# LO PUBLICO Y LO PRIVADO EN EL CIBERESPACIO

Nelson Manrique

**La privacidad en la comunicación informatizada es puesta en tela de juicio por las agencias de seguridad norteamericanas, que por eso mismo cuestionan el uso de códigos de encriptamiento.**

La tradición jurídica anglosajona, a diferencia de la latina, otorga un alto valor al derecho consuetudinario: la costumbre crea ley. De allí que las disputas legales tengan un gran importancia política, pues la sentencia dictada con relación a un tema legal inédito servirá como precedente al que podrán remitirse los litigantes en lo sucesivo para defender su causa.

Algunos de estos problemas vienen planteándose en el hiperespacio y han llegado hasta los tribunales. En los más importantes viene dándose un sordo enfrentamiento entre las agencias de seguridad norteamericanas -particularmente el FBI- y los organismos empeñados en la defensa de los derechos ciudadanos en la realidad virtual creada por las nuevas tecnologías.

Uno de los temas más importantes que así viene disputándose es el relativo a la seguridad nacional y el derecho a la privacidad de los ciudadanos.

## Hacking y agencias de seguridad

Los **hackers** pueden ser clasificados de diversas maneras. Una de las más gráficas distingue, en primer lugar, a los **snoopers** (fisgones), aficionados que husmean en las líneas y que eventualmente por un golpe de suerte pueden entrar en líneas protegidas. En segundo lugar, los **hackers** individuales, por lo general bastante individualistas, que trabajan para sí y sin mayor contacto con otros miembros del gremio; con motivaciones que van desde la curiosidad y el desafío intelectual que supone el **hacking** hasta la búsqueda de beneficios económicos. En tercer lugar, los **hackers** organizados, que suelen combinar la potencia de cálculo de sus computadoras enlazadas en red para realizar tareas complejas. La más espectacular fue el desciframiento de la clave 129-RSA, realizada por once mil computadoras trabajando en equipo.

En 1977 Whinfield Diffie y Martin Hellerman publicaron un artículo en **Scientific American** en el que presentaban un sistema de encriptación que habían patentado, que usaba 129 dígitos.

En su ensayo incluyeron un mensaje cifrado, desafiando al mundo académico a descifrarlo, tarea que, opinaban, demoraría millones de años. En 1993 un grupo de expertos combinó sus habilidades y la potencia de cálculo de sus computadoras enlazadas y lo descifró en menos de un año. Lo que Diffie y Hellerman no tuvieron en cuenta fue el carácter exponencial del incremento de la capacidad de cálculo de las computadoras, que hizo que la longitud de su clave fuera insuficiente. De hecho hoy se considera que sólo son seguros los programas de encriptamiento que están por delante de la capacidad de cálculo disponible.

**La guerra de las claves**

Así llegamos a las agencias de criptoanálisis: organizaciones secretas que a su vez pueden ser públicas o privadas, cuya importancia merece un análisis más detallado. Estas agencias disponen de tecnología militar muy sofisticada para realizar su trabajo. Un ejemplo es el sistema TEMPEST -Transient Electromagnetic Pulse Emanation Standard-, mencionado en el memorándum NACSIM 5100A de la National Security Agency (NSA, Agencia de Seguridad Nacional), que es capaz de reconstruir el contenido de una pantalla de computadora desde un kilómetro de distancia estudiando las frecuencias de radio que emite el monitor y que a menor distancia puede reconstruir inclusive el contenido del disco duro.

Para proteger la información contenida en las computadoras de las intrusiones suelen utilizarse básicamente dos métodos: 1) los **firewalls** (cortafuegos), que son sistemas perimetrales que tratan de impedir la penetración de fisgones a través de las redes en la computadora; y 2) la encriptación de la información. En este último caso, se convierte el texto original (**plaintext**) en un texto cifrado (**cyphertext**) ininteligible para quien no posea la clave adecuada para descifrarlo. Esta última puede ser una clave simétrica, si se usa una sola para encriptar un mensaje y para desencriptarlo, o una clave asimétrica, si se emplean claves distintas para encriptar y desencriptar; éstas son las más seguras y son las que actualmente se emplean en el ciberespacio.

En los Estados Unidos existe una importante controversia con relación al **software** de encriptamiento. Por una parte, los organismos defensores de los derechos cívicos están por la difusión de su empleo entre los usuarios, como un medio de defender la privacidad de su información y sus comunicaciones. Pero las agencias de seguridad se oponen por razones comprensibles, dado el tipo de actividades que realizan. Según el FBI y la National Security Agency, los programas de encriptamiento permiten a los criminales, a los terroristas y a los gobiernos extranjeros hacer circular libremente sus comunicaciones, impidiendo que los espías locales puedan descifrarlos. Las leyes norteamericanas prohiben la exportación de los programas informáticos de encriptamiento sin una licencia especial, que es la misma que se otorga a la exportación de municiones.

**Cuando se escapó el genio de la botella**

La controversia entre los partidarios y los detractores de la difusión de las técnicas de encriptamiento dejó de ser teórica cuando hacia julio de 1990 empezó a circular en Internet el programa PGP -**Pretty Good Privacy**[1]- elaborado por Philip Zimmermann, un experto en seguridad informática. Zimmermann es un activista antinuclear arrestado hasta en dos ocasiones y la sospecha de haber puesto su programa en Internet le valió ser acusado de haber violado las leyes de programas de encriptación, un cargo que podía acarrearle 51 meses de prisión.

El PGP está elaborado con una tecnología matemática muy sofisticada y es indescifrable con la capacidad de cálculo actualmente disponible en las computadoras. Su complejidad matemática no es problema para los usuarios, pues el programa se instala en la computadora que lo maneja automáticamente y la clave es protegida por una contraseña administrada por el usuario. Puede comprenderse la indignación de las agencias de seguridad que han perdido la capacidad de intervenir la correspondencia de quienes lo utilizan.

La elaboración del PGP le tomó a Zimmermann seis meses, trabajando doce horas diarias. Según explicó a un reportero del **Wall Street Journal**[2], su motivación fue cerrar el paso a una ley que venían impulsando el FBI y la NSA, que debía prohibir la elaboración de programas seguros de encriptación y obligar a los fabricantes de computadoras a construirlas de tal manera que permitieran descifrar los códigos de seguridad que se emplearan en lo sucesivo.

En 1990 Zimmermann decidió «inocular el cuerpo político» para inmunizarlo frente a los intentos gubernamentales de intrusión en las comunicaciones, fabricando un programa indescifrable que pudiera ser utilizado por cualquiera. Sin duda lo logró: según Stephen Walker, un experto en criptografía que trabajó en la National Security Agency y ahora es presidente de la compañía Trusted Information Systems Inc., la disponibilidad global de programas de encriptación distribuidos por Internet «hace de los controles de exportación una farsa». Walker afirma conocer funcionarios de gobiernos europeos que usan el PGP para proteger sus correos electrónicos personales.

El intento de las agencias de seguridad norteamericanas provocó el rechazo masivo tanto de los usuarios de computadoras cuanto de las empresas del ramo, y finalmente fracasó[3].

---

[1] El nombre es un homenaje a un popular programa radial denominado «**Pretty Good Grocery**».

[2] **The Wall Street Journal**, Vol. LXXV, No. 138, jueves 28 de abril de 1994.

[3] Un intento similar fue impulsado por el gobierno de EEUU cuando pretendió imponer a las empresas incorporar a sus máquinas el «**Clipper chip**», que constituiría una suerte de llave de seguridad de las

Recientemente Zimmermann ha sido absuelto de los cargos en su contra. Ante la acusación del FBI de difundir una tecnología que impedirá a la policía penetrar los mensajes cifrados de los delincuentes, su defensa ha sido impecable: «si la privacidad está fuera de la ley, sólo los delincuentes gozarían de seguridad»[4].

La situación para las agencias de seguridad de EEUU es gráficamente explicada por Leonard Mikus, presidente de ViaCrypt, una compañía de Fénix que vende una versión de PGP en $100 en EE.UU.: «El genio está fuera de la botella». Y una vez que el genio ha escapado, no hay cómo volver a meterlo...

**El ubicuo programa PGP**

El artículo del **Wall Street Journal** citado líneas arriba enumera algunos de los usos que que vienen dándose al PGP: protección de las comunicaciones entre diseñadores de **software** y de autores literarios que se comunican con sus editores, entre científicos interesados en defender la confidencialidad de sus descubrimientos para evitar que les roben sus derechos de propiedad intelectual, entre personas y empresas preocupadas por garantizar la seguridad de las transacciones comerciales que realizan usando tarjetas de crédito, etc.

Aún más importante es el uso que le dan personas como Daniel Salcedo, quien trabaja en el Human Rights Project of the American Association for the Advancement of Science en Washington y enseña a los activistas de su organización que laboran en El Salvador y Guatemala a usar el PGP.

«En este trabajo, una gran cantidad de personas ha sido muerta», dice para explicar la importancia que tiene el disponer de sistemas de encriptamiento seguros.

El PGP es también utilizado por los rebeldes que combaten el régimen de Birmania.

Antes de que se generalizara el uso del PGP, según el testimonio del escritor Alan Dawson, «la captura de documentos tuvo como resultado directo arrestos inclusive de familias enteras, su tortura y muerte.»

Naturalmente la opinión de los investigadores de las agencias de seguridad es diferente. Ellos opinan que el PGP y otros sistemas de encriptación ayudan a los criminales.

---

computadoras, con una copia que sería retenida por el gobierno para fisgonear en el contenido de las computadoras con la autorización de una corte judicial.

[4] Rais Busom: «La seguridad en Internet». Madrid, **PC World España**, mayo de 1996, p. 244.

William Spernow, un especialista en crimen por computadora, predice que en dos años éstos encriptarán rutinariamente su información, lo que podría ser el fin de la especialidad forense en el cómputo. Los narcotraficantes en Miami están encriptando su información. Se han producido casos de defraudación fiscal mediante el empleo de juegos dobles de libros contables, con el libro que lleva la contabilidad real encriptado, etc.

Pero no sólo las agencias de seguridad gubernamental están disgustadas. También son varias las compañías a las que no les hace gracia el empleo del **software** de encriptación, porque se sienten con derecho a revisar el correo electrónico de sus empleados.

Zimmermann lamenta el uso delictivo de encriptación, pero cree que el beneficio de proveer de privacidad electrónica a todos excede largamente los costos que esto acarrea: «Es imposible obtener privacidad verdadera en la edad de la información sin una buena criptografía», sostiene.

Para él el «quid» del asunto es que la encriptación computarizada «es una tecnología que, para variar, beneficia las libertades civiles», a diferencia de aquéllas que han favorecido a las agencias de seguridad a costa de los derechos de los ciudadanos, como las que hicieron indetectables las intervenciones teléfonicas.

Mientras tanto, varios **hackers** hacen una forma de propaganda singular a los sistemas de encriptamiento: penetran en los sistemas informáticos de los usuarios dejándoles un mensaje que, más o menos, dice así: «Si yo he podido hacerlo, ¿no cree que el gobierno también lo está haciendo?»