

# ESPIONAJE EN EL CIBERESPACIO.

*Alvaro A. Sánchez Bravo.*

*Doctor en Derecho.*

*Profesor de Filosofía del Derecho de la Universidad de Sevilla.*

*Profesor del Instituto Andaluz Interuniversitario de Criminología ( Sevilla).*

## 1. INTRODUCCIÓN.

Internet se ha consolidado actualmente como uno de los símbolos emblemáticos de nuestra realidad, hasta el punto de constituir una de los referentes de lo que hoy se denomina “sociedad de la información”<sup>1</sup>.

Es el resultado de un proceso tecnológico, impulsado por el desarrollo de las telecomunicaciones, que permite una difusión de enormes cantidades de información, en tiempo real, y con un grado de interconexión planetaria.

Pero, como señaló premonitoriamente Pérez Luño, el progreso tecnológico no puede considerarse de manera ideal, pues junto a innegables progresos y mejoras, ha puesto en evidencia fenómenos de agresión a los derechos y libertades de los ciudadanos<sup>2</sup>. Pues, como continua señalando el profesor de la Hispalense, “en las sociedades informatizadas del presente el poder no reside ya en el ejercicio de la fuerza física, sino en el uso de informaciones que permiten influir y controlar las actividades de los ciudadanos. De ahí que las posibilidades de intercambio en los procesos sociales, económicos y políticos se determinen realmente por el acceso a la información. La información deviene poder y ese poder se hace decisivo cuando transforma informaciones parciales y dispersas en informaciones en masa y organizadas”<sup>3</sup>.

De todos es conocido como la Red presenta un alarmante déficit de seguridad<sup>4</sup>, y se ha convertido en instrumento, en numerosas ocasiones contundentemente eficaz, para la realización o aseguramiento de diversas actividades delictivas<sup>5</sup>. En realidad, en los últimos tiempos, las tensiones a escala internacional han supuesto un recrudecimiento de los ataques contra los sistemas de información y, de manera concreta, contra los sitios Internet.

Todo ello ha movido a numerosos estados y organizaciones internacionales ha desarrollar propuestas legislativas y Convenios que prevengan y luchan contra esta amenaza, cuya extensión real se desconoce.

---

<sup>1</sup> SANCHEZ BRAVO, A., *Internet y la sociedad europea de la información: implicaciones para los ciudadanos*, Publicaciones de la Universidad de Sevilla, 2001.

<sup>2</sup> PEREZ LUÑO, A.E., “La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo”, en *Anuario de Derechos Humanos*, núm. 4, 1986-87, p. 259.

<sup>3</sup> PEREZ LUÑO, A.E., “Nuevos derechos fundamentales de la era tecnológica: la libertad informática”, en *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989-90, p. 172; y *Derechos Humanos, Estado de Derecho y Constitución*, 7ª edic., Tecnos, Madrid, p. 347.

<sup>4</sup> SANCHEZ BRAVO, A. “Una política comunitaria de seguridad en Internet”, en *Diario La Ley*, núm. 5414, 8 de noviembre de 2001.

<sup>5</sup> SANCHEZ BRAVO, A. “El Convenio del Consejo de Europa sobre cibercrimen: control vs. libertades públicas”, en *Diario La Ley*, núm.5528, 22 de abril de 2002.

Las iniciativas del Consejo de Europa <sup>6</sup>, de la Comisión Europea <sup>7</sup> y de otras organizaciones internacionales <sup>8</sup>, así como de numerosos Estados <sup>9</sup> son buena muestra de esta inquietud.

No obstante, esta preocupación se ha resuelto, casi generalizadamente, en una ampliación de las facultades investigadoras y represivas de las agencias policiales y de seguridad, con el resultado de una clara desprotección para los ciudadanos frente a las investigaciones prospectivas e intrusivas de nuestras comunicaciones electrónicas <sup>10</sup>.

La intimidad de los ciudadanos, y no sólo de los usuarios de la Red, está en peligro, sobre todo a raíz del 11 de septiembre, donde con el apoyo de una opinión pública conmocionada y aterrorizada, se ha dado la luz verde necesaria para impulsar todo un complejo sistema, al que ya se califica, sin pecar de hiperbólico, de *espionaje digital* <sup>11</sup>.

Pero los riesgos no derivan sólo de unas legislaciones represivas o insensibles a la protección de los derechos de los ciudadanos, sino que cobra verdadera carta de naturaleza cuando nos encontramos con la existencia de redes de espionaje mundial con capacidad para inmiscuirse en los sistemas de comunicaciones, poniendo en riesgo la intimidad de los ciudadanos; amén de sus implicaciones políticas y económicas a escala global.

A la consideración de dichas amenazas para las libertades, dedicaremos nuestras siguientes reflexiones.

---

<sup>6</sup> <http://conventions.coe.int/Treaty/FR/projets/FinalCybercrime.htm> La Convención fue abierta a la firma el día 23 de noviembre de 2001 en Budapest. Firmaron 26 Estados Miembros del Consejo de Europa: Albania, Alemania, Armenia, Austria, Bélgica, Bulgaria, Croacia, Chipre, España, Estonia, Finlandia, Francia, Grecia, Holanda, Hungría, Italia, Moldavia, Noruega, Polonia, Portugal, Reino Unido, Rumania, Suecia, Suiza, la "ex república yugoslava de Macedonia", y Ucrania. Canadá, Estados Unidos, Japón y Sudáfrica, que participaron en su elaboración, han firmado igualmente la Convención. Malta ha firmado el convenio en Estrasburgo el 17 de enero de 2002

<sup>7</sup> Propuesta de Decisión-Marco del Consejo relativa a los ataques de los que son objeto los sistemas de información, COM(2002) 173 final. 2002/086 (CNS), Bruselas, 19.04.2002.

<sup>8</sup> Naciones Unidas elaboró un "Manual sobre la prevención y el control de la delincuencia informática", que se ha actualizado recientemente. En 1983 la OCDE inició un estudio sobre la posibilidad de aplicar a escala internacional y armonizar los derechos penales para abordar el problema del abuso informático o de la delincuencia informática. En 1986, publicó el informe "Delincuencia informática: Análisis de las medidas jurídicas", donde se examinaban las leyes y propuestas existentes para la reforma en varios Estados miembros y se recomendaba una lista mínima de abusos que los países deberían prohibir y penalizar con leyes penales. Finalmente, en 1992, la OCDE elaboró un conjunto de directrices para la seguridad de los sistemas de información, que deberían en principio proporcionar una base sobre la cual los Estados y el sector privado pudieran construir un marco para la seguridad de los sistemas de información.

<sup>9</sup> De todos es sabido como a raíz de los atentados terroristas del 11 de Septiembre en EEUU se ha producido una oscilación casi universal hacia posturas que postulan una intervención de Internet, y un control sobre los usuarios y sobre la información que envían o consumen.

Así, con motivo de la aprobación en el Senado norteamericano de la nueva ley antiterrorista que limitará los poderes en la Cámara, una de las enmiendas de urgencia impulsadas tras los atentados permitiría a la fiscalía instalar en los proveedores de acceso a Internet sistemas de vigilancia de los servicios de mensajería electrónica. De hecho, unos horas después de los atentados agentes de la Oficina Federal de Investigación (FBI) se presentaron en las oficinas de los proveedores AOL, Earthlink y Hoptmail para instalar en sus servidores el programa "Carnivore", que permite interceptar las comunicaciones de sus clientes.

<sup>10</sup> <http://www.delitosinformaticos.com/articulos/102366322783568.shtml>

<sup>11</sup> NARRO, I., en <http://www.iblnews.com/news/noticia.php3?id=36294>

## 2. LA RED ECHELON.

“...no hay ninguna razón para seguir dudando de la existencia de un sistema de interceptación de las comunicaciones a nivel mundial en el que participan los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda...”. Con estas contundentes y esclarecedoras palabras se pronunció el Parlamento Europeo <sup>12</sup> sobre lo que ya es conocido coloquialmente como el sistema de interceptación; es decir, de espionaje, ECHELON <sup>13</sup>.

Este sistema de espionaje se diferencia de otros sistemas de información e inteligencia en dos características que no deben ser obviadas:

- Su capacidad para ejercer un control simultánea de todas las comunicaciones. Todo mensaje enviado por fax, teléfono, Internet o e-mail, con independencia de su remitente, puede captarse mediante estaciones de interceptación de comunicaciones, lo que permite conocer su contenido <sup>14</sup>.

- Se trata de un sistema que funciona a escala mundial gracias a la colaboración e interacción de los Estados *supra* citados, lo cual posibilita una vigilancia a nivel mundial de las comunicaciones por satélite. Poniendo en común iniciativas, recursos técnicos y lógicos, costes y objetivos, consiguen cubrir todo el planeta.

Pero, como señala el propio Parlamento Europeo, “los posibles peligros que un sistema como ECHELON encierra para la esfera privada y la economía no sólo derivan del hecho de que se trate de un sistema de interceptación especialmente poderoso; más bien se deriva de 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. Así, la persona objeto de observación, por ser extranjera para el país observador, no dispone de ninguna clase de protección jurídica intraestatal. Por ello, cada persona está en situación de completa indefensión frente a este sistema.” <sup>15</sup>.

Para entender, no obstante, el alcance real de esta red de espionaje creo necesario abordarlo desde una triple perspectiva, que vendrá a responder a las cuestiones más relevantes en torno a su funcionamiento, objetivos y, sobre todo, efectos sobre los derechos y libertades de los ciudadanos.

### 1. Funcionamiento de Echelon.

Echelon funciona como un *sniffer*, rastreando y analizando las comunicaciones, recogiendo información en forma de paquetes de datos, que se producen dentro de la Red, atendiendo a una serie de claves preprogramadas. Cuando la información ha sido

---

<sup>12</sup> Parlamento Europeo. **INFORME** sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON), final A5-0264/2001, 11 de julio de 2001.

<sup>13</sup> Echelon se desarrolla en el marco del Convenio UKUSA firmado en 1948 por el Reino Unido, Estados Unidos, Australia, Canadá y Nueva Zelanda, con el objetivo de reforzar la cooperación ya iniciada durante la Segunda Guerra Mundial. Hay que trasladarse al verano de 1940, tras la caída de Francia, cuando los británicos se hacen con *Enigma*, maquina capaz de descifrar los códigos secretos alemanes. Los éxitos de Enigma en la interceptación de mensajes y comunicaciones alemanas lleva a un acuerdo entre Reino Unido y Estados Unidos para compartir sistemas y técnicas criptográficas. Dicho acuerdo se reforzaría durante la Guerra del Pacífico y desembocaría en 1948 en el acuerdo UKUSA, por el cual los países citados acordaban poner en común sus sistemas de información y se dividían el mundo en zonas de control y espionaje electrónico. Cfr. EL PAIS, jueves 6 de julio de 2000, p. 5.

<sup>14</sup> Parlamento Europeo. **INFORME...**, cit., p. 28.

<sup>15</sup> Parlamento Europeo. **INFORME...**, cit., p. 29.

recopilada, el sistema indexa, selecciona y discrimina las palabras gracias a un “diccionario” que incorpora. Diccionario que, en realidad, no es más que una compleja red de ordenadores encargados de realizar un estudio posterior de la información recopilada, atendiendo a una serie de palabras claves, direcciones, encaminadores..., con el objetivo de discriminar la información útil, de aquella irrelevante a los efectos de espionaje<sup>16</sup>.

El *modus operandi* consiste en la interceptación a escala mundial de las comunicaciones por satélite, pero dado que en las regiones con densidad muy elevada el porcentaje de aquellas es muy elevada, lo que conlleva que no puedan interceptarse desde estaciones terrestres, se procede también interviniendo cables e incluso ondas, todo ello a través de una extensa red planetaria de estaciones de interceptación, de cuya existencia, e incluso denominación, ha quedado diáfana constancia<sup>17</sup>.

## 2. Objetivo.

El espionaje no es una cuestión novedosa, constituyendo incluso el elemento articulador de jugosas intrigas literarias y cinematográficas que a todos nos han entretenido, dado el halo de misterio que las rodean. Siendo prosaicos, todos los países necesitan servicios de inteligencia – espías – para garantizar la seguridad y los intereses nacionales. Junto a informaciones accesibles al público, existe otra de especial importancia, que los servicios secretos deben “apropiarse”<sup>18</sup>.

Así, respecto a Echelon, parece quedar claro como el objetivo de la red de la interceptación de las comunicaciones, privadas y económicas, no militares.

Especialmente importante, en lo que respecta a Europa y su sector industrial es la actividad desplegada por los servicios de inteligencia de los Estados Unidos, que no sólo informan de la situación económica general, sino que, amparándose en la lucha contra la corrupción, se instrumentan para espiar a la competencia y controlan a las empresas extranjeras a fin de lograr ventajas competitivas<sup>19</sup> para las empresas nacionales<sup>20</sup>. El informe del Parlamento Europeo ilustra un buen número de estos supuestos, bien conocidos por todos<sup>21</sup>.

## 3. La vulneración de los derechos de los ciudadanos.

Amparados en fines de persecución criminal, todos los Estados prevén la posibilidad de vulnerar los derechos a la intimidad y al secreto de las comunicaciones, con el objetivo de perseguir el delito, mantener la paz y proteger la seguridad del Estado<sup>22</sup>.

Ahora bien, la actividad de los servicios de información no puede ser ilimitada. La cacareada defensa de la seguridad nacional no puede devenir habilitación para el

<sup>16</sup> [http://www.yupimnsn.com/tecnologia/leer\\_articulo.cfm?article\\_id=27340](http://www.yupimnsn.com/tecnologia/leer_articulo.cfm?article_id=27340)

<sup>17</sup> Parlamento Europeo. **INFORME...**, cit., pp. 55-63, y los enlaces allí indicados.

<sup>18</sup> “El espionaje no es más que el robo organizado de información”. Cfr. Parlamento Europeo. **INFORME...**, cit., p. 30.

<sup>19</sup> El espionaje, en este sector, se refiere a la adquisición de informaciones que mantienen en secreto las empresas. Cuando el agresor es una empresa de la competencia, se habla de espionaje competitivo. Cuando el agresor es un servicio de inteligencia estatal, se habla de espionaje económico.

<sup>20</sup> Se calcula que esta vigilancia proporciona a las empresas norteamericanas hasta 7000 millones de dólares de ganancias en los contratos.

<sup>21</sup> Parlamento Europeo. **INFORME...**, cit., pp. 110-114.

<sup>22</sup> Tal y como informó Europa Press, responsables de agencias policiales y aduaneras de la Unión Europea responsables de labores de inteligencia se reunieron en Madrid, entre los días 21 a 24 de enero de 2002 para estudiar mecanismos jurídico-legales para la interceptación de comunicaciones vía satélite o a través de Internet en el campo de la lucha contra el crimen organizado. Cfr. [Delitosinformaticos.com/noticias/21-01-02](http://Delitosinformaticos.com/noticias/21-01-02).

*todo vale*; máxime cuando lo que está en juego es uno de los pilares inexcusables de los sistemas democráticos, cuales son los derechos y libertades de sus ciudadanos.

Es por ello, que resulta importante que se controle de manera global y eficaz a los servicios de información, puesto que al trabajar secretamente, ser su actividades de una duración ilimitada (al menos, no predeterminada con carácter general) en el tiempo, y contar con que los afectados nunca llegarán a enterarse de las injerencias de que han sido objeto, pueden llegar a recopilar gran cantidad de datos personales. Los riesgos para el derecho a la libertad informática de los ciudadanos son evidentes <sup>23</sup>.

Todo ello en un contexto, como es el europeo, caracterizado por un nivel de protección inadecuado, dada la disparidad de las legislaciones nacionales, tanto en lo referente a las competencias de los servicios de inteligencia, como a las condiciones de control <sup>24</sup>.

Llegados a este punto, cabe cuestionarse, ¿constituye una vulneración de nuestros derechos la existencia de un sistema mundial de interceptación de comunicaciones?.

La respuesta no puede dejar de ser positiva, y ello por que como señala el Parlamento Europeo, “Toda escucha de comunicaciones, así como la interceptación de datos mediante servicios de inteligencia con este objetivo <sup>25</sup>, es una violación grave de la intimidad de la persona. Únicamente en un “Estado policial” es admisible la escucha ilimitada por parte del Estado. En los Estados miembros de la UE, que son democracias

---

<sup>23</sup> Sobre la delimitación del derecho a la libertad informática, vid., y de entre su numerosa producción científica, PEREZ LUÑO, A.E., *Nuevas Tecnologías, Sociedad y Derecho. El impacto socio-jurídico de las N.T. de la información*, Fundesco, Madrid, 1987; “La libertad informática. Nueva frontera de los derechos fundamentales”, en la obra colectiva *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp. 185-213; “Nuevos derechos fundamentales de la era tecnológica: la libertad informática”, en *Anuario de Derecho Público y Estudios Públicos*, num. 2, 1989/90, pp. 171-195; “*Del Habeas Corpus al Habeas Data*”, en *Informática y Derecho*, num. 1, 1992, pp. 153-161; *Manual de Informática y Derecho*, Ariel, Barcelona, 1996; “Aspectos jurídicos y problemas en Internet”, en la obra colectiva, coord. Por J. De Lorenzo, *Medios de Comunicación Social y Sociedad: De información a Control y Transformación*, Consejo Social de la Universidad de Valladolid, 2000, pp. 107-134; y *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, 7ª edic., Madrid, 2001; y LUCAS MURILLO DE LA CUEVA, P., “La protección de los datos personales ante el uso de la informática”, en *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989/90, pp. 153-170; *El derecho a la autodeterminación informativa. La protección de los datos personales ante el uso de la informática*, Tecnos, Madrid, 1990; *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993; y “La construcción del derecho a la autodeterminación informativa”, en *Revista de Estudios Políticos*, num. 104, abril-junio 1999. Vid. asimismo, SANCHEZ BRAVO, A., *La protección del derecho a la libertad informática en la Unión Europea*, Publicaciones de la Universidad de Sevilla, 1998; e *Internet y la sociedad europea de la información: implicaciones para los ciudadanos*, Publicaciones de la Universidad de Sevilla, 2001.

<sup>24</sup> En Bélgica, Dinamarca, Alemania, Italia, los Países Bajos y Portugal existe una comisión parlamentaria de control que es competente para el control de los servicios de inteligencia, tanto civiles como militares. En el Reino Unido, la comisión especial de control sólo supervisa la actividad (de hecho, la más importante) de los servicios civiles de inteligencia; la actividad de los servicios de inteligencia militares la supervisa la comisión especializada de Defensa. En Austria, las dos ramas de los servicios de inteligencia son supervisadas por dos comisiones de control distintas que, de hecho, tienen la misma organización y disfrutan de las mismas competencias. En los Estados escandinavos Finlandia y Suecia, los Defensores del Pueblo asumen las tareas del control parlamentario, siendo elegidos por el Parlamento. En Francia, Grecia, Irlanda, Luxemburgo y España no existen comisiones parlamentarias específicas; las tareas de control las desempeñan, en este ámbito, las comisiones normales especializadas dentro del marco de la actividad parlamentaria general.

<sup>25</sup> Tribunal Constitucional Federal Alemán (BVerfG), 1BvR 2226/94 de 14.7.1999, apartado 187 “injerencia ya es [...] la propia interceptación, en la medida en que la comunicación se facilite al servicio federal de inteligencia y constituya la base del modelo de conceptos de búsqueda.”

consolidadas, es indiscutible que los órganos estatales deben respetar la vida privada y, por consiguiente, también deben respetarla los servicios de inteligencia, lo que, con frecuencia, se recoge así en las Constituciones de los Estados miembros. La esfera privada, por consiguiente, disfruta de una protección especial; las intervenciones se producen únicamente tras ponderar las ventajas e inconvenientes jurídicos y respetando el principio de proporcionalidad”<sup>26</sup>.

Establecido este principio general, cabe cuestionarse si en el actual *status quaestionis* se cumplen las exigencias de proporcionalidad y control exigidos para la adecuación de las actuaciones de los servicios secretos a los principios democráticos.

Todas las constituciones o la tradición constitucional de los Estados democráticos consagran el derecho a la intimidad, la discreción y el secreto postal y de las comunicaciones<sup>27</sup>. No obstante, la problemática de los derechos humanos en el ámbito de la interceptación de las comunicaciones presenta unas características especiales, dado que el ámbito de protección del derecho fundamental no comprende sólo el contenido de las comunicaciones, sino también el registro de datos ajeno a la conversación. Como ha señalado el Tribunal Europeo de Derechos Humanos, esto significa que incluso cuando los servicios de inteligencia registran datos como la hora y la duración de la comunicación, así como los números llamados, esto es una injerencia en la vida privada<sup>28</sup>.

No obstante, el derecho a la intimidad no goza de un carácter absoluto en las sociedades democráticas, por cuanto su contenido puede ser restringido, en aras de un interés prevalente.

En este sentido, y como referente inexcusable, el art. 8.2 del CEDH establece: "No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto esta injerencia esté prevista por la ley y constituya una medida que en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás"<sup>29</sup>.

Ahora bien, la apelación a la defensa de determinados valores o intereses colectivos, no debe ser óbice para un uso torticero de las habilitaciones legales<sup>30</sup>. La

---

<sup>26</sup> Parlamento Europeo. **INFORME...**, cit., p. 90.

<sup>27</sup> En el ámbito de las grandes declaraciones internacionales de derechos humanos, vid: Art. 12 de la Declaración Universal de 1948; art. 17.1 del Pacto Internacional de Derechos Civiles y Políticos de 1966; y art. 8.1 de la Convención Europea para la protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 (CEDH).

En el ámbito del Derecho Comunitario Europeo, destacan el art. 7 de la Carta de los Derechos Fundamentales de la Unión Europea; y en el núm. 6 del Título VIII del Proyecto de Constitución Europea, elaborado igualmente por el Parlamento Europeo, en su redacción de 1994. Además el TJCE ha manifestado que el respeto de la vida privada constituye un derecho fundamental protegido por el ordenamiento comunitario (Asunto C-62/90, Comisión vs. República Federal de Alemania, Rec. 1992-I).

<sup>28</sup> TEDH en su Sentencia Malone, de 2 de agosto de 1984.

<sup>29</sup> Vid. asimismo las manifestaciones del TEDH en sus Sentencias Klass y Leander (Corte Europea de Derechos Humanos, caso Klass y otros, sentencia de 6 de septiembre de 1978, serie A, núm. 28; recogida, y en trad. cast. de A.J. Martínez Higuera, por la que se cita, en *BJC. Tribunal Europeo de Derechos Humanos 1959-1983*, Secretaría General del Congreso de los Diputados, Madrid, 1984, pp. 470-485; y Corte Europea de Derechos Humanos, caso Leander, sentencia de 26 de marzo de 1987, recogida, y en trad. cast. por la que se cita, en *BJC. Tribunal Europeo de Derechos Humanos. Jurisprudencia 1984-1987*, pp. 909-932).

<sup>30</sup> Como ha señalado Rigaux, del interés general debe distinguirse claramente el interés del Estado. Mientras que el primero señala los valores comunes a la colectividad política y a la sociedad civil, valores inscritos en los textos constitucionales e internacionales, el interés del Estado señala la permanencia de las instituciones políticas y su protección frente al enemigo exterior. No obstante, cuando los detentadores del poder invocan el interés del Estado, la seguridad pública o la seguridad nacional para legitimar la limitación de determinados derechos fundamentales, están particularmente expuestos a confundir este interés con la perpetuación del

propia indefinición de los supuestos en los que es tolerable esa "limitación", coadyuva a la necesidad de una aplicación estricta de los mismos. Además los Estados no disponen de libertad para aplicar indiscriminadamente tales habilitaciones, sino que deberán, como regla general, usar el instrumento menos lesivo, y establecer unas garantías adecuadas frente a los abusos.

En este sentido si bien dichas limitaciones han de ser aceptadas, las mismas están sujetas a determinados requisitos que, ya desde lo señalado por el Convenio de 1981 del Consejo de Europa y el *Bundesverfassungsrichts* en su Sentencia sobre la Ley del Censo de Población de 1983<sup>31</sup>, pueden sistematizarse en dos ineludibles y concretas exigencias:

a. Un fundamento legal, del que pueda deducirse con claridad y de forma inteligible para el ciudadano los supuestos y el ámbito de las limitaciones, y que responda, por tanto, al imperativo de claridad normativa inherente al Estado de Derecho<sup>32</sup>.

A este respecto, el TEDH ha realizado unas importantes precisiones señalando como la expresión "prevista por la ley" indicada en el párrafo 2 del art. 8 del CEDH, implica que no basta con que la injerencia en los derechos esté prevista por una norma nacional, si no que ésta debe ser accesible al interesado, quien debe, además, poder prever las consecuencias que pueda tener para él. Además, cuando su práctica se realiza por medio de medidas secretas, que escapan al control de las personas afectadas, la misma ley debe definir el ámbito del poder atribuido a la autoridad competente con bastante claridad para proporcionar al individuo una protección adecuada contra la arbitrariedad<sup>33</sup>.

b. Ha de utilizarse el principio de proporcionalidad en la restricción de estos derechos fundamentales; es decir, que la medida sea adecuada - necesaria en una sociedad democrática - y, además, indispensable para la consecución de los respectivos y predeterminados fines. La interferencia que lleve aparejada no puede ser desproporcionada a la importancia del objeto y a las cargas que imponga al ciudadano.

El concepto de necesidad implica, según reiterada jurisprudencia del TEDH, una exigencia social imperiosa; y sobre todo, la medida tomada debe ser proporcionada a la finalidad legítima perseguida. Además, el alcance del margen discrecional que tienen las autoridades no depende solamente de la finalidad de la restricción, si no también de la naturaleza del derecho de que se trate<sup>34</sup>.

Por su parte, la regla de la proporcionalidad es de observancia obligada para proceder a la limitación de un derecho fundamental. Ello conduce a la negación de la legitimidad de aquellas limitaciones que incidan en el ejercicio de los derechos fundamentales de forma poco comprensible, de acuerdo con una ponderación razonada de bienes y proporcionada de los mismos en relación con el contenido y finalidad de la medida restrictiva<sup>35</sup>.

---

poder del que están democráticamente investidos. RIGAUX, F., "Introduction Generale", en *Revue Trimestrielle des droits de l'homme*, núm. 13 (monográfico "La liberté d'expression, son étendue et ses limites"), janvier 1993, p. 17.

<sup>31</sup> La sentencia se encuentra publicada, en trad. cast. de M. Daranas, en BJC, 1984, núm. 33, pp. 126-ss.

<sup>32</sup> PEREZ LUÑO, A.E., *La Seguridad Jurídica*, 2ª edic. revisada y puesta al día, Ariel, Barcelona, 1994.

<sup>33</sup> Sentencias, Silver y otros, de 25 de marzo de 1983; Malone, de 2 de agosto de 1984; y Leander, de 26 de marzo de 1987.

<sup>34</sup> Sentencias, Lingens, de 8 de julio de 1986; Gillow, de 24 de noviembre de 1986; y Leander, de 26 de marzo de 1987.

<sup>35</sup> GOMEZ TORRES, C., "El abuso de los derechos fundamentales", en la obra colectiva, edic. a cargo de A.E. Pérez Luño, *Los derechos humanos: significación, estatuto jurídico y sistema*, Publicaciones de la Universidad de Sevilla, Sevilla, 1979, pp. 301-332.

Por otra parte, las limitaciones del derecho no deben ser de tal calado que supongan un menoscabo de su contenido esencial. De nada sirve el reconocimiento de los derechos a favor de los ciudadanos si se limita su ejercicio de forma que, más que una limitación, debamos hablar de una derogación encubierta, de su propia naturaleza, atributos y funciones.

Ante la proliferación y constante apelación por parte de las autoridades públicas a estas limitaciones conviene insistir, siguiendo a Pérez Luño, en el carácter excepcional de estos supuestos; en que su razón de ser no puede ser otra que la conservación del orden democrático; y en que la existencia de tal motivación no puede quedar en manos de la Administración, sino que debe quedar ser reconocida por los Parlamentos como depositarios de la soberanía popular <sup>36</sup>.

#### 4. El necesario control de los servicios de inteligencia.

Como ha señalado el Parlamento Europeo, si para garantizar la seguridad nacional es necesario la interceptación de las telecomunicaciones por parte de las agencias y servicios de inteligencia, dicha posibilidad debe estar prevista en la legislación nacional de los Estados, y ser accesible para los ciudadanos, garantizando así la publicidad de la norma y su conocimiento por parte de los destinatarios (o, más bien, afectados) <sup>37</sup>

Pero de todos es sabido como la actividad de los servicios de inteligencia, se mantiene cuando menos opaca, amparada en esa confidencialidad, que sirve de banderín de enganche para justificar cualquier injerencia, por muy abusiva que ésta sea.

A ello hay que añadir la disparidad de las legislaciones nacionales, que en algunos Estados se manifiesta por la ausencia de órganos de control parlamentario.

El control se erige, por tanto, en elemento imprescindible para que la actividad de los servicios de inteligencia se adecue a los principios democráticos. Una mayor eficacia en el control, implicará una mayor garantía de legalidad de las injerencias cuando la autorización para la vigilancia de las telecomunicaciones es competencia del más alto nivel administrativo, y para su ejecución se precisa una autorización judicial previa y un órgano asimismo independiente controla la puesta en marcha de tales medidas <sup>38</sup>.

La labor de los Parlamentos nacionales en este campo resulta inexcusable. En cuanto depositarios de la soberanía, deben ser los órganos encargados de supervisar la restricción de los derechos de los ciudadanos, y conciliarlos con la necesaria garantía de la paz, la seguridad y el orden público; sobre todo, cuando en aras de la protección de estos se restringen aquéllos.

Ahora bien, el control debe ser un control específico, determinado y todo lo a fondo que sea posible. Así se evitará que las comisiones parlamentarias se conviertan en meros espectadores de actividades difusas que afectan a los ciudadanos, deviniendo meros salvapantallas de legitimidad democrática. Como ha señalado el Parlamento Europeo, deben crearse comisiones de control especiales, con una estructura formal que controle y examine las actividades de los servicios de inteligencia. Su ventaja frente a las comisiones ordinarias es que disfrutan de una mayor confianza entre los servicios secretos, ya que sus miembros están obligados a guardar silencio y sus reuniones son a puerta cerrada <sup>39</sup>.

---

<sup>36</sup> PEREZ LUÑO, A.E., "Informática jurídica y derecho de la informática en España", en *Informatica e Diritto*, 1983, nº 2, , p. 97.

<sup>37</sup> Parlamento Europeo. **INFORME...**, cit., p. 98.

<sup>38</sup> Parlamento Europeo. **INFORME...**, cit., pp. 99-102.

<sup>39</sup> Parlamento Europeo. **INFORME...**, cit., p. 101.

### 3. CARNIVORE.

“Vamos a perseguir el terrorismo en Internet, vamos a abrir sus correos electrónicos ante de que ellos los hagan, a escuchar sus mensajes telefónicos, a interceptar sus conversaciones”. Así se manifestaba Jhon Ascroft, Secretario de Justicia norteamericano tras la aprobación de la *Patriot Act*<sup>40</sup> que entre otras habilitaciones permite al gobierno el espionaje en Internet. *Carnivore* es uno de los instrumentos para la consecución de ese fin. No obstante su historia se remonta tiempo atrás.

En febrero de 1997, bajo el mandato de la Administración Clinton, el FBI<sup>41</sup> creó *Omnivore*<sup>42</sup>. Su objetivo era crear una aplicación capaz de intervenir las comunicaciones de Internet, de modo similar a como se intercepta una comunicación telefónica. Otra iniciativa pretendió incluir en varios productos de comunicación un chip llamado Clipper, que, pretendiendo ser una eficaz herramienta de protección, contenía una puerta trasera que sólo podría usarse por las autoridades para interceptar cualquier mensaje, siempre que fuera necesario por ley<sup>43</sup>. Asimismo, en 1999, la Comisión Federal de Comunicación aprobó nuevas reglas que permiten a la policía rastrear llamadas celulares.

Ese mismo año, una investigación del Centro de Información sobre la Privacidad Electrónica (EPIC)<sup>44</sup>, se descubrió que el FBI estaba interviniendo comunicaciones electrónicas. Tras estudiar el caso se demostró la realidad de *Omnivore*, y además que el mismo había mutado, transformando su capacidad rastreadora a *Carnivore*<sup>45</sup>.

Como veremos posteriormente, las enormes críticas acerca de la existencia y funcionamiento del “espía” llevaron al FBI a cambiar el nombre del programa, para hacerlo menos intrusivo, pasando a llamarse *DCSI000*.

Pero *Carnivore*, no es un hecho aislado, sino que es sólo uno de los programas que integran un programa más complejo de vigilancia del FBI denominado *Cyber Knight*, que también integra a *Magic Lantern*<sup>46</sup>.

Con *Carnivore* se ha iniciado una nueva forma de espionaje: la intervención del e-mail de individuos, algo que aparentemente no se podía hacer antes, y ello por que *Carnivore* le permite superar varias problemas que la nueva tecnología plantea al espionaje: 1) una persona puede recoger su e-mail en distintos sitios, así que no basta con intervenir su teléfono convencional; 2) las conexiones y movimientos a través de Internet utilizan vías altamente variadas, y 3) el volumen de e-mail aumenta exponencialmente<sup>47</sup>. La clave, por tanto, estará en el funcionamiento del sistema.

---

<sup>40</sup> <http://www.house.gov/judiciary/hr2975terrorismbill.pdf>

<sup>41</sup> <http://www.fbi.gov>

<sup>42</sup> *Omnivore* corría en máquinas Sun con Solaris. Como señala Casacuberta, la versión actual es para Windows NT. A partir de la documentación desclasificada, parece que *Omnivore* no era más que *Etherpekk*, que, según parece, seguiría estando en núcleo duro de *Carnivore*. Cfr. CASACUBERTA, D., en <http://www.spain.cpsr.org/boletin000c.php>

<sup>43</sup> NARRO, I., en <http://www.iblnews/noticias/>

<sup>44</sup> <http://www.epic.org>

<sup>45</sup> De *Carnivore* existen también varias versiones. Como ha señalado Casacuberta, “sabemos que una versión más antigua, la 1.2 leía “demasiadas cosas” cuando estaba en el modo grabar solamente el tráfico, así que desarrolló una versión 2.0 con “menos apetito”. Cfr. CASACUBERTA, D., en <http://www.spain.cpsr.org/boletin000c.php>

<sup>46</sup> Este macroprograma, además de recibir información, interviene en sala de chat, e-mail y mensajeros instantáneos como ICQ y Messenger. <http://www.quepasa.cl/revista/2002/04/05/t-05.04.OP.SOC.FBI>.

<sup>47</sup> <http://www.cipo.com.ar/tecnologia2/carnivore.htm>

## 1. Las “Cajas Negras”.

Carnivore es un sistema de software y hardware con capacidad para localizar y perseguir las comunicaciones de un usuario de Internet.

El sistema interviene la comunicación en un punto estratégico, como es el ISP (Proveedor de Servicio de Internet). Toda información pasa por los ISP, servidores que todos los internautas utilizamos para conectarnos a Internet. Cada palabra que escribimos o ejecutamos siempre es recogida por el ISP que nos da acceso a la Red. La *Caja Negra* del FBI se instala en el servidor del ISP. Pero además de software, el FBI incluye el hardware compuesto por una PC ensamblado en una caja modelo Rack para que pueda incorporarse fácilmente en las redes del ISP, como si fuera un concentrador o un router más, sin necesidad de dispositivos externos <sup>48</sup>.

El sistema puede copiar el e-mail de un usuario, lo cual permite que el FBI lo lea completamente, o simplemente puede registrar las direcciones del que manda y del que recibe. Pese a que existe software de codificación (encriptación), Carnivore permite registrar direcciones e identificar redes, superando técnicamente cualquier restricción. Puede incluso llegar a controlar todo el tráfico que circula por cualquiera de los protocolos utilizados en Internet.

Las discrepancias surgen, no obstante, respecto al alcance del espionaje. Según fuentes gubernamentales norteamericanas, el sistema realiza una búsqueda, única y exclusiva del usuario a investigar, autoeliminando la información que no le interesa; y no interfiriendo en los ordenadores de todos los internautas, sino sólo en los de aquellos sospechosos de infringir la ley <sup>49</sup>. Para los críticos del sistema su poder es ilimitado, suponiendo una grave amenaza para los derechos de los ciudadanos.

## 2. ¿Cómo espía Carnivore?

Carnivore “oficialmente” no realiza una captura indiscriminada de todo el tráfico que circula por un servidor, sino que se limita a mensajes dirigidos a una dirección específica y enviados desde una dirección específica. Por tanto, según siempre fuentes oficiales, no registra el contenido de los mensajes, ni de los que si o no investiga. Su *modus operandi* consistiría en la búsqueda selectiva en determinados campos (textos de chats y grupos de discusión; URL de las páginas que visita; y especialmente en los campos *de* y *para* (*to* y *from*) de los correos electrónicos que envía) mediante una selección de determinadas palabras <sup>50</sup> no sólo en inglés, sino en casi cualquier idioma..

No obstante, este último extremo es impugnado por otros expertos, que afirman que el sistema no procede a ningún filtrado de términos, no guardando relación con ningún filtrado de subversivos, sino que sólo se limita al almacenaje de datos de tráfico y/o mensajes completos de la dirección sospechosa <sup>51</sup>. Precisamente, este modo de actuar diferenciaría a Carnivore de otros sniffers, pues se trataría de un método más selectivo que, al no realizar búsquedas por términos sensibles, en el cuerpo de todos los mensajes evitaría que el tráfico capturado fuera desmesurado <sup>52</sup>.

---

<sup>48</sup> <http://www.cuyonoticias.com.ar/opinion/opinion124.htm>

<sup>49</sup> <http://www.el-mundo.es/navegante/2000/11/20/portada/974723816.html>

<sup>50</sup> Entra estas palabras estarían: *classfield, top-secret, government, restricted, data information, project, CIA, KGB, GRU, DISA, DoD, defense systems, military systems, spy, steal, warmod, terrorist, Allah, Natasha, Gregori, destroy, destruct, attack democracy, wil send, Russia, bank system, compromise, international, own, rule the world, ATSC, RTEM, ATMD, force power, enforce, sensitive directorate, TSP, NSTD, ORD, DD2-N, AMTAS, STRAP, warrior-T, presidential elections, policital, foreign embassy takeover*. Cfr. [http://www.yupimsn.com/tecnologia/leer\\_articulo.cfm?article\\_id=27375](http://www.yupimsn.com/tecnologia/leer_articulo.cfm?article_id=27375)

<sup>51</sup> Cfr., por todos, CASACUBERTA, D., cit.

<sup>52</sup> <http://www.cp.com.uy/73/carnivore73.htm>

La polémica sigue abierta, pues lo que se cuestiona, en el fondo, es el verdadero alcance del sistema, y su incidencia lesiva en los derechos de los ciudadanos. Sea como fuera los defensores de los derechos y libertades de los ciudadanos siguen reclamando un control del sistema y que se proporcione información detallada al ciudadano, de forma que pueda comprobarse que no realiza ninguna actividad contraria a los derechos de los usuarios de la Red. El FBI, por su parte, ha manifestado que Carnivore es necesario, moderado, altamente, regulado y limitado a un número reducido de sospechosos<sup>53</sup>.

### 3 ¿Cuándo puede utilizarse Carnivore?.

Cuando el FBI sospecha de una actividad ilícita, para capturar el contenido de las comunicaciones necesita la autorización de un juez federal. Una vez obtenida la autorización judicial, procederá a obtener la autorización del ISP concreto en el que instalar la “caja negra”. La cuestión a resolver, por tanto, será: ¿tienen los ISP obligación de colaborar en dicha actividad investigadora?.

La cuestión se resolvió cuando algunos ISP se opusieron a dicha instalación. Además de RMI.Net, el caso más conocido fue el de Earthlink. A requerimiento del FBI para instalar Carnivore, Earthlink se mostró dispuesto a colaborar con el FBI, pero se negó a dejarse instalar las cajas negras. Ofreció entregar los e-mails de ciertos usuarios, pero el FBI, no aceptó. El Departamento de Justicia demandó Earthlink, y el juez federal James W. MacMahon, en la ya famosa sentencia de 4 de febrero de 2000<sup>54</sup>, estableció la obligación de los ISP norteamericanos de colaborar con el FBI siempre que sea necesario. El caso nunca fue público, y solo se conoció cuando saltó a las páginas de *The Wall Street Journal*.

### 4. La verdadera extensión de Carnivore.

Las primeras noticias de la existencia de Carnivore movilizaron a un sinnúmero de grupos de defensa de las libertades civiles, de la confidencialidad de las comunicaciones electrónicas, y a internautas ha denunciar la existencia y el secretismo con el que parecía actuar el sistema. Anteriormente hemos considerado las opiniones que el FBI tiene al respecto, señalando siempre lo limitado, necesario y respetuoso de su actuación.

Sin embargo estos grupos, a cuya cabeza cabe situar en justicia a EPIC, reivindicaron desde el principio, que se diera a conocer el Código Fuente de Carnivore para que comprobarse su legalidad. El FBI naturalmente se ha negado sistemáticamente alegando que la publicación del mismo permitiría a los criminales elaborar formulas para evitar la interceptación de sus comunicaciones.

No obstante, las constantes demandas de EPIC consiguieron que el Congreso de Estados Unidos obligara al FBI a entregar documentos, entre los que se incluye un informe en el que se reconoce que el “Programa tiene capacidad para capturar información sin necesidad de utilizar filtros, y que se guarda en los discos duros de los internautas”<sup>55</sup>.

Las demandas de EPIC sirvieron para constatar de manera fehaciente que Carnivore existe, y arrojaron luz sobre su funcionamiento. No obstante, la información desclasificada, 750 páginas<sup>56</sup>, sigue sin arrojar luz sobre las verdaderas intenciones y extensión del sistema. Por si fuera poco, muchos párrafos han sido cercenados, emborronando chapuceramente con tinta aspectos considerado esenciales por el FBI.

---

<sup>53</sup> <http://www.cuyonoticias.com.ar/opinion/opinion124.htm>

<sup>54</sup> El texto de dicha sentencia puede verse en [http://www.epic.org/privacy/carnivore/cd\\_cal\\_order.html](http://www.epic.org/privacy/carnivore/cd_cal_order.html)

<sup>55</sup> <http://www.el-mundo.es/navegante/2000/11/20/portada/974723816.html>

<sup>56</sup> Estos documentos pueden obtenerse en [http://www.epic.org/privacy/carnivore/foia\\_documents.html](http://www.epic.org/privacy/carnivore/foia_documents.html)

La situación parece haber variado sustancialmente, por cuanto el 25 de marzo de 2002, el juez federal del Distrito de Columbia, James Robertson <sup>57</sup>, ha ordenado al FBI dar a conocer los detalles de funcionamiento del sistema Carnivore.

A requerimiento del EPIC el juez ha ordenado al FBI dar a conocer todos los expedientes relativos a los sistemas de interceptación y/o revisión de mensajes de correo electrónico. Se excluyen, de este modo, los argumentos del gobierno que amparándose en que la tecnología empleada es secreto de Estado, se negaba a facilitar información. Además, el juzgador establece como la información hasta entonces suministrada por el FBI es insuficiente, pese a que la agencia federal consideraba altamente cumplida su obligación de información, amparándose en el Informe Illions <sup>58</sup>

Como ha señalado David Sabel, portavoz del EPIC, “como crece la posibilidad de que el uso de este tipo de técnicas aumente, es cada vez más importante que conozcamos más de ella, de cómo se están utilizando y de cómo está considerando el Departamento de Justicia las cuestiones legales al respecto” <sup>59</sup>.

El Tribunal dio de plazo hasta el 24 de mayo para que se pusieran de manifiesto los extremos ordenados en la Sentencia. El día de expiración del plazo el FBI dio a conocer nuevos documentos secretos. Su alcance real se desconoce en su totalidad en la fecha de hoy, pero como ha señalado nuevamente David Sobel, “estos documentos confirman lo que hemos creído muchos de nosotros durante dos años. Carnivore es una herramienta de gran alcance, pero torpe, que pone en peligro a ciudadanos inocentes. Ahora hemos aprendido que su imprecisión puede también comprometer investigaciones importantes, incluyendo las relacionadas con terrorismo” <sup>60</sup>. Es por ello que se ha pedido la suspensión del sistema hasta que todas las cuestiones relativas a su funcionamiento y extensión sean resueltas. El curso de los acontecimientos nos hace ser muy pesimistas respecto a que una medida de ese calibre vaya a adoptarse.

Pese a todo, la lucha de EPIC y otras organizaciones de defensa de las libertades tienen el enorme valor de la insumisión frente al poder intrusivo descontrolado del Estado, y supone una llamada atención para que la ciudadanía exija el control democrático de todas las actividades estatales, incluidas las relativas a la seguridad.

#### 5. 11 de Septiembre.

Los atentados del ya desgraciado 11 de septiembre de 2001, han provocado, además de una nueva situación política internacional, que la idea de seguridad se consolide como uno de los elementos más relevantes, sino el que más, para la estabilidad de los Estados.

Los fallos en los sistemas de seguridad y espionaje han puesto de manifiesto como los mecanismos estatales de defensa no estaban al nivel que cabría esperar. La solución podía haber venido por una redefinición de los actuales sistemas, pero se ha optado por el endurecimiento de las medidas investigadoras y el espionaje.

---

<sup>57</sup> <http://www.techlawjournal.com/courts/epicvdoj/20020325order.asp>

<sup>58</sup> El Informe Illions, , realizado por el Instituto Illions de Tecnología, fue un informe encargado por el Departamento de Justicia par que hiciera un estudio sobre “Carnivore”. Después de dos meses de estudio se llegó a la conclusión de que el sistema no se extralimitaba, no siendo lesivo para los ISP. Sin embargo, noticias contrastadas han puesto de manifiesto como el proyecto original se había encargado a varias universidades, quienes rehusaron el encargo dadas la restricciones que se le imponían.

<sup>59</sup> <http://www.noticiasdot.com/publicaciones/2002/0402/0505/noticias0504-14.htm>

<sup>60</sup> [http://www.epic.org/privacy/carnivore/5\\_02\\_release.html](http://www.epic.org/privacy/carnivore/5_02_release.html)

Así, horas después de los atentados, el FBI solicitó a los ISP, proveedores de servicios web y correo electrónico que instalaran Carnivore, con el objetivo de recopilar datos acerca de los implicados en los atentados <sup>61</sup>.

Pero, tras la aprobación del *USA Patriot Act* <sup>62</sup>, Carnivore se ha visto potenciado de manera exponencial, al ampliar las competencias de las autoridades gubernamentales para intervenir líneas telefónicas y controlar el tráfico de Internet. En concreto, la norma amplía el estatuto *pen register*, para incluir la comunicaciones electrónicas y la navegación por Internet <sup>63</sup>. De este modo podrán obtenerse fácilmente datos sobre la actividad de los internautas al acceder a información privada en lugar de direcciones IP, pues éstas son a la Red lo que los números telefónicos <sup>64</sup>.

Pero lo más grave es que se elimina la autorización judicial previa para la interceptación. Cualquier fiscal podrá ordenar este tipo de intervención para rastrear la navegación de sospechosos o las direcciones de envío de sus e-mails. Los agentes tendrán un plazo de 48 horas para comunicarlo a la autoridad judicial competente. Durante ese plazo libertad absoluta, pues tampoco se indica que tecnología va a utilizarse, que amplitud tendrá la investigación, ni lo que se comunicará al juez <sup>65</sup>.

La actitud de los ISP ha variado también sustancialmente, bajo el temor de ser estigmatizados como antipatriotas. A las acciones de las primeras horas, se ha unido el total colaboracionismo de los servidores en la "lucha contra el mal". Así se ha denunciado como numerosas compañías han violado su política de privacidad con el fin de colaborar con las autoridades policiales. America Online ha reconocido su colaboración, si bien ha manifestado "tener un equilibrio muy responsable y práctico entre proteger la privacidad de sus miembros y proteger su seguridad" <sup>66</sup>. Earthlink, (la misma que tiempo atrás se había opuesto firmemente a instalar Carnivore) también manifestó su colaboración con el FBI desde el mismo 11 de septiembre. Por su parte, Microsoft colabora intensamente al someter a una profunda búsqueda en su servidor Hotmail de cuentas que contengan determinadas palabras o textos en árabe <sup>67</sup>.

Estas medidas, reducidas inicialmente a los Estados Unidos, pretenden imponerse a nivel global. Así, ha trascendido como el pasado 16 de octubre el Presidente Bush envió una carta al Presidente de la Comisión Europea, Romano Prodi, en la que "solicitaba" que la Unión Europea revisase su legislación sobre protección de datos para que las fuerzas y agencias de seguridad tengan acceso a ellos con fines de "investigación criminal" <sup>68</sup>. A nivel Europeo, no han parecido tener acogida estas solicitudes, si bien las propuestas legislativas en curso <sup>69</sup> parecen caminar en una línea

---

<sup>61</sup> Parece que Carnivore funcionó a la perfección: la información recopilada demostró que los autores de los atentados coordinaron su operación a través de terminales públicos de Internet e incluso adquirieron sus pasajes aéreos a través de "Travelocity". Cfr. <http://www.quepasa.cl.revista/2002/04/05/t-05.04.OP.SOC.FBI.html>

<sup>62</sup> Legislación antiterrorista que permite, además de interceptar las comunicaciones, la detención durante seis días sin cargos en caso de sospechosos inmigrantes, los registros secretos de domicilios y otras medidas, como permitir un censo de ADN de todos los reclusos.

<sup>63</sup> El dispositivo *pen register* es un dispositivo de seguimiento electrónico que se conecta a una línea de teléfono para registrar los números telefónicos marcados.

<sup>64</sup> <http://www.elrinconcito.com/noticias/not64.htm>

<sup>65</sup> [http://www.bravu.net/portadaprincipal/cont\\_rede/manifiesto/paginas/r\\_2.html](http://www.bravu.net/portadaprincipal/cont_rede/manifiesto/paginas/r_2.html)

<sup>66</sup> <http://www.comunica.org/chasqui/76/periscopio76.htm>

<sup>67</sup> <http://www.baquia.com/com/20010912/not00013.print.html>

<sup>68</sup> <http://www.statewacht.org/eufbi/index.html>

<sup>69</sup> Propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, COM(2000) 385 final 2000/0189 (COD), Bruselas, 12.07.2000; y Propuesta de Decisión-Marco del Consejo relativa a los ataques de los que son objeto los sistemas de información, COM(2002) 173 final 2002/0086 CNS, Bruselas, 19.04.2002.

restrictiva para la protección de los datos personales, acogiendo la tendencia actualmente mayoritaria, sobre todo por los gobiernos nacionales, de reformar las Directivas de protección de datos<sup>70</sup> que incorporan la garantía de anonimato y la eliminación por los ISP de los datos que circulan, salvo los necesarios para facturación y prestación del servicio.

Las críticas a estas iniciativas no se han hecho, lógicamente esperar. Los defensores de las libertades han manifestado su preocupación por la posibilidad de que se establezca una caza generalizada de sospechosos, que amparada en la lucha contra el terrorismo, pueda afectar a ciudadanos inocentes. Así, tras el 11-S se han multiplicado espectacularmente (algunas fuentes hablan de que se han quintuplicado<sup>71</sup>) las peticiones de las autoridades a los ISP para la interceptación de comunicaciones de sus clientes.

A este respecto, Alan Davidson, Director Asociado del Centro para la Democracia y la Tecnología, ha manifestado que “ lo que tememos es el surgimiento de un sistema que almacene vastas cantidades de información acerca de la gente y luego la use con propósitos diferentes de los que motivaron su creación”<sup>72</sup>.

Pero estas reivindicaciones han tenido, y seguramente tendrán escaso éxito entre una ciudadanía alarmada por los déficits de seguridad, que vive, y se les quiere hacer vivir, bajo la permanente amenaza del atentado y el desorden. Los celos que provocó Carnivore parecen haberse volatilizado. Como se ha apuntado recientemente, una encuesta realizada durante el mes de octubre de 2001 reveló que el 72% de los norteamericanos eran favorables a que su gobierno utilizara medios electrónicos para espiar a posibles sospechosos<sup>73</sup>.

#### 6. *Magic Lantern* (Linterna Mágica).

Con este nombre se designa la que al parecer constituye la última creación del FBI en su “lucha contra el crimen”, y que, además, se complementará con Carnivore .

Se trataría de un virus troyano muy similar al conocido Black Orifice. El objetivo del programa sería acceder, y apropiarse, de las contraseñas de los sospechosos que usaran correo electrónico encriptado en sus comunicaciones. Para tal objetivo, se enviaría, como señala López, a cualquier sospechoso, como un mensaje aparentemente inocente<sup>74</sup>.

Como ha señalado Itziar Narro, “la ventaja de Linterna Mágica sobre Carnivore es que puede interceptar toda la información de un computador cualquiera de manera remota a través de la apertura de un archivo adjunto, y de momento no hay jurisdicción que exija a la inteligencia estadounidense una autorización judicial previa”<sup>75</sup>.

Pero si de virus estamos hablando: ¿qué pasa con los antivirus?. El FBI habría buscado la colaboración de las empresas de antivirus para solicitarles que excluyeran a

---

<sup>70</sup> Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos, DOCE L 281 de 23.11.1995, p. 31; y Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, DOCE L 24 de 30.01.1998, p. 1. Vid. a este respecto, SANCHEZ BRAVO, A., *La protección del derecho a la libertad informática en la Unión Europea*, Publicaciones de la Universidad de Sevilla, 1998, 224 p.

<sup>71</sup> Según Gidari, las solicitudes se han quintuplicado respecto a los niveles observados antes del 11-S. Entre sus clientes figuran America On Line, así como AT&Twireless y Cingular. Cfr. <http://www.iblnews/noticias/14.06.02>.

<sup>72</sup> <http://www.elrinconcito.com/noticias/not64.htm>

<sup>73</sup> <http://www.def.com.ar.ar/news>.

<sup>74</sup> LOPEZ, J.L., *El FBI y sus troyanos*, en <http://www.vsantivirus.com/22-11-01.htm>

<sup>75</sup> NARRO, I., *El FBI refuerza su “espionaje digital” a través de Linterna Mágica*, en <http://www.iblnews.com/news/images/blank.gif>

Linterna Mágica de los virus detectables, así como que se le permitiera instalar una “puerta trasera” para permitir su instalación. Los datos conocidos respecto a la eficacia de estas peticiones son difusas. Si bien su aceptación, pese a no ser reconocido por las empresas, no debe descartarse por lo imperativo de la legislación antiterrorista norteamericana, y las presiones del propio gobierno para no convertirse en encubridores o antiamericanos <sup>76</sup>.

El FBI, por supuesto, ni confirma ni desmiente la existencia de este nuevo mecanismo de control. Nuevamente, el secretismo en estas cuestiones es el principal riesgo de abuso sobre los derechos y libertades de los ciudadanos.

#### **4. A MODO DE CONCLUSIÓN.**

Las nuevas sociedades tecnológicas presentan nuevos retos a los que debe darse cumplida respuesta. Retos que en unas ocasiones se cifran en la ampliación de nuestros sistemas de bienestar y de nuestras posibilidades de interacción con el mundo que nos rodea, pero que en otras deben responder a la lucha constante contra nuevos peligros y modalidades de agresión hasta ahora desconocidos.

En esa doble vía la función estatal continúa la ya tradicional función asignada al Estado, o al menos a los Estados democráticos: garantizar los derechos y libertades de los ciudadanos, y protegerlos a las amenazas a las que puedan verse sometidos. Amenazas que se manifiestan con un nuevo rostro, con una terminología casi mística: ciberterrorismo, biotecnología, hackers, etc...

Es por ello que, también desde una larga tradición ya consolidada el Estado se provea de una serie de instituciones y mecanismos que de una manera, abierta, unas veces, y velada, otras, intenten ser la cabeza de puente que constantemente desembarca en la playa de los peligros.

La idea de seguridad se consolida de esta forma como uno de los elementos a garantizar indubitablemente para el correcto desenvolvimiento de las funciones estatales, y garantizar el clima adecuado para el ejercicio y desarrollo de los derechos por parte de los ciudadanos; de las condiciones para que su ejercicio sea real y efectivo como señala el art. 9.2 de nuestra Carta Magna, en relación con el capital precepto que nos ocupa en esta materia, y que no es otro que su art. 18.4, cuando manifiesta como la ley limitará el uso de la informática, no sólo para garantizar el honor y la intimidad de los ciudadanos, sino también el pleno ejercicio de sus derechos.

Pero la seguridad no sólo entendida como defensa o prevención frente al enemigo exterior, sino también como seguridad interior, en los términos ya apuntados. No es asumible, en estas coordenadas, que el Estado pretenda, amparado en lo indeterminado de la seguridad, protegerse de sus propios ciudadanos, pues desposeído de la base social y legitimadora que lo sustenta, sus acciones carecen de sentido, deviniendo pura arbitrariedad. La seguridad es fácilmente obtenible en Estados totalitarios que ven a sus ciudadanos como potenciales delincuentes frente a los cuales todo, o casi todo, vale,

---

<sup>76</sup> Los datos hasta ahora conocidos evidencian como McAfee, y posteriormente Symantec habrían manifestado su disposición a colaborar con el gobierno; aunque las propias empresas se apresuraron a desmentirlo. Otras empresas han manifestado su oposición al troyano. Desde Network Associates se aseguró que estaban en el negocio de los antivirus para proporcionar seguridad a sus clientes y no iban a hacer nada que comprometiera su actividad. Sophos y Kasperky indicaron que el software “malo” es siempre malo y no es adecuado establecer excepciones. Trend Micro manifestó su disponibilidad a colaborar con el Gobierno, pero manifestó que su trabajo consiste en proteger a sus clientes. Sobre estas cuestiones vid. LOPEZ, J.J., *La mayoría rechaza que no se detecte Linterna Mágica*, en <http://www.vsantivirus.com/03-12-01.htm>.

pues lo relevante y prioritario es mantener la estructura de poder al precio que sea menester.

Situaciones de esta naturaleza son las que parecen arribar a nuestra cotidianeidad, amparados en la novedad y eficacia de lo tecnológico y/o cibernético.

Como hemos desarrollado en estas reflexiones, las modernas tecnologías permiten espiar de manera más eficaz, más global, pero también más intrusiva. Son sistemas altamente lesivos no sólo por el secretismo con el que actúan (como es de suyo) y con total desconocimiento de los afectados, sino que además carecen en la mayoría de los casos de los necesarios controles democráticos que garanticen su necesidad, su legitimidad y su campo de actuación.

Echelon y Carnivore, son sólo la punta del iceberg de este proceso intrusivo en los derechos de los ciudadanos. Sería pacato pensar en la abolición de los servicios de información e inteligencia. Máxime en una época de convulsiones, como el que nos ha tocado vivir.

Ahora bien, eso no significa que todos debamos asumir su actuación sin limitaciones, sin control, sin distinción, en aras de una hipotética seguridad, de la que se desconocen sus agresores y los medios para mantenerla y restaurarla.

Debe restablecerse de nuevo el ideario democrático de que el estatuto de los derechos y libertades figure en el frontispicio de cualquier actuación que pueda lesionarlos.

En estas cuestiones tan sensibles, ahí que reivindicar el estatuto de ciudadano, no el de súbdito. Seguridad, sí. Libertad, por supuesto, también.

## **RESUMEN.**

Internet se ha consolidado como el símbolo indiscutible de las sociedades tecnológicas. Pero junto a innegables ventajas presenta riesgos que no deben olvidarse. La Red se ha convertido en el territorio de operaciones de nuevas formas de delincuencia y terrorismo contra las que debe lucharse. Para ello los Estados se han provisto de mecanismos de investigación y espionaje, con lo que hacer frente a los nuevos desafíos.

Pero se ha constatado como la actuación de aquéllos no siempre responden a los cauces y exigencias de las sociedades democráticas, deviniendo elementos de control sobre el total de la ciudadanía, a quien se pide una aceptación resignada de la intromisión en sus derechos.

Echelon y Carnivore son la muestra palpable de ese proceder, sobre todo a raíz del desgraciado 11-S. Su secretismo, su forma de proceder, la extensión de sus poderes, son buena muestra de ese ataque a los derechos de los ciudadanos amparados desde los Estados.

Ahora más que nunca debe reivindicarse el estatuto de ciudadano, frente al de súbdito. La seguridad nunca debe conseguirse a costa de la libertad, pues sin libertad nunca podremos estar seguros.

## **ABSTRACT.**

Internet has consolidated like the unquestionable symbol of the technological societies. But you/he/she/it next to undeniable advantages present risks that should not forget. The Net has become the territory of operations of new forms of delinquency and terrorist against which you/he/she/it should fight. For this the States there is been provided of mechanisms of investigation and espionage, with what make in front of the new challenges.

But you/he/she/it have been verified like the behavior of those they not always respond to the beds and demands of the democratic societies, be converted elements of control on the total of the citizenship, to whom an acceptance resigned of the interference in their rights is requested.

Echelon and Carnivore are the palpable sample of that proceed, mainly soon after the unfortunate 11-S. Their secret, their form of proceeding, the extension of their powers, they are good sample of that attack to the rights of the citizens aided from the States.

Now more than you/he/she/it should never claim the statute of citizen, in front of that of subject. The security should never get to coast of the freedom, because we without freedom will never be sure