Seguridad

Cuaderno Red de Cátedras Telefónica

Universidad de Salamanca

EL CONTROL DEL CIBERESPACIO POR PARTE DE GOBIERNOS Y EMPRESAS

Cátedra Telefónica de la Universidad de Salamanca

Miguel Ángel Castellano Osuna , Pedro David Santamaría Hernández

No. 9. Diciembre de 2012. Número extraordinario

Actualizado enero de 2013

www.catedras.telefonica.es
http://catedraseguridad.usal.es

Cuaderno Red de Cátedras Telefónica

El control del ciberespacio por parte de gobiernos y empresas

Cátedra de Seguridad Universidad de Salamanca

Dirección y Coordinación:

Prof. Dr. D. Fernando Pérez Álvarez, Profesor titular Derecho Penal. Director Ciencias de la Seguridad (CISE).

Profa. Dra. Dña. Angélica González Arrieta, Profesora titular Ciencias de la Computación e Inteligencia artificial.

Profa. Dra. Dña. Lina Mariola Díaz Cortés. Profesora Ciencias de la Seguridad (CISE).

Coordinación:

Dña. María Teresa Heredero Campo. Doctoranda Derecho Civil, Universidad de Salamanca.

Despacho:

291 Facultad de Derecho, Campus Miguel de Unamuno.

Teléfono:

923294400 Ext. 1622

Correo electrónico:

catedratelefonica@usal.es

CISE

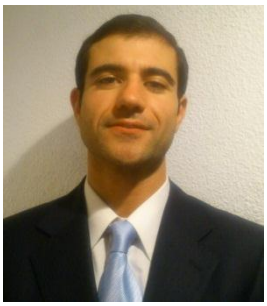
VNiVERSiDAD D SALAMANCA

Miguel Ángel Castellano Osuna

Funcionario del Ministerio del Interior, ocupa en la actualidad un puesto de Profesor Titular en el Centro de Altos Estudios Policiales. Anteriormente, era Técnico Especialista del Área de Telecomunicaciones de la Dirección General de la Policía, en la cual llevó proyectos de investigación y desarrollo, auditorías de sistema y seguridad, y colaboración en reuniones internacionales del área.

Realizó estudios de Licenciatura en Tecnologías de Internet (una especialidad de las Telecomunicaciones) en la Universidad de Portsmouth, Inglaterra, tras lo cual obtuvo una plaza de Investigador Titular en la misma, reuniendo fondos para su proyecto investigador en Inteligencia Artificial al obtener una beca estatal. Ha impartido labores docentes universitarias, cursos tanto oficiales como privados y diversas ponencias en conferencias inglesas y de la Universidad de Salamanca. Realizó tareas de representación en el ámbito universitario y profesional. Colabora en el desarrollo de un satélite de la constelación 'HumSAT' auspiciado por la Agencia Espacial Europea (ESA).

Su actividad investigadora se centra en la inteligencia artificial, programación, redes e internet.



Pedro David Santamaría Hernández

Funcionario del Ministerio del Interior, Profesor Titular en el Centro de Altos Estudios Policiales. Anteriormente, con plaza de Técnico Especialista del Área de Telecomunicaciones de la Dirección General de la Policía, desempeñando funciones de investigador. Obtuvo la titulación de Técnico Superior de Telecomunicaciones e Informática y finaliza sus estudios de Grado en Ingeniería Telemática por la Universidad de Alcalá. Su actividad profesional se ha desarrollado en multinacionales de telecomunicaciones como MediaPro, France Telecom, Hewlett-Packard y Vodafone, desempeñando en las mismas distintos puestos técnicos en las ramas de ingeniería de redes hasta su ingreso en el Ministerio del Interior. En su tarea investigadora, durante su formación cursó estudios de Seguridad IT en el Copenhagen University College of Engineering, y colabora en el proyecto de la constelación de satélites HumSAT de la Agencia Espacial Europea (ESA) desarrollando el módulo de comunicaciones de uno de los satélites cuyo lanzamiento está previsto para verano de 2014. Recientemente ha impartido Conferencias en la Universidad de Salamanca en un seminario organizado por el CISE.

Índice

1. INTRODUCCIÓN 8
2. DESARROLLO DE LA NORMATIVA APLICABLE 12
3. ORGANISMOS E INSTITUCIONES INVOLUCRADAS. 16
4. LA INTERCEPTACIÓN ILEGAL DE COMUNICACIONES POR PARTE DE GOBIERNOS 18
5. LA INTERCEPTACIÓN ILEGAL DE COMUNICACIONES POR PARTE DE CORPORACIONES 21
5.1 El espionaje competitivo y económico. 21
5.2 Corporaciones que registran datos personales de usuarios. 24
5.3 Proveedores de servicios de búsqueda en Internet. 24
5.4 Proveedores de acceso a Internet o telefonía. 25
6. TÉCNICAS UTILIZADAS PARA EL CONTROL DEL CIBERESPACIO Y LA INTERCEPTACIÓN DE LAS COMUNICACIONES. 26
6.1 Sistemas globales de interceptación: Echelon. 26
6.2 Sistemas personales de interceptación: Troyanos. 29
6.3 Datos registrados en memorias informáticas. 30
6.4 Comunicaciones y datos registrados en la red. 30
7. NUEVAS TÉCNICAS. EL CASO DEL RECONOCIMIENTO FACIAL 34
8. REFLEXIONES FINALES 38
9. BIBLIOGRAFÍA 40

ISSN: 2174-7628

Abreviaturas

- ACTA : Acuerdo Comercial Anti-Falsificación. Acuerdo multilateral (internacional) de adhesión voluntaria.
- ART : Artículo. Cada una de las partes en que se divide un escrito, tratado o ley.
- CE : Constitución Española, o Carta Magna. Norma suprema del ordenamiento jurídico.
- CEDH : Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.
- CP: Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, y sus posteriores modificaciones. Recoge la mayor parte de las normas jurídicas punitivas.
- ETSI : "European Telecommunications Standards Institute" o "Instituto Europeo de Estándares en Telecomunicaciones".
- GPS : "Global Positioning System" o "Sistema de Posicionamiento Global". Sistema de navegación que provee la posición terrestre basándose en un sistema de satélites.
- ILETS : "International Law Enforcement Telecommunications Seminar" o "Seminario Internacional de Telecomunicaciones en Fuerzas y Cuerpos de Seguridad".
- ISP : Proveedor de Acceso a Internet. Compañía que da acceso a la red.
- LCD : Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- LECrim : Ley de Enjuiciamiento Criminal, Real Decreto de 14 de septiembre de 1882, y sus posteriores modificaciones. Regula los procedimientos legales.
- LES : Ley 2/2011 de Economía Sostenible.
- LGT : Ley 32/2003 General de Telecomunicaciones.
- LOPD : Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

- NSA : “National Security Agency” o “Agencia Nacional de Seguridad”. Agencia de inteligencia estadounidense responsable de obtener y analizar todas las comunicaciones y señales, así como proteger las gubernamentales, y realizar funciones de criptoanálisis.
- PIPA : “Protect IP Act”. Proyecto de Ley en EE.UU.
- SOPA : “Stop Online Piracy Act”. Proyecto de Ley en EE.UU.
- STC : Sentencia del Tribunal Constitucional.
- STS : Sentencia del Tribunal Supremo.
- TC : Tribunal Constitucional. Máximo órgano judicial en materia constitucional.
- TEDH : Tribunal Europeo de Derechos Humanos.
- TS : Tribunal Supremo. Máximo órgano judicial, junto con el Tribunal Constitucional.
- UKUSA : “United Kingdom-United States Security Agreement” o “Acuerdo de Seguridad entre Reino Unido y Estados Unidos”. Anteriormente denominado “BRUSA”, es un acuerdo de cooperación e intercambio de inteligencia de señales entre los firmantes: Reino Unido, Estados Unidos, Canadá, Australia y Nueva Zelanda.

Resumen

En un mundo globalizado, en el cual las comunicaciones, internet y los sistemas de almacenamiento y proceso de información han adquirido gran relevancia, transmitiendo y guardando información de la esfera más privada de individuos y corporaciones, el control de los mismos los convierte en una eficaz y potente herramienta por parte de gobiernos y corporaciones, que resulta muy peligrosa si se hace un uso pernicioso de la misma, conllevando una exposición y pérdida de libertades individuales en este caso intolerable.

Palabras clave

Control, interceptación, retención, espionaje, internet, ciberespacio, telefonía, comunicaciones, datos, información, inteligencia, huella digital, intimidad, privacidad y Echelon.

Abstract

In a world that is globalized, where communications, internet and information storage and processing systems acquired great importance, transmitting and saving information of the private sphere of individuals and corporations, the control of the aforementioned systems results in an efficient and powerful tool for governments and corporations, which proves to be very dangerous if harmful use of such tools happens, and involves an unacceptable exposure and loss of the individual liberties where this is the case.

Key - words

Control, interception, retention, espionage, internet, cyberspace, telephony, communications, data, information, intelligence, digital fingerprint, privacy and Echelon.

1. Introducción

El progresivo uso masivo de Internet y servicios de telefonía por ciudadanos y empresas y el acceso y uso masivo de estas de redes para distintos y variados fines, como el comercio electrónico, las redes sociales e incluso los aspectos más íntimos de la vida de una persona, están convirtiendo a estos servicios en el medio más eficaz para controlar y vigilar a los usuarios por parte de gobiernos y corporaciones, siendo dichos usuarios inconscientes de la exposición a la que están sometidos y de la consecuente pérdida de sus libertades individuales.

El fin último esgrimido por parte de gobiernos, agencias de seguridad y distintas corporaciones va desde recopilar los datos necesarios para su correcto funcionamiento a garantizar la seguridad mundial, pero existe la gran tentación de que tal cúmulo de información se use con el pernicioso fin de ejercer el control sobre multitud de aspectos de la vida de dichos usuarios.

Con este documento se pretende concienciar a los usuarios de sistemas de comunicaciones de los riesgos existentes en su control por parte de gobiernos o corporaciones, realizando un estudio de las tecnologías empleadas para tal fin, las empresas que obtienen beneficios de dichas actividades y las leyes y tratados cuyo desarrollo está dirigido a protegernos de semejante observación de la 'huella digital'[1] que dejamos.

Antes de exponer en profundidad el tema, y debido a la heterogeneidad del nivel de conocimientos técnicos y jurídicos de aquéllos a los que está destinada esta publicación, se hace conveniente una adecuada introducción que establezca las raíces del mismo y muestren su importancia, la diferenciación entre interceptación legal e ilegal de las comunicaciones, núcleo principal del control del ciberespacio existente, los conocimientos básicos y mecanismos judiciales que rigen dicha interceptación legal y lo más polémico, los casos en que se producen por parte de gobiernos o corporaciones interceptación ilegal de las telecomunicaciones.

Cualquier ciudadano de un país democrático que tenga inquietudes en la materia, al contemplar noticias relacionadas con ésta, o esfuerzos legislativos de sus gobernantes en relación con la interceptación legal

[1] Por 'huella digital' se pretende hacer una analogía a los múltiples vestigios -registros- que se dejan en soportes informáticos al usar tecnología o comunicaciones, como son los datos y contenido de la comunicación establecida.

de las comunicaciones o incluso casos en que pueda existir una interceptación ilegal de las mismas, se puede plantear entre otras las siguientes dudas, cuya resolución es el objetivo primordial de este documento:

- ¿Es el control de las telecomunicaciones y el ciberespacio tan importante?
- ¿Cuál es el motivo de que los gobiernos actuales legislen, con tanto celo, todo lo relativo a la interceptación legal de las comunicaciones?
- ¿Se podrían utilizar, de forma arbitraria, dichos mecanismos legales, saltándose el control existente sobre ellos y conculcando mi derecho a la intimidad?
- ¿Supone dicho control una merma grave a mi intimidad y las garantías constitucionales que la amparan?
- ¿Se encuentran equilibradas las herramientas legislativas de control de las Fuerzas y Cuerpos de Seguridad necesarias para la investigación de delitos graves, con el mencionado derecho a la intimidad?
- Dejando a un lado los casos recogidos por ley, ¿existe la posibilidad de una interceptación ilegal, incluso indiscriminada, de las comunicaciones por parte de servicios de inteligencia o agencias gubernamentales? Y en el caso de que se realice con fines loables, ¿dicho fin justifica los medios? En nuestra opinión, la última cuestión es la más relevante y polémica del tema.

La importancia del -discutible- control del ciberespacio y las comunicaciones es fácil de vislumbrar. En un mundo globalizado, en el cual las telecomunicaciones y los sistemas de almacenamiento y proceso de información (ordenadores personales, tablets y teléfonos móviles inteligentes entre otros) adquieren cada día mayor relevancia, es de esperar que éstos hayan terminado convirtiéndose en elementos indispensables para el trabajo o la vida cotidiana. Dichos sistemas almacenan, procesan y/o transmiten datos personales de millones de usuarios, tan personales o sensibles que llegan a la esfera más íntima de la persona o los secretos mejor guardados de una empresa.

Desde esta perspectiva, es razonable pensar que un control sobre estos sistemas suponga un grave atentado a los derechos a la intimidad personal. Sin embargo, como en cualquier herramienta de este

mundo nos encontramos con un arma de doble filo: su uso para cometer delitos graves comenzó y ha ido creciendo en igual medida que se han vuelto indispensables en labores cotidianas. Y con los agravantes añadidos del anonimato -impunidad- que pueden ofrecer, su fácil acceso por la población y la velocidad y facilidad de proceso que han adquirido. Esto último hace necesario una mayor reflexión sobre dónde se encuentra el fiel de la balanza entre la intimidad y el control racional de un medio delictivo en potencia.

La madurez técnica adquirida por la electrónica actual permite diseños -incluso versiones miniaturizadas como las producidas para terminales móviles- con capacidad de proceso similar que un superordenador de los 70. Como ejemplo, el "Cray-1", considerado el primer supercomputador "moderno", que requería ser instalado en una amplia sala y con un coste de 700.000 dólares de la época[2], tenía una capacidad de cómputo global de 100 Mflop/s[3]. Un Ipad, en su tercera generación, arroja datos de 200 a 400 Mflop/s según la prueba realizada, duplicando al menos el rendimiento del "Cray-1". Esto, junto con la producción en masa y la competitividad actual del sector facilitan como se indicó el acceso a la población general.

Otro ejemplo más reciente y que acaparó la prensa mundial es el supercomputador de IBM "Deep Blue", que venció en 1997 a Gary Kaspárov, campeón del mundo de ajedrez vigente en la fecha. Esta máquina alcanzó una capacidad de cómputo de 11,38 Gflop/s[4].En comparación, un ordenador portátil actual de gama baja-media, como los que usan procesadores 'Intel® Core i3 3120M', ronda los 40 Gflop/s.

Debido a los avances anteriores, y a la interconexión de estos equipos en redes -ya sean informáticas o telefónicas, aunque cada vez se hace más estrecha esta división- la velocidad de proceso ha llegado a cotas tales de poder realizar casi cualquier transacción instantánea de información entre continentes. La facilidad de su uso ha requerido de una continua mejora de las interfaces de usuario[5] actuales: inicialmente estaban dedicadas a personal muy especializado, por lo que su complejidad técnica no suponía problema, pasando a ser diseñadas para su uso por usuarios con conocimientos medios/bajos, convirtiéndose en intuitivas y gráficas.

[2]Según las tablas de IPC del gobierno de EE.UU. provistas por el 'Bureau of Labor Statistics' (http://www.bls.gov) para calcular la inflación, 700.000 dólares del año 1975 equivaldrían a unos 3 millones de dólares en la actualidad.
[3] 'Mflop/s' es una unidad comúnmente utilizada para medir la capacidad de cómputo -cálculo- de un ordenador. En palabras sencillas, a mayor valor más rendimiento. Aquí se utiliza simplemente como comparador, sin pretender que se comprenda su valor de forma aislada. Técnicamente, consiste en el número de millones de operaciones de coma flotante por segundo -cálculos aritméticos simples usando números reales, como son sumas y multiplicaciones-.
[4] 'Gflop/s' equivale a 1.000 Mflop/s, es decir, mil millones de operaciones de coma flotante por segundo.
[5] 'Interfaz' es el conjunto de métodos que permiten comunicar a usuario y máquina, como son los menús e iconos.

Y si lo anterior no resulta suficientemente atractivo para la delincuencia actual, el -en muchos casos aparente- anonimato que permiten ayuda enormemente a la impunidad de los mismos: ficheros informáticos con datos confidenciales pueden ser encriptados[6], así como conversaciones y transmisiones, dificultando la investigación y evitando su uso como prueba; hay una absoluta falta de control del registro de la identidad personal en e-mail, foros o chats, que se pueden utilizar sin indicar nuestra identidad real, o falseando ésta al registrarse en el sistema; y la masiva utilización de éstos, generando miles de millones de datos guardados y transacciones realizadas cada día que hacen pensar al delincuente lo realmente difícil que es encontrar lo que éste oculta.

Llegados a este punto, se debe establecer la distinción entre los conceptos de interceptación legal e ilegal de las comunicaciones. Con respecto a la primera, la **interceptación legal**, España es un país legislativamente garantista, en el cual los ciudadanos disponen de múltiples garantías para salvaguardar sus derechos y en el que nadie duda en alzar la voz para hacer efectivos los mismos. Por otra parte, es evidente que dichas garantías deben equipararse con obligaciones y deberes justos para salvaguardar garantías de otros, razón inicial esgrimida por los gobiernos de que exista dicha interceptación de las comunicaciones. Finalmente, se presupone legal ya que su concepto y mecanismos están delimitados en nuestro ordenamiento jurídico (ver punto 2), siguiendo el principio de proporcionalidad, y con el fin último de la prevención, averiguación o esclarecimiento de delitos.

Con respecto a la segunda, la **interceptación ilegal**, lo compone cualquier interceptación de las comunicaciones que se salga del concepto y mecanismos legales y judiciales establecidos, por las razones que sean. Éstos van desde el soporte a una actividad puramente ilegal, ya sea una organización criminal o un delincuente; pasando por el soporte a una actividad supuestamente legal, obteniendo información privilegiada que aumente el éxito de dicha actividad, hasta la persecución de delitos especialmente graves por parte de gobiernos, aumentando su efectividad al obtener una gran flexibilidad de actuación saltándose dichos mecanismos. Más adelante se mostrarán casos en los que algunos gobiernos democráticos han realizado y realizan esta conducta.

[6] La encriptación es una técnica utilizada para convertir información confidencial en datos ilegibles por terceros.

2. Desarrollo de la normativa aplicable

Este apartado pretende exponer la normativa considerada pertinente al control de las comunicaciones, ya sea contenida en el ordenamiento jurídico[7] español, de otros países o en los tratados internacionales. Esta exposición se hace necesaria para saber las herramientas jurídicas que protegen nuestras libertades en la temática del artículo y las posibles deficiencias que ésta presenta, así como los casos legales en que dichas libertades pueden vulnerarse con el fin de la prevención, averiguación o esclarecimiento de delitos.

- La '**Constitución Española**' (a partir de ahora, CE) en su articulado ya prevé tanto las garantías constitucionales al derecho a la intimidad, el secreto de las telecomunicaciones y el uso racional de datos informáticos como la posibilidad de limitarlos en ciertos casos.

  Sus artículos 18.1 y 18.3 indican: "Se garantiza el derecho al honor, a la intimidad personal y a la propia imagen", y "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial". La violación de ambos preceptos se encuentra sancionada en el Código Penal (a partir de ahora, CP), con los delitos de su "Título X, Capítulo I, del Descubrimiento y Revelación de Secretos".

  Su artículo 18.4 indica: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

- No obstante, queda patente la posibilidad de limitar el secreto de las comunicaciones mediante resolución judicial, expresado al final del art. 18.3 CE. Debemos reiterar la necesidad de dicha resolución judicial que además debe ser motivada para la intervención de comunicaciones, diferencia clara con otros países que recogen escuchas telefónicas administrativas, como ocurrió en Estados Unidos tras el 11-S[8] u ocurre en la amplia mayoría de países no democráticos.

[7] El ordenamiento jurídico lo componen todas las normas jurídicas vigentes en un lugar concreto.
[8] Autorización concedida a la NSA (Agencia de Seguridad Nacional) mediante Orden Presidencial del 2002.

Lo anterior se encuentra desarrollado en la '**Ley de Enjuiciamiento Criminal**' (a partir de ahora, LECrim), artículos 579 a 588, la cual es complementada por diversa jurisprudencia[9] debido a las críticas recibidas por su insuficiencia per se de cumplir con los compromisos internacionales en materia de protección al derecho del secreto de las comunicaciones. En otros países europeos ya ocurrió dicha insuficiencia, y es declarada en varias sentencias del TEDH como la de 24 de abril de 1990 -por vulneraciones al Art. 8 del CEDH, en casos Huvig y Kruslin (Francia) en la cual se admite la posibilidad de completar jurisprudencialmente la ley. Basándose en ello, nuestro TS y TC complementaron la LECrim sobre la intervención de las comunicaciones con sentencias como STC 181/1995 -necesidad de resolución judicial motivada, negando el uso de providencia- y las STC 166/1999, 171/1999, 126/2000, 299/2000, 14/2001, 138/2001 y 202/2001 -estar legalmente prevista con suficiente precisión, autorización por autoridad judicial en el curso de un proceso y estricta observancia del principio de proporcionalidad (como cuando se adopta para la prevención y represión de delitos graves)-.

La LECrim, acerca de este tema, recoge en sus artículos: 579.2 y 579.3 la intervención y observación de las comunicaciones, sus plazos y prórrogas; y 579.4 su aplicación de urgencia para delitos de bandas armadas o elementos terroristas.

> Con respecto a la interceptación de las comunicaciones, se debe distinguir entre la interceptación legal y la retención o preservación de datos. La primera es la interceptación tal y como se percibe inicialmente, esto es, captar la información que se transmite en una comunicación y sus datos asociados (como la identidad de los intervinientes), que se inicia tras orden de la autoridad correspondiente. La segunda se refiere al almacenamiento, por parte de proveedores de servicios, de listados detallados de llamadas o datos de transacciones telefónicas o de red -Internet-, sin incluir el contenido de la comunicación, de forma global -todos sus clientes- e ininterrumpida.

- La '**Ley 32/2003 General de Telecomunicaciones**' (en adelante, LGT) desarrolla la interceptación legal de comunicaciones, y las obligaciones de proveedores, como los Proveedores de Acceso a Internet (en adelante, ISP). Asimismo, la "**Ley Orgánica 2/2002, reguladora del control judicial**

[9] La jurisprudencia consiste en el conjunto de sentencias de los tribunales (como aquéllas del Tribunal Supremo o el Tribunal Constitucional) que constituyen un precedente para justificar otros casos no regulados por Ley.

previo del Centro Nacional de Inteligencia" detalla entre sus preceptos el control judicial en medidas que afecten al secreto de las comunicaciones, como el caso de la interceptación legal.

- La "**Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**" (en adelante, LCD) es la que desarrolla la retención de datos mencionada, tras la Directiva Europea 2006/24/CE que se creó a tal efecto.

  Se debe reseñar que una parte de la polémica existente en la interceptación legal de las comunicaciones en España viene de que ésta se desarrolla principalmente en simples leyes, que deberían ser provistas por ley orgánica al limitar derechos fundamentales contenidos en la parte esencial de la Carta Magna.

- Las garantías recogidas en el mencionado artículo 18.4 de la Carta Magna se encuentran desarrolladas en la "**Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal**" (en adelante, LOPD). En este caso sí se ha previsto de una Ley Orgánica como corresponde, cuya finalidad es garantizar los derechos al honor, intimidad y privacidad en el tratamiento de datos personales. Aunque pueda parecer lo contrario, tiene gran relevancia con el tema de este artículo ya que gran parte de la información controlada en el ciberespacio es de carácter personal y privada, y por tanto se deberían seguir preceptos marcados por leyes como ésta.

- La "**Ley 2/2011 de Economía Sostenible**" (en adelante, LES), en su disposición final cuadragésima tercera, recoge la protección de la propiedad intelectual por la regulación de descargas de contenido protegido por derechos de autor, tanto en sitios Web que lo alojen directamente como que enlacen a ellos, a través de una comisión creada al efecto, llegando a autorizar el corte del acceso a Internet a usuarios que reiteradamente violen dichos derechos. Resulta cuando menos curioso que se desarrolle en el articulado de una ley de temática muy distinta, y en el citado lugar, como si el legislador pretendiera que esta disposición pasara por alto, o evitar la exposición mediática que supone una ley aparte.

  Esta ley, aunque sin relación directa con la interceptación de comunicaciones, y a pesar de suscitar una polémica distinta -el cierre de sitios Web de enlaces es una medida con tal amplitud

que buscadores Web como Google, Yahoo o Bing estarían violando los preceptos recogidos- abre camino para crear instrumentos de control de comunicaciones de los ciudadanos que verifiquen si la vulneran con descargas de contenido protegido, tarea que dista mucho de la importancia de las tradicionales de interceptación legal, dedicadas casi en exclusiva a delitos graves como el tráfico de drogas, una de las actividades delictivas con mayor número de teléfonos intervenidos.

- Además de los instrumentos provistos en el ordenamiento jurídico nacional, existen acuerdos a nivel internacional que sólo obligan a los estados firmantes. Entre ellos, el "**Acuerdo Comercial Anti-Falsificación**" (en adelante, ACTA), acuerdo internacional de aceptación voluntaria en el que entre sus firmantes se encuentran Estados Unidos, Canadá, Europa, Australia y Japón, propone dar protección a la propiedad intelectual, obligando -entre otros preceptos- a los ISP a vigilar todos los paquetes de datos cargados o descargados desde Internet. Este acuerdo se halla en el citado camino que la Ley de Economía Sostenible puede estar abriendo, que limitaría derechos a la intimidad personal sin contar con el principio de proporcionalidad, ya que se equiparan a interceptaciones legales realizadas para la investigación o esclarecimiento de delitos graves. Un proyecto de ley similar en EE.UU. es el "Protect IP Act" (en adelante, PIPA), respaldado por el "Stop Online Piracy Act" (en adelante, SOPA), proyecto de ley que provee las previsiones para controlar a infractores de los anteriores.

De todo lo expuesto quedan al margen los posibles sistemas, por parte de servicios de inteligencia tanto civiles como militares, que realicen interceptaciones bordeando o traspasando dicha legalidad. Más adelante se verá cómo ocurre en muchos casos.

Para finalizar, se pretende hacer una reflexión sobre la medida en que las garantías constitucionales de cualquier estado quedan cubiertas de forma efectiva. En nuestra opinión, depende de cómo el legislador de turno las entienda y desarrolle de forma acertada en leyes de menor orden. Es decir, de si interpreta correctamente el espíritu de la norma y la sabe plasmar en leyes orgánicas u ordinarias sobre la materia. Por tanto es el legislador el que, a la hora de realizar su labor, debe centrarse únicamente en la protección de dichas libertades y las limitaciones justas a éstas para la salvaguarda de las garantías de otros, todo ello tras una profunda reflexión y análisis que evite errores, ambigüedades o malas interpretaciones, y evitando cualquier otro interés o propósito.

3. Organismos e instituciones involucradas.

A continuación se citan brevemente las entidades, tanto públicas como privadas, consideradas relevantes en la interceptación de las comunicaciones, con el fin de introducirlas y establecer una clasificación, ya que más tarde serán analizarán en sus apartados correspondientes.

Clasificación de entidades públicas -organismos o instituciones- involucradas:

- Agencias de inteligencia gubernamentales (ver punto 4)
- Alianzas entre agencias de inteligencia (ver UKUSA, puntos 4 y 6.1)
- Institutos y seminarios integrados por entidades públicas
    - ETSI (Instituto Europeo de Estándares en Telecomunicaciones). Entre otras funciones, realiza el diseño de protocolos[10] de interceptación legal de comunicaciones en Europa, aplicando la normativa europea y consensuando las aportaciones de sus miembros.
    - ILETS (Seminario Internacional de Telecomunicaciones en Fuerzas y Cuerpos de Seguridad). Este seminario posibilita el intercambio de información entre sus estados miembros, lo cual sirve de ayuda en el diseño o mejora de sistemas de interceptación.

Clasificación de entidades privadas -empresas- involucradas:

- Empresas que proveen sistemas de interceptación (ver punto 5.1)
- Empresas que realizan actos de espionaje industrial (ver punto 5.1)
- Empresas que, sin tener como objetivo inicial proveer o realizar interceptaciones, recaban un volumen masivo de datos para su actividad -debido a su gran volumen de usuarios o minería de datos-, con el potencial peligro que conlleva (ver puntos 5.2, 5.3, 5.4 y 7)

Clasificación de actividades involucradas:

- Desarrollo de sistemas de interceptación por empresas (ver punto 5.1)
- Diseño de protocolos de interceptación legal de comunicaciones:
    - ETSI.
    - ILETS.

[10] Un protocolo es el conjunto de reglas utilizadas por dos sistemas para comunicarse a través de una red.

Clasificación de redes de interceptación de comunicaciones a nivel global

- La red ECHELON (ver punto 6.1)

4. La interceptación ilegal de comunicaciones por parte de gobiernos

Para garantizar la seguridad de sus respectivos territorios la mayor parte de gobiernos mantienen, junto a los cuerpos de policía, uno o varios servicios de inteligencia. Dado que, por lo general, la actividad de estos servicios es secreta, se les denomina también servicios secretos. El cometido de estos servicios es:

- Obtener información para alejar peligros para la seguridad del Estado.
- Ejercer actividades de contraespionaje en general.
- Prevenir riesgos que puedan amenazar a las fuerzas armadas.
- Obtener información sobre distintos aspectos de la situación en el extranjero.

Para conseguir los fines antes mencionados se utilizan masivamente sistemas tecnológicos para la interceptación de las telecomunicaciones que facilitan el cometido de estas agencias o servicios de seguridad, siendo las más famosa a nivel mundial la agencia estadounidense NSA.

La 'Agencia de Seguridad Nacional' (en inglés: 'National Security Agency', o NSA), es una agencia de inteligencia criptológica del Gobierno de los Estados Unidos, administrada como parte del Departamento de Defensa. Creada el 4 de Noviembre de 1952 por el Presidente Harry S. Truman, la NSA es responsable de obtener y analizar información de cualquier medio de comunicación, y de garantizar la seguridad de las comunicaciones del gobierno contra otras agencias extranjeras similares, lo que conlleva la utilización del criptoanálisis o estudio de sistemas criptográficos[11].

Desde el 2008, la NSA puso en marcha un sistema para ayudar a supervisar las redes informáticas de las agencias federales de Estados Unidos para protegerlos ante cualquier ataque. Asimismo, es un componente clave de la Comunidad de Inteligencia de Estados Unidos, encabezada por el Director de la Inteligencia Nacional. El Servicio Central de Seguridad es una agencia encargada de servir de enlace y combinar las acciones de la NSA con las fuerzas armadas, que sirven de apoyo a la agencia. Por ley, la

[11] Sistemas que aplican técnicas destinadas a convertir información confidencial en datos ilegibles por terceros.

recopilación de datos de inteligencia por ésta se limita a comunicaciones extranjeras, aunque ha habido numerosos informes que aseguran que la agencia no siempre cumple estas leyes.

Una de las organizaciones más importantes de espionaje a nivel mundial dirigidas por la NSA y la UKUSA es la red ECHELON, con capacidad de espiar prácticamente cualquier sistema de comunicación en cualquier área del mundo.

Los gobiernos buscan formas de utilizar el ciberespacio para sus intereses, como ocurriría con cualquier tecnología de gran potencial. Sin embargo hay casos que van mucho más allá.

> Las autoridades de Irán han llegado a hacer públicos sus esfuerzos por controlar Internet, creando el 'Consejo Supremo del Ciberespacio' con amplia autoridad en la materia. Asimismo estableció un grupo denominado 'El Ciberejército', el cual se estima en 120.000 miembros incluyendo hackers, blogueros y otros activistas online, adiestrados y asistidos por el gobierno, y realizando sus actividades desde una red segura y privada creada a tal efecto.

Otras agencias o servicios de seguridad de los que hay fuertes indicios de que realizan interceptación ilegal de las comunicaciones, llegándose a hacer público este extremo en algunos casos, son:

- **GCSB**: Government Communications Security Bureau, Nueva Zelanda (UKUSA-Echelon). Se hizo pública su implicación en espionaje ilegal en el caso 'Kim Dotcom' -ver apartado de bibliografía-.
- **DSD**: Defence Signals Directorate, Australia (UKUSA-Echelon)
- **GCHQ**: Government Communications Headquarter, Reino Unido (UKUSA-Echelon)
- **CSE**: Communications Security Establishment, Canadá (UKUSA-Echelon)
- **MOSSAD**: Instituto de Inteligencia y Operaciones Especiales Israelí.
- **ISI**: Inter-Services Intelligence, Pakistán.
- **FAPSI**: Agencia Federal de Comunicaciones e Información, Rusia.
- **BND**: Servicio de Inteligencia Federal Alemán.
- **DGSE**: Dirección General de la Seguridad Exterior, Francia.
- **SISMI**: Servicio de Inteligencia Italiano.

La interceptación ilegal de comunicaciones es hoy en día la tecnología principal en el espionaje, permitiendo acceder a grandes cantidades de información cuyo poseedor desea poner fuera del alcance de extraños. Así pues, éste suele utilizar dispositivos o tecnologías de protección interpuestos que dificultan dicha tarea, lo que requiere burlarlos o quebrarlos. Mención aparte del uso de tecnologías de protección de datos como la encriptación, que consiste en cifrar dichos datos en un código el cual no se podrá visualizar sin su contraseña o sin averiguar cómo quebrar dicha técnica de cifrado. Se puede aplicar tanto a comunicaciones de datos como a información sensible almacenada en un disco o memoria.

Todo lo mencionado ocurre tanto en el espionaje político como en el económico. Por lo tanto, el espionaje plantea los mismos problemas en ambos terrenos, y por esta razón se aplican técnicas de espionaje muy similares en dichos ámbitos. Desde el punto de vista técnico no existe diferencia entre uno y otro. La primera diferencia es que, en el económico, el nivel de protección suele ser menor, por lo cual, en dichas ocasiones, este espionaje resulta de ejecución más sencilla. Otra diferencia reseñable es la conciencia de riesgo entre los usuarios de sistemas de comunicación interceptables. En el mundo de la economía, ésta es menos aguda que en los ámbitos de la seguridad del Estado, donde los usuarios suelen estar más formados y concienciados sobre el tema.

5. La interceptación ilegal de comunicaciones por parte de corporaciones.

5.1 El espionaje competitivo y económico.

Generalmente, el fin último perseguido por este tipo de interceptación es el espionaje económico entre empresas o una actividad subsidiaria para servicios policiales o de inteligencia de distintos gobiernos de todo el mundo; en este caso, el espionaje de interceptación se puede definir como la adquisición de información que mantengan en secreto empresas o incluso particulares por su carácter reservado, con el fin de utilizar dicha información privilegiada para perseguir un objetivo empresarial -económico-. Con respecto a su tipología se puede diferenciar entre espionaje competitivo, industrial o laboral si el agresor es una empresa de la competencia; y espionaje económico si el agresor es un servicio de inteligencia estatal. Los datos estratégicos, que son importantes para el espionaje destinado al sector económico, se pueden clasificar por las distintas áreas o sectores empresariales.

> El espionaje competitivo se produce entre empresas del mismo sector y suele realizarse sobre las que ostenten una mayor posición estratégica, ya que la información de su estructura, líneas de producción o financiación son muy interesantes para cualquier competidor. Habitualmente, puede afirmarse que este espionaje competitivo siempre termina por descubrirse y, aunque la magnitud de las cifras reales en perjuicios económicos no se conoce, se calculan astronómicas por su dimensión. Varias fuentes como las publicaciones del FBI en su área de contrainteligencia estiman pérdidas en los EE.UU. de billones de dólares anuales por este tipo de espionaje.

Los sectores empresariales que son objetivos de ataques se encuentran, lógicamente, en investigación y desarrollo, adquisiciones, personal, producción, distribución, ventas, comercialización, líneas de productos y finanzas. Con frecuencia se subestima la importancia y el valor de tales datos, cuando en realidad, bien empleados, pueden inclinar en gran medida la balanza entre empresas competidoras, utilizar una estrategia empresarial de éxito ya probada, iniciar el desarrollo de productos o líneas de las que no se tenía experiencia o investigación previa, o ahorrar masivos costes de I+D, entre otros.

Entre dichos sectores, los más golosos actualmente -sobre todo por la dificultad de iniciar la actividad sin gran experiencia previa, altos costes de investigación y/o la alta competencia, en la cual una mejora puede marcar el éxito- son: la biotecnología, técnica médica, ingeniería genética, equipos informáticos de alto rendimiento, aplicaciones informáticas, optoeléctronica, tecnología de señales y sensores ópticos, memorias electrónicas y nanotecnología. No obstante, es una lista que cambia constantemente en función de nuevos avances tecnológicos. En estos ámbitos, la interceptación de las comunicaciones consiste sobre todo en el robo de los resultados de la investigación o técnicas especiales de producción.

Por su actividad empresarial, más de 150 empresas privadas de todo el mundo tienen acceso a datos en dispositivos móviles y otros equipos tecnológicos. En algunos países, dichos datos -conversaciones, documentos, imágenes, etcétera- pueden ser interceptados en los dispositivos sin vulnerar la legalidad vigente, aunque en otros, dichas técnicas de interceptación no tienen cobertura legal.

Julian Assange, fundador del conocido sitio Web "Wikileaks", cuya función es publicar información reservada de gobiernos y corporaciones filtrada por algún empleado de éstos, señaló a Estados Unidos, Reino Unido, Sudáfrica, Canadá y Australia como los países con mayor industria de estos sistemas de vigilancia e interceptación.

A continuación, agrupadas por países se indican empresas de la industria de la interceptación y vigilancia (fuente: grupo de derechos humanos "Privacy International")

- **Alemania:** Alarm, ATIS Systems GmbH, Elaman, Datakom, EBS Electronic, IP Fabrics, Rohde & Schwartz, Syborg, Trovicor, AGT, DigiTask, Ipoque, Medav, Selectronic y Siemens.
- **Brasil:** Suntech Intelligence.
- **Canada:** Vineyard Networks, Advanced IO y Sandvine.
- **China:** ZTE Corporation, Huawei Technologies y Vixtel.
- **Colombia:** Asoto.
- **Dinamarca:** Spectronic Systems A/S, ETI Connect y Napatech.
- **Francia:** Alcatel, Qosmos, Thales, Aqsacom, Amesys (Bull), Scan & Target, Septier y Vupen.
- **Holanda:** Group 2000, Pine Digital Security y Fox-It.
- **Hungría:** Neti.

- **India:** Shogi Communications, ClearTrail y Shield Security.
- **Israel:** Ability, Nice Systems, Cellbrite, Elta Systems, Allot, News Datacom Research Ltd., Tracespan, Amdocs Ltd., Elkat y Semptian Technologies.
- **Italia:** Innova, BEA, Ips, RCS, Resi Group, Hacking Team y Loquendo.
- **Nueva Zelanda:** Security Software International y Endace Accelerated.
- **Polonia:** Macro System.
- **Reino Unido:** Gamma Group, Comstrac, Telesoft Technologies, Utimaco Safeware, Creativity Software, Datong Files, Autonomy, BAE Systems, Panoptech Files, Qinetiq, Sophos, ThorpeGlen, Audiotel International, Cobham, Hidden Technology Systems International Ltd., Roke y Sesp.
- **Republica Checa:** Inveatech y Phonexia.
- **Suiza:** Dreamlab Technologies AG.
- **Sur África:** Seartech y VAS Tech.
- **Turquía:** Inforcept Networks.
- **Ucrania:** Delta SPE y Altron.
- **EE.UU.:** Area Spa, ATCI, Bivio, BlueCoat, Broadsoft, Comverse, Cisco Systems, Cubic, Harris, Narus, Net Optics, Northop Grumman, Nuances Technology, Omni Wildpackets, SAIC, Meganet, Access Data, Glimmerglass, HP, Mantech, NetQuest, SS8 Networks, Ultrareach, Brightplanet, Packet Forensics, Radisys, Sonus Networks, Pen Link, Verint, Netezza, Polaris Wireless y Rainstor.

Como se puede observar, a algunos les sorprenderá ver en esta lista a grandes corporaciones con áreas de negocio tradicionales, mientras otras se dedican exclusivamente a equipamiento y/o software de interceptación y vigilancia, ya sea para su posterior uso con fines legales o ilegales.

> Al igual que ocurría con el espionaje competitivo, tampoco se debe subestimar la importancia de datos obtenidos por el espionaje económico, producido si el agresor es un servicio de inteligencia estatal. Éstos pueden, desde favorecer en un contrato internacional a una empresa estatal en detrimento de una extranjera gracias a la ventaja por la información técnica o de negociaciones interceptada, a favorecer directamente la economía del país, gracias a la toma de decisiones políticas basadas en datos estratégicos interceptados de terceros.

5.2 Corporaciones que registran datos personales de usuarios.

A partir de este punto, se señalarán aquellas empresas y sistemas que, sin tener como objetivo inicial proveer o realizar interceptaciones, recaban un volumen masivo de datos para su actividad -por su gran volumen de usuarios o minería de datos-, siendo peligroso el control que establecen de su cuota de ciberespacio por el uso final que puedan tener dichos datos.

Los primeros a mencionar son las corporaciones que registran datos personales de usuarios, sobre todo aquéllas con una alta cuota de mercado. Entre ellas, cabe citar proveedores de mensajería instantánea o e-mail, blogs, foros, portales, redes sociales y el comercio electrónico. Es de lógica que dichos datos, si son utilizados para fines deshonestos, pueden atentar gravemente a la intimidad de sus usuarios.

Un caso de corporación privada que registra gran cantidad de datos personales de sus usuarios se encuentra desarrollado en el punto 7, junto al potencial uso deshonesto que se podría dar a dichos datos.

5.3 Proveedores de servicios de búsqueda en Internet.

Los proveedores de servicios de búsqueda son corporaciones privadas que ofrecen sistemas para realizar búsquedas de páginas Web en todo el ciberespacio según los criterios que sean introducidos (como son contenido a buscar, idioma o fecha entre otros), mostrando aquellos resultados coincidentes. Entre ellos, se pueden citar a corporaciones mundialmente conocidas como son Google, Yahoo y Bing -esta última, propiedad de Microsoft-, las cuales entre sus múltiples servicios ofertados disponen de dichos sistemas de búsqueda. Algunos, como es el caso de Google, iniciaron su actividad empresarial exclusivamente con dicho servicio.

Dichas empresas, en el desarrollo de sus funciones, procesan y almacenan una gran cantidad de datos, necesarios para diversas operaciones como ordenar los múltiples resultados de búsqueda -intentando dar prioridad a páginas Web de mayor relevancia- o realizar estadísticas de criterios utilizados en búsquedas.

En los últimos años, se inició una tendencia en estas corporaciones a ofrecer múltiples funcionalidades que requieren de un registro y posterior 'login' (ingreso en el sistema) del usuario, identificando al mismo por su e-mail y demás datos personales suministrados. Si se añade esto al registro de los sitios Web que se buscan y se visitan al entrar en ellos desde la lista de resultados de búsqueda, se obtiene información muy valiosa sobre usos y preferencias del usuario, que como mínimo se pueden utilizar para realizar una publicidad enfocada a éste, o fines mucho más perniciosos, atentando contra la intimidad personal.

Además, hay sospechas fundadas de que alguna de estas corporaciones realiza minería de datos, técnica moderna la cual mediante procesos analíticos, estadística e inteligencia artificial permite -entre otros- establecer patrones complejos en sus bases de datos. De esta forma, se transforman en una estructura comprensible para su uso futuro, permitiendo realizar búsquedas en los mismos por criterios complejos y/o convertirlos en inteligencia. Dicho de forma más llana, se obtiene una estructura de la cual se pueden obtener no sólo datos personales del usuario, sino información más útil y compleja como sus hábitos, preferencias y cómo este se relaciona -conexiones- con el ciberespacio.

La posibilidad del uso de minería de datos para obtener inteligencia se desarrolla en el mencionado caso del punto 7, recomendándose de nuevo su lectura.

5.4 Proveedores de acceso a Internet o telefonía.

En esta categoría se engloban aquellas empresas que, aparte de registrar una ingente cantidad de datos personales de sus usuarios, tienen la capacidad técnica -que no jurídica- de interceptar las comunicaciones entre ellos, ya que son los dueños de la red física por la que éstas viajan.

Por lo tanto, no es de extrañar que, en muchos países, y dentro de su legislación sobre telecomunicaciones, se encuentren obligaciones específicas a proveedores de servicios de telecomunicación, entre las cuales está suministrar información y comunicaciones solicitadas en interceptaciones legales a Fuerzas y Cuerpos de Seguridad, y ordenadas -en el caso de España- por Jueces y Tribunales.

6. Técnicas utilizadas para el control del ciberespacio y la interceptación de las comunicaciones.

6.1 Sistemas globales de interceptación: Echelon.

El sistema de interceptación denominado Echelon se distingue de otros sistemas de inteligencia en dos propiedades que le confieren características consideradas muy peculiares: en primer lugar, se le atribuye la capacidad de ejercer una vigilancia simultánea de la totalidad de las comunicaciones. Según se afirma, todo mensaje enviado por teléfono, telefax, Internet o correo electrónico, sea cual sea su remitente, puede captarse mediante estaciones de interceptación de comunicaciones por satélite y satélites espía, permitiendo conocer su contenido.

Como segunda característica de Echelon se menciona que este sistema funciona a escala mundial gracias a la cooperación de varios estados, los cuales de por sí ya tienen individualmente una fuerte actividad en inteligencia: el Reino Unido, los Estados Unidos, Canadá, Australia y Nueva Zelanda. Esto significa un valor añadido en comparación con los sistemas nacionales de estados participantes en el sistema Echelon, o los estados UKUSA.

Por su colaboración, pueden ponerse mutuamente a disposición instalaciones de escucha e interceptación y sufragar conjuntamente los gastos resultantes, cubriendo de esta forma áreas tecnológicas y de territorios muy amplia, y usar de forma conjunta la información obtenida. Esta cooperación es imprescindible, justamente, para la vigilancia a escala mundial de comunicaciones por satélite, puesto que sólo de esta manera puede garantizarse la captación de mensajes de dos o más interlocutores en un intercambio en comunicaciones internacionales. Es evidente que las estaciones de interceptación de comunicaciones por satélite, por sus dimensiones, no pueden construirse en el territorio

de un Estado sin el consentimiento de éste. En este terreno es imprescindible el acuerdo mutuo y la cooperación de varios Estados situados en distintos continentes.

> Los posibles peligros que un sistema como Echelon encierra en la esfera privada y la economía no sólo se derivan del hecho de que se trate de un sistema de interceptación especialmente poderoso; más bien se deben a que este sistema funciona en un ámbito carente casi por completo de regulación jurídica.

Por lo general, un sistema de interceptación de comunicaciones internacionales no apunta a la población del propio país. En este caso, el individuo o corporación objeto de observación, por ser extranjero para el país observador, no dispone de ninguna clase de protección jurídica interestatal. Por ello, se encuentran en situación de completa indefensión frente al sistema. El control parlamentario resulta en este ámbito igualmente insuficiente, puesto que los electores, que parten de la base de que el problema no les afecta a ellos sino "sólo" a personas en el extranjero, no muestran especial interés en que se controle tal actividad, y sus representantes electos cuidan, en primer lugar, intereses de sus electores. Así, no es de extrañar que en las audiencias celebradas en el Congreso de los Estados Unidos sobre la actividad de la NSA sólo se examine la cuestión de si estas actividades afectan a ciudadanos de los Estados Unidos, sin que el sistema en sí suscite mayores reparos.

El Convenio “UKUSA” nace de la continuación de la cooperación entre los Estados Unidos y el Reino Unido, muy estrecha ya durante la Segunda Guerra Mundial, y que ya se había perfilado en la Primera Guerra Mundial.

La iniciativa para el establecimiento de una alianza SIGINT (Inteligencia de señales) partió de los estadounidenses en una reunión celebrada en agosto de 1940 entre estadounidenses y británicos. En febrero de 1941, los criptoanalistas estadounidenses entregaron una máquina de cifrado (PURPLE) al Reino Unido. En la primavera de 1941 empezó la cooperación en el ámbito criptoanalítico. La cooperación en el ámbito de la inteligencia se reforzó con la intervención conjunta de las flotas en el Atlántico Norte durante el verano de 1941. En junio de 1941, los británicos consiguieron descifrar el código de la flota alemana ENIGMA, lo que supuso un mazazo enorme a sus operaciones navales.

La entrada de los EE.UU. en la guerra reforzó en mayor medida la cooperación SIGINT. En 1942, los criptoanalistas estadounidenses de la "Naval SIGINT Agency" empezaron a trabajar en el Reino Unido. Las comunicaciones entre las "U-Boot Tracking-Rooms" (salas de seguimiento de submarinos) en Londres, Washington y, a partir de mayo de 1943, también Ottawa en el Canadá fue tan estrecha que, según declaraciones de un antiguo colaborador, trabajaban como una organización única.

En la primavera de 1943 se firmó el Acuerdo BRUSA-SIGINT entre Reino Unido y los Estados Unidos, y se inició un intercambio de personal. El acuerdo se refiere, entre otras cosas, al reparto del trabajo y se resume en sus tres primeras frases: tiene por objeto el intercambio de toda información relativa al descubrimiento, identificación e interceptación de señales, así como desciframiento de códigos y claves. Los estadounidenses eran principales responsables para Japón y los británicos para Alemania e Italia.

Tras la guerra, la iniciativa de la continuación de la Alianza SIGINT partió del Reino Unido. Las bases para ello se acordaron en una gira mundial realizada en la primavera de 1945 por miembros británicos de los servicios de inteligencia (como Sir Harry Hinsley). Uno de los objetivos era enviar personal europeo al Pacífico para la guerra con Japón. En este contexto, se acordó con Australia poner recursos y personal británicos a disposición de los servicios australianos. Durante el viaje de vuelta a los EE.UU., Hinsley pasó por Nueva Zelanda y Canadá para contar con sus recursos y personal.

En septiembre de 1945, Truman firmó el memorándum altamente confidencial que constituyó la pieza clave de la Alianza SIGINT en tiempos de paz. A raíz de ello, iniciaron negociaciones para el acuerdo entre británicos y estadounidenses. Una delegación británica inició contactos con canadienses y australianos sobre una posible participación. En febrero y marzo de 1946, se celebró con el mayor secreto una conferencia SIGINT angloamericana para negociar los detalles. Los británicos recibieron autorización de canadienses y australianos. El resultado de la conferencia fue un documento, aún clasificado, de unas veinticinco páginas, con los pormenores de un acuerdo SIGINT entre Estados Unidos de América y la Commonwealth británica.

En los dos años siguientes se produjeron otras negociaciones, desembocando en la firma del texto definitivo del llamado acuerdo UKUSA en junio de 1948.

6.2 Sistemas personales de interceptación: Troyanos.

El troyano informático, también denominado caballo de Troya, consiste en un software malicioso que debe su nombre a su forma de infección y actuación: mediante la apariencia de un software legítimo, al utilizarlo infecta el equipo con diversos fines siendo el más común permitir el acceso y control total remoto de éste a través de la creación de una "puerta trasera" o "backdoor" en inglés.

Sin embargo, con la proliferación del uso de internet y nuevas tecnologías por un gran número de usuarios, se atisbó su enorme potencial como herramienta de espionaje. Existen diversos troyanos creados específicamente con el fin de registrar, en el equipo infectado, las comunicaciones -conversaciones, e-mails, chats, navegación Web, etcétera-, contraseñas utilizadas, archivos informáticos abiertos o copiados y cualquier otra información según su diseño. Más tarde, envía regularmente dichos registros mediante la conexión a Internet al espía, todo ello de forma oculta, y como puede verse con enorme potencial de daño.

Desde hace varios años, los creadores de troyanos se han centrado cada vez más en la ejecución del mismo de forma automática sin necesidad de la intervención del usuario, a través de vulnerabilidades -fallos de diseño- de los navegadores de Internet. Por ello conviene actualizar regularmente este tipo de software. En otras palabras, ocurre al abrir una Web aparentemente inocua con código malicioso que descarga e instala el caballo de Troya. Otras veces, camuflan la Web para que aparente un sitio de descarga de aplicaciones, imágenes o vídeos, y aprovechan que se realiza una descarga para enviar el troyano requiriendo en este caso intervención del usuario para su infección.

Finalmente, señalar que el gran incremento del uso de smartphones, o teléfonos móviles inteligentes -iPhone, que usa sistema operativo Apple iOS, o cualquiera que use sistema operativo Android o Symbian- hace muy atractivo el diseño de troyanos dedicados, habiendo aumentado su uso de forma considerable. Según datos del portal de seguridad "Securelist"[12], en Android el software malicioso (categoría dentro de la que se encuentran los troyanos-espía, con el 34% del total) se ha multiplicado en los últimos 18 meses.

[12]Securelist es propiedad de 'Kaspersky Lab', cuarto proveedor mundial de 'endpoint security' en 2011 (soluciones entre las que se encuentran los antivirus) según ranking del IDC, proveedor de inteligencia de mercado y consultoría.

Como ejemplo, el número de nuevas amenazas del primer semestre de 2011variaba de 4 a 112 por mes, pasando a ser en el segundo de 161 a 1179 (este último número registrado en diciembre). Android es la plataforma más atacada (65%) debido a su gran crecimiento y número de usuarios (40-50% del total).

6.3 Datos registrados en memorias informáticas.

Este punto no trata de técnicas de control o interceptación de comunicaciones; no obstante se expondrá brevemente debido a su relación con la vulneración del derecho a la intimidad. Los datos almacenados en memorias informáticas como discos duros, memorias internas o por USB y otros medios son un objetivo de ciertos sistemas de interceptación, como se vio en el punto 6.2 o en el 5.1.

Sin embargo, estos dispositivos no sólo almacenan nuestros datos personales, ya que las memorias internas de un equipo guardan datos temporales y "logs" (registros) del software usado por éste. En ciertos casos, el acceso a estos datos es una potente herramienta de control. Como ejemplo, hace tiempo se descubrió que el navegador GPS de IPhone almacenaba las rutas por las que se viajaba, aunque no estuviese configurado el software explícitamente para ello, con lo que su obtención permitiría saber buena parte de los movimientos del objetivo.

Asimismo, los datos almacenados por gobiernos y corporaciones son una posible e importante fuente de control, como se vio en los puntos 4 y 5. En este caso, hay que recordar que cualquier dato personal registrado por éstos debe cumplir las leyes de protección de datos del país en cuestión (LOPD, punto 2).

6.4 Comunicaciones y datos registrados en la red.

Existe la creencia por gran parte de sus usuarios de que Internet ofrece un alto grado de anonimato. Si bien es cierto que la red de redes soporta un número masivo de usuarios, dificultando su identificación, que su regulación y control por algunos países es insuficiente o inexistente y que hay sistemas específicos para establecer comunicaciones anónimas o seguras por la red, la gran mayoría

de transacciones realizadas dejan nuestra "huella digital" quedando registradas en diversos sistemas, y permitiendo un control efectivo del usuario.

El término "huella digital" se usa en este escrito como analogía a los múltiples vestigios -registros- que se dejan en soportes informáticos al usar tecnología o comunicaciones, como son los datos y contenido de la comunicación. A continuación, se exponen los diferentes casos que determinan esta "huella digital", es decir, los diferentes vestigios que se almacenan, agrupados por la entidad o sistema que los registra.

i. Datos registrados a través de navegadores Web.

La tecnología en navegadores Web ha avanzado desde su inicio, en el cual sólo podían mostrar texto, imágenes e hipervínculos (enlace a otra página, base de la navegación Web) a permitir visualizar vídeos, juegos y otros elementos interactivos. Para ello se requiere que el equipo realice acciones desde su lado que superan el mero hecho de mostrar información.

Una de estas tecnologías son las "Cookies". Consiste en almacenar datos en el equipo suministrados por el sitio Web visitado, que los puede leer posteriormente, permitiendo varias funciones como recordar una sesión (que el usuario se identificó en la Web) mientras se visitan varias páginas, o las preferencias de éste.

Aunque éstos son almacenados en una zona dedicada, y no se da cabida a que se almacene más que texto -no podría entrar un virus de esta forma-, su peligrosidad estriba en que pueden usarse para almacenar preferencias, opciones elegidas, artículos adquiridos, sitios visitados y un largo etcétera, sirviendo de rastro de las acciones que se realizan en la red. Es común su uso para mostrar publicidad específica a nuestros gustos, siendo discutible desde el punto de vista de la privacidad, e intolerable si se va más allá.

La otra tecnología relevante es el "Javascript", lenguaje de programación del lado del cliente. Esto significa que el sitio Web envía automáticamente un programa que el navegador ejecuta para realizar sus funciones. Como ejemplo, los menús desplegables suelen diseñarse en Javascript. Al

ser una tecnología peligrosa -aquí si cabría que nos enviasen un virus-, las posibles funciones de este código se limitaron considerablemente.

Entre las funciones permitidas, aún permite suministrar al sitio Web datos potencialmente peligrosos, como son nuestra dirección IP (identificativa de nuestro equipo en la red), navegador y versión que se utiliza, incluso la ubicación física proveniente del GPS del móvil o módem/router ADSL desde el que se está conectados. Datos que, sin ser de los más privados, pueden ser de aplicación para fines tan útiles como perniciosos.

A pesar de las citadas limitaciones, existe código Javascript "malicioso", que aprovecha una vulnerabilidad -error de diseño- del navegador para realizar funciones no permitidas, siendo la más común automáticamente descargar e infectar el equipo con un virus o troyano. Una vez dentro del equipo podría realizar cualquier función, desde las más comunes (mostrar publicidad no deseada o registrar acciones para aplicarlas a estadísticas de marketing) a las más peligrosas (fraudes o control de nuestras acciones).

La forma de protección en este caso requiere tener instalado un antivirus y, lo que es más importante, actualizarlo regularmente, e instalar todas las actualizaciones del navegador que solventen estas vulnerabilidades.

ii. Datos registrados por formularios, blogs y foros Web.

Todo el mundo tiene claro que datos y opiniones vertidas en blogs y foros Web quedan registradas, así como formularios de todo tipo (registro en un sistema, solicitudes de información, etcétera).

Si estos datos son públicos, aparte de ser visibles por cualquiera, permiten el uso de herramientas que combinan técnicas de extracción de información (para incorporar de forma estructurada estos datos en una base de datos propia) y minería de datos (mediante técnicas de análisis, inteligencia artificial y estadística entre otras permite establecer patrones en grandes volúmenes de datos) convirtiéndolos en una estructura comprensible para uso futuro. Así, se podrían realizar búsquedas en dicha estructura de datos por criterios complejos y/o convertirlos en inteligencia. De esta forma

conversaciones, opiniones y comentarios vertidos en estos sistemas pueden usarse para obtener desde datos estadísticos a fines de control poco éticos y peligrosos.

Si estos datos son privados, se debe tener muy en cuenta que al menos los propietarios del sistema tendrán acceso total a los mismos.

iii. Datos de tráfico de un sitio Web.

Por razones principales de obtención de estadísticas, el propio servidor -equipo- donde se aloja una página Web almacena información varia de los usuarios que conectan a ella, y es suministrada por el navegador en el proceso de conexión, como son la dirección IP, navegador y versión usada y otros datos. Las mismas consideraciones explicadas en el punto anterior son de aplicación aquí.

iv. Datos de tráfico en la red. Los ISP.

Los sistemas y equipos que componen la red de la operadora de telefonía o el proveedor de acceso a Internet (en adelante, ISP) por motivos técnicos, de seguridad y legales almacenan información de nuestras transacciones.

A menos que exista una orden de interceptación legal sobre un objetivo, no debe almacenarse el contenido de las comunicaciones. No obstante, el resto de la información registrada es amplia y útil: intervinientes en la comunicación, número de abonado -teléfono- o direcciones IP de éstos, fecha/hora, duración o tamaño de datos transmitidos, etcétera. Si un tercero obtiene estos datos o el operador los utiliza de forma poco ética, se incurre en los peligros indicados en los puntos anteriores. Todo ello, sin perjuicio de que el operador o proveedor posee los medios técnicos, que no jurídicos, para interceptar el contenido de las comunicaciones, cosa poco probable pero factible. Por ello se hace necesario un control jurídico férreo sobre corporaciones que almacenan o tienen la posibilidad técnica de obtener datos de dicha naturaleza.

7. Nuevas técnicas. El caso del reconocimiento facial

Una de las características más notables del ámbito científico actual es su rápida y constante evolución, aportando grandes avances técnicos y sociales e incrementando la calidad de vida en un amplio número de personas. Incluso se ha llegado a derrocar gobiernos totalitarios gracias al uso de nuevas tecnologías que permiten superar la falta de información y censura existente en el país. Pese a las obvias ventajas, se debe estar atento a las nuevas técnicas que puedan vulnerar la privacidad personal y que aparecen de forma continua. Por la multiplicidad de las mismas, se restringirá este punto al estudio del caso del reconocimiento facial.

El reconocimiento facial es una técnica reciente basada en complejos algoritmos matemáticos que calculan una "plantilla" biométrica del rostro y la comparan con una base de datos, como el ya maduro reconocimiento dactilar. Estos datos, a pesar de que no revelen características del comportamiento del individuo, pertenecen a una esfera muy privada del mismo, ya que permiten su inequívoca identificación. Por tanto, deberían tratarse con las mayores garantías jurídicas, ajustándose entre otros a la normativa de protección de datos y, sobre todo, al principio de proporcionalidad.

Hasta hace poco, ha estado restringido a los ámbitos de la seguridad -control de entrada en edificios o sistemas informáticos para corporaciones mayormente privadas que pudieran asumir su coste- y de la inteligencia militar o policial -reconocimiento de objetivos o interrelaciones entre éstos almacenados en una "lista negra" mediante su cotejo con imágenes obtenidas por distintos medios-. Los casos mencionados se dirigen hacia un grupo muy concreto de individuos: empleados de una empresa -de los cuales recursos humanos ya posee suficiente información privada- u objetivos concretos, objeto de investigación criminal -siendo razonable siempre que su uso se restrinja a éstos-.

Esta tecnología tiene múltiples aplicaciones aparte de las descritas, como son el etiquetado de imágenes o vídeo por quienes aparezcan en ellas, interrelacionar dichos individuos apoyándose en lo anterior y en información de otras bases de datos que se posean, y la tecnología del entretenimiento y los videojuegos.

Por ello planteamos la siguiente cuestión, ¿Y si grandes corporaciones, públicas o privadas, que posean ingentes bases de datos de clientes o usuarios utilizan el reconocimiento facial para mejorar sus servicios, pero de forma global, indiscriminada o sin informar suficientemente de los riesgos que conlleva? Aunque su objetivo sea inicialmente inocente genera una información del ámbito privado muy valiosa, probable objetivo de grandes abusos aunque sólo sea con motivos comerciales. Incluso la ayuda de algoritmos de inteligencia artificial permiten establecer las interrelaciones mencionadas, produciéndose "inteligencia" en cierto grado, mucho más peligrosa que la simple información que, para poder ser utilizada de forma eficaz, debe ser procesada para convertirla en inteligencia.

Grandes corporaciones como Google, Microsoft, Apple, Sony y Facebook han desarrollado o adquirido sistemas de reconocimiento facial para varios usos. Google pretende utilizarlo como control de acceso a zonas que requieran una fuerte protección de privacidad. Microsoft presentó el año pasado OneVision, que obtiene una alta tasa de éxito en caras de baja resolución, y anunciando que estará en su sistema operativo Windows 8. Apple, a pesar de no introducir ninguna aplicación propia, la cede a otros desarrolladores de aplicaciones. Sony lo implementó en su consola PlayStation Vita, permitiendo interactuar con ella mediante gestos faciales, con una fidelidad muy alta.

> El caso de Facebook ha generado una gran polémica en diversas autoridades y organismos, como las europeas en Protección de Datos; Senadores y Fiscales Generales de Estados Unidos. Empresa con alrededor de un billón de usuarios -unos 19 millones sólo en España-, posee una de las mayores bases de datos de imágenes, información demográfica y personal de éstos, siendo en buena parte menores de edad, grupo de especial riesgo y vulnerabilidad. Recientemente adquirió "Face.com", empresa tecnológica israelí que desarrolló una tecnología muy eficiente de reconocimiento facial, para integrarlo en su sistema.

Su sistema consiste en sugerir el etiquetado de imágenes de usuarios por los individuos que aparezcan en ellas. No obstante, oculta el uso de reconocimiento facial -lo mencionaba en una sola página, requiriendo pasar por seis anteriores-, lo introdujo con explicaciones muy vagas de sus funciones y ejecución técnica, no ofrecen información del uso posterior de dichos datos y, aunque en principio sólo sugiere etiquetas de amigos del usuario, ya ha adquirido una riquísima base de datos biométrica.

El éxito de Facebook se basa en su minería de datos, en los que ya poseen de sus usuarios y en compartir éstos entre ellos, por lo cual su lema nunca ha sido la "privacidad por defecto". Y esto lo aplicó a su nuevo sistema de reconocimiento facial. Inicialmente, no sólo se activaba por defecto sino que no permitía desactivarlo. A este respecto, Google desactivó por defecto su propio sistema creyendo que la información es "tan sensible que los usuarios deben optar a ella de forma consciente". Posteriormente, Facebook anunció que permitirá rechazar el etiquetado, posiblemente influidos por las presiones a las que fue sometido.

Lo que es más, consultas a Facebook sobre si alguna vez vendería sus perfiles biométricos a terceros, obtuvieron como respuesta que "es difícil saber cómo Facebook será dentro de 5 ó 10 años, por lo que es difícil responder a esto".

> A estos respectos -datos que ya tenían, los que constantemente van adquiriendo por minería, los biométricos y su postura con respecto a la privacidad y el uso de datos obtenidos- Facebook se encuentra en una clara posición de privilegio, con recursos que, en las manos equivocadas, pueden causar graves daños. Tradicionalmente, dichos recursos sólo han sido confiados a los gobiernos, de forma reticente y siempre siguiendo el principio de proporcionalidad, como puede ser de aplicación para la averiguación de delitos y la seguridad nacional.

Ahora imaginemos que cualquier empresa como ésta o una tercera corporación privada o pública que adquiera sus bases de datos, implemente un algoritmo de inteligencia artificial que, partiendo de perfiles biométricos, datos personales, demográficos y de navegación de los mismos, obtenga inteligencia de ellos. Se podrían establecer interrelaciones por diversos criterios, como: amigos, cercanía de las caras -la invasión del espacio personal se considera signo de intimidad-, geolocalización de fotografías (cada vez más cámaras incorporan dichos datos mediante GPS integrado), geolocalización obtenida del GPS del teléfono móvil (a través de la aplicación para móviles de Facebook), cotejamiento de gustos, lugares visitados, páginas visitadas y biografía anual del usuario. Con ello, se obtendría una amplísima red de sus relaciones personales, sus movimientos junto a otros usuarios de interés y un largo etcétera. Y da mucho que pensar si está ocurriendo ya, viendo que grandes inyecciones de capital a estas empresas provienen de fondos relacionados con agencias de inteligencia, como son los 27,5 millones de dólares de Greylock Venture Capital (con fuertes vínculos a la CIA) inyectados en Facebook recientemente.

Todo ello genera incertidumbres sobre si existe un control efectivo de empresas como Facebook, y quién ejerce o debería ejercer dicho control. Una cuestión que, por su complejidad y densidad, correspondería responderla en un análisis aparte del presente documento.

En nuestra opinión, cualquier tecnología con tan enorme potencial de violación de derechos fundamentales debería ser objeto de la mayor protección jurídica, sobre todo si está en manos de corporaciones privadas cuyo funcionamiento está dictado por objetivos puramente empresariales. Y como un mínimo indispensable, obligar a aplicar la "privacidad por defecto", y a solicitar permiso expreso y sobradamente informado de políticas que afecten a la privacidad, de forma clara y concisa, evitando documentos extensos que por falta de tiempo o motivación nadie lee.

8. Reflexiones finales

En los casos de interceptación de las comunicaciones legalmente establecidos puede justificarse la invasión a los derechos fundamentales que presupone la misma, siempre que haya un equilibrio racional entre los derechos limitados y las conductas delictivas perseguidas, según el principio de proporcionalidad. No obstante, si se saltan los mecanismos legalmente establecidos, aunque sea promovida por gobiernos en su celo de garantizar la seguridad en casos tan graves como terrorismo o bandas organizadas, existe una indefensión de dichos derechos por parte del individuo y aumenta enormemente la posibilidad de un uso pernicioso de la información obtenida, al faltar un control legal, máxime si las intervenciones se realizan de forma arbitraria o indiscriminada.

Es evidente que toda interceptación ilegal de comunicaciones u otros datos por servicios de inteligencia o corporaciones es una violación grave de la intimidad de la persona. Únicamente en un 'estado policial' se admite la escucha arbitraria e ilimitada por parte del Estado. En los Estados Miembros de la Unión Europea, democracias ya consolidadas, es indiscutible que sus órganos estatales deben respetar la privacidad e intimidad de sus ciudadanos y, por consiguiente, también los servicios de inteligencia lo cual, con frecuencia, viene recogido así en la Constitución de dichos Estados. La esfera privada de la persona, por tanto, disfruta de una protección especial; las intervenciones se producen únicamente tras ponderar las ventajas e inconvenientes jurídicos y respetando siempre el principio de proporcionalidad.

También en los estados pertenecientes al Acuerdo UKUSA existe conciencia del problema. Sin embargo, las normas protectoras previstas por éstos tienen como objetivo el respeto de la esfera privada de su propia población, de tal manera que los ciudadanos europeos, por lo general, no se benefician de tales medidas. En las disposiciones de los EE.UU., por ejemplo, se reglamentan las condiciones de vigilancia electrónica; el interés estatal en servicios de inteligencia operativos no está en contradicción con una protección eficaz de derechos fundamentales. Aunque el respeto de la esfera privada es un derecho fundamental recogido en numerosos convenios internacionales algunos países incumplen flagrantemente los mismos en aras de proteger su seguridad nacional, violando la intimidad de ciudadanos y empresas extranjeros principalmente y en menor medida la de sus propios ciudadanos.

El desarrollo legislativo de la materia tiene ambigüedades, errores y omisiones que debieran ser revisados y subsanados. En España, es criticable que el mismo se realice principalmente en leyes de menor orden a las adecuadas para legislar derechos fundamentales, que deben tener reserva de ley orgánica tal y como se recoge en el artículo 81 de la CE, lo que obliga a un mayor consenso necesario al regular materias tan sensibles. Asimismo, la insuficiencia de las disposiciones de la LECrim para cumplir los compromisos internacionales en esta materia ha obligado a la jurisprudencia a complementar las mismas. Además, se ve una clara tendencia a implantar instrumentos de control de las comunicaciones para infracciones de menor entidad, como las descargas particulares de contenido protegido con copyright, vulnerando el principio de proporcionalidad.

Para terminar, se debería legislar de forma muy específica y restrictiva -y velar con especial celo su cumplimiento- el registro, protección y uso de información por corporaciones que, por su ingente cantidad de usuarios y el registro intensivo de sus transacciones al usar el sistema, tengan potencial de vulnerar de forma grave, masiva y arbitraria los derechos mencionados, como buscadores Web, redes sociales e ISPs. Y bajo ninguna circunstancia se debería permitir el análisis o minería de datos con fin distinto del estricto funcionamiento del sistema ni, lo más aberrante, venderlos a terceras partes.

En otros países, el abanico de críticas es más amplio, desde las “interceptaciones administrativas”, entendiendo por éstas las que no requieren de control judicial, hasta la falta en mayor o menor medida de legislación sobre el tema. Y siendo el ciberespacio una tecnología global, deberían producirse esfuerzos legislativos conjuntos, mediante acuerdos internacionales cuyo fin sea la protección de los derechos fundamentales de usuarios de servicios de comunicaciones.

9. Bibliografía

LEGISLACIÓN

España. La Constitución Española de 1978. *Boletín Oficial del Estado*, 29 de diciembre de 1978, núm. 311, p. 29317

España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado*, 24 de noviembre de 1995, núm. 281, p. 34010-34011

España. Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado*, 23 de junio de 2010, núm. 152, p. 54844

España. Ley de Enjuiciamiento Criminal. Real Decreto de 14 de septiembre de 1882. *Boletín Oficial del Estado*, 17 de septiembre de 1882, núm. 260.

España. Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal. *Boletín Oficial del Estado*, 26 de mayo de 1988, núm. 126, p. 16160

España. Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. *Boletín Oficial del Estado*, 4 de noviembre de 2003, núm. 264, p. 38900-38902

España. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. *Boletín Oficial del Estado*, 19 de octubre de 2007, núm. 251, p. 42517-42520

España. Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. *Boletín Oficial del Estado*, 7 de mayo de 2002, núm. 109, p. 16439

España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, 14 de diciembre de 1999, núm. 298, p. 43088-43097

España. Ley 2/2011, de 4 de marzo, de Economía Sostenible. *Boletín Oficial del Estado*, 5 de marzo de 2011, núm. 55, p. 25222-25226

España. Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social. *Boletín Oficial del Estado*, 31 de diciembre de 2003, núm. 313, p. 46928

Europa. Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. *Corte Europea de Derechos Humanos*, 1 de Junio de 2010, p. 10

Europa. Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de Marzo de 2006sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. *Diario Oficial de la Unión Europea*, 13 de Abril de 2006, núm. 105, p. 54-60

EE.UU. “Protect IP Act of 2011” o “Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011”, Propuesta de Ley de Mayo de 2011. *Senado de los Estados Unidos*, núm. GRA11400, p.5-6,16-18,24

EE.UU. “Stop Online Piracy Act”, Propuesta de Ley de 26 de Octubre de 2011. *Cámara de Representantes de los Estados Unidos*, núm. H.R.3261, p. 11-19

Internacional. Acuerdo Comercial Anti-Falsificación de Mayo de 2011. *Ministerio de Asuntos Exteriores de Japón*, Mayo de 2011, p.1-17

INFORMES

SCHMID, Gerhard, et al. *Informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON) (2001/2098(INI)).* [Bruselas]: Parlamento Europeo, 2001, núm. PE 305.391, 204 p.

ESTÁNDARES

Interceptación Legal; Conceptos de Interceptación en una Arquitectura de Red Genérica. [Sophia-Antipolis]: ETSI (Instituto Europeo de Estándares en Telecomunicaciones), 2006, núm. TR 101 943, 31 p.

Interceptación Legal; Requisitos de las Fuerzas y Cuerpos de Seguridad. [Sophia-Antipolis]: ETSI (Instituto Europeo de Estándares en Telecomunicaciones), 2009, núm. TS 101 331, 30 p.

Interceptación Legal; Interfaz de Entrega para la Interceptación Legal de Tráfico de Telecomunicaciones [Sophia-Antipolis]: ETSI (Instituto Europeo de Estándares en Telecomunicaciones), 2007, núm. ES 201 671, 124 p.

Interceptación Legal; Interfaz de Entrega para la Interceptación Legal de tráfico de Telecomunicaciones [Sophia-Antipolis]: ETSI (Instituto Europeo de Estándares en Telecomunicaciones), 2012, núm. TS 101 671, 160 p.

Interceptación Legal; Retención de Datos [Sophia-Antipolis]: ETSI (Instituto Europeo de Estándares en Telecomunicaciones), 2007, núm. TS 102 656, 17 p.

Interceptación Legal; Tratamiento de la Retención de Datos; Interfaz de Entrega para la solicitud y envío de Retención de Datos [Sophia-Antipolis]: ETSI (Instituto Europeo de Estándares en Telecomunicaciones), 2008, núm. TS 102 657, 84 p.

LIBROS Y PUBLICACIONES

VV.AA. *Echelon. La red de espionaje planetario*. 1ª Edición. Santa Cruz de Tenerife: Editorial Melusina, 2007. 203 p. ISBN: 978-84-96614-34-5

KEEF, Patrick Raaden. *Chatter: Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping.* Reprint Edition. New York: Random House Trade Paperbacks, 2006. 336 p. ISBN: 978-08-12968-27-9

PUBLICACIONES ON-LINE

Proyectos diversos sobre Privacidad [en línea]. Privacy International (Grupo de Derechos Humanos) <https://www.privacyinternational.org/projects/> [Consulta: 7 de Noviembre de 2012]

Informes diversos sobre Privacidad [en línea]. Privacy International (Grupo de Derechos Humanos) <https://www.privacyinternational.org/reports/> [Consulta: 7 de Noviembre de 2012]

Surveillance Industry Index [en línea]. Privacy International (Grupo de Derechos Humanos) <https://www.privacyinternational.org/sii/> [Consulta: 7 de Noviembre de 2012]

Artículos diversos de Contrainteligencia [en línea]. Oficina Federal de Investigación (FBI), área de Contrainteligencia. <http://www.fbi.gov/about-us/investigate/counterintelligence/> [Consulta: 10 de Noviembre de 2012]

Economic Espionage [en línea]. Oficina Federal de Investigación (FBI), área de Contrainteligencia. <http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage/> [Consulta: 10 de Noviembre de 2012]

Artículos diversos de Seguridad Informática [en línea]. Securelist, Kaspersky Lab. <http://www.securelist.com/en/analysis/> [Consulta: 25 de Noviembre de 2012]

MASLENNIKOV, Denis. *Mobile Malware Evolution, Part 5* [en línea]. Securelist, Kaspersky Lab. <http://www.securelist.com/en/analysis/204792222/Mobile_Malware_Evolution_Part_5/> [Consulta: 25 de Noviembre de 2012]

RAIU, Costin. *Kaspersky Security Bulletin 2012. Malware Evolution* [en línea]. Securelist, Kaspersky Lab. <http://www.securelist.com/en/analysis/204792254/Kaspersky_Security_Bulletin_2012_Malware_Evolution/> [Consulta: 15 de Diciembre de 2012]

Documentación procedente de diversos gobiernos y corporaciones, filtrada y divulgada [en línea]. Wikileaks <http://www.wikileaks.org/> [Consulta: 25 de Noviembre de 2012]

Documentación procedente de diversos gobiernos y corporaciones, filtrada y divulgada [en línea]. Wikileaks Spyfiles <http://wikileaks.org/the-spyfiles.html/> [Consulta: 25 de Noviembre de 2012]

Catálogo de dispositivos y software de interceptación de tráfico de red y comunicaciones por satélite de la empresa Vastech [en línea]. Wikileaks Spyfiles <http://wikileaks.org/spyfiles/list/service-product/capture-and-recording-of-all-traffic.html/> [Consulta: 25 de Noviembre de 2012]

Catálogo de software de interceptación y obtención de inteligencia de la empresa Vastech [en línea]. Wikileaks Spyfiles <http://wikileaks.org/spyfiles/docs/vastech/18_a-new-generation-system-architecture-for-intelligence.html/> [Consulta: 25 de Noviembre de 2012]

Catálogo de software de interceptación y obtención de inteligencia, permitiendo monitorización en tiempo real, de la empresa SS8 [en línea]. Wikileaks Spyfiles <http://wikileaks.org/spyfiles/list/service-product/intelligence-analysis-software.html/> [Consulta: 25 de Noviembre de 2012]

Catálogo de dispositivos de interceptación, permitiendo monitorización en tiempo real, de tráfico de red de la empresa Utimaco [en línea]. Wikileaks Spyfiles <http://wikileaks.org/spyfiles/list/service-product/monitoring-center.html/> [Consulta: 25 de Noviembre de 2012]

Catálogo de dispositivos de análisis forense de terminales móviles de la empresa Cellebrite [en línea]. Wikileaks Spyfiles <http://wikileaks.org/spyfiles/list/service-product/cellphone-forensic.html/> [Consulta: 25 de Noviembre de 2012]

TAJITSU, Naomi. *NZ launches inquiry into spying in Megaupload case* [en línea]. Reuters (Agencia de Noticias). <http://in.reuters.com/article/2012/09/24/newzealand-dotcom-inquiry-idINDEE88N03W20120924/> [Consulta: 15 de Diciembre de 2012]

TAJITSU, Naomi. *Megaupload's Dotcom gains access to NZ spy records* [en línea]. Reuters (Agencia de Noticias). <http://in.reuters.com/article/2012/12/06/megaupload-spying-evidence-idINL5E8N601G20121206/> [Consulta: 15 de Diciembre de 2012]