jurada y

una propuesta para la orden que cumpla con la Norma 41. Véase 18 U.S.C. § 2703(a). Sin embargo, cuando un magistrado firma la orden, normalmente no son los propios investigadores los que registran los ordenadores del proveedor en busca de los materiales descritos en la misma. En lugar de ello, entregan la orden al proveedor como lo harían con una citación y éste suministra el material descrito en la orden.

Recientemente un tribunal de distrito sentenció que la práctica de hacer que los proveedores de servicios faciliten los materiales especificados en una orden de registro era ilegal. Véase Estados Unidos v. Bach, 2001 WL 1690055 (D. Minn. 14 de diciembre de 2001). En el caso Bach, unos oficiales de las fuerzas de seguridad estatales obtuvieron una orden de registro conforme a la ley estatal para obtener información relativa a una cuenta de correo electrónico de Yahoo y la enviaron por fax a Yahoo, que facilitó los documentos en cuestión. El tribunal de distrito anuló los resultados del registro por considerarlo una infracción de la Cuarta Enmienda. El tribunal concluyó que la Cuarta Enmienda concede las protecciones codificadas en 18 U.S.C. § 3105, que exige que esté presente un oficial de las fuerzas de seguridad y actúe en la ejecución de una orden de registro. Según el tribunal, "la sección 2703 no es una excepción y no ofrece un modo alternativo de ejecución con respecto a la sección 3105", por lo que se ordena por ley que los oficiales de las fuerzas de seguridad cumplan con § 3105 al ejecutar una orden de registro en virtud de 2703(a). El tribunal sentenció que aun en ausencia de obligación jurídica, la Cuarta Enmienda exige que esté presente un oficial de las fuerzas de seguridad y que actúe en la ejecución de órdenes de registro, incluyendo las emitidas conforme a 2703(a).

El gobierno ha apelado el fallo de Bach. El informe del gobierno destaca que, dejando a un lado la cuestionable jurisprudencia de la Cuarta Enmienda en el caso Bach y lo inadecuado de la anulación, la ECPA deja clara la intención del Congreso de autorizar el uso de órdenes de registro conforme a § 2703 para obtener contenidos de un abonado como una forma de proceso obligatorio dirigido a proveedores de red, no como una orden de registro tradicional. Véase por ejemplo 18 U.S.C. §§ 2702(b)(2), (c)(1) (en el que se establece explícitamente que un proveedor puede revelar registros pertenecientes a un abonado en respuesta a un proceso conforme a § 2703). Por otra parte, aunque 18 U.S.C. § 3105 fuera aplicable a las órdenes entregadas conforme a la ECPA, § 3105 no exige la presencia de las fuerzas de seguridad cuando los proveedores de servicios recaban y facilitan la información en virtud de una orden de registro, ya que no se incurre en los problemas asociados con el ejercicio privado de poderes de registro y confiscación cuando los proveedores recaban y suministran la información como respuesta a una orden. Véase Solicitud In re de Estados Unidos de una orden que autorice un seguimiento en progreso de comunicaciones por cable mediante dispositivos telefónicos, 616 F.2d 1122, 1130 (9° Cir. 1980); Solicitud In re de Estados Unidos de una orden que autorice la instalación de un registro de llamadas o de un decodificador de tonos e identificador de llamadas, 610 F.2d 1148, 1154 (3° Cir. 1979). Por otra parte, desde el sentido práctico, exigir la presencia de las fuerzas de seguridad durante la ejecución de estas órdenes de registro resultaría extraordinariamente oneroso, ya que los registros pueden precisar mucho tiempo y los PSI conservan la información de las cuentas en diversos lugares. Asimismo, es difícil imaginar de qué manera puede ser útil un oficial de las fuerzas de seguridad durante la recuperación de los registros especificados por parte de un proveedor de servicios.

No obstante, para ser prudentes y hasta que no se resuelvan definitivamente los problemas de Bach, se aconseja a los oficiales de las fuerzas de seguridad que preparen una orden en virtud de § 2703 que pidan en su solicitud de la orden de registro que el magistrado permita expresamente el envío por fax al PSI y la ejecución de la orden sin la presencia de oficiales. Para consultar el tipo de lenguaje u otra información y asesoramiento en relación con el caso Bach, póngase en contacto con la Sección de Delitos Cibernéticos y Propiedad Intelectual a través del número de teléfono (202) 514-1026.

[Índice]

E. Revelación voluntaria

Los proveedores de servicios que no sean públicos pueden revelar libremente tanto el contenido como otros registros relativos a las comunicaciones almacenadas. La ECPA impone restricciones a

la revelación voluntaria por parte de proveedores de servicios públicos, aunque también incluye excepciones a dichas restricciones.

Las directrices de la ECPA sobre la revelación voluntaria aparecen en 18 U.S.C. § 2702. Estas directrices determinan cuándo un proveedor de SIR o SCE puede revelar contenidos y otra información voluntariamente, tanto al gobierno como a entidades no gubernamentales. Si el proveedor puede revelar la información al gobierno y está dispuesto a hacerlo de forma voluntaria, las fuerzas de seguridad no necesitan obtener una orden legal para forzar la revelación. Si el proveedor no puede o no está dispuesto a revelar la información, los agentes deben acogerse a las directrices de revelación forzosa y obtener las órdenes jurídicas correspondientes.

A la hora de considerar si un proveedor de SIR o SCE puede revelar contenidos o registro, la primera pregunta que se deben formular los agentes es si el servicio en cuestión ofrecido por el proveedor está disponible "para el público". Si el proveedor no presta el servicio correspondiente "al público", la ECPA no pone ninguna restricción a la revelación. Véase 18 U.S.C. § 2702(a). Por ejemplo, en Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998), la compañía petrolífera UOP contrató a la empresa de consultoría Andersen Consulting y dio a los empleados de Andersen cuentas en la red informática de UOP. Tiempo después, cuando las relaciones entre UOP y Andersen empeoraron, UOP reveló al *Wall Street Journal* correos electrónicos que los empleados de Andersen habían dejado guardados en la red de UOP. Andersen presentó una denuncia basada en que la revelación de sus contenidos por parte del proveedor UOP había infringido la ECPA. El tribunal de distrito desestimó la demanda alegando que UOP no prestaba servicios de comunicaciones electrónicas al público.

Conceder acceso a Andersen al sistema de correo electrónico [de UOP] no equivale a prestar servicio de correo electrónico al público. UOP contrató a Andersen para llevar a cabo un proyecto y por ello se le dio acceso al sistema de correo electrónico de UOP de igual manera que a los empleados de ésta. Andersen no era un miembro de la comunidad en general, sino un contratista.

Id. en 1043. En vista de que UOP no prestaba servicios al público, la ECPA no prohibía la revelación de los contenidos pertenecientes a los "abonados" de UOP.

Si los servicios ofrecidos por el proveedor están disponibles para el público en general, la ECPA prohíbe tanto la revelación del contenido a terceras partes como la de otros registros a *cualquier entidad gubernamental*, a menos que sea aplicable una excepción legal.[(21)] La sección 2702(b) incluye excepciones para la revelación de contenidos y § 2702(c), a su vez, incluye excepciones para la revelación de otros datos sobre clientes.

La ECPA prevé la revelación voluntaria de contenidos cuando:

1) la divulgación "pueda repercutir sobre la prestación del servicio o para la protección de los derechos o propiedades del proveedor de dicho servicio", § 2702(b)(5);

2) la divulgación se realice "a un organismo de las fuerzas de seguridad […] si los contenidos […] fueron obtenidos de manera involuntaria por el proveedor del servicio […] [y] aparentemente están relacionados con la comisión de un delito", § 2702(b)(6)(A);

3) el proveedor "crea de manera razonable que una emergencia que implique riesgo inmediato de muerte o lesiones físicas graves a personas exige la revelación sin demora de la información", § 2702(b)(6)(C);

4) la Ley de Protección de Menores y Castigo de Agresores Sexuales de 1998, 42 U.S.C. § 13032, ordena la revelación, 18 U.S.C. § 2702(b)(6)(B); o

5) la revelación se realice al destinatario de la comunicación con el consentimiento de éste o del remitente, a una dirección de reenvío o en virtud de una orden judicial o proceso jurídico. § 2702(b)(1)-(4).

La ECPA prevé la revelación voluntaria de registros de clientes, sin incluir contenidos, por parte de un proveedor a una entidad gubernamental si:[(22)]

1) la divulgación "puede repercutir sobre la prestación del servicio o para la protección de los derechos o propiedades del proveedor de dicho servicio", § 2702(c)(3);

2) el proveedor "cree de manera razonable que una emergencia que implique riesgo inmediato de muerte o lesiones físicas graves a personas" justifica la revelación", § 2702(c)(4); o

3) la divulgación se realiza con el consentimiento del destinatario o en virtud de una orden judicial o proceso jurídico § 2702(c)(1)-(2).

En general, estas excepciones permiten que un proveedor haga públicos datos cuando las necesidades de seguridad pública y de los proveedores del servicio pesen más que los problemas de privacidad de los clientes o si es poco probable que la revelación suponga una amenaza grave a los intereses de privacidad.

[Índice]

F. Guía rápida de referencia

Revelación voluntaria **¿Permitida?**		**Mecanismos para forzar la revelación**		
Proveedor público	Proveedor privado		Proveedor público	Proveedor privado
Datos básicos sobre el abonado, de sesión y facturación	Al gobierno no, a menos que sea aplicable la excepción § 2702(c) [§ 2702(a)(3)]	Sí [§ 2702(a)(3)]	Citación; orden 2703(d) u orden de registro [§ 2703(c)(2)]	Citación; orden 2703(d) u orden de registro [§ 2703(c)(2)]
Otros registros sobre transacciones o cuentas	Al gobierno no, a menos que sea aplicable la excepción § 2702(c) [§ 2702(a)(3)]	Sí [§ 2702(a)(3)]	Orden 2703(d) u orden de registro [§ 2703(c)(1)]	Orden 2703(d) u orden de registro [§ 2703(c)(1)]
Comunicaciones consultadas (correo electrónico y de voz abierto) almacenado por el proveedor y otros archivos guardados	No a menos que sea aplicable la excepción § 2702(b) [§ 2702(a)(2)]	Sí [§ 2702(a)(2)]	Citación con aviso; orden 2703(d) con aviso u orden de registro [§ 2703(b)]	Citación; La ECPA no es aplicable [§ 2711(2)]
Comunicación no consultada, incluyendo correo electrónico y de voz	No a menos que sea aplicable la excepción	Sí [§ 2702(a)(1)]	Citación con aviso; orden 2703(d) con aviso u orden de	Citación con aviso; orden 2703(d) con aviso u orden de

(en almacenamiento electrónico durante más de 180 días)	§ 2702(b) [§ 2702(a)(1)]		registro [§ 2703(a,b)]	registro [§ 2703(a,b)]
Comunicación no consultada, incluyendo correo electrónico y de voz (en almacenamiento durante 180 días o menos)	No a menos que sea aplicable la excepción § 2702(b) [§ 2702(a)(1)]	Sí [§ 2702(a)(1)]	Orden de registro [§ 2703(a)]	Orden de registro [§ 2703(a)]

[Índice]

G. La colaboración con los proveedores de red: conservación de pruebas, evitar la revelación a los sospechosos y dificultades relacionadas con la Ley sobre Comunicaciones por Cable

Por lo general, los investigadores se deben poner en contacto con los proveedores de servicios de red antes de emitir citaciones o de obtener órdenes judiciales que les obliguen a revelar información.

Los oficiales de las fuerzas de seguridad que obtienen registros en virtud de la ECPA entienden pronto la importancia de comunicarse con los proveedores de servicios de red. Esto pasa porque cada proveedor trabaja de una forma. Unos conservan registros muy completos durante mucho tiempo, mientras que otros apenas conservan algunos registros o incluso ninguno. Para algunos proveedores es muy fácil cumplir con las solicitudes de información de las fuerzas de seguridad; a otros les cuesta mucho esfuerzo satisfacer incluso peticiones simples. Estas diferencias tienen su origen en las diversas filosofías, recursos, equipos y programas de los distintos proveedores de servicios de red. En vista de estas diferencias, los agentes suelen preferir comunicarse antes con los proveedores para saber cómo funcionan *antes* de obtener una orden legal que les obligue a actuar.

La ECPA cuenta con dos disposiciones concebidas para ayudar a los oficiales de las fuerzas de seguridad que trabajan con proveedores de servicios de red. Si se utilizan adecuadamente, estas disposiciones contribuyen a garantizar que los proveedores no eliminen los registros necesarios o comuniquen a otros que se está llevando a cabo una investigación.

1. Conservación de pruebas con arreglo al 18 U.S.C. § 2703(f)

Los agentes pueden dar instrucciones a los proveedores de que conserven los registros existentes a la espera de la autorización del proceso legal obligatorio. No obstante, estas solicitudes no tienen efecto futuro.

En general, no hay ninguna ley que regule cuánto tiempo deben conservar los proveedores de servicios de red los datos de cuenta en Estados Unidos. Algunos los conservan durante meses, otros unas horas y otros no los conservan. Desde el punto de vista práctico, esto implica que se pueden destruir o perder las pruebas antes de que las fuerzas de seguridad puedan obtener la orden legal correspondiente que fuerce la revelación. Por ejemplo, los agentes pueden enterarse de un caso de pornografía infantil el día 1, comenzar a trabajar en la orden de registro el día 2, obtenerla el día 5 y averiguar que el proveedor de servicios de red eliminó los registros como parte de la actividad normal de la empresa el día 3. Para reducir al mínimo el riesgo, la ECPA permite que el gobierno dé instrucciones a los proveedores para que "congelen" las comunicaciones y los registros almacenados en virtud de 18 U.S.C. § 2703(f). Concretamente, § 2703(f)(1) establece que:

Un proveedor de servicios de comunicaciones por cable o electrónicas o de servicios informáticos remotos que reciba una solicitud procedente de una entidad gubernamental adoptará todas las medidas necesarias para conservar los registros y otras pruebas que obren en su poder durante el tiempo que se tarde en emitir una orden judicial u otro proceso.

No existe ningún formato prescrito jurídicamente para las solicitudes § 2703(f). Por tanto, a pesar de que una simple llamada de teléfono sería adecuada, es aconsejable hacerlo mediante un fax o un correo electrónico por dos razones: primero porque supone una prueba documental y además porque evita los malentendidos. Al recibir la solicitud del gobierno, el proveedor deberá conservar los registros durante 90 días, renovables durante otro período de 90 días si así lo pide el gobierno. Véase 18 U.S.C. § 2703(f)(2). En el Apéndice F se ofrece una carta § 2703(f) de muestra.

Los agentes que envíen cartas § 2703(f) a proveedores de servicios de red deben ser conscientes de dos limitaciones. En primer lugar, la autoridad para ordenar a los proveedores que conserven datos y otras pruebas no tiene incidencia en el futuro. Es decir, una carta conforme a § 2703(f) puede dar instrucciones a un proveedor para que conserve los registros que ya se han creado, pero no puede ordenarle que guarde registros que no se han creado todavía. Si los agentes desean que los proveedores registren información sobre comunicaciones electrónicas futuras, deberán cumplir con las leyes de vigilancia electrónica mencionadas en el capítulo 4.

Otra limitación de § 2703(f) es que cabe la posibilidad de que algunos proveedores no puedan cumplir de manera efectiva las solicitudes § 2703(f). En la fecha en que se elaboró este escrito, por ejemplo, el software utilizado por America Online normalmente precisa que AOL restablezca la contraseña de una cuenta si pretende cumplir con una solicitud § 2703(f) para conservar correos electrónicos guardados. Esta operación puede perfectamente poner sobre aviso al sospechoso. Por ello, los agentes enviarán o no cartas § 2703(f) a AOL u otros proveedores que utilicen un software similar, dependiendo de la situación. La clave es una comunicación eficaz: los agentes deben ponerse en contacto con el proveedor de red antes de ordenarle que adopte medidas que pueden tener consecuencias adversas no planeadas. No pueden tomar decisiones fundadas sobre la investigación sin conocer las prácticas concretas, los puntos fuertes y las limitaciones del proveedor.

2. Mandamiento de no revelación de la existencia de una orden, citación u orden judicial

18 U.S.C. § 2705(b) establece que:

Un organismo gubernamental que actúe con arreglo a la sección 2703, siempre y cuando no esté obligado a notificar al abonado o cliente conforme a la sección 2703(b)(1) o en tanto en cuanto pueda demorar dicho aviso en virtud del apartado (a) de esta sección, puede solicitar una orden a un tribunal mediante la cual se den instrucciones a un proveedor de servicios de comunicaciones electrónicas o servicios informáticos remotos a los que esté dirigida una orden, citación u orden judicial, durante el tiempo que el tribunal estime oportuno, para que no comunique a ninguna persona la existencia de dicha orden, citación u orden judicial. El tribunal aprobará esta medida si determina que existen motivos para pensar que la notificación de la existencia de la orden, citación u orden judicial:

(1) pondrá en peligro la vida o la integridad física de una persona;

(2) provocará la huida del proceso judicial;

(3) causará la destrucción o manipulación de pruebas;

(4) podrá dar pie a la intimidación de testigos potenciales; o

(5) puede poner en peligro de cualquier otra forma una investigación o retrasar indebidamente un juicio.

18 U.S.C. § 2705(b).

Esto permite a los agentes solicitar una orden judicial por la que se den instrucciones a los proveedores de servicios de red para que no revelen la existencia de un proceso forzoso cuando el propio gobierno no tenga la obligación jurídica de comunicar el proceso al cliente o abonado. Si el proceso en cuestión es una orden § 2703(d) o § 2703(a), los agentes pueden incluir sencillamente el texto adecuado en la solicitud y en la orden propuesta. Si, por el contrario, los agentes pretenden forzar la revelación de información mediante una citación, deberán solicitar esta orden por separado.

3. La Ley sobre Comunicaciones por Cable, 47 U.S.C. § 551

La Ley sobre Comunicaciones por Cable restringe el acceso del gobierno a los registros de los operadores de comunicaciones por cable cuando los datos guarden relación con servicios normales por cable. No limita el acceso del gobierno a los registros relacionados con el acceso a Internet o el servicio telefónico prestado por un operador de cable.

En 1984, el Congreso aprobó la Ley sobre la Política de las Comunicaciones por Cable ("la Ley sobre Comunicaciones por Cable"), 47 U.S.C. § 551, exponiendo un sistema restrictivo de normas para controlar el acceso de las fuerzas de seguridad a los datos que obraran en posesión de una compañía de servicios por cable. Conforme a estas normas, ni siquiera una orden de registro era suficiente para poder acceder a los registros de estas empresas. La única forma mediante la cual podía el gobierno obtener "información personal sobre los abonados de un servicio de cable" era venciendo una pesadísima carga de pruebas en un proceso adverso en un tribunal, como se especifica en 47 U.S.C. § 551(h).

Después de la aprobación de la Ley sobre Comunicaciones por Cable en 1984, los distribuidores comenzaron a prestar servicios telefónicos y de acceso a Internet. Algunas de estas empresas afirmaron que las estrictas restricciones de divulgación de la Ley sobre Comunicaciones por Cable no sólo regían la prestación de servicios de programación por cable tradicionales, sino también la de servicios de teléfono e Internet. El Congreso respondió con la Ley USA PATRIOT de 2001, enmendando la Ley sobre Comunicaciones por Cable para especificar que sus restricciones sobre la divulgación son aplicables únicamente a los registros que revelen qué programación habitual de televisión por cable compra un cliente, como pueden ser canales premium concretos o espectáculos en "pay per view". Véase Ley PATRIOT § 211, 115 Stat. 272, 283-84 (2001). Concretamente, los distribuidores de servicios por cable pueden revelar información sobre abonados al gobierno de conformidad con la ECPA, Título III, y la ley sobre el Registro de llamadas y control y rastreo, exceptuando "datos que revelen la selección del abonado de los servicios de cable de la programación de vídeo". 47 U.S.C. § 551(c)(2)(D). La información que incluya la selección de la programación de vídeo por parte de los abonados permanece sujeta a las restricciones de 47 U.S.C. § 551(h).

[Índice]

H. Remedios

1. Anulación

La ECPA no contempla la anulación. Véase 18 U.S.C. § 2708 ("Las soluciones y sanciones [frente a los daños] descritas en este capítulo son las únicas soluciones y soluciones judiciales para infracciones inconstitucionales de este capítulo"). Por consiguiente, la infracción inconstitucional de la ECPA no da como resultado la anulación de las pruebas. Véase Estados Unidos v. Smith, 155 F.3d 1051, 1056 (9° Cir. 1998) ("La Ley sobre Comunicaciones Almacenadas desestima de forma expresa la exclusión como solución"); Estados Unidos v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("La anulación no es un remedio que contemple la ECPA"); Estados Unidos v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("El Congreso no contempló la anulación cuando una de las partes obtuviera datos o registros almacenados sobre transacciones infringiendo la ley"), afirmado, 225 F.3d 656, 2000 WL 1062039 (4° Cir. 2000); Estados Unidos v. Charles, 1998 WL 204696, en *21 (D. Mass. 1998) ("La ECPA solamente prevé una solución civil frente a la contravención de § 2703"); Estados Unidos v. Reyes, 922

F. Supp. 818, 837-38 (S.D.N.Y. 1996) ("La exclusión de las pruebas no se encuentra entre las soluciones disponibles para esta infracción de la ECPA […] El remedio para la infracción de [18 U.S.C. § 2701-11] reside en una acción civil").[(23)]

Si un consejo de la defensa persigue la anulación de pruebas obtenidas vulnerando la ECPA, es probable que apelen a McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998). En este caso que se sale de lo común, el juez Sporkin prohibió a la marina de Estados Unidos que despidiera al veterano Timothy R. McVeigh, con una antigüedad de 17 años en este cuerpo, después de averiguar que McVeigh era homosexual. La marina se enteró de la orientación sexual de McVeigh cuando éste envió un correo electrónico firmado como "Tim" desde su cuenta con el nombre de usuario "boysrch" de AOL a otra cuenta de AOL de una voluntaria civil de la marina. Cuando la voluntaria examinó el "directorio de perfil de miembros" de AOL, averiguó que "boysrch" pertenecía a un militar varón destinado en Honolulu que consignaba "homosexual" en su estado civil. La voluntaria, sospechando que el mensaje provenía de McVeigh, reenvió el correo electrónico y su perfil del directorio a los oficiales del submarino en el que éste prestaba servicio. Fue entonces cuando los oficiales comenzaron a investigar la orientación sexual de McVeigh. A fin de confirmar la identidad de McVeigh, un abogado asistente de la marina contactó por teléfono con AOL y se inventó un pretexto para explicar por qué necesitaba saber el nombre real de "boyrsch". El abogado no informó a su interlocutor de que era un militar de la marina. Una vez que el representante de AOL confirmó que el nombre de usuario "boysrch" pertenecía a la cuenta de McVeigh, la marina inició un proceso de despido contra éste. Poco antes de que se produjera su despido, McVeigh interpuso una demanda y solicitó un mandamiento judicial preliminar que bloqueara su cese. El juez Sporkin concedió a McVeigh su solicitud el día antes del despido.

La opinión del juez Sporkin refleja tanto la cargada atmósfera política del caso como la prensa de los acontecimientos que rodearon la emisión de la opinión.[(24)]

Al criticar a la marina por sustituir el proceso legal de la ECPA por subterfugios para obtener de AOL la información básica de abonado de McVeigh, el juez Sporkin realizó declaraciones que se podían interpretar como una lectura del remedio de anulación de la ECPA por infracciones flagrantes de la ley:

Es elemental que la información obtenida de forma inadecuada se puede anular si se han vulnerado los derechos de una persona. En la era de "Gran Hermano", donde se pasan por alto o se marginan los intereses de privacidad de las personas en todos los ámbitos de la vida mediante la tecnología y otros medios, es fundamental que se observen estrictamente las leyes que protegen explícitamente estos derechos.

Id. en 220. Mientras que la ECPA se debe observar estrictamente, la afirmación de que la anulación es adecuada cuando la información se obtenga mediante la contravención de "los derechos de una persona" es cuando menos sorprendente. Tanto la jurisprudencia como el texto de la ECPA propiamente dicha establecen claramente que ésta no contempla el remedio de la anulación para infracciones inconstitucionales. Por consiguiente, esta afirmación se debe interpretar como que hace referencia únicamente a los derechos *constitucionales*.

2. Acciones civiles y revelación

Aunque la ECPA no contempla la anulación para infracciones constitucionales, sí prevé daños civiles (incluyendo, en ocasiones, sanciones punitivas), así como la posibilidad de acciones disciplinarias contra oficiales y empleados de Estados Unidos que se hayan visto implicados en infracciones voluntarias de la ley. La responsabilidad y disciplina no solamente se pueden derivar de la infracción de las normas mencionadas en este capítulo, sino también de la revelación inadecuada de cierto tipo de información relacionada con la ECPA. La información obtenida por medio de un proceso (citación, orden u orden de registro) conforme a la ECPA y que se pueda definir como "registro" en virtud de la Ley de Privacidad, 5 U.S.C. § 552a(a), no puede ser revelada voluntariamente por un oficial o entidad gubernamental sin infringir la ECPA. Véase 18 U.S.C. § 2707(g). No obstante, no constituye infracción la revelación "en el curso del correcto desempeño de las funciones oficiales del funcionario u organismo gubernamental que la realice", así como tampoco es ilegal divulgar información que haya sido revelada

previa y legalmente al público. Id. Sección 2707(g), salvo prórroga, expirará el 31 de diciembre de 2005. Véase Ley PATRIOT §§ 223, 224, 115 Stat. 272, 293-95 (2001).

La ECPA incorpora disposiciones separadas para pleitos contra Estados Unidos y contra personas o entidades. 18 U.S.C. § 2707 permite que una "persona afectada" por una infracción de la ECPA emprenda un proceso civil contra la "persona o entidad, excluyendo Estados Unidos, implicada en dicha infracción". 18 U.S.C. § 2707(a). Entre las sanciones se pueden incluir indemnizaciones no inferiores a 1.000 $ por persona, reparación equitativa y declarativa y los honorarios razonables del abogado más otros costes razonables del litigio. La infracción consciente o intencionada también puede tener como consecuencia sanciones punitivas, véase § 2707(b)-(c), mientras que los funcionarios de Estados Unidos se pueden ver sujetos a acciones disciplinares por infracciones conscientes o intencionadas. Véase § 2707(d). La confianza de buena fe en una orden judicial, citación de gran jurado, autorización legislativa o autorización legítima proporciona una defensa completa ante cualquier acción civil o penal relacionada con la ECPA. Véase § 2707(e). También puede estar disponible la inmunidad reconocida. Véase el capítulo 4.D.2.

Se pueden interponer demandas contra Estados Unidos en virtud de 18 U.S.C. § 2712 por infracción consciente de la ECPA, Título III, o de las secciones específicas de la Ley de Vigilancia de Inteligencia Extranjera de 1978, 50 U.S.C. § 1801. Esta sección autoriza a los tribunales a conceder daños y perjuicios o 10.000 $, la cantidad que sea mayor, además de los costes razonables del litigio. La sección 2712 también define los procedimientos para demandas contra Estados Unidos y un proceso para procedimientos permanentes cuando el litigio civil pueda interferir con una investigación o proceso penal relacionados. Véase 18 U.S.C. § 2712 (b), (e). A menos que se prorrogue, § 2712 expirará el 31 de diciembre de 2005. Véase Ley PATRIOT §§ 223, 224, 115 Stat. 272, 293-95 (2001).

[índice]

IV. VIGILANCIA ELECTRÓNICA EN REDES DE COMUNICACIONES

A. Introducción

Con frecuencia en las investigaciones penales se utiliza la vigilancia electrónica. En casos de delitos cibernéticos, es posible que los agentes quieran vigilar a un pirata cuando éste entre en el sistema informático de una víctima o crear un buzón "clonado" de correo electrónico para supervisar si un sospechoso envía o recibe pornografía infantil por Internet. En un contexto más tradicional, los agentes pueden contemplar la posibilidad de pinchar el teléfono de un sospechoso o averiguar los destinatarios y la hora de las llamadas. En este capítulo se explica cómo funcionan las leyes de vigilancia electrónica en las investigaciones criminales relacionadas con ordenadores.

Existen dos leyes federales que rigen la supervisión electrónica en tiempo real en investigaciones criminales federales. La primera y más importante de ella es la ley sobre escuchas telefónicas, U.S.C. §§ 2510-2522, aprobada inicialmente como el Título III de la Ley General para el Control del Crimen y Seguridad en las Calles de 1968 (conocida como "Título III"). La segunda ley es el capítulo sobre Registro de llamadas y dispositivos de control y rastreo del Título 18 ("la Ley de registro y control de llamadas"), 18 U.S.C. §§ 3121-3127, que rige los registros de llamadas y los dispositivos de control y rastreo. El incumplimiento de estas leyes puede derivar en responsabilidades civiles y penales y, en el caso del Título III, incluso en la anulación de las pruebas.

[Índice]

B. Contenido frente a datos domiciliarios

En general, la ley de registro y control de llamadas regula la obtención de información de dirección y otros datos que no incluyan el contenido para las comunicaciones por cable y electrónicas. El Título III regula la obtención del contenido de este tipo de comunicaciones.

El Título III y la ley de registro y control de llamadas coexisten porque cada una de ellas regula el acceso a distintos tipos de información. El Título III permite al gobierno obtener el contenido de comunicaciones por cable y electrónicas transmitidas. Por el contrario, la ley de registro y control de llamadas afecta a la obtención en tiempo real de información de dirección y otros datos que no incluyan el contenido en relación con estas comunicaciones. Véase 18 U.S.C. § 2511(h)(i) (en el que se establece que la utilización de un dispositivo de registro, control y rastreo de llamadas no supone una infracción del Título III); United States Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000); Brown v. Waddell, 50 F.3d 285, 289-94 (4° Cir. 1995) (hace una distinción entre los registros de llamadas y los dispositivos de interceptación del Título III).

La diferencia entre la información de dirección y el contenido está clara en el caso de las comunicaciones tradicionales, como las llamadas de teléfono. La información de dirección para una llamada telefónica es el número marcado para una llamada saliente y el número de origen (datos identificativos de la persona que realiza la llamada) en el caso de las llamadas entrantes. Por el contrario, el contenido de la comunicación es la conversación propiamente dicha mantenida entre el emisor y el receptor de la llamada.

La distinción entre la información de dirección y el contenido también es aplicable a las comunicaciones por Internet. Por ejemplo, cuando dos ordenadores conectados a Internet se comunican entre sí, estos descomponen los mensajes en pequeñas piezas llamadas "paquetes" para enviar a continuación cada paquete a su destino final. Todos y cada uno de los paquetes contiene información de dirección en el "título" del mismo, similar a las direcciones de destino y remitente que se escriben en un sobre, seguida del contenido del mensaje, como la carta que va en el interior del sobre. La ley de registro y control de llamadas permite a las fuerzas de seguridad obtener información de dirección de comunicaciones de Internet de la misma manera en que lo haría para llamadas telefónicas tradicionales. Sin embargo, la lectura del paquete completo normalmente afecta al Título III. La principal diferencia entre un dispositivo de control y rastreo en Internet y uno de interceptación en Internet conforme al Título III, llamado a veces "rastreador", es que el primero está programado para capturar y retener solamente la información de dirección, mientras que el último se programa para capturar y conservar todo el paquete.

En el correo electrónico por Internet se aplica la misma distinción. Todos los mensajes de correo electrónico constan de una serie de títulos que contienen información de dirección y enrutamiento generada por el programa de correo, seguida del contenido propiamente dicho del mensaje redactado por el remitente. La información de dirección y enrutamiento incluye la dirección de correo electrónico tanto del remitente como del destinatario, así como información sobre cuándo y dónde se envió el mensaje, bastante similar al matasellos de una carta. La ley de registro y control de llamadas permite a las fuerzas de seguridad obtener la información de dirección de correos electrónicos (exceptuando la línea del asunto, que puede incluir contenido) por medio de una orden judicial, de la misma manera que permite a las fuerzas de seguridad obtener información de dirección para llamadas telefónicas y "paquetes" individuales de Internet mediante una orden judicial. Por el contrario, la interceptación de contenidos de correos electrónicos, incluyendo la línea del asunto, exige una observación minuciosa de las estrictas directrices del Título III.

En determinadas circunstancias puede haber controversia sobre la distinción entre información de dirección y contenido. Los fiscales o agentes que se topen con estos problemas deben ponerse en contacto con la Sección de Delitos Cibernéticos y Propiedad Intelectual a través del teléfono (202) 514-1026 o con el CTC de su distrito (véase la introducción, pág. ix).

[Índice]

C. La ley de registro y control de llamadas, 18 U.S.C. §§ 3121-3127

La ley de registro y control de llamadas autoriza a un abogado del gobierno a solicitar una orden a un tribunal por la que se le permita instalar un dispositivo para el registro de llamadas y/o su control o rastreo en la medida en la que "la información que se pueda obtener sea relevante para una investigación criminal que se esté desarrollando". 18 U.S.C. § 3122(b)(2). En pocas palabras, un registro de llamadas captura la información de dirección saliente como el número marcado en un teléfono que se esté vigilando, mientras que un dispositivo de control y rastreo registra la información de dirección entrante, como la información identificativa de la persona que llama. A pesar de que la ley de registro y control de llamadas incluía anteriormente referencias específicas a las comunicaciones por cable, son muchos los tribunales que han aplicado esta ley para comunicaciones de redes informáticas. En 2001, la Ley USA PATRIOT confirmó que la ley de registro y control de llamadas se aplica a un amplio abanico de tecnologías de la comunicación. Véase Ley PATRIOT § 216, 115 Stat. 272, 288-90 (2001).

1. Definición de registro de llamadas y dispositivo de control y rastreo

La ley de registro y control de llamadas define los registros de llamadas y los dispositivos de control y rastreo de una forma muy general. Según se define en 18 U.S.C. § 3127(3), un "registro de llamadas" es un dispositivo o proceso por el cual se registra o descodifica información de marcación, enrutamiento, dirección o señal transmitida por un instrumento o instalación desde la que se transmite una comunicación por cable o electrónica, siempre y cuando dicha información no incluya el contenido de la comunicación. . . .

La definición de registro de llamadas excluye también los dispositivos o procesos utilizados para la facturación o la contabilidad de costes. Véase 18 U.S.C. § 3127(3). La ley define "dispositivo de control y rastreo" como un aparato o proceso que captura la información electrónica entrante u otros impulsos que identifican el número de origen, así como otros datos de marcación, enrutamiento, dirección o señal con los que sea razonablemente probable identificar el origen de una comunicación por cable o electrónica, siempre y cuando dicha información no incluya el contenido de la comunicación.

18 U.S.C. § 3127(4). Dado que los encabezamientos en Internet contienen información tanto del remitente como del destinatario, un aparato que lea el encabezamiento completo (salvo la línea del asunto en el caso de títulos de correo electrónico) se conoce simplemente como un dispositivo de control y rastreo.

La amplitud de estas definiciones se deriva del alcance de sus componentes. En primer lugar, "un instrumento o instalación desde la que se transmite una comunicación por cable o electrónica" abarca una gran variedad de tecnologías de la comunicación, incluyendo un teléfono, un móvil, una cuenta de usuario de Internet, una cuenta de correo electrónico o una dirección IP. Por otra parte, la inclusión en la definición de toda la "información de marcación, enrutamiento, dirección o señal" engloba casi la totalidad de la información de una comunicación no relacionada con el contenido. En tercer lugar, dado que la definición de registro de llamadas y dispositivo de control y rastreo incluye los términos "dispositivo" y "proceso", la ley cubre tanto las rutinas de programas como los dispositivos físicos. Teniendo en cuenta que las definiciones están redactadas en un estilo general y neutral en cuanto a la tecnología, es posible que los fiscales y agentes tengan dudas acerca de si un aparato concreto es un registro de llamadas o un dispositivo de control y rastreo, en cuyo caso deberán dirigirse a la Sección de Delitos Cibernéticos y Propiedad Intelectual a través del teléfono (202) 514-1026, a la Oficina de Operaciones de Seguridad, en el número (202) 514-6809, o al CTC de su distrito (véase la introducción, pág. ix).

2. Órdenes de registro y control de llamadas: solicitud, emisión, entrega y presentación de informes

Para obtener una orden de registro y control de llamadas, el solicitante debe identificarse, identificar al organismo de las fuerzas de seguridad que esté llevando a cabo la investigación y, por último, certificar su convencimiento de que la información que probablemente obtenga será relevante para la investigación criminal que esté desarrollando el organismo en cuestión. Véase 18 U.S.C. § 3122(b)(1)-

(2). El tribunal que vaya a emitirla también debe tener jurisdicción sobre el delito investigado. Véase 18 U.S.C. § 3127(2)(a). Si la solicitud incluye estos elementos, el tribunal autorizará la instalación y el uso de un dispositivo de registro, control y rastreo de llamadas en cualquier lugar de Estados Unidos. Véase 18 U.S.C. § 3123(a)(1). El tribunal no emprenderá una "investigación judicial independiente para corroborar la veracidad de los hechos expuestos". Solicitud In re de Estados Unidos, 846 F. Supp. 1555, 1558-59 (M.D. Fla. 1994). Véase también Estados Unidos v. Fregoso, 60 F.3d 1314, 1320 (8° Cir. 1995) ("El papel judicial en la aprobación del uso de dispositivos de registro y control de llamadas es de tipo ministerial").

Una orden federal de registro y control de llamadas puede tener validez fuera del distrito del tribunal que la emita. En el caso de un solicitante federal, la orden "es aplicable a cualquier persona o entidad que preste servicios de comunicaciones por cable o electrónicas en Estados Unidos y cuya colaboración pueda facilitar la ejecución de la orden". 18 U.S.C. § 3123(a)(1). Por ejemplo, un fiscal federal puede obtener una orden para rastrear las llamadas telefónicas realizadas a un teléfono particular. La orden se aplica no sólo al distribuidor local que provee esa línea, sino también a otros proveedores (como distribuidores de larga distancia y regionales en otros lugares del país) a través de los que las llamadas llegan al teléfono de destino. De igual forma, en el contexto de Internet, un fiscal federal puede obtener una orden para rastrear las comunicaciones del ordenador o la dirección IP de una víctima particular. Si un hacker enruta las comunicaciones a través de una cadena de ordenadores intermedios de paso, la orden se aplicaría a cada uno de los ordenadores de la cadena, desde el de la víctima hasta la fuente de las comunicaciones.

La ley de registro y control de llamadas no exige que se especifiquen en la solicitud o en la orden todos los proveedores sujetos a la misma, si bien sí se debe mencionar en la orden el proveedor inicial. Véase 18 U.S.C. § 3123(b)(1)(A). Lo único que necesita hacer un investigador para obtener la colaboración de un proveedor es hacerle llegar la orden. Si el proveedor así lo solicita, las fuerzas de seguridad también le facilitarán una "certificación escrita o electrónica" que establezca que la orden es aplicable a dicho proveedor. Véase 18 U.S.C. § 3123(a)(1). Existen motivos de carácter práctico para este proceso relativamente informal. En el momento de solicitar una orden de registro y control de llamadas, normalmente los fiscales conocen la identidad de los proveedores de la cadena de comunicaciones cubierta por la orden. Si se pidiera al personal de las fuerzas de seguridad que volviera a presentarse ante el tribunal cada vez que descubrieran la identidad de un nuevo proveedor, las investigaciones se retrasarían de forma significativa.

Una orden de registro y control de llamadas puede autorizar el uso de un dispositivo de registro y rastreo de llamadas durante sesenta días, que se pueden prorrogar en plazos adicionales de otros sesenta días. Véase 18 U.S.C. § 3123(c). Asimismo, la orden judicial da instrucciones al proveedor para que no revele la existencia de la misma "a ninguna […] persona, a menos o hasta que no lo indique el tribunal", 18 U.S.C. § 3123(d)(2), y puede forzar a proveedores de servicios de comunicaciones por cable o electrónicas, arrendadores, guardas o a otras personas a que "proporcionen […] de manera inmediata toda la información, instalaciones y asistencia técnica que sea necesaria" para instalar los dispositivos de control y rastreo de llamadas. Véase 18 U.S.C. § 3124(a), (b). Los proveedores a los que ordene prestar asistencia en la instalación de estos dispositivos en virtud de § 3124 tienen derecho a una compensación razonable por los gastos en los que hayan podido incurrir durante la prestación de sus medios o servicios técnicos a las fuerzas de seguridad. Véase 18 U.S.C. § 3124(c). La confianza de Buena fe por parte de un proveedor en una orden judicial proporciona una defensa completa ante cualquier acción civil o penal que pueda surgir a partir de su colaboración de conformidad con lo dispuesto en la orden. Véase 18 U.S.C. § 3124(d), (e).

La ley de registro y control de llamadas incluye un requisito de cobertura para el tipo limitado de casos en los que los oficiales de las fuerzas de seguridad instalan sus propios dispositivos en una red de intercambio de paquetes de un proveedor de servicios de comunicaciones electrónicas. Véase 18 U.S.C. § 3123(a)(3)(A). Cuando las fuerzas de seguridad entregan una orden de registro y control de llamadas a un proveedor, lo normal es que éste recopile la información especificada y se la facilite. En aquellos casos en los que el proveedor no pueda hacerlo, o en otras situaciones poco comunes, el gobierno puede instalar su propio dispositivo de registro y control de llamadas, como el DCS 1000 del FBI. En estos casos, el gobierno debe facilitar la siguiente información sellada al tribunal en el plazo de treinta días

tras el vencimiento de la orden: (1) la identidad de los oficiales que instalaron o tuvieron acceso al dispositivo; (2) la fecha y la hora de instalación, acceso y desinstalación del dispositivo; (3) la configuración del aparato en el momento de la instalación y posteriores modificaciones de dicha configuración; y (4) la información recogida por el dispositivo. Véase 18 U.S.C. § 3123(a)(3). Si el gobierno instala un dispositivo de registro y control de llamadas, éste debe utilizar "la tecnología más apropiada" a fin de evitar registrar o descodificar el contenido de una comunicación por cable o electrónica. Véase 18 U.S.C. § 3121(c).

Es importante observar que el limitado análisis judicial de las órdenes de registro y control de llamadas coexiste con un contundente mecanismo de cumplimiento para infracciones de la ley. Véase 18 U.S.C. § 3121(d) (contempla sanciones penales por infracciones de la ley de registro y control de llamadas). Como explicó un tribunal, la finalidad más destacada de exigir la solicitud al tribunal de una orden es establecer la responsabilidad de la veracidad de la solicitud (esto es, para garantizar que el Fiscal de Estados Unidos que dé fe de ella sea fácilmente identificable y jurídicamente competente), así como para confirmar que el Fiscal de Estados Unidos ha prestado juramento de que la investigación en cuestión está en curso […] Como medio disuasorio y garantía de conformidad, la ley prevé […] penas de prisión y sanciones económicas como penalización por la infracción [de la ley].

Solicitud In re de Estados Unidos, 846 F. Supp. en 1559.

La ley de registro y control de llamadas garantiza asimismo a los proveedores de servicios de comunicaciones electrónicas o por cable una amplia autoridad para utilizar estos dispositivos en su red sin una orden judicial. 18 U.S.C. § 3121(b) establece que los proveedores pueden utilizar dispositivos de registro y control de llamadas sin una orden

(1) en relación con el funcionamiento, mantenimiento y comprobación de un servicio de comunicación por cable o electrónica o para la protección de los derechos o de la propiedad de dicho proveedor, así como para salvaguardar a los usuarios del servicio frente a un abuso del servicio o un uso ilegal del mismo; o

(2) para registrar el hecho de que se haya iniciado o terminado una comunicación por cable o electrónica con objeto de proteger al proveedor, a otro proveedor que preste sus servicios para completar la comunicación telefónica o al usuario del servicio frente a un uso fraudulento, ilícito o abusivo del servicio; o

(3) cuando se haya obtenido el consentimiento del usuario del servicio.

18 U.S.C. § 3121(b).

[Índice]

D. La Ley sobre escuchas telefónicas ("Título III"), 18 U.S.C. §§ 2510-2522

1. Introducción: la prohibición general

Desde su promulgación en 1968 y su posterior enmienda en 1986, el Título III ha proporcionado el marco legal que rige la vigilancia electrónica en tiempo real del contenido de las comunicaciones. Si un agente quiere pinchar el teléfono de un sospechoso, vigilar a un hacker cuando irrumpa en un sistema informático o aceptar los resultados de las escuchas telefónicas realizadas por un ciudadano particular que haya descubierto pruebas de un delito, primero deberá considerar las implicaciones del Título III.

La estructura del Título III es sorprendentemente simple. Los encargados de su redacción asumieron que cada comunicación privada se puede entender como una conexión de doble sentido entre dos participantes, como una llamada entre A y B. En un plano básico, la ley prohíbe que una tercera parte,

como puede ser el gobierno, que no participe de la comunicación intercepte comunicaciones privadas entre las partes utilizando un "dispositivo electrónico, mecánico o de otro tipo", a menos que sea aplicable una o varias excepciones legales. Véase 18 U.S.C. § 2511(1). Cabe destacar que esta prohibición es bastante amplia. Al contrario de lo que ocurre con algunas leyes sobre privacidad que regulan sólo determinados casos o lugares específicos, el Título III prohíbe de forma generalizada la interceptación de señales electrónicas (sujeta a determinadas excepciones y requisitos interestatales) en prácticamente todo el territorio de Estados Unidos. Independientemente de si los investigadores pretenden llevar a cabo la vigilancia en casa, en el trabajo, en despachos gubernamentales, en la cárcel o en Internet, deben asegurarse de que observe las prohibiciones del Título III.

Las preguntas que se deben formular los agentes y fiscales para confirmar el cumplimiento del Título III son sencillas, al menos en la forma: 1) ¿La comunicación que se va a vigilar pertenece a una de las protegidas según la definición de 18 U.S.C. § 2510? 2) ¿La vigilancia propuesta derivará en la "interceptación" de las comunicaciones? 3) Si la respuesta a la primera pregunta es afirmativa, ¿existe una excepción legal aplicable que permita la interceptación?

2. Expresiones clave

El Título III prohíbe de forma generalizada la "interceptación" de "comunicaciones orales", "comunicaciones por cable" y "comunicaciones electrónicas". Estas expresiones se definen en la ley. Véase 18 U.S.C. § 2510. En los casos de delitos cibernéticos, los agentes y fiscales que planeen llevar a cabo una vigilancia electrónica deben comprender la definición de "comunicación por cable", "comunicación electrónica" y de "interceptar". (La vigilancia de comunicaciones orales no suele darse en casos de delitos cibernéticos, por lo que no se abordará aquí. Los agentes y fiscales que precisen asistencia en casos relacionados con comunicaciones orales se deben poner en contacto con la Oficina de Operaciones de Seguridad del Departamento de Justicia a través del número de teléfono (202) 514-6809).

"Comunicación por cable"

Por lo general, las conversaciones telefónicas son comunicaciones por cable.

Según § 2510(1), "comunicación por cable" implica toda transmisión auditiva realizada total o parcialmente mediante el uso de herramientas para la transmisión de comunicaciones con la ayuda de un cable u otra conexión similar entre el punto de origen y el de recepción (incluyendo el uso de dicha conexión en una estación de distribución) facilitada por una persona dedicada a la provisión o gestión de dichas instalaciones para la transmisión de comunicaciones interestatales o exteriores o comunicaciones que influyan sobre el comercio interestatal o exterior.

En esta compleja definición, el requisito más importante es que el contenido de la comunicación incluya la voz humana. Véase § 2510(18) (en donde se define "transmisión" como una "transmisión que incluye la voz humana en algún punto, así como un punto de origen y uno de destino"). Si una comunicación no incluye una voz humana, ya sea de forma aislada o en una conversación en grupo, no puede tratarse de una comunicación por cable. Véase S. Rep. No. 99-541, en 12 (1986), reimpreso en 1986 U.S.C.C.A.N. 3555; Estados Unidos v. Torres, 751 F.2d 875, 885-86 (7° Cir. 1984) (en la que se concluye que la "vigilancia de televisión en silencio" no puede llevar a la interceptación de comunicaciones por cable conforme al Título III porque no se produce ningún intercambio auditivo).

El requisito adicional de que las comunicaciones por cable deben enviarse "total o parcialmente […] con la ayuda de un cable u otra conexión similar […]" supone un obstáculo muy fácil de salvar. En tanto en cuanto la señal viaje por cable en algún punto en la ruta entre el punto de origen y el de destino, el requisito se ve satisfecho. Por ejemplo, todas las transmisiones telefónicas de voz, incluyendo las que proceden de señales de satélite y teléfonos móviles, entran dentro de las comunicaciones por cable. Véase H.R. Rep. N° 99-647, en 35 (1986). Se incluyen de forma expresa en la definición de comunicación por cable debido a que dichas transmisiones se transportan por cable en las estaciones de distribución. Es necesario hacer hincapié en que la presencia de cables en el interior de los equipos

durante el envío o la recepción de una comunicación, como en un teléfono móvil individual, no satisface el requisito de que una comunicación se envíe "parcialmente" por cable. El cable debe transmitir la comunicación "en un grado significativo" a lo largo de la ruta de la transmisión, fuera del equipo que envíe o reciba la comunicación. Id.

Cabe destacar que antes de la aprobación de la Ley USA PATRIOT de 2001, la definición de "comunicación por cable" incluía de forma explícita "todo almacenamiento electrónico de dicha comunicación". La Ley USA PATRIOT eliminó esta frase y corrigió el § 2703 de la ECPA para garantizar que las comunicaciones por cable almacenadas, como los correos de voz, por ejemplo, estén cubiertas no por el Título III, sino por las disposiciones de la ECPA que también se aplican a las comunicaciones electrónicas almacenadas o correos electrónicos. Véase Ley PATRIOT § 209, 115 Stat. 272, 283 (2001). La consecuencia práctica de estas modificaciones es que el acceso del gobierno al correo de voz almacenado ya no se rige por el Título III. En lugar de ello, el correo de voz está cubierto por la ECPA y las normas de divulgación para este tipo de comunicación son ahora idénticas a las que rigen el correo electrónico. Este cambio expirará el 31 de diciembre de 2005, a menos que lo prorrogue el Congreso. Véase el capítulo 3.A, más arriba.

"Comunicación electrónica"

La mayor parte de las comunicaciones por Internet, incluyendo el correo electrónico, son comunicaciones electrónicas.

18 U.S.C. § 2510(12) define "comunicación electrónica" como toda transmisión de signos, señales, escritos, imágenes, sonidos, datos o información de cualquier tipo, transmitida total o parcialmente por un sistema de cable, radio, electromagnético, fotoeléctrico o fotoóptico que influya sobre el comercio interestatal o exterior, pero no incluye

(A) comunicaciones por cable u orales;

(B) comunicaciones realizadas mediante dispositivos de buscapersonas con sólo tono;

(C) comunicaciones desde un dispositivo de rastreo; o

(D) información sobre transferencias electrónicas de fondos almacenada por una institución financiera en un sistema de comunicaciones utilizado para el almacenamiento electrónico y la transferencia de fondos;

Como sugiere la definición, la comunicación electrónica es una categoría muy amplia que abarca todo. Véase Estados Unidos v. Herring, 993 F.2d 784, 787 (11° Cir. 1993). "Por lo general, una comunicación se considera electrónica si no es transportada por ondas de sonido ni se puede caracterizar como que contiene voz humana (transportada parcialmente por cable)". H.R. Rep. N° 99-647, en 35 (1986). La mayor parte de las señales eléctricas o electrónicas que no entran en la definición de comunicaciones por cable se consideran comunicaciones electrónicas. Por ejemplo, casi todas las comunicaciones por Internet, incluyendo el correo electrónico, entran dentro de la categoría de comunicaciones electrónicas.

"Interceptar"

La estructura y el lenguaje de la ECPA y del Título III exigen que el término "interceptar" se aplique solamente a las comunicaciones que se desarrollen de forma simultánea a su transmisión y no a la adquisición de comunicaciones por cable o electrónicas almacenadas. La mayoría de tribunales han adoptado este enfoque, aunque este asunto sigue sin resolverse en el Noveno Circuito.

La sección 2510(4) define "interceptar" como "la adquisición auditiva o de otra forma de los contenidos de una comunicación por cable, electrónica u oral mediante el uso de un dispositivo electrónico,

mecánico o de otro tipo". La palabra "adquisición" resulta ambigua en esta definición. Por ejemplo, si el equipo de vigilancia de las fuerzas de seguridad graba el contenido de una comunicación, esta comunicación puede "adquirirse" en tres puntos distintos: primero, cuando el equipo graba la comunicación; segundo, cuando las fuerzas de seguridad obtienen posteriormente la grabación; o tercero, cuando las fuerzas de seguridad reproduce la grabación y escucha o ve el contenido de la comunicación. El texto de § 2510(4) no especifica cuál de estas situaciones constituye una "adquisición" en relación con el objeto del Título III. Véase Estados Unidos v. Turk, 526 F.2d 654, 657-58 (5° Cir. 1976).

Por otra parte, la definición de "interceptar" no aborda expresamente la cuestión de si la adquisición puede ser simultánea a la transmisión. Sin embargo, la relación entre el Título III y la ECPA requiere que se restrinja el significado de "interceptar" a las adquisiciones de comunicaciones simultáneas a su transmisión. Por ejemplo, un correo electrónico o de voz puede pasar un tiempo en almacenamiento electrónico hasta que finalmente lo consulte su destinatario. Si las fuerzas de seguridad obtienen dicha comunicación a partir del almacenamiento electrónico, no habrán interceptado la comunicación según la interpretación del Título III, ya que la adquisición de los contenidos de las comunicaciones electrónicas o por cable está regida por § 2703(a) de la ECPA, no por el Título III.

La mayoría de tribunales ha adoptado esta interpretación y sostienen que tanto las comunicaciones por cable como las electrónicas solamente se interceptan si se adquieren de forma simultánea a su transmisión. En otras palabras, la interceptación de las comunicaciones hace referencia únicamente a su adquisición en tiempo real en el momento de la transmisión entre las partes que participan en la comunicación. Un investigador que obtenga acceso posteriormente a una copia almacenada de la comunicación, no la "interceptará". Véase por ejemplo Steve Jackson Games, Inc. v. Servicio Secreto de Estados Unidos, 36 F.3d 457, 460-63 (5° Cir. 1994) (acceso a comunicaciones de correo electrónico almacenadas); Wesley College v. Pitts, 974 F. Supp. 375, 384-90 (D. Del. 1997) (similar); Estados Unidos v. Meriwether, 917 F.2d 955, 960 (6° Cir. 1990) (acceso a comunicaciones de busca almacenadas); Estados Unidos v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996) (similar); Bohach v. Ciudad de Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (similar); Estados Unidos v. Moriarty, 962 F. Supp. 217, 220-21 (D. Mass. 1997) (acceso a comunicaciones por cable almacenadas; Litigio In re de la Policía Estatal, 888 F. Supp 1235, 1264 (D. Conn. 1995) (similar); Payne v. Norwest Corp., 911 F. Supp. 1299, 1303 (D. Mont. 1995), afirmado parcialmente y revelado parcialmente, 113 F.3d 1079 (9° Cir. 1997) (similar). Asimismo, teniendo en cuenta que las comunicaciones sólo se interceptan si se adquieren de forma simultánea a la transmisión, un dispositivo de registro del teclado de un ordenador personal no interceptará las comunicaciones si se configura de tal manera que no se registre la pulsación de las teclas cuando se esté utilizando el modem. Véase Estados Unidos v. Scarfo, 180 F. Supp. 2d 572, 582 (D.N.J. 2001).

En el Noveno Circuito, por razones que precisan una explicación histórica, sigue sin estar clara la cuestión de si la definición de "interceptar" se limita a adquisiciones en tiempo real. Antes de la aprobación de la Ley USA PATRIOT, la definición de "comunicación por cable" de § 2510(1), a diferencia de la definición de "comunicación electrónica" de § 2510(12), incluía de forma explícita "todo almacenamiento electrónico de dicha comunicación". En Estados Unidos v. Smith, 155 F.3d 1051, 1058-59 (9° Cir. 1998), el Noveno Circuito concluyó que una parte puede interceptar una comunicación por cable mediante la obtención de una copia de la comunicación en "almacenamiento electrónico", como se define en § 2510(17). El tribunal consideró que las comunicaciones por cable se deben tratar de forma distinta a las electrónicas, ya que la definición de comunicación por cable incluía expresamente la expresión "todo almacenamiento electrónico de dicha comunicación" y porque limitar las interceptaciones de las comunicaciones por cable a las adquisiciones simultáneas habría hecho que esa expresión no tuviera sentido, puesto que las comunicaciones por cable en almacenamiento electrónico no se podían interceptar en ningún caso. Véase id. en 1057-58.[(25)] El tribunal siguió con la definición de "interceptar" conforme al Título III en relación con "acceso" conforme a § 2701 de la ECPA, exponiendo que una interceptación "comprende la adquisición de los contenidos de una comunicación, mientras que la palabra "acceso" implica simplemente estar en disposición de adquirir los contenidos de una comunicación". Id. en 1058.

Ahora bien, la Ley USA PATRIOT ha eliminado, sin embargo, la base jurídica de la sentencia del Noveno Circuito en el caso Smith al excluir la expresión "todo almacenamiento electrónico de dicha comunicación" de la definición de comunicación por cable y al incluir de forma explícita las comunicaciones por cable almacenadas en el § 2703 de la ECPA. Actualmente existe una distinción jurídica clara y uniforme entre comunicaciones electrónicas y por cable almacenadas, sujetas a la ECPA, e interceptaciones de comunicaciones electrónicas y por cable, que se rigen por el Título III.

3. Excepciones al Título III

El Título III prohíbe de forma generalizada la interceptación, la utilización o la divulgación intencionadas[(26)] de comunicaciones por cable o electrónicas a menos que sea aplicable una excepción jurídica. Véase 18 U.S.C. § 2511(1). En general, esta prohibición impide que terceras partes, incluyendo al gobierno, pinchen teléfonos e instalen "rastreadores" electrónicos que lean el tráfico en Internet.

La amplitud de la prohibición del Título III implica que la legalidad de la mayoría de las técnicas de vigilancia sujetas al Título III depende de si es aplicable una excepción jurídica a la norma. El Título III contiene decenas de excepciones, las cuales pueden ser o no ser aplicables en cientos de situaciones diferentes. No obstante, en los casos de delitos cibernéticos son siete las excepciones aplicables más frecuentes:

A) interceptación en virtud de una orden conforme al § 2518;

B) la excepción de la "autorización", § 2511(2)(c)-(d);

C) la excepción del "proveedor", § 2511(2)(a)(i);

D) la excepción del "intruso informático", § 2511(2)(i);

E) la excepción de la "extensión telefónica", § 2510(5)(a);

F) la excepción de las "pruebas criminales obtenidas de forma involuntaria", § 2511(3)(b)(iv); y

G) la excepción por ser "accesible al público", § 2511(2)(g)(i).

Los fiscales y agentes han de comprender el alcance de estas siete excepciones con el fin de determinar si las distintas estrategias de vigilancia cumplirán con el Título III.

a) Interceptación autorizada por una orden en virtud del Título III, 18 U.S.C. § 2518.

El Título III permite a las fuerzas de seguridad interceptar comunicaciones por cable o electrónicas en virtud de una orden judicial conforme a 18 U.S.C. § 2518 (una "orden de Título III"). Para las solicitudes de órdenes federales de Título III es necesaria la aprobación de alto nivel del Departamento de Justicia, por ley en el caso de las comunicaciones por cable y por la política del Departamento de Justicia en el de las comunicaciones electrónicas, excepto para buscas númericos. Una vez autorizada por el Departamento de Justicia y firmada por un juez de tribunal de distrito o tribunal de apelaciones de Estados Unidos, una orden de Título III permite a las fuerzas de seguridad interceptar comunicaciones durante un plazo máximo de treinta días. Véase § 2518.

18 U.S.C. §§ 2516-2518 impone varios requisitos restrictivos que se deben cumplir antes de que los investigadores pueden obtener una orden de Título III. Lo más importante es que en la solicitud de la orden se debe indicar causa probable para pensar que la interceptación revelará pruebas de un delito grave citado en § 2516. Véase § 2518(3)(a)-(b). En el caso de agentes federales, el delito grave debe ser uno de los que se citan de forma específica en § 2516(1)(a)-(r) para interceptar comunicaciones por cable o bien un delito grave federal para interceptar comunicaciones electrónicas. Véase 18 U.S.C. § 2516(3). La lista de delitos graves para investigaciones estatales figura en 18 U.S.C. § 2516(2). Por

otra parte, la solicitud de una orden de Título III (1) debe demostrar que se han intentado utilizar procedimientos normales de investigación y que estos no han dado los resultados esperados o bien que aparentemente es poco probable que tengan éxito o que pueden resultar demasiado peligrosos, véase § 2518(1)(c); (2) han de establecer causa probable de que la herramienta de comunicación se está utilizando en una actividad delictiva; y (3) deben mencionar que la vigilancia se llevará a cabo de tal manera que se reduzca lo máximo posible la interceptación de comunicaciones que no aporten pruebas de un delito. Véase § 2518(5). Si desean una orientación completa acerca de los requisitos de 18 U.S.C. § 2518, agentes y fiscales han de consultar a la Oficina de Operaciones de Seguridad del Departamento de Justicia a través del número de teléfono (202) 514-6809.

b) Autorización de un participante de la comunicación, 18 U.S.C. § 2511(2)(c)-(d)

18 U.S.C. § 2511(2)(c) y (d) establecen que:

(c) De conformidad con este capítulo, no será ilícito que una persona que actúe en nombre de la ley intercepte una comunicación por cable, oral o electrónica, si dicha persona forma parte de la comunicación o si uno de los participantes en la misma ha dado su autorización previamente para proceder a la interceptación.

(d) De conformidad con este capítulo, no será ilícito que una persona que no actúe en nombre de la ley intercepte una comunicación por cable, oral o electrónica, si dicha persona forma parte de la comunicación o si uno de los participantes en la misma ha dado su autorización previamente para proceder a la interceptación, a menos que el objeto de la interceptación de la comunicación sea cometer un acto delictivo o ilícito que infrinja la Constitución o las leyes de Estados Unidos o de cualquier estado.

Este texto autoriza la interceptación de comunicaciones cuando una de las partes de la misma lo autorice.[(27)] Por ejemplo, si un agente secreto o informador del gobierno graba una conversación telefónica que mantenga él mismo con un sospechoso, su consentimiento para la grabación permite la interceptación. Véase por ejemplo Obron Atlantic Corp. v. Barr, 990 F.2d 861 (6° Cir. 1993) (acogiéndose a § 2511(2)(c)). De igual manera, si un particular graba sus propias conversaciones telefónicas con otras personas, su consentimiento permite la interceptación a menos que uno de los principales factores que motivaran la interceptación de la comunicación por parte de esa persona fuera la comisión de actos delictivos o ilícitos. Véase Estados Unidos v. Cassiere, 4 F.3d 1006, 1021 (1° Cir. 1993) (se interpreta § 2511(2)(d)).

La autorización para la vigilancia conforme al Título III puede ser explícita o implícita. Véase Estados Unidos v. Amen, 831 F.2d 373, 378 (2° Cir. 1987). La autorización implícita se produce cuando las circunstancias indican que una de las partes de la comunicación era "objetivamente consciente" de la supervisión y a pesar de ello utilizó el sistema que estaba siendo vigilado. Estados Unidos v. Workman, 80 F.3d 688, 693 (2° Cir. 1996); véase también Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1° Cir. 1990) ("El consentimiento implícito es aquél que se puede inferir de una situación que indique que la parte en cuestión accedió conscientemente a la vigilancia"). (Se omiten citas internas). En la mayoría de los casos, la clave para determinar la autorización implícita consiste en demostrar que la parte que brindó su consentimiento recibió aviso de la vigilancia y utilizó el sistema a pesar de ello. Véase Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998). Una forma de acreditar la conclusión de que la parte tenía noticia de la vigilancia es presentar una copia del aviso. Véase Workman, 80 F.3d. en 693. En ausencia de ésta, si el gobierno quiere validar la conclusión de consentimiento implícito, debe demostrar "de modo convincente" que la parte sabía de la interceptación por las circunstancias que le rodeaban. Estados Unidos v. Lanoue, 71 F.3d 966, 981 (1° Cir. 1995).

i) Los banners y el consentimiento implícito

La vigilancia de una red informática no vulnera el Título III si el usuario recibe un "banner de red" apropiado en el que se le informe de que el uso de la misma implica su consentimiento a la supervisión.

En casos relacionados con ordenadores, la doctrina del consentimiento implícito permite vigilar una red informática en la que hayan colocado los "banners" correspondientes. Un banner es un aviso mediante el cual se informa a los usuarios en el momento de entrar en una red de que se puede supervisar el uso que hacen de ella, así como que el uso posterior del sistema implicará su autorización a dicha supervisión. Todo usuario que lea el banner antes de entrar en la red habrá recibido así aviso de la vigilancia: si utiliza la red a pesar del mismo, el usuario autorizará de forma implícita la supervisión en virtud del 18 U.S.C. § 2511(2)(c)-(d). Véase por ejemplo Workman, 80 F.3d. en 693-94 (en el que se concluye que las advertencias explícitas de que los teléfonos de la cárcel se vigilaban generaban la autorización implícita para vigilar a los internos que utilizaran los teléfonos posteriormente); Estados Unidos v. Amen, 831 F.2d 373, 379 (2° Cir. 1987) (similar). Sin embargo, véase Estados Unidos v. Thomas, 902 F.2d 1238, 1245 (7° Cir. 1990) (sentencias) (en el que se pone en tela de juicio el razonamiento del caso Amen).

El alcance de la autorización generada por un banner depende normalmente del texto que aparezca en el mismo: los banners de red no son universales. Un aviso en el que aparezca un texto muy limitado puede autorizar sólo algunos tipos de vigilancia, mientras que más amplio puede permitir la supervisión en multitud de situaciones por muchos motivos. A la hora de decidir cuál es el tipo de banner correcto para una red informática determinada, los proveedores de sistema se fijan en la finalidad de la red, las necesidades del administrador de sistemas y la cultura del usuario. Por ejemplo, una red informática delicada del Departamento de Defensa puede requerir un aviso amplio, mientras que en una red universitaria estatal utilizada por profesores y estudiantes puede valer uno más limitado. En el Apéndice A se incluyen varios banners de muestra que reflejan una serie de enfoques sobre la vigilancia de redes.

ii) ¿Quién es "participante de la comunicación" en la intrusión en una red?

Las secciones 2511(2)(c) y (d) permiten a cualquier "persona" que sea "participante de la comunicación" autorizar la vigilancia de la comunicación. En el caso de comunicaciones por cable, un "participante de la comunicación" suele ser fácilmente identificable. Por ejemplo, cualquiera de las personas que toman parte en una conversación telefónica de doble sentido es un participante de la comunicación. Véase por ejemplo Estados Unidos v. Davis, 1 F.3d 1014, 1015 (10° Cir. 1993). En un entorno de redes informáticas, por el contrario, se rompe el marco simple de una comunicación de doble sentido entre dos partes. Si un pirata inicia un ataque contra una red informática, por ejemplo, puede enrutarlo a través de una serie de sistemas intermedios antes de dirigir el ataque hacia la víctima final. En el ordenador de ésta, el hacker puede dirigir el ataque hacia la cuenta de red de un usuario, hacia la cuenta "origen" del administrador de sistemas o hacia los archivos comunes. Encontrar a una "persona" que sea un "participante de la comunicación", aparte del propio hacker, lógicamente, puede ser una labor extremadamente difícil, cuando no metafísica. En vista de estas dificultades, los agentes y fiscales deben adoptar un enfoque prudente ante la excepción del consentimiento de un "participante de la comunicación". En los casos de piratería, la excepción del intruso informático mencionada en el apartado (d), más abajo, puede ofrecer una base más segura para vigilar comunicaciones.

Varios tribunales han sugerido que el dueño del sistema informático puede satisfacer la expresión "participante de la comunicación" si un usuario envía una comunicación al sistema del propietario. Véase Estados Unidos v. Mullins, 992 F.2d 1472, 1478 (9° Cir. 1993) (en el que se establece que la excepción del consentimiento expresada en § 2511(2)(d) autoriza la vigilancia del uso inadecuado de un sistema informático porque el propietario del mismo es un participante de la comunicación); Estados Unidos v. Seidlitz, 589 F.2d 152, 158 (4° Cir. 1978) (en el que se concluye en *sentencias* que una empresa que alquiló en régimen de leasing y que se encargó del mantenimiento de un sistema informático implicado era "a todos los efectos un participante de las comunicaciones" cuando los empleados de la compañía interceptaron intrusiones en el sistema por parte de un usuario no autorizado que utilizaba la cuenta secuestrada de un supervisor). No obstante, aun aceptando esta interpretación, acogerse a ella puede plantear graves dificultades prácticas. Dado que los hackers suelen pasar del ordenador de una víctima a otro, creando una "guirnalda" de sistemas que transportan el tráfico, los agentes no tienen forma de saber con antelación qué ordenador será el destino final de cualquier comunicación futura. Si una víctima intermedia no se puede considerar una "parte de la comunicación", un tema que aún no ha sido abordado por los tribunales, la decisión de un hacker de pasar de una víctima a otra podría cambiar quién puede autorizar la vigilancia. En este caso, los agentes que

pretendan llevar a cabo la vigilancia con la autorización de la víctima no tendrían ningún modo de saber si la víctima será un "participante de la comunicación" para comunicaciones futuras.

c) La excepción del proveedor, 18 U.S.C. § 2511(2)(a)(i)

Los empleados o agentes de proveedores de servicios de comunicaciones pueden interceptar y revelar comunicaciones para proteger los derechos o la propiedad del proveedor. Por ejemplo, los administradores de sistema de redes informáticas normalmente pueden vigilar a los hackers cuando entran en sus redes y después comunican lo que han averiguado a través de la vigilancia a las fuerzas de seguridad, sin que por ello infrinjan el Título III. Este privilegio corresponde únicamente al proveedor, sin embargo, y no puede ser ejercido por las fuerzas de seguridad. Una vez que el proveedor se haya puesto en contacto con éstas, la excepción del intruso informático puede servir de base para la supervisión por parte de la policía.

18 U.S.C. § 2511(2)(a)(i) permite a un operador de una centralita, o a un oficial, empleado o agente de un proveedor de servicios de comunicaciones por cable o electrónicas, interceptar, revelar o utilizar la comunicación durante el desarrollo normal de su empleo mientras participe en una actividad que sea necesaria para la prestación del servicio o para la protección de los derechos o de la propiedad del proveedor de dicho servicio, salvo en el caso de que un proveedor de servicios públicos de comunicaciones por cable no practique la observación del servicio o la supervisión aleatoria más que para comprobaciones mecánicas o de control de calidad.

La cláusula sobre "protección de los derechos o propiedad del proveedor" de § 2511(2)(a)(i) garantiza a los proveedores el derecho a "interceptar y supervisar [comunicaciones] transmitidas a través de sus medios para combatir el fraude y el robo del servicio". Estados Unidos v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). Por ejemplo, un empleado de una empresa de telefonía móvil puede interceptar comunicaciones desde un terminal móvil "clonado" de forma ilegal durante la operación de localización de su fuente. Véase Estados Unidos v. Pervaz, 118 F.3d 1, 5 (1° Cir. 1997). La excepción permite también a los proveedores vigilar el uso inadecuado de un sistema para protegerlo frente a daños, robo o invasión de la privacidad. Por ejemplo, los administradores de sistemas pueden rastrear a los hackers en sus redes con el fin de evitar que vuelvan a causar daños. Cf. Mullins, 992 F.2d en 1478 (en el que se concluye que la necesidad de supervisar el uso inapropiado de un sistema informático justificó la interceptación de comunicaciones electrónicas en virtud del § 2511(2)(a)(i)).

Cabe destacar que la excepción del proveedor mencionada en el § 2511(2)(a)(i) no autoriza a los proveedores a llevar a cabo vigilancias de forma ilimitada. Véase Estados Unidos v. Auler, 539 F.2d 642, 646 (7° Cir. 1976) ("Esta autoridad de la compañía telefónica para interceptar y revelar comunicaciones por cable no es ilimitada"). En lugar de ello, la excepción permite a los proveedores y a sus empleados realizar una vigilancia razonable que aúne la necesidad de proteger sus derechos y propiedad con el derecho de los abonados a la privacidad de sus comunicaciones. Véase Estados Unidos v. Harvey, 540 F.2d 1345, 1350 (8° Cir. 1976) ("Los tribunales federales […] han interpretado que la ley impone un determinado grado de razonabilidad en el proveedor de la comunicación que lleva a cabo la investigación"). Los proveedores que investiguen el uso no autorizado de sus sistemas tienen autoridad para vigilar y revelar posteriormente las pruebas de dicho uso en virtud del § 2511(2)(a)(i), si bien han de intentar adaptar su supervisión y divulgación de tal forma que se reduzca al máximo la interceptación y divulgación de comunicaciones privadas que no guarden relación con la investigación. Véase por ejemplo Estados Unidos v. Freeman, 524 F.2d 337, 340 (7° Cir. 1975) (en el que se concluye que una compañía telefónica que investigó el uso de "cajas azules", unos dispositivos diseñados para robar el servicio de larga distancia, actuó de forma lícita conforme al § 2511(2)(a)(i) cuando interceptó los dos primeros minutos de todas las conversaciones realizadas mediante una "caja azul", pero no interceptó las comunicaciones autorizadas legalmente). En especial, debe existir una "conexión importante" entre la vigilancia y la amenaza hacia los derechos o la propiedad del proveedor. Estados Unidos v. McLaren, 957 F. Supp. 215, 219 (M.D. Fla. 1997). Asimismo, aunque los proveedores pueden proteger legítimamente sus derechos o propiedades recabando pruebas de actos ilegales para iniciar después un proceso penal, véase Estados Unidos v. Harvey, 540 F.2d 1345, 1352 (8° Cir. 1976), no pueden hacer uso de la excepción de los derechos o propiedades para obtener pruebas de delitos que

no guarden relación con los derechos o la propiedad citados. Véase Bubis v. Estados Unidos, 384 F.2d 643, 648 (9° Cir. 1967) (en el que se interpreta la ley anterior al Título III, 47 U.S.C. § 605, y se califica de inadmisible la vigilancia que realizó un proveedor a un usuario de cajas azules sancionado de la transmisión interestatal de información sobre apuestas).

Agentes y fiscales deben reprimir la tendencia a utilizar la excepción del proveedor para satisfacer las necesidades de las fuerzas de seguridad. Aunque la excepción permite a los proveedores interceptar y revelar comunicaciones a las fuerzas de seguridad para proteger sus derechos o propiedades, véase Harvey, 540 F.2d en 1352, no permite a los oficiales que den instrucciones o pidan a los administradores de sistemas que realicen labores de vigilancia con fines que conciernan a las fuerzas de seguridad. Por ejemplo, en McClelland v. McGrath, 31 F. Supp. 2d 616 (N.D. Ill. 1998), unos oficiales de policía que investigaban un secuestro rastrearon las llamadas del secuestrador hasta un teléfono móvil "clonado" de forma ilegal. Con el fin de averiguar más datos acerca de la identidad y la ubicación del secuestrador, la policía pidió al proveedor de los servicios telefónicos que interceptara sus comunicaciones y transmitiera a los oficiales toda la información que pudiera ayudarles a localizar al secuestrador. El proveedor aceptó, escuchó sus llamadas y posteriormente transmitió la información a la policía, que procedió a arrestar al delincuente. Posteriormente, el secuestrador denunció a los oficiales por interceptar sus llamadas telefónicas y estos adujeron que el § 2511(2)(a)(i) autorizaba la interceptación porque el proveedor podía vigilar el teléfono clonado para proteger sus derechos contra el robo. A pesar de que el tribunal destacó que esta denuncia "era la definición perfecta de un caradura", concluyó que el § 2511(2)(a)(i) no autorizaba la interceptación en la medida en la que la policía había dado instrucciones al proveedor para que vigilara al sospechoso con fines relacionados con la investigación y ajenos a los derechos o la propiedad del proveedor:

Lo que los oficiales parecen no comprender […] es que no pueden pedir o dar instrucciones [al proveedor] para que intercepte llamadas telefónicas o revele su contenido, o al menos no puede hacerlo sin cumplir con las disposiciones sobre la autorización judicial correspondientes a la Ley de Escuchas Telefónicas, independientemente de si [el proveedor] tiene derecho a interceptar esas llamadas por iniciativa propia.

Id. en 619. Teniendo en cuenta que la finalidad de la vigilancia era localizar e identificar al secuestrador (en interés de las fuerzas de seguridad), en lugar de combatir el fraude telefónico (en interés del proveedor), el tribunal rechazó dictar sentencia sumaria para los oficiales sobre la base del § 2511(2)(a)(i). Véase id; véase también Estados Unidos v. Savage, 564 F.2d 728, 731 (5° Cir. 1977) (en el que corrobora la sentencia del tribunal de distrito por la que se establece que un oficial de policía sobrepasó la excepción del proveedor al requisar las escuchas de un operador telefónico).

En vista de estas dificultades, agentes y fiscales han de adoptar un enfoque prudente a la hora de aceptar los resultados de una vigilancia futura desarrollada por proveedores conforme a la excepción del proveedor. (Como se comenta más abajo, las fuerzas de seguridad pueden evitar este problema acogiéndose a la excepción del intruso informático). Por lo general, los agentes de las fuerzas de seguridad tienen libertad para aceptar los resultados de una supervisión que un proveedor haya recopilado en virtud del § 2511(2)(a)(i) antes de poner en conocimiento de la policía la actividad delictiva de la que sospechaban. Una vez que la policía y el proveedor hayan entablado la comunicación, sin embargo, los primeros sólo podrán aceptar los resultados de una vigilancia si se han observado determinados requisitos que indiquen que el proveedor lleva a cabo la supervisión y divulga la información para proteger sus derechos o propiedad. Estos requisitos son: 1) que el proveedor sea víctima del delito y desee interceptar y revelar la información para proteger sus derechos o propiedad, 2) que las fuerzas de seguridad comprueben que la interceptación y revelación por parte del proveedor estuvieron motivadas por su voluntad de proteger sus derechos o propiedad, más que para ayudar a la policía, 3) que las fuerzas de seguridad no haya encargado, ordenado, solicitado o preparado la vigilancia o divulgación con fines propios y 4) que las fuerzas de seguridad no participen ni controlen la supervisión propiamente dicha. Aunque no lo exija la ley, es muy recomendable que los agentes obtengan un documento escrito del proveedor privado en el que se indique que éste comprende sus derechos y desea realizar la vigilancia y revelar los resultados para proteger sus derechos o propiedad. Asimismo, también se recomienda que lo revise un CTC del distrito correspondiente (véase la Introducción, pág. ix) o la Sección de Delitos Cibernéticos y Propiedad Intelectual, llamando al teléfono

(202) 514-1026. Si se siguen estos procedimientos, los agentes pueden reducir en gran medida el riesgo de que la supervisión y revelación por parte de un proveedor supere los límites aceptables del § 2511(2)(a)(i). En el Apéndice G se ofrece un escrito de ejemplo de un proveedor.

La excepción del intruso informático, que se comenta más adelante en el apartado (d), se creó en parte para permitir a las fuerzas de seguridad evitar la necesidad de depender de una posible vigilancia de un proveedor. Es importante que tanto agentes como fiscales tengan presente que la excepción del intruso informático ofrecerá en algunos casos una base más fiable que la excepción del proveedor para vigilar a un intruso una vez que el proveedor se haya puesto en contacto con las fuerzas de seguridad. *La implicación de las fuerzas de seguridad en la supervisión de redes gubernamentales por parte del proveedor plantea problemas especiales. Dado que los límites de la autoridad a menudo son borrosos, los agentes deben mostrarse extremadamente cautelosos.*

Los motivos de la excepción del proveedor presuponen que existe una línea firme entre los proveedores y los oficiales. Conforme a este planteamiento, los proveedores se muestran inquietos por proteger sus redes frente al abuso, mientras que los oficiales se preocupan por investigar delitos y perseguir a los delincuentes. Sin embargo, esta línea se puede borrar cuando la red que se va a proteger pertenece a un organismo o delegación del gobierno. Por ejemplo, entidades gubernamentales federales como la NASA, el servicio de correos y el ejército cuentan con redes informáticas enormes y con una presencia considerable de oficiales de las fuerzas de seguridad, tanto en los servicios de investigación penal del ejército como en las oficinas generales de los inspectores de los organismo civiles. Los oficiales de las fuerzas de seguridad y los administradores de sistemas del gobierno normalmente se consideran parte "del mismo equipo", por lo que resulta tentador que los primeros se apropien de los resultados de una vigilancia por parte del proveedor y justifiquen su acción mediante una interpretación amplia de la protección de los "derechos o la propiedad" de éste. Aunque los tribunales todavía no han abordado la viabilidad de esta teoría de la supervisión del proveedor, una interpretación así, al menos en su expresión más amplia, puede resultar muy difícil de conciliar con algunos de los casos que interpretan la excepción del proveedor. Véase por ejemplo McLaren, 957 F. Supp. en 219. La CCIPS recomienda un enfoque prudente: agentes y fiscales deben dar por sentado que los tribunales que interpreten el § 2511(2)(a)(i) en el marco de una red del gobierno harán cumplir la misma distinción entre los intereses de los oficiales y los del proveedor que en los casos de redes privadas. Véase por ejemplo Savage, 564 F.2d en 731; McClelland, 31 F. Supp. 2d en 619. Una vez más es recomendable una Buena dosis de prudencia si un agente se plantea aceptar los resultados de una vigilancia conforme a la excepción del proveedor llevada a cabo por un proveedor gubernamental. Los agentes y fiscales pueden llamar a la CCIPS al número de teléfono (202) 514-1026 o al CTC de su distrito (véase la Introducción, pág. ix) si necesitan orientación adicional en casos específicos.

La cláusula "necesario para la prestación del servicio" del § 2511(2)(a)(i) supone el segundo contexto en el que se aplica la excepción del proveedor. Esta expresión permite a los proveedores interceptar, utilizar o revelar comunicaciones durante la actividad normal de su negocio cuando la interceptación es inevitable. Véase Estados Unidos v. New York Tel. Co., 434 U.S. 159, 168 n.13 (1977) (en el que se destaca que el § 2511(2)(a)(i) "excluye todas las prácticas comerciales normales de las compañías telefónicas" de la prohibición del Título III). Por ejemplo, un operador de una centralita puede captar fragmentos de conversaciones al conectar las llamadas. Véase por ejemplo Estados Unidos v. Savage, 564 F.2d 728, 731-32 (5° Cir. 1977); Adams v. Sumner, 39 F.3d 933, 935 (9° Cir. 1994). De igual modo, una persona encargada de llevar a cabo una reparación puede escuchar parte de una conversación al intervenir líneas telefónicas durante el arreglo. Véase Estados Unidos v. Ross, 713 F.2d 389, 392-93 (8° Cir. 1983). Aunque la expresión "necesario para la prestación del servicio" no se ha interpretado en el contexto de comunicaciones electrónicas, estos casos sugieren que esta frase permitiría igualmente que un administrador de sistemas interceptase comunicaciones durante las labores de reparación o mantenimiento de una red.[(28)]

d) La excepción del intruso informático, 18 U.S.C. § 2511(2)(i)

18 U.S.C. § 2511(2)(i) permite a las víctimas de ataques informáticos autorizar a las fuerzas de seguridad a interceptar comunicaciones por cable o electrónicas de un intruso informático. La policía puede interceptar las comunicaciones de un intruso informático "transmitidas hacia, a través de o desde"

un ordenador protegido si se cumplen cuatro condiciones. En primer lugar, el propietario o el operador del ordenador protegido deben dar su consentimiento a la interceptación de las comunicaciones del intruso. 18 U.S.C. § 2511(2)(i)(I). Por lo general, a pesar de que no lo exige la ley de forma específica, es recomendable que los investigadores obtengan por escrito la autorización para la interceptación del propietario del ordenador o de un representante de alto nivel del mismo. Seguidamente, la persona que intercepte las comunicaciones debe "participar legalmente en la investigación". 18 U.S.C. § 2511(2)(i)(II). En tercer lugar, la persona que intercepte las comunicaciones debe tener "motivos razonables para creer que el contenido de las comunicaciones del intruso informático será relevante para la investigación". 18 U.S.C. § 2511(2)(i)(III). La cuarta y última condición es que la interceptación no debe adquirir otras comunicaciones que las transmitidas hacia o desde el ordenador del intruso. 18 U.S.C. § 2511(2)(i)(IV). De esta manera, los investigadores no pueden acogerse a la excepción de intrusión informática a menos que puedan evitar interceptar comunicaciones de usuarios que estén autorizados a utilizar el ordenador y no hayan permitido la supervisión.

El Título III define "intruso informático" como una persona que accede a un ordenador protegido sin autorización. Asimismo, la definición excluye a las personas "de las que el dueño u operador del ordenador protegido sepa que tienen una relación contractual vigente con él para acceder a todo o parte del ordenador protegido". 18 U.S.C. § 2510(21). Conforme a esta definición, los clientes de un proveedor de servicios que infrinjan las condiciones de servicio del proveedor no se convierten en intrusos informático, ya que simplemente superan el ámbito de su autorización. De igual manera, un empleado de una compañía que contravenga la política de uso de los ordenadores no es un intruso informático. Por último, en 18 U.S.C. § 1030(e)(2) se da una definición de "ordenador protegido" que incluye cualquier ordenador que se utilice para el comercio interestatal o exterior o para la comunicación, así como la mayor parte de los ordenadores utilizados por el gobierno y las instituciones de Estados Unidos. Así, casi cualquier equipo conectado a Internet será un "ordenador protegido". A menos que el Congreso la prorrogue, la excepción del intruso informático, que forma parte de la Ley USA PATRIOT de 2001, expirará el 31 de diciembre de 2005. Véase Ley PATRIOT §§ 217, 224, 115 Stat. 272, 290-91, 295 (2001).

La excepción del intruso informático se puede utilizar en combinación con otras autoridades, como la excepción del proveedor del § 2511(2)(a)(i). Un proveedor que haya supervisado su sistema para proteger sus derechos y propiedad en virtud del § 2511(2)(a)(i) y que posteriormente se haya puesto en contacto con las fuerzas de seguridad para informar de alguna actividad delictiva, puede continuar vigilando dicha actividad en su sistema bajo la dirección de la policía acogiéndose a la excepción del intruso informático. En tales circunstancias, el proveedor pasará a actuar en nombre de la ley y como agente del gobierno.

e) La excepción de la extensión telefónica, 18 U.S.C. § 2510(5)(a)

Según 18 U.S.C. § 2510(5)(a), el Título III no se infringe mediante el uso de un instrumento, equipo o instalación telefónicos o telegráficos, o cualquier componente de los mismos, (i) facilitado al abonado o usuario por un proveedor de servicios de comunicaciones por cable o electrónicas como parte del desarrollo normal de su actividad y que el abonado o usuario utilice normalmente, o que haya sido suministrado por dicho abonado o usuario para la conexión a las instalaciones de dicho servicio y que se utilice en el transcurso normal de su actividad; o (ii) que sea utilizado por un proveedor de servicios de comunicaciones por cable o electrónicas en el desarrollo normal de su actividad, o por un oficial que esté llevando a cabo una investigación o por las fuerzas de seguridad durante el desempeño de sus obligaciones.[(29)]

Tal y como se redactó originalmente, la intención del Congreso es que esta excepción tuviera una finalidad muy limitada: la excepción se concibió fundamentalmente para permitir a las empresas supervisar por medio de una "extensión telefónica" el rendimiento de los empleados que hablaran por este medio con sus clientes. La excepción de la "extensión telefónica" deja claro que cuando una compañía telefónica proporciona a un empleador una extensión telefónica con una finalidad legítima asociada al trabajo, la supervisión de los empleados por parte del empresario mediante este dispositivo con fines laborales no infringe el Título III. Véase Briggs v. American Air Filter Co., 630 F.2d 414, 418 (5° Cir. 1980) (en el que se revisa la trayectoria legislativa del Título III); Watkins v. L.M. Berry & Co.,

704 F.2d 577, 582 (11° Cir. 1983) (en el que se aplica la excepción para permitir la supervisión de representantes de ventas); James v. Newspaper Agency Corp. 591 F.2d 579, 581 (10° Cir. 1979) (en el que se aplica la excepción para permitir la supervisión de las conversaciones de los empleados del periódico con los clientes).

La jurisprudencia que interpreta la excepción de la extensión telefónica es considerablemente irregular, debido en gran parte a la ambigüedad de la expresión "desarrollo normal de la actividad". Algunos tribunales han interpretado que "desarrollo normal de la actividad" significa en sentido general "en el ámbito de los asuntos legítimos de una persona" y han llegado a aplicar la excepción de la extensión telefónica en contextos como el de disputas familiares. Véase por ejemplo Simpson v. Simpson, 490 F.2d 803, 809 (5° Cir. 1974) (en el que se concluye que el marido no infringió el Título III al grabar las llamadas telefónicas de su mujer); Anónimo v. Anónimo, 558 F.2d 677, 678-79 (2° Cir. 1977) (en el que se concluye que el marido no infringió el Título III al grabar las conversaciones que su mujer mantenía con la hija que él tenía bajo su custodia). Otros tribunales han rechazado esta interpretación tan general y han excluido implícita o explícitamente las actividades subrepticias de conducta del "desarrollo normal de la actividad". Véase Kempf v. Kempf, 868 F.2d 970, 973 (8° Cir. 1989) (en el que se concluye que el Título III prohíbe toda actividad de escuchas telefónicas a menos que haya sido autorizada explícitamente, así como que no existe ninguna excepción expresa par alas escuchas telefónicas entre cónyuges); Estados Unidos v. Harpel, 493 F.2d 346, 351 (10° Cir. 1974) ("Concluimos como cuestión de derecho que una extensión de teléfono utilizada sin autorización para grabar de manera subrepticia una conversación telefónica privada no se realiza en el desarrollo normal de una actividad"); Pritchard v. Pritchard, 732 F.2d 372, 374 (4° Cir. 1984) (en el que se rechaza la idea de que el § 2510(5)(a) exime las escuchas telefónicas entre cónyuges de la responsabilidad con respecto al Título III). Algunos de los tribunales que han adoptado la interpretación más limitada de la excepción de la extensión telefónica han destacado que permite solamente una supervisión en el entorno laboral y por parte de los empleadores. Véase por ejemplo Deal v. Spears, 980 F.2d 1153, 1158 (8° Cir. 1992) (en el que se concluye que la supervisión de un empleado por parte del empresario no estaba autorizada por la excepción de la extensión telefónica, en parte porque el ámbito de la interceptación era más amplio de lo que normalmente se necesita en el desarrollo normal de la actividad).

La excepción de 18 U.S.C. § 2510(5)(a)(ii) que permite el uso de "cualquier instrumento, equipo o instalación telefónicos o telegráficos o cualquier componente de los mismos" por parte de "un oficial que esté llevando a cabo una investigación durante el desempeño de sus obligaciones" es una fuente habitual de confusiones. Este texto no permite que los agentes intercepten comunicaciones privadas con arreglo a la teoría de que un agente de las fuerzas de seguridad puede verse en la necesidad de interceptar comunicaciones "en el desarrollo normal de sus obligaciones". Como ha explicado el Juez Decano Posner:

La investigación entra dentro de la actividad normal de las fuerzas de seguridad, por lo que si "normal" se interpretara literalmente, prácticamente no se tendrían que solicitar órdenes para la interceptación de datos electrónicos, lo que casi con toda seguridad no era la intención del Congreso. Dado que la finalidad de la ley era principalmente regular el uso de la intervención de teléfonos y otros tipos de vigilancia electrónica con una finalidad relacionada con la investigación, "normal" no se debe interpretar de una manera tan amplia; es más razonable pensar que hace referencia a la grabación rutinaria de conversaciones telefónicas sin afán de investigación. . . . Esta grabación rara vez invadirá demasiado la privacidad, por una razón que, después de todo, acerca bastante la exclusión del desarrollo normal a la exclusión de la autorización: lo que es normal tiende a ser conocido; comporta un aviso implícito.

Amati v. Ciudad de Woodstock, 176 F.3d 952, 955 (7° Cir. 1999). Por ejemplo, la grabación habitual de todas las llamadas telefónicas entrantes y salientes de una comisaría de policía puede entrar en esta excepción en cumplimiento de la ley, pero normalmente una grabación que se saliera de lo habitual dirigida a un sospechoso concreto no lo haría. Véase id.; acuerdo Estados Unidos v. Hammond, 286 F.3d 189, 192 (4° Cir. 2002) (en el que se concluye que la grabación habitual de llamadas realizadas desde la cárcel entran dentro de la excepción en cumplimiento de la ley); Estados Unidos v. Van Poyck, 77 F.3d 285, 292 (9° Cir. 1996) (similar).

f) La excepción de las "pruebas penales obtenidas involuntariamente", 18 U.S.C. § 2511(3)(b)(iv)

18 U.S.C. § 2511(3)(b) menciona varios contextos muy concretos en los que un proveedor de servicios de comunicaciones electrónicas al público puede divulgar los contenidos de comunicaciones. La más importante de estas excepciones permite a un proveedor público divulgar los contenidos de cualquier comunicación que el proveedor del servicio haya obtenido de forma involuntaria y que aparentemente guarden relación con la comisión de un delito y siempre que dicha divulgación se haga a un organismo de las fuerzas de seguridad.

18 U.S.C. § 2511(3)(b)(iv). Esta excepción aún no ha sido aplicada por los tribunales en ningún caso publicado relacionado con ordenadores. Aun así, su redacción aparentemente permite a los proveedores informar de conductas delictivas, como por ejemplo, pornografía infantil o pruebas de un fraude, en determinadas circunstancias sin infringir el Título III. Cf. 18 U.S.C. § 2702(b)(6)(A) (en el que se crea una norma análoga para comunicaciones almacenadas).

g) La excepción "accesible al público, 18 U.S.C. § 2511(2)(g)(i)

18 U.S.C. § 2511(2)(g)(i) permite que "cualquier persona intercepte una comunicación electrónica realizada mediante un sistema "configurado de tal forma […] [que] la comunicación sea fácilmente accesible para el público en general". Aunque esta excepción aún no ha sido aplicada por los tribunales en ningún caso publicado relacionado con ordenadores, su redacción aparentemente permite la interceptación de una comunicación electrónica que se haya publicado en un tablón de anuncios público, en un Chat público o en un grupo de noticias de Usenet. Véase S. Rep. N° 99-541, en 36 (1986), reimpreso en 1986 U.S.C.C.A.N. 3555, 3590 (en el que se comentan los tablones de anuncios).

[Índice]

E. Remedios para infracciones del Título III y de la Ley de registro y control de llamadas

Los agentes y fiscales deben seguir estrictamente las directrices del Título III y de la ley de registro y control de llamadas al planificar una vigilancia electrónica, ya que la infracción de estas leyes puede acarrear sanciones civiles y penales, además de la anulación de las pruebas obtenidas. Véase 18 U.S.C. § 2511(4) (sanciones penales para infracciones del Título III); 18 U.S.C. § 2520 (indemnizaciones civiles por infracción del Título III); 18 U.S.C. § 3121(d) (sanciones penales por infracciones de la ley de registro y control de llamadas); 18 U.S.C. § 2518(10)(a) (anulación para determinadas infracciones del Título III). En la práctica, no obstante, los tribunales pueden concluir que se produjo la infracción de las leyes de vigilancia electrónica incluso aunque los agentes y fiscales hayan actuado de buena fe y observando estrictamente la ley. Por ejemplo, un ciudadano particular puede realizar escuchas telefónicas de su vecino y transmitir posteriormente las pruebas a la policía o un agente puede interceptar comunicaciones en virtud de una orden judicial y averiguar después que es incorrecta. De igual forma, un tribunal puede interpretar una parte ambigua del Título III de una forma distinta a cómo lo hicieron los investigadores, lo que puede llevar al tribunal a sentenciar que se infringió el Título III. En estas circunstancias, los fiscales y agentes han de comprender no sólo qué tipos de conducta prohíben las leyes sobre vigilancia, sino también cuáles pueden ser las repercusiones si un tribunal sentencia que éstas se han vulnerado.

1. Remedios de anulación

El Título III contempla la anulación legítima de comunicaciones orales y por cable interceptadas de forma improcedente, pero no de comunicaciones electrónicas. La ley de registro y control de llamadas no contempla la anulación legal como sanción. Las infracciones constitucionales pueden dar como resultado la anulación de las pruebas obtenidas ilegalmente.

a) Remedios de anulación legal

i) General: interceptación sólo de comunicaciones por cable

Las leyes que regulan la vigilancia electrónica conceden remedios de anulación legal a los demandados únicamente en una serie concreta de casos. Concretamente, un demandado sólo puede solicitar la anulación por motivos legales cuando fuera participante de una comunicación oral o por cable que se interceptara vulnerando el Título III. Véase 18 U.S.C. §§ 2510(11), 2518(10)(a). Véase también Estados Unidos v. Giordano, 416 U.S. 505, 524 (1974) (en el que se establece que "el tipo de revelaciones que están prohibidas [en virtud del § 2515] y las que están sujetas a solicitudes de anulación […] se regula en el § 2518(10)(a)"); Estados Unidos v. Williams, 124 F.3d 411, 426 (3° Cir. 1997). La sección 2518(10)(a) expone que:

Toda persona afectada […] puede solicitar la anulación de los contenidos de una comunicación por cable u oral que haya sido interceptada con arreglo a lo expresado en este capítulo, o de las pruebas derivadas de la misma, en el caso de que:

(1) la comunicación se interceptara de manera ilegal;

(ii) la orden de autorización o aprobación en virtud de la cual se interceptara sea aparentemente insuficiente; o

(iii) la interceptación no se realizó de conformidad con la orden de autorización o aprobación.

18 U.S.C. § 2518(10)(a). Cabe destacar que el Título III no contempla e remedio de la anulación legal en caso de interceptación ilícita de comunicaciones electrónicas. Véase Steve Jackson Games, Inc. v. Servicio Secreto de Estados Unidos, 36 F.3d 457, 461 n.6 (5° Cir. 1994); Estados Unidos v. Meriwether, 917 F.2d 955, 960 (6° Cir. 1990). Igualmente, la ley de registro y control de llamadas no prevé el remedio de la anulación legal para infracciones. Véase Estados Unidos v. Fregoso, 60 F.3d 1314, 1320-21 (8° Cir. 1995); Estados Unidos v. Thompson, 936 F.2d 1249, 1249-50 (11° Cir. 1991).

ii) Partes no autorizadas

El texto del Título III aparentemente ofrece el remedio de la anulación para cualquier parte en el caso de una comunicación por cable interceptada ilegalmente, independientemente de si la parte tenía autorización o no para utilizar el sistema de comunicación. Véase 18 U.S.C. § 2510(11) (en donde se define la "persona afectada" que puede solicitar la anulación conforme al § 2518(10)(a) como "una persona que participó en una comunicación por cable, oral o electrónica interceptada contra la cual se dirigió la interceptación"). A pesar de esta definición tan amplia, no queda del todo claro si un pirata informático podría solicitar la anulación de pruebas que registraran su actividad ilícita en la red informática de la víctima. Sólo ha habido un tribunal que ha evaluado esta cuestión y expresó serias dudas. Véase Estados Unidos v. Seidlitz, 589 F.2d 152, 160 (4° Cir. 1978) (en el que se expone en *la sentencia* que "dudamos seriamente de que [un pirata cuyas comunicaciones fueran vigiladas por el administrador de sistemas de la red de una víctima] tenga derecho a poner […] objeciones a las pruebas [en virtud del Título III]").

La sugerencia del Cuarto Circuito en el Caso Seidlitz no es coherente con otras decisiones que interpretan la definición de "persona afectada" en 18 U.S.C. § 2510(11). Si nos atenemos al historial legislativo del Título III, el Tribunal Supremo ha hecho hincapié en que la intención del remedio de la anulación del Título III no era "ampliar de forma generalizada el papel de la anulación más allá de la ley actual de registro y confiscación". Scott v. Estados Unidos, 436 U.S. 128, 139 (1978) (se cita S. Rep. N° 90-1097, en 96 (1968), y Alderman v. Estados Unidos, 394 U.S. 165, 175-76 (1969)). Según sugiere el caso, si la supervisión no contraviene la expectativa razonable de privacidad del sospechoso conforme a la Cuarta Enmienda, éste no puede ser una persona "afectada" que pueda solicitar la anulación conforme al Título III. Véase Estados Unidos v. King, 478 F.2d 494, 506 (9° Cir. 1973) ("Un demandado puede solicitar la anulación de los resultados de una escucha telefónica [en virtud del Título III] solamente si

se invadió su privacidad"); Estados Unidos v. Baranek, 903 F.2d 1068, 1072 (6° Cir. 1990) ("No aceptamos la opinión del demandado de que la ley de la Cuarta Enmienda no guarda relación con los asuntos de la anulación de la resolución del Título III. . . . En los casos en los que, como aquí, tengamos una situación objetiva que no esté claramente contemplada por la ley, creemos que puede resultar útil en cuanto al asunto de la anulación […] referirse a la ley de la Cuarta Enmienda").

Dado que la supervisión del ataque de un hacker normalmente no infringe la expectativa razonable de privacidad de éste, véase "Remedios constitucionales de anulación", más adelante, no está claro si un hacker se puede considerar una "persona afectada" con derecho a la anulación de dicha vigilancia conforme al § 2518(10)(a). Hasta la fecha, ningún tribunal ha abordado directamente esta cuestión. Ni que decir tiene que siguen existiendo las sanciones civiles y penales para la vigilancia ilícita, incluso aunque esté dirigida contra un uso no autorizado. Véase por ejemplo McClelland v. McGrath, 31 F. Supp. 616 (N.D. Ill. 1998) (en el que se rechaza desestimar un pleito civil interpuesto por un secuestrador contra oficiales de la policía por la vigilancia ilegal del uso no autorizado de un teléfono móvil clonado por parte del delincuente).

iii) Anulación por interceptación con una orden incorrecta conforme al Título III

De conformidad con el § 2518(10)(a), los tribunales optarán generalmente por anular las pruebas obtenidas como resultado de una interceptación ilegal de una comunicación por cable de la parte afectada que se haya producido sin una orden judicial. No obstante, si los investigadores disponen de una orden conforme al Título III que posteriormente resulta ser incorrecta, los tribunales anularán las pruebas obtenidas con dicha orden únicamente si ésta "no cumplía ninguna de las condiciones legales que reflejan directa y sustancialmente la intención del Congreso [al promulgar el Título III] de limitar el uso de procedimientos de inspección a aquellas situaciones en las que sea claramente necesario el empleo de estos extraordinarios dispositivos de investigación". Estados Unidos v. Giordano, 416 U.S. 505, 527 (1974).

Esta norma requiere que los tribunales distingan los fallos técnicos de los importantes. Si el defecto de la orden conforme al Título III tiene que ver solamente con aspectos técnicos del Título III, no se anularán los resultados de la interceptación. Por el contrario, los tribunales anularán las pruebas si el fallo refleja el incumplimiento de alguna de las condiciones importantes del Título III. Compárese Giordano, 416 U.S. en 527-28 (en donde se concluye que al no recibirse autorización del oficial del Departamento de Justicia según figura en el § 2516(1) para una orden que autorice la interceptación de comunicaciones por cable, esto exige la anulación debido a la importancia de dicha autorización en relación con la ley) con Estados Unidos v. Moore, 41 F.3d 370, 376-77 (8° Cir. 1994) (en el que se aplica la excepción de buena fe de Estados Unidos v. Leon, 468 U.S. 897 (1984) frente al recurso contra la orden conforme al Título III y se revoca la orden de anulación del tribunal de distrito al considerar que el hecho de que el juez no firmara la orden conforme al Título III en el lugar adecuado fue simplemente un fallo técnico). Cuando un fallo guarde relación directa con un asunto constitucional como la causa probable o la particularidad, véase Berger v. New York, 388 U.S. 41, 58-60 (1967), por lo general se considerará un fallo importante que exige la anulación. Véase Estados Unidos v. Ford, 553 F.2d 146, 173 (D.C. Cir. 1977).

iv) La excepción "manos limpias" del Sexto Circuito

18 U.S.C. § 2518(10)(a)(i) estipula que una persona afectada puede solicitar la anulación de los contenidos de comunicaciones por cable si "la comunicación se interceptó de manera ilegal". El texto de esta ley es susceptible de interpretarse como que el gobierno no puede utilizar los resultados de una comunicación por cable interceptada ilícitamente como pruebas ante un tribunal, incluso aunque el gobierno no fuera el autor de la interceptación. Conforme a esta interpretación, si un particular realiza escuchas telefónicas a otro particular y después entrega los resultados al gobierno, éste no podrá utilizar las pruebas en un juicio. Véase Estados Unidos v. Vest, 813 F.2d 477, 481 (1° Cir. 1987).

No obstante, el Sexto Circuito ha creado una excepción de "manos libres" que permite al gobierno utilizar comunicaciones interceptadas ilegalmente en tanto en cuanto éste no "participara en la

interceptación ilícita". Estados Unidos v. Murdock, 63 F.3d 1391, 1404 (6° Cir. 1995). En el caso Murdock, la esposa del demandado había grabado subrepticiamente las conversaciones telefónicas de su marido desde lejos en su empresa familiar de pompas fúnebres. Cuando escuchó posteriormente las grabaciones, oyó pruebas de que su marido había aceptado un soborno de 90.000 $ para conceder un contrato gubernamental a una central lechera local durante su mandato como presidente de la Detroit School Board. La Sra. Murdock envió una copia anónima de la grabación a otro licitador de la competencia que optaba a la oferta, el cual hizo la llegar a las fuerzas de seguridad. El gobierno imputó cargos de evasión de impuestos contra el sr. Murdock basándose en la teoría de que éste no había informado del soborno de 90.000 $ como ingresos sujetos a impuestos.

Después de un juicio en el que se admitió la grabación como prueba contra él, el jurado condenó al Sr. Murdock, el cual apeló. El Sexto Circuito corroboró la sentencia y sentenció que a pesar de que la sra. Murdcok había infringido el Título III al grabar las llamadas de su marido, esta infracción no debía suponer un obstáculo para admitir las grabaciones en un juicio penal posterior. El tribunal consideró que la interceptación ilegal de la Sra. Murdock se podía comparar con un registro privado conforme a la Cuarta Enmienda y concluyó que el Título III no impedía al gobierno "utilizar pruebas que literalmente ponían en sus manos", ya que esto no tendría ningún efecto disuasorio sobre la conducta del gobierno. Id. en 1403.

Desde la sentencia del Sexto Circuito en el caso Murdock, tres circuitos han rechazado la excepción de "manos limpias" y han optado por adoptar la norma de derecho del Primer Circuito según la cual el gobierno no puede hacer uso de los resultados e una interceptación ilegal aun en el caso de que no haya participado en la interceptación inicial. Véase Berry v. Funk, 146 F.3d 1003, 1013 (D.C. Cir. 1998) (sentencias); Chandler v. Ejército de Estados Unidos, 125 F.3d 1296, 1302 (9° Cir. 1997); Gran Jurado In re, 111 F.3d 1066, 1077-78 (3° Cir. 1997). El resto de circuitos aún no se han pronunciado sobre si reconocerían la excepción de "manos limpias" en relación con el Título III.

b) Remedios de anulación constitucional

Los demandados pueden solicitar la anulación de pruebas obtenidas a través de la vigilancia electrónica de redes de comunicaciones aduciendo motivos legales o constitucionales relacionados con la Cuarta Enmienda. Aunque la infracción de la Cuarta Enmienda suele provocar la anulación de las pruebas, véase Mapp v. Ohio, 367 U.S. 643, 655 (1961), son raras las ocasiones en las que los demandados esgrimen motivos constitucionales para solicitar la anulación de los resultados de una vigilancia electrónica. Esto ocurre por dos razones interrelacionadas: en primer lugar, los remedios constitucionales de anulación del Congreso tienden a ser tan o más amplios en cuanto a su alcance que sus equivalentes constitucionales. Véase por ejemplo Chandler, 125 F.3d en 1298; Ford, 553 F.2d en 173. Cf. Estados Unidos v. Torres, 751 F.2d 875, 884 (7° Cir. 1984) (en el que se destaca que el Título III constituye un "esfuerzo minuciosamente concebido y constitucionalmente válido […] para aplicar los requisitos de la Cuarta Enmienda"). En segundo lugar, las leyes de supervisión electrónica regulan con frecuencia el acceso del gobierno a las pruebas que no estén protegidas por la Cuarta Enmienda. Véase Estados Unidos v. Hall, 488 F.2d 193, 198 (9° Cir. 1973) ("No todos los casos de vigilancia electrónica están proscritos por la constitución y el hecho de si una interceptación se ha de anular se debe estudiar a la luz de la situación en cada caso"). Por ejemplo, el Tribunal Supremo ha concluido que el uso e instalación de registros de llamadas no constituye un "registro" conforme a la Cuarta Enmienda. Véase Smith v. Maryland, 442 U.S. 735, 742 (1979). Como consecuencia de ello, el uso de estos dispositivos infringiendo la ley de de registro y control de llamadas normalmente no lleva a la anulación de pruebas por motivos relacionados con la Cuarta Enmienda. Véase Estados Unidos v. Thompson, 936 F.2d 1249, 1251 (11° Cir. 1991).

No es probable que un pirata informático pudiera tener un derecho constitucional conforme a la Cuarta Enmienda a la anulación de la supervisión improcedente de su actividad no autorizada. Como apuntó el Cuarto Circuito en el caso Seidlitz, un pirata informático que entre en el ordenador de una víctima "entra en la propiedad física [de la víctima] de la misma forma que si hubiera irrumpido en sus […] instalaciones y hubiera dado instrucciones a los ordenadores desde uno de los terminales conectado directamente a las máquinas". Seidlitz, 589 F.2d en 160. Véase también Compuserve, Inc. v. Cyber Promotions, Inc. 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (en el que se destacan casos en los que

comparan la piratería informática con el allanamiento). Un intruso no tiene una expectativa razonable de privacidad en un lugar donde su presencia sea ilegal. Véase Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (en el que se destaca que "un ladrón que ejerza su oficio en un apartamento de verano durante la temporada baja puede tener, rigurosamente hablando, una expectativa razonable de privacidad justificada, pero no del tipo que la ley reconoce como "legítima"); Amezquita v. Colon, 518 F.2d 8, 11 (1° Cir. 1975) (en el que se concluye que unos ocupas no tenían una expectativa razonable de privacidad en un terreno del gobierno sobre el que no tenían ninguna justificación para ocupar). Por consiguiente, un hacker no tendría una expectativa razonable de privacidad sobre sus actividades no autorizadas si éstas se vigilaran desde el ordenador de una de sus víctimas. "Al pillarlo con las manos en la masa", el pirata informático no tiene el derecho constitucional a la anulación de las pruebas de sus actividades ilícitas. Seidlitz, 589 F.2d en 160.

2. Defensa ante acciones civiles y penales

Los agentes y fiscales generalmente están protegidos frente a responsabilidades conforme al Título III por decisiones razonables tomadas de buena fe durante el desempeño de sus obligaciones oficiales.

Si los oficiales de las fuerzas de seguridad vulneran las leyes de vigilancia electrónica, pueden emprenderse acciones civiles y penales. Normalmente la ley permite estas acciones cuando los oficiales abusen de su autoridad, pero los protege en pleitos por errores razonables realizados de buena fe durante el desempeño normal de sus cometidos oficiales. El enfoque básico ya fue expuesto hace más de medio siglo por el juez Learned Hand:

Ciertamente debe haber medios para castigar a los oficiales públicos que falten a sus obligaciones, pero esto es muy diferente a exponerles a un litigio por haberse equivocado honestamente emprendido por alguien que haya sufrido sus errores. Como suele ocurrir, la respuesta se debe hallar en un equilibrio entre los males inevitables de cualquiera de las alternativas.

Gregoire v. Biddle, 177 F.2d 579, 580 (2° Cir. 1949). Cuando los agentes y fiscales se ven sometidos a procesos civiles o penales por vigilancia electrónica, el equilibrio entre males se topa con una defensa legal de buena fe, por un lado, y con otra defensa ampliamente (aunque no uniformemente) aceptada de cierta inmunidad adoptada por el juez.

a) Defensa de buena fe

Tanto el Título III como la ley de registro y control de llamadas ofrecen una defensa legal de buena fe. Con arreglo a estas leyes, la confianza de buena fe en […] una orden judicial, citación de gran jurado, autorización legislativa o autorización legal […] constituye una defensa completa ante una acción civil o penal emprendida con arreglo a este capítulo o a otra ley.

18 U.S.C. § 2520(d) (defensa de buena fe para infracciones del Título III). Véase también 18 U.S.C. § 3124(e) (defensa de buena fe para infracciones de la ley de registro y control de llamadas).

Los relativamente pocos casos que han interpretado la defensa de buena fe son considerablemente irregulares. Por lo general, no obstante, los tribunales han permitido a los oficiales de las fuerzas de seguridad acogerse a la defensa de buena fe cuando cometen errores honestos en el desarrollo de sus obligaciones. Véase por ejemplo Kilgore v. Mitchell, 623 F.2d 631, 633 (9° Cir. 1980) ("Los oficiales con acusaciones de infracción del Título III pueden invocar la defensa de buena fe con arreglo al § 2520 si pueden demostrar: (1) que tienen el convencimiento subjetivo de buena fe de que estaban actuando de conformidad con la ley; y (2) que este convencimiento era en sí razonable"); Hallinan v. Mitchell, 418 F. Supp. 1056, 1057 (N.D. Cal. 1976) (la excepción de buena fe protege al Fiscal General de un proceso civil después de que el Tribunal Supremo rechazara la interpretación de aquél del Título III). Por el contrario, los tribunales no han permitido a particulares acogerse a defensas de "errores de ley" de buena fe en casos de escuchas telefónicas civiles. Véase por ejemplo Williams v. Poulos, 11 F.3d 271, 285 (1° Cir. 1993); Heggy v. Heggy, 944 F.2d 1537, 1541-42 (10° Cir. 1991).

b) Inmunidad reconocida

Los tribunales han aceptado de forma generalizada una defensa por inmunidad reconocida ante acciones civiles por el Título III, así como la defensa legal de buena fe. Véase Tapley v. Collins, 211 F.3d 1210, 1216 (11° Cir. 2000) (en el que se concluye que los oficiales públicos denunciados en virtud del Título III pueden apelar a la inmunidad reconocida además de a la defensa de buena fe); Blake v. Wright, 179 F.3d 1003, 1013 (6° Cir. 1999) (en el que se concluye que la inmunidad reconocida protege al jefe de policía de un proceso emprendido por los empleados que fueron vigilados ya que el "vacío legal que rodea a la […] ley no establece claramente si las actividades [del demandado] infringieron la ley"): Davis v. Zirkelbach, 149 F.3d 614, 618, 620 (7° Cir. 1998) (la defensa por inmunidad reconocida se aplica a oficiales de policía y fiscales en caso civil de escuchas telefónicas); Zweibon v. Mitchell, 720 F.2d 162 (D.C. Cir. 1983). Sin embargo, véase Berry v. Funk, 146 F.3d 1003, 1013-14 (D.C. Cir. 1998) (en el que se distingue el caso Zweibon y se concluye que la inmunidad reconocida no se aplica a infracciones del Título III puesto que ya existe la defensa legal de buena fe).

Con arreglo a la doctrina de la inmunidad reconocida, los funcionarios gubernamentales que desempeñen funciones discrecionales por lo general están protegidos frente a responsabilidades por daños civiles en tanto en cuanto su conducta no infrinja los derechos legales o constitucionales claramente establecidos de los que una persona razonable habría tenido constancia.

Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982). En general, la inmunidad reconocida protege a los oficiales del gobierno frente a litigios si "el perfil de un derecho" que se haya infringido no estaba tan claro como para que un oficial razonable entendiera que su conducta vulneraba la ley. Anderson v. Creighton, 483 U.S. 635, 640 (1987); Burns v. Reed, 500 U.S. 478, 496 (1991) (los fiscales reciben la a inmunidad reconocida por facilitar asesoramiento jurídico a la policía).

Lógicamente, el hecho de si un derecho legal conforme al Título III está "claramente establecido" en lo referente a la inmunidad reconocida es algo totalmente subjetivo. Los intereses sensibles de privacidad amparados por el Título III puede inducir a algunos tribunales a sentenciar que un derecho de privacidad en virtud del Título III está "claramente establecido", incluso aunque ningún tribunal haya reconocido el derecho en una situación similar. Véase por ejemplo McClelland v. McGrath, 31 F. Supp. 2d 616, 619-20 (N.D. Ill. 1998) (en el que se concluye que la policía infringió los derechos "claramente establecidos" de un secuestrador que utilizó un teléfono móvil clonado cuando la policía solicitó al proveedor de servicios del teléfono que interceptar las comunicaciones no autorizadas del delincuente para ayudar a localizarlo y agrega que el derecho del secuestrador a que no se le vigile es indudable a pesar del § 2511(2)(a)(i)).

[Índice]

V. PRUEBAS

A. Introducción

Si bien la finalidad esencial de este manual es obtener datos informáticos en investigaciones criminales, el fin último es obtener pruebas admisibles en un tribunal. Este manual no es una guía completa para ofrecer datos informáticos como pruebas. Sin embargo, en este capítulo se explican algunos de los problemas más importantes que pueden surgir cuando el gobierno pretende la admisión de datos informáticos con arreglo a las Normas Federales sobre Pruebas.

La mayor parte de los tribunales que han evaluado la admisibilidad de datos informáticos se han centrado en ellos como referencias potenciales. Por lo general, los tribunales han admitido los datos informáticos al demostrar que entran dentro de la excepción de datos comerciales, Norma Federal sobre Pruebas 803(6):

Datos sobre actividades realizadas con regularidad. Un memorándum, informe, registro o conjunto de datos, en cualquier forma, de hechos, sucesos, condiciones, opiniones o diagnósticos, realizado en o próximo al momento por o a partir de información transmitida por una persona con conocimiento, si se considera parte del desarrollo de una actividad comercial normal, así como si era una práctica habitual de dicha actividad comercial el realizar el memorándum, informe, registro o conjunto de datos, todo ello según indique el testimonio de la persona al cargo o de otro testigo competente, o mediante una certificación que cumpla la Norma 902(11), la Norma 902(12) o una ley que permita la certificación, a menos que la fuente de información o el método o las circunstancias de elaboración indiquen falta de veracidad. El término "comercial", en el sentido en que se utiliza en este párrafo, comprende empresas, instituciones, asociaciones, profesión, ocupación y llamadas de todo tipo, realizadas o no con ánimo de lucro.

Véase por ejemplo Estados Unidos v. Salgado, 250 F.3d 438, 452 (6° Cir. 2001); Estados Unidos v. Cestnik, 36 F.3d 904, 909-10 (10° Cir. 1994); Estados Unidos v. Goodchild, 25 F.3d 55, 61-62 (1° Cir. 1994); Estados Unidos v. Moore, 923 F.2d 910, 914 (1° Cir. 1991); Estados Unidos v. Briscoe, 896 F.2d 1476, 1494 (7° Cir. 1990); Estados Unidos v. Catabran, 836 F.2d 453, 457 (9° Cir. 1988). Al aplicar esta prueba, los tribunales han indicado que los datos informáticos se pueden admitir generalmente como registros comerciales si se han conservado con arreglo a un procedimiento habitual por motivos que tiendan a garantizar su exactitud.

Sin embargo, lo más probable es que los tribunales federales rehúyan este enfoque "universal" a medida que se vayan familiarizando con los datos informáticos. Al igual que ocurre con los registros en papel, los datos informáticos no son monolíticos: los problemas relacionados con las pruebas generados por su admisión dependerán de los tipos de datos informáticos que el defensor pretenda que se acepten. Por ejemplo, los datos informáticos que incluyan texto normalmente se pueden dividir en dos categorías: datos generados por ordenador y datos que simplemente están almacenados en el ordenador. Véase People v. Holowko, 486 N.E.2d 877, 878-79 (Ill. 1985). La diferencia estriba en si el creador del contenido del registro fue una persona o una máquina. Los registros almacenados en un ordenador hacen referencia a documentos que contienen escritos de una o varias personas y que están en formato electrónico. Entre los ejemplos más comunes podemos citar mensajes de correo electrónico, archivos de procesamiento de textos y mensajes de chats en Internet. Al igual que con cualquier otro testimonio o prueba documental que incluya declaraciones humanas, los datos almacenados en un ordenador han de cumplir con la norma referencial. Si se admite que los datos demuestran la veracidad del asunto que afirman, el proponente de los mismos debe mostrar las circunstancias que indiquen que las declaraciones humanas incluidas en ellos son fiables y fidedignas, véase Notas del Comité Consultivo a la Norma Propuesta 801 (1972), y los registros deben ser auténticos.

Por el contrario, los registros generados por ordenador contienen son el resultado de programas informáticos, sin la intervención de personas. Los datos de registro de proveedores de servicios de Internet, registros telefónicos y los recibos de los bancos suelen ser registros generados por ordenador. A diferencia de los almacenados en un ordenador, los registros generados por ordenador no contienen "declaraciones" humanas, sino solamente el resultado de un programa informático diseñado para procesar las entradas conforme a un algoritmo definido. Naturalmente, un programa informático puede ordenar a un ordenador que genere un registro que imite una declaración humana: un programa de correo electrónico puede anunciar "tiene un mensaje" cuando entra correo en la bandeja de entrada, mientras que un recibo de su banco puede informarle de que se ha ingresado una cantidad de 100 $ en su cuenta a las 14.25. No obstante, el hecho de que haya sido un ordenador y no una persona el creador del registro altera los problemas relativos a las pruebas que conllevan los registros generados por ordenador. Véase por ejemplo 2 J. Strong, McCormick on Evidence (*A propósito de las pruebas*)§ 294, en 286 (4ª ed. 1992). El problema en cuanto a las pruebas ya no es si una declaración humana extrajudicial es veraz y precisa, lo cual es una cuestión referencial, sino si el programa informático que generó el registro funcionaba correctamente, lo que supone una cuestión de autenticidad. Véase id.; Richard O. Lempert & Steven A. Saltzburg, A Modern Approach to Evidence (*Un enfoque moderno sobre las pruebas)* 370 (2d ed. 1983); Holowko, 486 N.E.2d en 878-79.

Por último, existe una tercera categoría de registros informáticos: algunos de ellos son tanto generados por ordenador como almacenados en ordenador. Por ejemplo, un sospechoso en un caso de fraude puede

utilizar un programa de cálculo para procesar las cifras económicas relacionadas con la actividad fraudulenta. Un registro informático que incluyera el resultado de este programa se derivaría tanto de la acción humana (la introducción de datos por parte del sospechoso en el programa de cálculo) como del procesamiento informático (las operaciones matemáticas realizadas por el programa). Por consiguiente, el registro combinará los problemas relacionados con las pruebas que suelen plantear los registros almacenados y generados en un ordenador. La parte que desee la admisión del registro tendrá que abordar los problemas referenciales que conlleva la introducción original de datos y los de autenticidad que plantea el procesamiento informático.

Dado que los tribunales federales desarrollan una apreciación más matizada de las distinciones que se deben realizar entre los diferentes tipos de registros informáticos, es probable que observen que la admisión de este tipo de registros suele llevar aparejados dos dificultades. En primer lugar, el gobierno debe dejar clara la autenticidad de todos los registros informáticos aportando "pruebas suficientes que respalden la conclusión de que el tema en cuestión es lo que el proponente afirma que es". Norma Federal sobre Pruebas 901(a). En segundo lugar, si los registros informáticos son datos almacenados en un ordenador que contienen declaraciones humanas, el gobierno debe demostrar que éstas no son referencias inadmisibles.

[Índice]

B. Autenticación

Para que una persona pueda solicitar la admisión de un registro informático o de otras pruebas, el proponente debe demostrar antes que es auténtico. Es decir, el gobierno debe aportar indicios "suficientes que respalden la conclusión de que [el registro informático o las pruebas] en cuestión son lo que el proponente afirma que son". Norma Federal sobre Pruebas 901(a). Véase Estados Unidos v. Simpson, 152 F.3d 1241, 1250 (10° Cir. 1998).

La norma para probar la autenticidad de registros informáticos es la misma que para otros registros. El grado de autenticación no varía por el mero hecho de que un registro esté (o haya estado en algún momento) en formato electrónico. Véase Estados Unidos v. Vela, 673 F.2d 86, 90 (5° Cir. 1982); Estados Unidos v. DeGeorgia, 420 F.2d 889, 893 n.11 (9° Cir. 1969). En cambio, véase Estados Unidos v. Scholle, 553 F.2d 1109, 1125 (8° Cir. 1977) (se establece en la sentencia que "la naturaleza compleja del almacenamiento informático requiere una base más completa"). Por poner un ejemplo, las personas que atestiguan la autenticidad de registros informáticos no tienen por qué tener una preparación especial. No es necesario que el testigo haya sido quien ha programado el ordenador, ni siquiera tiene por qué entender el mantenimiento y el funcionamiento técnico del equipo. Véase Estados Unidos v. Salgado, 250 F.3d 438, 453 (6° Cir. 2001) (en el que se establece que "no es necesario que el programador informático testifique para probar la autenticidad de datos generados por ordenador"); Estados Unidos v. Moore, 923 F.2d 910, 915 (1° Cir. 1991) (se citan casos). Es suficiente con que el testigo conozca de primera mano los hechos relevantes en relación con lo que testifique. Véase Estados Unidos v. Whitaker, 127 F.3d 595, 601 (7° Cir. 1997) (un agente del FBI que estaba presente en el momento en que se produjo la confiscación del ordenador del demandado puede dar fe de la autenticidad de los archivos requisados); Estados Unidos v. Miller, 771 F.2d 1219, 1237 (9° Cir. 1985) (el supervisor de facturación de una compañía telefónica puede dar fe de la autenticidad de los registros de la compañía); Moore, 923 F.2d en 915 (el director de un departamento de préstamos de un banco puede corroborar la autenticidad de los datos relativos a los préstamos).

Normalmente, cuando se recurre la autenticidad de registros electrónicos, estos recursos pueden adoptar tres formas distintas. En la primera de ellas, la parte puede recurrir la autenticidad de registros tanto generados como almacenados en un ordenador al cuestionar si estos han sido modificados, manipulados o dañados después de su creación. En el Segundo caso, la parte puede poner en tela de juicio la autenticidad de registros generados por ordenador cuestionando la fiabilidad del programa informático que los creó. Y por último, la parte puede recurrir la autenticidad de registros almacenados en un ordenador cuestionando la identidad de su autor.

1. Autenticidad y alteración de registros informáticos

Es muy sencillo modificar registros informáticos, por lo que la parte contraria suele alegar que estos carecen de autenticidad porque han sido manipulados o modificados después de su creación. Por ejemplo, en Estados Unidos v. Whitaker, 127 F.3d 595, 602 (7° Cir. 1997), el gobierno recuperó archivos informáticos del ordenador de un distribuidor de narcóticos llamado Frost. Entre los archivos hallados en su ordenador se encontraron documentos detallados sobre la venta de narcóticos por parte de tres alias: "Yo" (el propio Frost, presumiblemente), "Gator" (apodo del otro demandado, además de Frost) y "Cruz" (apodo de otro distribuidor). Después de que el gobierno permitiera a Frost colaborar en la recuperación de pruebas de su ordenador y rechazó crear una vigilancia formal del ordenador durante el juicio, Whitaker adujo que los archivos que le implicaban a través de su apodo no estaban correctamente autentificados. Según él, "Frost, con sólo pulsar unas cuantas teclas, podía haber añadido el alias de Whitaker, "Gator", a los listados con el fin de delatar a éste y parecer más colaborador con el gobierno". Id.

Los tribunales han respondido con bastante escepticismo ante alegaciones de este tipo argumentando que los registros han sido alterados. En ausencia de pruebas específicas de que se haya producido la modificación, la simple posibilidad de modificación no influye sobre la autenticidad de un archivo informático. Véase Whitaker, 127 F.3d en 602 (en la que se rechaza modificar la sentencia del juez en la que consideraba admisibles los registros informáticos porque la alegación de alteración era "mera especulación […] [sin] pruebas que respalden tal circunstancia"). Estados Unidos v. Bonallo, 858 F.2d 1427, 1436 (9° Cir. 1988) ("El hecho de que sea posible modificar los datos de un ordenador claramente no es suficiente para establecer su falta de veracidad"); Estados Unidos v. Glasser, 773 F.2d 1553, 1559 (11° Cir. 1985) ("La existencia de un sistema de seguridad hermético [para evitar la alteración] no es, sin embargo, requisito previo para admisibilidad de documentos informáticos. Si existiera tal requisito, sería prácticamente imposible admitir registros generados por ordenador, puesto que a la parte que se opusiera a su admisión le valdría simplemente con demostrar que es posible utilizar un sistema de seguridad mejor"). Esto es coherente con la norma utilizada para determinar la autenticidad de otro tipo de pruebas, como narcóticos. Véase Estados Unidos v. Allen, 106 F.3d 695, 700 (6° Cir. 1997) ("La mera sugerencia de la posibilidad de alteración es insuficiente para considerar inadmisible una prueba"). En ausencia de pruebas específicas de alteración, las alegaciones de que un registro informático ha sido modificado caen por su propio peso, no su admisibilidad. Véase Bonallo, 858 F.2d en 1436.

2. Determinación de la fiabilidad de programas informáticos

La autenticidad de registros generados por ordenador implica en ocasiones la fiabilidad de los programas informáticos que los crean. Por ejemplo, un registro generado por ordenador puede no ser auténtico si el programa que lo ha creado contiene errores graves de programación. Si el resultado del programa es impreciso, el registro puede no ser "lo que el proponente afirma que es" de acuerdo con la Norma Federal sobre Pruebas 901.

Los demandados en juicios penales suelen cuestionar la autenticidad de los registros generados por ordenador poniendo en tela de juicio la fiabilidad de los programas. Véase por ejemplo Estados Unidos v. Salgado, 250 F.3d 438, 452-53 (6° Cir. 2001); Estados Unidos v. Liebert, 519 F.2d 542, 547-48 (3° Cir. 1975). Los tribunales han indicado que el gobierno puede vadear esta cuestión en tanto en cuanto pueda proporcionar hechos suficientes que garanticen la conclusión de que los registros son fidedignos y a la parte contraria se le dé la oportunidad de cuestionar su exactitud.

Estados Unidos v. Briscoe, 896 F.2d 1476, 1494-95 (7° Cir. 1990). Véase también Estados Unidos v. Oshatz, 912 F.2d 534, 543 (2° Cir. 1990) (en el que se establece que la defensa debe tener el tiempo suficiente para comprobar la validez de un programa y contrainterrogar a los expertos del gobierno con respecto a los posibles errores en los cálculos); Liebert, 519 F.2d en 547; DeGeorgia, 420 F.2d. en 893 n.11. Cf. Normas Federal sobre Pruebas 901(b)(9) (en la que se indica que se puede dar fe de la autenticidad de los materiales creados de acuerdo a un proceso o sistema mediante "pruebas que describan el proceso o sistema utilizado […] y que demuestren que éste genera un resultado correcto"). En la mayoría de los casos, la fiabilidad de un programa informático se puede determinar demostrando que los usuarios del mismo confían en él regularmente, durante el desarrollo normal de su actividad, por

ejemplo. Véase por ejemplo Salgado, 250 F.3d en 453 (en la que se concluye que "la prueba de que el ordenador era lo bastante preciso es que la empresa dependía de él para desarrollar su actividad" era suficiente para confirmar su fiabilidad); Estados Unidos v. Moore, 923 F.2d 910, 915 (1° Cir. 1991) ("Las circunstancias laborales habituales descritas sugieren su fiabilidad, […] al menos en la medida en que no hay absolutamente nada en el registro que implique en modo alguno la ausencia de la misma"). (Datos fiscales informatizados en posesión del I.R.S. (la Agencia Tributaria estadounidense)); Briscoe, 896 F.2d en 1494 (registros telefónicos informatizados en poder de Illinois Bell). Si el programa informático no se utiliza regularmente y el gobierno no puede establecer su fiabilidad basándose en la confianza depositada sobre él durante el desarrollo de una actividad comercial, puede que sea necesario que el gobierno revele "qué operaciones se le han encargado realizar al ordenador [así como] las instrucciones precisas que se le han dado", si así lo solicita la parte contraria. Estados Unidos v. Dioguardi, 428 F.2d 1033, 1038 (C.A.N.Y. 1970). Es importante destacar que una vez se haya establecido un mínimo de fiabilidad, las cuestiones referentes a la exactitud de los registros informáticos "derivadas de […] el funcionamiento del programa informático" solamente influyen sobre la importancia de las pruebas, no sobre su admisibilidad. Estados Unidos v. Catabran, 836 F.2d 453, 458 (9° Cir. 1988).

Los fiscales pueden subrayar el solapamiento conceptual entre la determinación de la autenticidad de un registro generado por ordenador y la determinación de la fiabilidad de un registro informático en cuanto a la excepción del registro comercial a la norma de la referencia. De hecho, con frecuencia los tribunales federales que analizan la autenticidad de registros generados por ordenador asumen que estos contienen elementos referenciales y posteriormente aplican la excepción de registros comerciales. Véase por ejemplo Salgado, 250 F.3d en 452-53 (en la que se aplica la excepción de registros comerciales a archivos telefónicos generados "automáticamente" por un ordenador) Estados Unidos v. Linn, 880 F.2d 209, 216 (9° Cir. 1989) (similar); Estados Unidos v. Vela, 673 F.2d 86, 89-90 (5° Cir. 1982) (similar). Como ya se ha comentado en este capítulo, este análisis es incorrecto en muchos casos desde el punto de vista técnico: los registros informáticos generados completamente por ordenadores no pueden contener elementos referenciales y no se pueden considerar susceptibles de la excepción de registros comerciales porque no incluyen "declaraciones" humanas. Véase el capítulo 5.C, más adelante. No obstante, en la práctica, la parte demandante que pone la base para considerar como comercial un registro generado por ordenador, también establecerá los fundamentos para determinar la autenticidad del mismo. La prueba de que un programa informático es lo bastante fiable como para que sus resultados se consideren registros comerciales de acuerdo con la Norma Federal sobre Pruebas 803(6) establece a su vez la autenticidad del registro. Cf. Estados Unidos v. Saputski, 496 F.2d 140, 142 (9° Cir. 1974).

3. Identificación del autor de registros almacenados en un ordenador

Mientras que un documento escrito a mano puede redactarse con estilos muy distintos de escritura, los archivos almacenados en un ordenador consisten en una larga serie de ceros y unos que no necesariamente identifican a su autor. Esto supone un problema especialmente en el ámbito de las comunicaciones por Internet, que ofrecen a sus autores un grado inusual de anonimato. Por ejemplo, las tecnologías de Internet permiten a los usuarios enviar correos electrónicos anónimos, mientras que los canales de chat interactivos permiten la comunicación entre usuarios sin revelar su nombre real. Cuando la parte demandante persigue la admisión de estos registros almacenados en un ordenador contra un demandado, éste puede poner en duda la autenticidad del registro cuestionando la identidad de su autor.

Por lo general, suelen ser pruebas circunstanciales las que ofrecen la clave para determinar la autoría y autenticidad de un registro informático. Por ejemplo, en Estados Unidos v. Simpson, 152 F.3d 1241 (10° Cir. 1998), los fiscales pretendían demostrar que el demandado había conversado con un agente secreto del FBI en un chat de Internet dedicado a la pornografía infantil. El gobierno facilitó una copia impresa de una conversación de chat por Internet entre el agente y un individuo identificado como "Stavron" e intentó demostrar que "Stavron" era el demandado. El tribunal de distrito admitió el impreso como prueba en el juicio. Tras declarársele culpable, Simpson recurrió aduciendo que "puesto que el gobierno no podía identificar que las afirmaciones a él atribuidas llevaran su escritura, su estilo al escribir o su voz", la copia no se había autenticado y debería haber quedado excluida. Id. en 1249.

El Décimo Circuito rechazó este argumento, destacando las significativas pruebas circunstanciales que demostraban que "Stavron" era el demandado. Véase id. en 1250. Por ejemplo, "Stavron" había comunicado al agente secreto que su nombre real era "B. Simpson", le indicó una dirección postal que coincidía con la de Simpson y aparentemente accedía a Internet desde una cuenta registrada a nombre de Simpson. Por otra parte, la policía halló registros en casa de Simpson en los que aparecía el nombre, la dirección y el número de teléfono que el agente secreto había enviado a "Stavron". Por consiguiente, el gobierno había proporcionado indicios suficientes para respaldar la conclusión de que el demandado era "Stavron" y la copia quedaba correctamente autentificada. Véase id. en 1250; véase también Estados Unidos v. Tank, 200 F.3d 627, 630-31 (9° Cir. 2000) (en el que se concluye que el tribunal de distrito actuó correctamente al admitir copias impresas de conversaciones de chat en situaciones similares a las del caso Simpson); Estados Unidos v. Siddiqui, 235 F.3d 1318, 1322-23 (11° Cir. 2000) (en el que se concluye que se había establecido la autenticidad de los mensajes de correo electrónico puesto que estos incluían la dirección de correo electrónico y el apodo del demandado y porque éste realizaba llamadas telefónicas después de enviar los mensajes). Sin embargo, véase Estados Unidos v. Jackson, 208 F.3d 633, 638 (7° Cir. 2000) (en el que se concluye que los comentarios publicados en Internet atribuidos a grupos defensores de la supremacía blanca quedaron correctamente excluidos por motivos de autenticidad al no haber pruebas de que fueran publicados por estos grupos); St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999) (en el que se concluye que las pruebas procedentes de una página web no se pudieron autenticar porque la información procedente de Internet es "inherentemente digna de poca fiabilidad").

[Índice]

C. Referencias

Los tribunales federales han asumido a menudo que todos los registros informáticos contienen referencias. Una perspectiva más matizada sugiere que esto sólo ocurre en una parte de los registros informáticos. Cuando un registro informático contiene las afirmaciones de una persona, procesadas o no por una persona, y se ofrece para probar la veracidad del asunto defendido, el registro puede contener referencias. En estos casos, el gobierno debe adecuar el registro a una excepción referencial, como la de registros comerciales, Norma Federal sobre Pruebas 803(6). Sin embargo, si un registro informático contiene únicamente datos generados por ordenador en los que no ha participado la mano humana, el registro no puede contener elementos referenciales. En estos casos, el gobierno debe demostrar la autenticidad del registro, pero no es necesario que establezca que es aplicable una excepción referencial a los registros para que sean admitidos en el juicio.

1. Inaplicabilidad de las normas sobre referencias a los registros generados por ordenador

La finalidad de las normas sobre referencias consiste en evitar que una declaración extrajudicial no fidedigna realizada por declarantes humanos pueda influir de manera inapropiada sobre el resultado de un juicio. Dado que las personas pueden malinterpretar o deformar sus experiencias, las normas sobre referencias muestran una gran preferencia por poner a prueba las afirmaciones humanas ante un tribunal, donde se puede situar al declarante en el estrado y someterle a un contrainterrogatorio. Véase Ohio v. Roberts, 448 U.S. 56, 62-66 (1980). Estos motivos no se aplican en el caso de afirmaciones de un animal o de una máquina, ya que no se puede someter a un contrainterrogatorio a una máquina que emita pitidos o a un perro que ladre. Las Normas Federales han adoptado esta lógica. Por definición, una afirmación no puede contener referencias si no es realizada por una persona. Véase Norma Federal sobre Pruebas 801(a) ("Una "declaración" es (1) una afirmación oral o escrita o (2) la conducta no verbal de una persona, si ésta pretende que sea entendida como tal"). (Se hace hincapié en este punto); Norma Federal sobre Pruebas 801(b) ("Un declarante es una persona que realiza una declaración"). (Se hace hincapié en este punto).

Como han destacado varios tribunales y estudiosos, esta limitación a las normas sobre referencia implica necesariamente que los registros generados por ordenador sin intervención humana no pueden

contener elementos referenciales. El tribunal supremo de un estado expresó la diferencia en un caso relacionado con el uso de registros telefónicos automáticos:

La impresión de los resultados de las operaciones internas del ordenador no es una prueba referencial. No representa los resultados de las declaraciones introducidas en el ordenador por declarantes extrajudiciales. Asimismo, tampoco podemos afirmar que esta impresión sea en sí misma una "declaración" que constituya una prueba referencial. Las razones subyacentes de la norma sobre referencias es que dichas declaraciones se realizan sin juramente y no se puede comprobar su veracidad mediante un contrainterrogatorio. Sí atañe al caso la posibilidad de que un testigo pueda tergiversar consciente o inconscientemente lo que el declarante le dijo o que el declarante pueda tergiversar consciente o inconscientemente un hecho o suceso. Sin embargo, con una máquina no existe la posibilidad de una tergiversación consciente, mientras que la posibilidad de generar datos imprecisos o que puedan inducir a error solamente se produce si la máquina no funciona correctamente.

State v. Armstead, 432 So.2d 837, 840 (La. 1983). Véase también People v. Holowko, 486 N.E.2d 877, 878-79 (Ill. 1985) (registros automáticos de control y rastreo); Estados Unidos v. Duncan, 30 M.J. 1284, 1287-89 (N-M.C.M.R. 1990) (registros informatizados de transacciones bancarias de ATM); 2 J. Strong, McCormick on Evidence § 294, en 286 (4ª ed.1992); Richard O. Lempert & Stephen A. Saltzburg, A Modern Approach to Evidence 370 (2ª ed. 1983). Cf. Estados Unidos v. Fernandez-Roque, 703 F.2d 808, 812 n.2 (5° Cir. 1983) (en el que se rechaza la objeción por referencias en cuanto a la admisión de registros telefónicos automáticos porque "el hecho de que estas llamadas se produjeron no es una declaración referencial"). Por consiguiente, un registro generado por ordenador cuya autenticidad se haya comprobado correctamente es admisible. Véase Lempert & Saltzburg, en 370.

La idea de que los registros generados por ordenador no pueden contener referencias es importante porque los tribunales que asumen la existencia de éstas pueden excluir por error pruebas generadas por ordenador si no se aplica la excepción por referencias. Por ejemplo, en Estados Unidos v. Blackburn, 992 F.2d 666 (7° Cir. 1993), un atracador de un banco se dejó sus gafas en un coche robado que abandonó. Entre las pruebas presentadas por la parte demandante contra el demandado se incluía una copia impresa de una máquina que comprueba la curvatura de las lentes de las gafas; ésta reveló que la graduación de las gafas halladas en el coche robado coincidía exactamente con la del demandado. En el juicio, el tribunal de distrito asumió que la copia informática era un elemento referencial, pero concluyó que se trataba de un registro comercial admisible conforme a la Norma Federal sobre Pruebas 803(6). Durante la apelación que siguió a la condena, el Séptimo Circuito también asumió que la copia incluía elementos referenciales, pero se mostró de acuerdo con el demandado en que no se podía admitir como registro comercial:

el informe [generado por ordenador] en este caso no se registró durante una actividad comercial habitual, sino que se preparó de forma específica a instancias del FBI y a sabiendas de que la información que proporcionara se utilizaría en una investigación criminal en curso. . . . Al hallar inadmisible este informe conforme a la Norma 803(6), observamos la norma establecida de que los documentos realizados en previsión de un litigio no son admisibles en virtud de la excepción de registros comerciales.

Id. en 670. Véase también la Norma Federal sobre Pruebas 803(6) (en la que se estipula que los registros comerciales deben ser "realizados o transmitidos por una persona").

Por fortuna, el tribunal de Blackburn corroboró en última instancia esta idea al concluir que la copia impresa era lo bastante fiable como para que se hubiera admitido en virtud de la excepción residual por referencias, Norma 803(24). Véase id. en 672. No obstante, el lugar de considerar la posibilidad de invertir la condena en vista de que la Norma 803(6) no era de aplicación, el tribunal debería haberse preguntado si la copia informática de la máquina de prueba de lentes contenía elementos referenciales. Esta pregunta habría revelado que la copia generada por ordenador no se podía excluir correctamente por motivos de referencia puesto que no contenía ninguna "declaración" humana.

2. Aplicabilidad de las normas sobre referencias a registros guardados en un ordenador

Los registros almacenados en equipos informáticos que contengan declaraciones humanas deben cumplir una excepción de la norma sobre referencias si se presentan para demostrar la veracidad de un asunto expuesto. Antes de que un tribunal admita los registros, éste debe determinar que las declaraciones incluidas en el mismo se realizaron en circunstancias que tienden a garantizar su fiabilidad. Véase por ejemplo Jackson, 208 F.3d en 637 (en el que se concluye que los comentarios publicados en páginas web pertenecientes a grupos defensores de la supremacía blanca contenían elementos referenciales y se rechaza el argumento de que los comentarios eran registros comerciales de los proveedores de servicios de Internet que albergaban las páginas).

Como se comenta en la introducción a este capítulo, los tribunales permiten normalmente admitir registros almacenados en un ordenador como registros comerciales de acuerdo con la Norma Federal sobre Pruebas 803(6). Los distintos circuitos han expresado perspectivas ligeramente diferentes con respecto a la admisibilidad de registros comerciales almacenados en un ordenador. Algunos tribunales se limitan a aplicar literalmente el texto de la Norma Federal sobre Pruebas 803(6), que aparece al principio de este capítulo. Véase por ejemplo Estados Unidos v. Moore, 923 F.2d 910, 914 (1° Cir. 1991); Estados Unidos v. Catabran, 836 F.2d 453, 457 (9° Cir. 1988). Otros circuitos han expresado pruebas doctrinales para registros informáticos que siguen en gran medida, aunque no exactamente, los requisitos de la Norma 803(6). Véase por ejemplo Estados Unidos v. Cestnik, 36 F.3d 904, 909-10 (10° Cir. 1994) ("Los registros comerciales informáticos son admisibles si (1) se mantienen conforme a un procedimiento habitual concebido para asegurar su exactitud, (2) se crean por motivos encaminados a garantizar la precisión (por ejemplo, sin incluir los que se preparan para un litigio) u (3) no son en sí mismo simples acumulaciones de referencias"). (Se cita Capital Marine Supply v. M/V Roland Thomas II, 719 F.2d 104, 106 (5° Cir. 1983)); Estados Unidos v. Briscoe, 896 F.2d 1476, 1494 (7° Cir. 1990) (los registros almacenados en un ordenador son registros comerciales admisibles si se "mantienen durante el desarrollo de una actividad comercial habitual y si es una práctica regular de dicha actividad mantener registros, lo que se demostrará mediante el testimonio del encargado u otro testigo competente"). (Se cita Estados Unidos v. Chappell, 698 F.2d 308, 311 (7° Cir. 1983)). Cabe destacar que la copia impresa propiamente dicha se puede realizar en previsión de un juicio sin infringir la excepción de registro comercial. El requisito de que el registro se mantenga "durante el desarrollo de una actividad comercial habitual" hace referencia a los datos subyacentes, no a la impresión en sí de los datos. Véase Estados Unidos v. Sanders, 749 F.2d 195, 198 (5° Cir. 1984).

Desde un punto de vista práctico, el procedimiento para admitir un registro almacenado en un ordenador con arreglo a la excepción de registros comerciales es similar al de cualquier otro registro comercial. Pensemos en un caso de acoso por correo electrónico. Con el fin de demostrar que el demandado fue la persona que envió los mensajes de acoso, la parte demandante puede querer que se introduzcan registros del proveedor de servicios de Internet del remitente que demuestren que el demandado era el propietario registrado de la cuenta desde la que se enviaron los correos. Por lo general, para ello es necesario que un empleado del PSI ("el encargado u otro testigo competente") testifique que el PSI mantiene de forma regular registros de las cuentas de clientes por motivos de facturación y otros fines, así como que los registros cuya admisión se va a solicitar son registros realizados en o cerca del momento de los hechos que describen durante el desarrollo normal de las actividades del PSI. Una vez más, la clave consiste en demostrar que el sistema informático desde el que se obtuvo el registro se mantiene durante el desarrollo normal de la actividad y que la empresa confía habitualmente en esos registros por su precisión.

La excepción del registro comercial es la excepción sobre referencias más común aplicada a registros informáticos. Lógicamente, existen otras excepciones sobre referencias que pueden ser aplicables en los casos adecuados, como la excepción de registros públicos de la Norma Federal sobre Pruebas 803(8). Véase por ejemplo Estados Unidos v. Smith, 973 F.2d 603, 605 (8° Cir. 1992) (copias impresas de ordenador de la policía); Hughes v. Estados Unidos, 953 F.2d 531, 540 (9° Cir. 1992) (copias informatizadas del IRS).

[índice]

D. Otras dificultades

El requisito de verificación de la autenticidad y la norma sobre referencias suelen ser los obstáculos más significativos con los que se toparán los fiscales al intentar que se admitan registros informáticos. No obstante, algunos agentes y fiscales han hecho referencia en ocasiones a dos dificultades adicionales: la aplicación de la norma de la mejor prueba a los registros informáticos y el hecho de si las copias informatizadas son "resúmenes" que deban cumplir con la Norma Federal sobre Pruebas 1006.

1. La norma de la mejor prueba

La norma de la mejor prueba establece que para probar el contenido de un escrito, grabación o fotografía, normalmente se exigirá el escrito, grabación o fotografía "original". Véase la Norma Federal sobre Pruebas 1002. En ocasiones, agentes y fiscales expresan su inquietud porque una simple impresión de un archivo electrónico guardado en un ordenador puede no ser un "original" en el sentido de la norma de la mejor prueba. Después de todo, el archivo original no es más que una serie de ceros y unos, mientras que la copia, por el contrario, es el resultado de manipular el archivo por medio de una serie de complicados procesos electrónicos y mecánicos.

Por fortuna, las Normas Federales sobre Pruebas han abordado expresamente este tema. Las Normas Federales estipulan que si los datos están guardados en un ordenador o dispositivo similar, toda copia o impresión legible a simple vista que refleje con exactitud los datos es un "original".

Norma Federal sobre Pruebas 1001(3). Por consiguiente, una copia precisa de datos informáticos cumple siempre la norma de la mejor prueba. Véase Doe v. Estados Unidos, 805 F. Supp. 1513, 1517 (D. Haw. 1992); véase también Laughner v. State, 769 N.E.2d 1147, 1159 (Ind. Tr. Ap. 2002) (en el que se concluye que los registros de mensajería instantánea de AOL que la policía había cortado y pegado en un archivo de procesamiento de textos satisface la norma de la mejor prueba). De acuerdo con las Notas del Comité Consultivo que acompañaron a esta norma cuando se propuso por primera vez, ésta se adoptó por razones de carácter práctico:

Si bien es cierto que se podría pensar que, en rigor, el original de una fotografía sólo puede ser el negativo, el sentido práctico y el uso común exigen que cualquier impresión del negativo se considere un original. De igual forma, el sentido práctico y el uso confieren la cualidad de original a cualquier copia informática impresa.

Notas del Comité Consultivo, propuesta de Norma Federal sobre Pruebas 1001(3) (1972).

2. Copias informáticas impresas consideradas "resúmenes"

La Norma Federal sobre Pruebas 1006 permite a las partes facilitar resúmenes cuando se trate de pruebas voluminosas en forma de "gráfica, resumen o cálculo", aunque con ciertas restricciones. Los agentes y fiscales se preguntan en ocasiones si una copia informática impresa es necesariamente un "resumen" de una prueba que deba observar la Norma Federal sobre Pruebas 1006. Generalmente, la respuesta es no. Véase Sanders, 749 F.2d en 199; Catabran, 836 F.2d en 456-57; Estados Unidos v. Russo, 480 F.2d 1228, 1240-41 (6° Cir. 1973). Lógicamente, si la copia informática impresa es simplemente un resumen de otras pruebas admisibles, la Norma 1006 se aplicará de la misma manera que a otros resúmenes de pruebas. Véase Estados Unidos v. Allen, 234 F.3d 1278, 2000 WL 1160830, en *1 (9° Cir. 11 de agosto de 2000) (sin publicar).

# # #

[Índice]

NOTAS FINALES

1. Técnicamente, la Ley de Privacidad de las Comunicaciones Electrónicas de 1986 enmendó el capítulo 119 del Título 18 del Código de Estados Unidos, codificado en 18 U.S.C. §§ 2510-22, y creó el capítulo 121 del Título 18, codificado en 18 U.S.C. §§ 2701-12. A consecuencia de ello, algunos tribunales y entendidos utilizan el término "ECPA" para hacer referencia de forma conjunta tanto a los §§ 2510-22 como a los §§ 2701-12. El presente manual adopta una convención más simple en aras de la claridad: los §§ 2510-22 se nombrarán por su denominación original, "Título III", (como Título III de la Ley General para el Control del Crimen y Seguridad en las Calles, aprobada en 1968), mientras que los §§ 2701-12 se hará referencia como "ECPA".

2. Tras observar pruebas de un delito almacenadas en un ordenador, es posible que los agentes tengan que confiscarlo de forma temporal para garantizar la integridad y la disponibilidad de las mismas antes de que puedan obtener una orden para registrar el contenido del ordenador. Véase por ejemplo Hall, 142 F.3d en 994-95; Estados Unidos v. Grosenheider, 200 F.3d 321, 330 n.10 (5° Cir. 2000). La Cuarta Enmienda permite a los agentes requisar un ordenador temporalmente siempre y cuando tengan causa probable para creer que contienen pruebas de un delito, que soliciten la orden con presteza y que la duración de la confiscación en ausencia de orden no sea "irrazonable" en función de la situación. Véase Estados Unidos v. Place, 462 U.S. 696, 701 (1983); Estados Unidos v. Martin, 157 F.3d 46, 54 (2° Cir. 1998); Estados Unidos v. Licata, 761 F.2d 537, 540-42 (9° Cir. 1985).

3. La autorización por parte de empleadores y compañeros de trabajo se comenta de forma individual en la sección de registros en el lugar de trabajo de este capítulo. Véase el capítulo 1.D.

4. Como es natural, los agentes que ejecuten un registro de conformidad con una orden válida o una excepción al requisito de la orden no necesitan acogerse a la doctrina de simple vista para justificar el registro. La propia orden o excepción lo justifica. Véase el capítulo 2.D, "Registro de ordenadores que ya estén bajo la custodia de las fuerzas de seguridad".

5. Entre los actuales miembros se incluyen Australia, Austria, Bielorrusia, Brasil, Canadá, Dinamarca, Finlandia, Francia, Alemania, India, Indonesia, Israel, Italia, Japón, la República de Corea, Luxemburgo, Malasia, Marruecos, Países Bajos, Noruega, Filipinas, Rumania, Rusia, España, Suecia, Tailandia, Reino Unido y Estados Unidos.

6. Crear una copia duplicada de una unidad entera (lo que a menudo se conoce simplemente como crear una imagen) no es lo mismo que realizar una copia electrónica de archivos individuales. Al guardar un archivo en un disco de almacenamiento, se guarda en sectores separados aleatoriamente en el disco, en lugar de en bloques contiguos y unidos. Cuando se recupera el archivo, las piezas separadas se vuelven a combinar a partir del disco en la memoria del ordenador y se presentan como un único archivo. Realizar una imagen del disco copia el disco completo tal y como está, incluyendo las piezas desperdigadas de los distintos archivos, así como otros datos, como pueden ser fragmentos de documentos eliminados. La imagen permite a un especialista informático recrear (o montar) el disco de almacenamiento completo y obtener una copia idéntica al original. Por el contrario, una copia archivo por archivo (también llamadas "copia lógica de archivos") simplemente crea una copia de un documento individual ensamblando y copiando los sectores sueltos de datos asociados con el archivo en cuestión.

7. Estas diferencias pueden ser relevantes en relación con la confiscación de bienes. Las propiedades que se hayan utilizado para cometer o promover un delito relacionado con material obsceno se pueden requisar de forma penal en virtud del 18 U.S.C. § 1467. Las propiedades utilizadas para cometer o promover delitos relacionados con la pornografía infantil se pueden requisar de forma penal en virtud del 18 U.S.C. § 2253 y civil conforme al 18 U.S.C. § 2254. Los agentes y fiscales pueden ponerse en contacto con la Sección de Confiscación de Bienes y Blanqueo de Dinero a través del número de teléfono (202) 514-1263 si precisan asistencia.

8. El juicio de Steve Jackson Games planteó muchas cuestiones importantes con respecto a la PPA y a la ECPA ante el tribunal de distrito. Durante la apelación, no obstante, el único asunto que se planteó fue "uno muy limitado: el hecho de si la confiscación de un ordenador en el cual haya almacenados correos electrónicos enviados a un tablón de anuncios electrónico, pero aún sin leer (recuperar) por parte de los receptores, constituye una "interceptación" prohibida conforme al 18 U.S.C. § 2511(1)(a)". Steve Jackson Games, 36 F.3d en 460. Este asunto se comenta en el capítulo dedicado a la vigilancia electrónico. Véase el capítulo 4, más adelante.

9. Esto plantea una diferencia fundamental que se pasó por alto en el caso Steve Jackson Games: la diferencia entre una orden de registro conforme a la Norma 41 que autorice a las fuerzas de seguridad a ejecutar una inspección y una orden de registro conforme a la ECPA que fuerce a un proveedor de servicios de comunicaciones electrónicas o servicios informáticos remotos a revelar a la policía el contenido de la cuenta de red de un abonado. A pesar de que las dos se denominan "órdenes de registro", en la práctica son muy diferentes. Las órdenes de registro conforme a la ECPA exigidas en virtud del 18 U.S.C. § 2703(a) son mandamientos judiciales que se entregan de una forma muy similar a las citaciones: normalmente, los investigadores trasladan la orden al proveedor, quien se encarga de transmitirles la información que en ella se describe en un plazo determinado de tiempo. Por el contrario, las órdenes de registro normales conforme a la Norma 41 suelen autorizar a los agentes a entrar en una propiedad privada, buscar y confiscar las pruebas descritas en la misma. Compárese el capítulo 2, en el que se comenta un registro y confiscación conforme a la Norma 41, con el capítulo 3, en el que se habla de las pruebas electrónicas que se pueden obtener en virtud de la ECPA. Esta diferencia cobra una relevancia especial cuando un tribunal decide que se ha infringido la ECPA y ha de determinar el remedio. Teniendo en cuenta que el requisito de la orden del 18 U.S.C. § 2703(a) es sólo una norma legal, una infracción no constitucional del § 2703(a) no debería dar como resultado la anulación de las pruebas obtenidas. Véase el capítulo 3.H (en el que se comentan los remedios para infracciones de la ECPA).

10. A este respecto, las órdenes de registro conforme a la Norma 41 son distintas a las órdenes de registro federales conforme a la ECPA sujetas al 18 U.S.C. § 2703(a), que se pueden entregar fuera del distrito en que se emitan. Véase el capítulo 3.D.5, más adelante.

11. Centrarse en los ordenadores en lugar de en la información puede tener como consecuencia que la orden sea demasiado limitada. Si la información relevante está en papel o formato fotográfico, es posible que los agentes no tengan autoridad para confiscarla.

12. Un número inusitado de resoluciones de registros informáticos y confiscaciones está relacionado con la pornografía infantil. Esto ocurre por dos razones. La primera de ellas es que las redes informáticas suponen un medio muy sencillo de poseer y transmitir imágenes de contrabando de pornografía infantil. En segundo lugar, el hecho de que la posesión de pornografía infantil transmitida a través de fronteras estatales sea un delito suele dejar al demandado sin otra salida que recurrir el procedimiento por el cual las fuerzas de seguridad obtuvieron las imágenes de contrabando. Los investigadores y fiscales deben ponerse en contacto con la Sección de Explotación y Obscenidad Infantil a través del número de teléfono (202) 514-5780 o con un Abogado Asistente de Estados Unidos designado como Coordinador contra la Explotación y Obscenidad Infantil si necesitan asesoramiento y ayuda en casos e investigaciones relacionados con la explotación de niños.

13. Naturalmente, el hecho de que los agentes puedan retener legalmente equipos durante un periodo amplio de tiempo no les impide aceptar solicitudes del consejo de la defensa para la devolución de los equipos y archivos requisados. En algunos casos los agentes han ofrecido a los sospechosos copias electrónicas de archivos inocentes con valor económico o personal que estaban guardados en los ordenadores confiscados. Si los sospechosos pueden demostrar la necesidad legítima de acceder a los archivos o equipos requisados y los agentes pueden acceder a su petición sin poner en peligro la investigación ni hacer que el gobierno incurra en costes prohibitivos, estos deberán considerar la posibilidad de ofrecer su asistencia por cortesía.

14. Esto es así por dos razones. Primeramente, los titulares de una cuenta no pueden tener una "expectativa razonable de privacidad" sobre la información enviada a los proveedores de red puesto que

el envío de la información puede constituir una revelación con arreglo a los principios del caso Estados Unidos v. Miller, 425 U.S. 435, 440-43 (1976) (en el que se concluye que los registros bancarios son información revelada y, por tanto, no están sujetos a la protección de la Cuarta Enmienda) y Smith v. Maryland, 442 U.S. 735, 741-46 (1979) (no se halla expectativa razonable de privacidad en los números de teléfono marcados). Véase el capítulo 1.B.3 ("Expectativa razonable de privacidad y posesión de terceras partes"). En segundo lugar, la Cuarta Enmienda permite por lo general al gobierno emitir una citación por la que ordene la revelación de información y propiedad aunque ésta esté protegida por una "expectativa razonable de privacidad" conforme a la Cuarta Enmienda. Si el gobierno no lleva cabo el registro en busca de pruebas, sino que obtiene simplemente una orden judicial que exija al receptor de la misma que entregue las pruebas al gobierno en un plazo de tiempo determinado, la orden cumple con la Cuarta Enmienda en tanto en cuanto no sea demasiado general, persiga la información relevante y se entregue de una forma legal. Véase Estados Unidos v. Dionisio, 410 U.S. 1, 7-12 (1973); In re Horowitz, 482 F.2d 72, 75-80 (2° Cir. 1973) (Friendly, J.). Este análisis también es aplicable cuando un sospechoso haya almacenado materiales de forma remota con una tercera parte y el gobierno entrega la citación a la tercera parte. Los casos indican que siempre y cuando la tercera parte tenga en su poder los materiales en cuestión, el gobierno puede emitir una citación para que ésta los entregue sin necesidad de obtener primero una orden sobre causa probable, incluso en el caso de que sea necesaria una orden para ejecutar directamente un registro. Véase Estados Unidos v. Barr, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (citación entregada a un servicio privado de correo de una tercera parte ordenando la revelación del correo no entregado del demandado en posesión de la tercera parte); Estados Unidos v. Schwimmer, 232 F.2d 855, 861-63 (8° Cir. 1956) (citación entregada a una instalación de almacenamiento de una tercera parte ordenando la entrega de los documentos privados del demandado en poder de la tercera parte); Newfield v. Ryan, 91 F.2d 700, 702-05 (5° Cir. 1937) (citación entregada a una compañía de telégrafos ordenando la entrega de copias de los telegramas del demandado en poder de la compañía).

15. La inclusión de comunicaciones por cable en esta categoría, como el correo de voz, hecha efectiva con la Ley PATRIOT, expirará el 31 de diciembre de 2005, a menos que el Congreso la prorrogue. Véase Ley PATRIOT §§ 209, 224, 115 Stat. 272, 283, 295 (2001).

16. El gobierno puede extender la demora de aviso durante plazos adicionales de 90 días si así se solicita ante un tribunal. Véase 18 U.S.C. § 2705(a)(4).

17. A menos que el Congreso la prorrogue, la definición que aparece en la Ley PATRIOT de "tribunal con jurisdicción competente" en el 18 U.S.C. §§ 2711(3) expirará el 31 de diciembre de 2005, y la referencia del § 2703(d) a un "tribunal con jurisdicción competente volverá a remitir directamente al § 3127(2)(A). Véase Ley PATRIOT §§ 220, 224, 115 Stat. 272, 291-92, 295 (2001).

18. La inclusión de comunicaciones por cable en esta categoría, como el correo de voz, expirará el 31 de diciembre de 2005, a menos que el Congreso la prorrogue. Véase Ley PATRIOT §§ 209, 224, 115 Stat. 272, 283, 295 (2001).

19. La inclusión de comunicaciones por cable en esta categoría, como el correo de voz, expirará el 31 de diciembre de 2005, a menos que el Congreso la prorrogue. Véase Ley PATRIOT §§ 209, 224, 115 Stat. 272, 283, 295 (2001).

20. La enmienda a la ECPA que contempla órdenes de registro fuera del distrito expirará el 31 de diciembre de 2005, a menos que el Congreso la prorrogue. Véase Ley PATRIOT §§ 220, 224, 115 Stat. 272, 291-92, 295 (2001).

21. Incluso un proveedor público puede revelar libremente registros de un cliente que no incluyan el contenido a cualquier persona que no guarde relación con un organismo gubernamental. Véase 18 U.S.C. §§ 2702(a)(3), (c)(5).

22. Las disposiciones de revelación por emergencia que figuran en el § 2702(b)(6)(C) y § 2702(c) se añadieron a la Ley PATRIOT. Asimismo, la Ley PATRIOT simplificó el tratamiento de las revelaciones voluntarias de registros sin contenido por parte de proveedores (al pasar todas estas

disposiciones del § 2703(c) al § 2702) y al aclarar que los proveedores de servicios tienen autoridad para revelar registros que no incluyan contenidos en aras de proteger sus derechos y propiedades. Todos estos cambios expirarán el 31 de diciembre de 2005, a menos que el Congreso los prorrogue. Véase Ley PATRIOT §§ 212, 224, 115 Stat. 272, 284-85, 295 (2001).

23. A este respecto, al igual que en otros, la ECPA refleja la Ley del Derecho a la Privacidad Económica, 12 U.S.C. § 3401 et seq. ("RFPA"). Véase Organización JD Ltda. v. Departamento de Justicia de Estados Unidos , 124 F.3d 354, 360 (2° Cir. 1997) (en el que se destaca que el "Congreso redactó […] la ECPA después de la RFPA" y en la que se recurre a la RFPA para orientarse sobre cómo interpretar "cliente y abonado" según se utilizan en la ECPA); Tucker v. Waddell, 83 F.3d 688, 692 (4° Cir.1996) (en el que se analiza la RFPA para interpretar la ECPA). Los tribunales han rechazado unánimemente la interpretación de un remedio de anulación legal en la disposición análoga de la RFPA. Véase Estados Unidos v. Kington, 801 F.2d 733, 737 (5° Cir. 1986); Estados Unidos v. Frazin, 780 F.2d 1461, 1466 (9° Cir.1986) ("Si el Congreso hubiera pretendido autorizar un remedio de anulación [para infracciones de la RFPA], seguramente lo habría incluido entre los remedios autorizados expresamente").

24. Por ejemplo, la opinión incluye varias afirmaciones sobre los requisitos de la ECPA que no son coherentes entre sí y que son incorrectas por separado. En un momento dado, la opinión establece que la ECPA exigía a la marina que o bien obtuviera una orden de registros que forzara a AOL a revelar la identidad de McVeigh, o bien que diera aviso previo a McVeigh y que posteriormente utilizara una citación o una orden judicial conforme al § 2703(d). Véase 983 F. Supp. en 219. En la siguiente página la opinión determina que la marina debía recibir una "orden o similar" para obtener el nombre de McVeigh de AOL. Véase id. en 220. No obstante, en virtud del antiguo 18 U.S.C. § 2703(c)(1)(C), la marina podría haber obtenido el nombre de McVeigh legalmente con una citación de la cual no tenía que dar aviso a McVeigh.

25. El Noveno Circuito amplió temporalmente el alcance del término "interceptaciones" a las comunicaciones electrónicas almacenadas en un caso civil per se, Konop v. Hawaiian Airlines, 236 F.3d. 1305 (9° Cir. 2001). En el caso Konop, el tribunal rechazó el razonamiento de Smith y la distinción legal anterior a la Ley PATRIOT entre comunicaciones por cable y electrónicas, para concluir que no tendría sentido tratar de forma diferente las comunicaciones por cable y las electrónicas. Id. en 1046. Por consiguiente, el tribunal sentenció que obtener una copia de una comunicación electrónica en "almacenamiento electrónico" puede constituir una interceptación de la comunicación. Véase id. Posteriormente, en cambio, el tribunal retiró esta opinión. Véase Konop v. Hawaiian Airlines, 262 F.3d. 972 (9° Cir. 2001).

26. El "uso" y "revelación" prohibidos no entran dentro del ámbito de este manual.

27. Las leyes estatales sobre vigilancia pueden diferir. Algunos estados prohíben la interceptación de comunicaciones a menos que todas las partes la autoricen.

28. La última cláusula del § 2511(2)(a)(i), que prohíbe a las compañías telefónicas públicas llevar a cabo "observaciones del servicio y supervisiones aleatorias" que no guarden relación con el control de calidad, limita las supervisiones aleatorias por parte de compañías telefónicas a interceptaciones diseñadas para garantizar que el equipo de la compañía esté en buen estado de funcionamiento. Véase James G. Carr, The Law of Electronic Surveillance *(La ley de vigilancia electrónica)*, § 3.3(f), en 3-75. Esta cláusula no es aplicable a las transmisiones de red informáticas que no sean de voz.

29. A diferencia de otras excepciones al Título III, la excepción de la extensión telefónica es una restricción desde el punto de vista técnico a la definición legal de "interceptar". Véase 18 U.S.C. § 2510(4)-(5). Sin embargo, la disposición actúa de la misma manera que otras excepciones al control del Título III que autorizan la interceptación en determinadas circunstancias.

[Índice]