Revista de Ciencias de la Comunicación e Información. (Diciembre 1997). *Año XI* (14), 48- 52
ISSN: 0213-070-X

ECHELON, LA AMENAZA DE LA INTIMIDAD Y EL SECRETO INDUSTRIAL

Fernando Ramos Fernández

Profesor Titular de Derecho de la Información y la Publicidad.

Universidad de Vigo

0. Introducción

Woosley, que mandó la CÍA entre 1993 y 1995, aseveraba que el espionaje industrial tiene poco interés, porque tecnológicamente -dijo- muy pocas áreas de Europa superan a los Estados Unidos. Pero con la misma sinceridad reconocía que efectivamente se habían investigado las operaciones del "Air Bus" debido a que *"los amigos continentales usan del soborno*". Por último, se permitió recomendar a los europeos que fueran más serios, reformaran sus estructuras e hicieran sus empresas más seguras y competitivas*. "Entonces no tendremos que espiaros",* concluyó. Esto demuestra que, en nuestros días, por encima del propio espionaje militar, las redes dedicadas a esta actividad tienen un amplio campo en los sectores industriales, especialmente en los que compiten desde Europa con América. Echelon es la gran plataforma para esas actividades.

Nada, ni el mejor código de cifrado es invulnerable ante "ECHELON". Todos los sistemas de barrera, incluidos los más sofisticados son fácilmente burlados. Si teníamos alguna duda, la existencia de "ECHELON" ha sido confirmada no sólo por el ex director de la CIA (Agencia Central de Inteligencia), James Woosley, sino por una "arrepentida", una programadora que contribuyó a la creación de esa red. Hoy vive con falsa identidad. Pero su testimonio es demoledor.

Los europeos hemos de ser conscientes, de que todo correo electrónico y las comunicaciones realizadas por teléfono y fax pueden interceptadas de forma rutinaria por la Agencia de Seguridad Nacional de Estados Unidos, transmitiéndose estas informaciones por satélite donde se procesan, Los objetivos de vigilancia son seleccionados por las agencias de inteligencia participantes, de las cuales sólo una de ellas es europea, en principio para detectar a terroristas potenciales, sólo que el hecho es que en esos mensajes se contiene mucha información de carácter económico.

Con cierto sentido del humor, típicamente británico, se supo que la premier Margaret Thatcher llegó a espiar a sus propios compañeros de gabinete. Así lo declaró el ex espía canadiense Mike Frost a la CBS. *"La dama de hierro" quería saber lo que comentaban aquellos ministros menos conformes con su política*". Este hecho habría vulnerado las leyes inglesas que impiden espiar a sus propios ciudadanos.

Hay que definir los casos en que es lícito interceptar los mensajes privados. En este sentido, se sabe que al Parlamento Europeo se propone realizar un estudio sobre las consecuencias de orden constitucional, derivadas de la existencia de mecanismos de *vigilancia*, con particular referencia a las garantías legales de los estados de la Unión Europea, y, sobre todo, de su autonomía, tanto política como cultural, e incluso económica.

1. Lo que se sabe de Echelon

Recibido: 01/03/1997---Aceptado: 16/04/1997---Publicado: 12/11/1997

La red "ECHELON" dispone de plantas de seguimiento en todo el mundo, para el control de las comunicaciones de gobiernos, particulares y empresas. A su servicio se hallan una diversidad de aparentemente inocentes programas de Internet, cables subterráneos, una malla de fibras ópticas, redes digitales, sistemas de microondas y radio. La información mundial recogida por este sistema es procesada por diversas agencias, entre otras el FBI, que rastrea todas las conversaciones a través de potentes ordenadores para entresacar las palabras clave que pueden dar la pista de un terrorista. Pero la red sirvió para otras muchas más cosas, por ejemplo, para que los Estados Unidos ayudaran a la Gran Bretaña a ganar la guerra de las Malvinas.

Lo peor de todo este asunto no es solamente que Estados Unidos y otros países anglófonos espíen al resto del mundo, lo peor es que la malla sirve en gran medida al interés económico norteamericano y se orienta hacia el mundo industrial, tal y como evidencias las pruebas recogidas.

Poco después de concluida la II Guerra Mundial, Estados Unidos y sus principales aliados anglófilos crearon una especie de corporación del espionaje, cuyos servicios fueron rápidamente requeridos por la Agencia Central de Inteligencia. La red se fue reconvirtiendo hacia objetivos comerciales y usos civiles, tales como el espionaje industrial. El avance de las telecomunicaciones se convirtió en un aliado de la causa, Internet es su principal campo de operaciones. Todo cuanto circule por la red es vulnerable de ser espiado.

2. Los datos emergentes

Una eficiente programadora, arrepentida, ahora protegida bajo identidad falsa, que contribuyó decisivamente a crear el programa de aplicación a la red de espionaje, reveló, que, entre 1974 y 1984, la red de espionaje se dedicó a investigar a todo tipo de personas, políticos, empresas y grupos sociales. Los satélites y los programas de espionaje fueron desarrollados en la sede de Lockheed Martin (que es al tiempo el mayor proveedor de municiones para el Ejército) y en Sunnyvale (California). Otro de los elementos esenciales de la red fue el centro de escuchas más importante del mundo que se encuentra en Menwith Hill en el Reino Unido.

La red "ECHELON" es capaz de seguir y monitorizar las comunicaciones de cualquier persona en tiempo real. Entre las estaciones que reciben esta información está el cuartel general de la NASA. El caso es que tanto esta agencia como la CÍA mantienen en activo una red de espionaje ilegal que amenaza a todo el mundo. Bajo el pretexto de que la red sirve al orden social, para perseguir el delito, se espía a cualquier ciudadano y se espía a las empresas a favor de concretos y determinados intereses norteamericanos. *"Echelon es tan grande* - dice la arrepentida- *que rebasa nuestra comprensión"*.

Y para hacernos una idea de que todos somos vulnerables, se sabe que hasta el Vaticano víctima de las escuchas. Los satélites espías han recogido, entre otras muchas, las conversaciones telefónicas del romano pontífice, luego reflejadas a las antenas parabólicas en tierra que, a su vez, las reenvían a las computadoras, donde se rastrean las palabras sospechosas.

3. Apenas desarrollado

Lo peor es que la utilización de la red como instrumento al servicio del espionaje apenas se ha desarrollado. Sin embargo, el Gobierno inglés insiste: *"No se puede consentir que el terrorismo y el crimen organizado dispongan de un medio de comunicación intocable, totalmente seguro".* De todos modos, la interceptación de las comunicaciones a través de Internet requerirá - lo mismo que ocurre ahora para las escuchas telefónicas - que los servicios secretos obtengan la preceptiva autorización judicial. Ahora bien, ¿se cumple siempre este precepto? En los Estados Unidos se hallan en marcha diversas iniciativas parlamentarias en orden a disponer de una ley que armonice los sistemas de vigilancia y control de las comunicaciones, ante la diversidad de recursos que actualmente se emplean. Los grupos de defensa de los derechos civiles confían en el control judicial de los referidos instrumentos de espionaje.

Ante la respuesta de las asociaciones en defensa de los derechos civiles, el Gobierno británico alega que, pese a su propósito de introducir la mayor transparencia en la vida pública y reforzar el derecho a la libertad de expresión, los servicios de inteligencia precisan ser dotados de medios adecuados para cumplir sus misiones en orden al interés nacional. Se trata de un recurso peligroso y socorrido, usado con frecuencia para vulnerar los más elementales derechos humanos del mundo civilizado, empezando por la garantía de la propia intimidad de los ciudadanos.

4. La sensibilidad en España y el encriptado

En España, la Asociación de Usuarios de Internet es una de las instituciones españolas empeñada en la defensa de los cibernautas de nuestro país. Entre otros muchos, ha producido diversos e interesantes documentos que contienen recomendaciones y advertencias a la hora de adentrarse por este proceloso mar.

Ante la menor duda, el usuario debe abstenerse de realizar operación alguna a través de un sistema no fiable. Por el contrario, las transacciones seguras precisan, en todo caso, utilizar la confidencialidad de los datos transmitidos mediante un sistema de cifrado. La firma digital garantiza, a su vez, que el contenido de las comunicaciones no podrá ser manipulado por terceros. La verificación de la autenticidad de la firma digital, a través de entidades de certificación se garantiza la identidad de las partes que intervienen en la operación.

Con respecto al comercio electrónico, fenómeno en creciente desarrollo, la Asociación advierte que, por lo general, cuando utilizamos este servicio hemos de aportar decisivos datos personales (nombre, dirección, número de la tarjeta de crédito, etc.) que pueden ser observados y utilizados por terceros. Lo menos grave que puede ocurrir es que se estudien nuestras preferencias, lugares más visitados o demandas más frecuentes, para elaborar nuestra ficha de consumidor e inundarnos posteriormente, por las vías que sea preciso, de publicidad o promociones no deseadas ni solicitadas.

En Internet los mensajes no se transmiten directamente al receptor, sino viajan de un ordenador reconocido a otro ordenador reconocido, pasando por ordenadores intermedios, que están situados en diferentes países, que cooperan a orientar la transmisión del mensaje. El texto pasa por varios lugares no controlados por su emisor o receptor; es decir, que los mensajes pueden ser leídos e incluso alterados por terceras personas. Nuestros mensajes son muy vulnerables.

Es una flagrante vulneración de los derechos fundamentales de la persona, especialmente el de la propia intimidad y el secreto de las comunicaciones.

El uso de Internet genera otros muchos problemas, además de los referidos a la identificación de los usuarios de la red. Se trata de los relativos a la garantía de la conservación de la integridad de los mensajes s a la garantía del secreto de comunicaciones, la libertad de expresión y la vulneración del principio de seguridad jurídica que está en poder de los registros y fedatarios públicos desde el siglo pasado.

La aplicación de las técnicas criptográficas parece ser la única solución para evitar que terceros intercepten y penetren en nuestro correo electrónico. La utilización de las técnicas de cifrado de clave pública que permiten cifrar los mensajes, impedir la observación de su contenido y garantizar la integridad de los mismos utilizando la combinación de las claves pública y privada de los interlocutores, es la solución más adecuada para evitar la inseguridad de las comunicaciones que conlleva la utilización de Internet.

5. La seguridad del encriptado

De todos modos, estas medidas no satisfacen a todos, puesto que algunos entienden que las técnicas de cifrado son todavía vulnerables y que las agencias oficiales tienen enorme facilidad para el control de la intimidad de los ciudadanos corrientes.

Existen dos procedimientos de encriptación. La de carácter SIMÉTRICO requiere que los dos polos de la comunicación (el que emite y el que recibe) empleen la misma clave para codificar y descodificar el mensaje. El procedimiento ASIMÉTRICO se denomina también de claves públicas y responde al principio de pares de claves: un componente del par encripta una información que solamente el otro componente del par puede desencriptar. Una de las partes del par es solamente conocida por el propietario, en tanto la otra tiene carácter público y es divulgada ampliamente.

Dicho de otro modo, en el primer caso, clave simétrica: emisor y receptor comparten la misma clave: el documento es descifrado mediante la misma clave con que fue cifrado. En el sistema asimétrico o binario, la clave pública es de general conocimiento, pero la privada solamente la conoce la misma persona que la posee o a la que pertenece. En este sistema, la clave pública se emplea para cifrar el mensaje y la clave privada para descifrarlo.

Nuestro futuro pasa por Internet. En el año 2001, todas las escuelas de Europa deberán estar conectadas a Internet, y se espera que para 2005, todos los ciudadanos de la Unión dispongan de dominio propio.

Y el negocio de Internet seguirá aumentando.

Bibliografía

BEQUAI, A., Computer crime., Lexington, Heath Lexington Books, 1978.

BERCOVITZ, Alberto, La propiedad intelectual en las autopistas de la información. Derecho de las telecomunicaciones. (Javier Cremades, coordinador), La Ley Actualidad-Ministerio de Fomentom Madrid, 1987.

BERMEJO VERA J., Alcance y límites de las garantías jurídicas de las libertades de expresión e información, en "La protección jurídica del ciudadano". Tomo II. Madrid, Civitas, 1990.

BORRUSO, R. y TIBERI, C., L´informática per il giurista. Milán, Giuffré, 1990.

BOTANA, M., La protección de los programas informáticos en el derecho español, Volumen de Derecho Informático. Zaragoza, Facultad de Derecho, 1989.

CARRASCOSA LÓPEZ, V., Derecho a la intimidad e informática. Informática y Derecho, número 2, 1992.

CORREA, C.M. y otros, Derecho informático. Buenos Aires, Depalma, 1987.

DAVARA, M.A., Derecho informático. Pamplona, Aranzadi, 1993.

FARR, R., The electronic criminals. Nueva York, MaC GRAW-HILL Book Co., 1975.

FROSINE, V., Informatica, diritto e societá. Milán, Giuffré, 1992. .

GIANNANTONIO, E., Introduzione all´ informatica giuridica. Milán, Giuffré, 1984.

HERNANDO, I., La transmisión electrónica de datos (EDI) (perspectiva jurídica). Actualidad informátiza Aranzadi, número 10, 1994.

IMPLICACIONES SOCIO-JURÍDICAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN: Encuentros 1980-1990: Los juristas ante la revolución informática. Madrid, Citema, 1991.

-KNAPP, V., L´ applicabilitá della cibernetica al diritto. Turín, Einaudi, 1978.

LLANEZA GONZÁLEZ, Paloma, La liberación de las infraestructuras de las telecomunicaciones. Madrid, Otrosí, mayo 1996.

MASSUDA, Y., La sociedad informatizada como sociedad postindustrial. Madrid, Tecnos, 1984.

PÉREZ LUÑO, Antonio Enrique., La incorporación del convenio europeo sobre protección de datos personales al ordenamiento jurídico español. Revista de la Facultad de Derecho y Ciencias Económica y Empresariales, sobre Informática y Derecho, número 17. 1989.

Manual de informática y Derecho. Barcelona, Ariel Derecho, 1996.

SÁCHEZ BRAVO, A., El tratamiento automatizado de bases de datos en el marco de la Comunidad Económica Europea: su protección. III Congreso Iberoamericano de Informática y Derecho. Mérida, septiembre de 1992. Revista Informática y Derecho número 4, 1994.