

---

*Comité de Inspection*

---

# **LAS TECNOLOGÍAS DE IDENTIFICACIÓN POR RADIOFRECUENCIA (RFID): RETOS INDUSTRIALES Y CUESTIONES SOCIETALES**

---

**Informe presentado por**

**Françoise ROURE, Inspector general  
Jean-Claude GORICHON, Inspector general  
Emmanuel SARTORIUS, Ingeniero general**

**INFORME N° II-B.9 - 2004 - Enero de 2005**

---

*Comité de Inspección*

---

# **LAS TECNOLOGÍAS DE IDENTIFICACIÓN POR RADIOFRECUENCIA (RFID): RETOS INDUSTRIALES Y CUESTIONES SOCIETALES**

---

**Informe presentado por**

**Françoise ROURE, Inspector general  
Jean-Claude GORICHON, Inspector general  
Emmanuel SARTORIUS, Ingeniero general**

**Informe N° II-B.9 - 2004  
Enero de 2005**

Informe n°II-B.9 - 2004  
Enero de 2005

**Relatores:**  
Françoise ROURE, Inspector general  
Jean-Claude GORICHON, Inspector general,  
Emmanuel SARTORIUS, Ingeniero general

**Las tecnologías de identificación por radiofrecuencia (RFID):  
Retos industriales y cuestiones societales**

**S Í N T E S I S**

La problemática de la identificación digital es uno de los principales retos que enfrentan la industria, la sociedad y la soberanía. Las aplicaciones de esta tecnología abarcan no sólo los objetos o grupos de objetos físicos en forma de existencias o de flujo, así como los objetos digitales, sino también las entidades vivas animales y humanas.

Las tecnologías RFID modifican profundamente el equilibrio informacional de los intercambios internacionales basado en el etiquetaje y la gestión de bienes materiales mediante un sistema de códigos de barras, favoreciendo una trazabilidad generalizada y un control permanente de los flujos de bienes, de los soportes de acceso a servicios y de los desplazamientos de las personas. **Por ello, el control de los sistemas de información en red que sustentan la identificación digital constituye un desafío importante para la soberanía en un contexto de guerra económica.**

Por su naturaleza, esta situación conferirá a los primeros actores que controlen la oferta tecnológica e industrial de la identificación digital, especialmente mediante las tecnologías RFID, una ventaja competitiva considerable y duradera gracias a su acceso *asimétrico* a la inteligencia económica y comercial de suma importancia en una economía abierta y mundializada.

Durante los últimos años, las tecnologías de marcado y trazabilidad han experimentado una notable evolución gracias a la conjunción de la desmaterialización de los procesos de seguimiento, la baja de costes de los soportes y las capacidades de tratamiento de la información (etiquetas, lectores, redes de comunicación electrónica, inteligencia software), y de la lectura sin contacto por radio identificación.

La sustitución de los códigos de barras por chips RFID (*radio-frequency identification*) se ha iniciado en los mercados de masa profesionales y gran público. Sumada a las opciones tecnológicas escogidas por compradores influyentes – entre los que se encuentra el departamento de defensa norteamericano –, permite entrever una generalización mundial al servicio de un comercio internacional en fuerte expansión.

Los estándares tecnológicos y las arquitecturas de sistemas de información que agregan los datos y producen tantos más servicios con valor añadido cuanto más progresa la capacidad de memoria de los marcadores RFID, conducen a **una importante concentración de conocimientos en manos de un número muy limitado de actores industriales, los cuales se cuentan entre los mismos que han sido seleccionados para la gobernanza “técnica” mundial de Internet.** Por ejemplo, se ha escogido a la sociedad VeriSign para administrar el servidor raíz de la red de información mundialmente integrada de EPC Global, distribuidor de los códigos electrónicos de producto que reemplazan los códigos de barras.

Sin duda, la exigencia de trazabilidad resultará facilitada por las tecnologías de radio identificación, especialmente en lo que respecta a las nuevas obligaciones legales relativas a la

seguridad alimenticia y sanitaria. La RFID coadyuva también en la lucha contra la piratería y el fraude, así como en los esfuerzos tendientes a ganar productividad a todo lo largo de la cadena logística. No obstante, aplicada a las personas, a sus desplazamiento e incluso a su comportamiento como compradoras u otros, plantea inquietantes cuestiones de protección de datos de carácter personal sensibles, que ponen en tela de juicio los equilibrios institucionales por la generalización de la RFID. La protección de los datos sensibles individuales puede llegar a estar seriamente comprometida, lo mismo que la capacidad de los poderes públicos para hacer respetar las leyes al respecto.

La generalización de la trazabilidad constituye en sí misma un desafío económico y societal de primer orden por la calidad y diversidad de las soluciones que ofrecen las tecnologías RFID en materia de rapidez y seguridad de las cadenas logísticas en general, aunque también, por la revolución de las estructuras clásicas de la oferta en este campo.

Dada la magnitud de los desafíos industriales y societales que plantean las tecnologías de radio identificación, la presencia de la industria francesa y europea en las dinámicas de investigación aplicada, de normalización y de desarrollo de nuevos mercados resulta muy insuficiente. **La amplitud de los mercados, las soluciones aportadas a las empresas, a los particulares (especialmente en el ámbito de la salud y la ayuda a las personas con movilidad reducida) y a los poderes públicos en su búsqueda del justo equilibrio entre una mayor seguridad con igual libertad y a un coste aceptable, las ganancias de productividad y el combate contra la piratería que permiten las tecnologías RFID, son todos motivos que justifican que se defina y se ponga en práctica una política pública de promoción de las RFID, bien entendida, que dinamice la oferta y contribuya a la innovación.**

El informe recomienda una vigorosa iniciativa de los poderes públicos a favor de una sensibilización de todos los actores concernidos a las oportunidades que brindan las tecnologías de radio identificación, al tiempo que evalúa sus impactos negativos para contenerlos mejor, **empezando por los actores de la oferta:**

- sensibilizar a los actores de la oferta y de la demanda en materia de RFID a las considerables oportunidades de productividad, innovación y creación de valor que ofrece esta tecnología;
- efectuar un análisis profundizado de las amenazas que implican las tecnologías RFID, ya sea que estén relacionadas con aspectos relativos a la trazabilidad de las personas, el control de informaciones estratégicas para las empresas desde el punto de vista económico, o con la soberanía nacional, principalmente por su facilidad de uso; dar a conocer los resultados a todas las partes interesadas, con el fin de sensibilizarlas;
- implementar la pedagogía correspondiente (coloquios, foros, artículos) de tal manera que se suscite la confianza del público en general y se fortalezca a los poderes públicos para su acción de preservación de la soberanía nacional;
- adaptar la oferta de servicios en materia de RFID a la luz de las lecciones aprendidas, o tomar incluso medidas incitativas para reforzar la oferta francesa y europea en este campo;
- favorecer la participación de Francia en las instancias de normalización y foros internacionales en materia de tecnologías RFID, de asignación alternativa de nombre y de direccionamiento;
- favorecer las iniciativas profesionales, ya sea que procedan de fabricantes o de usuarios, con miras al desarrollo de aplicaciones RFID que puedan generar una confianza bien entendida por el consumidor y el ciudadano;

- invertir en la investigación sobre los efectos económicos y sociales de las tecnologías RFID y de los sistemas de información sobre los que se basan las aplicaciones con repercusiones societales;
- evaluar, desde el punto de vista de la tecnología de radio identificación digital, la aplicabilidad de la ley que garantiza la protección de los datos de carácter personal.

# ÍNDICE

<b>Introducción</b> .....	<b>1</b>
<b>PARTE I – Identificación Digital de los Objetos y Desafíos Industriales</b> .....	<b>2</b>
1.1. Las tecnologías RFID y los actores de la oferta .....	2
1.1.1. Definición, hoja de ruta tecnológica, aplicaciones industriales .....	2
1.1.2. El proceso de normalización EPC .....	3
1.1.3. Los actores de la oferta de tecnologías RFID para la identificación de objetos.....	4
1.2. La relación estratégica entre el ONS y el DNS y los principales actores de la demanda..	5
1.2.1. La relación estratégica entre el ONS y el DNS .....	5
1.2.2. Los actores de la demanda, sus exigencias y su influencia sobre el desarrollo del mercado .....	9
<b>ParTE II – IDENTIFICACIÓN DIGITAL DE LAS PERSONAS Y EQUILIBRIOS INSTITUCIONALES</b> .....	<b>12</b>
2.1. Recordatorio de las disposiciones jurídicas francesas; alcance y límites .....	13
2.1.1. Los nuevos medios para la CNIL, insuficientes con respecto a las necesidades nacidas de la nuevas amenazas .....	14
2.1.2. Tratamientos automáticos, fusión de ficheros y realidad del consentimiento previo.	15
2.1.3. Nuevos riesgos tecnológicos contra la aplicabilidad de la ley .....	16
2.1.4. Del ejercicio del derecho de rectificación.....	18
2.2. El poder público es responsable del marco fijado para la trazabilidad digital de las personas, a todos los niveles de subsidiariedad .....	18
2.2.1. Protección de la identidad digital en salud: contexto y alcance.....	20
2.2.2. El Supervisor Europeo de Protección de Datos .....	23
2.2.3. La Agencia Europea de Seguridad de las Redes y la Información (ENISA).....	24
2.2.4. Riesgos específicos inherentes a la centralización de los datos digitales de carácter personal. ....	25
<b>Conclusión</b> .....	<b>27</b>
<b>RECOMENDACIONES</b> .....	<b>29</b>

## INTRODUCCIÓN

Los retos de la identidad digital, tal como nos proponemos analizarlos en este informe, se limitan al conjunto de las cuestiones tecnológicas y societales planteadas por la recolección, el archivado y el tratamiento de las informaciones relacionadas con el uso de las tecnologías sin contacto (principalmente microchips y antenas impresas), los sistemas de información que tienen los objetos comunicantes y, en particular, los softwares de trazabilidad.

En primer lugar, nos referiremos, desde un punto de vista institucional, a las informaciones que, tomadas como un conjunto, permiten, al recogerlas, almacenarlas y usarlas, realizar la identificación de una persona, cualquiera que sea la licitud de esta identificación y/o de su uso, y presentaremos las distintas opciones tecnológicas así como las evoluciones del marco reglamentario a nivel nacional, europeo e internacional.

Analizaremos después, desde un punto de vista industrial, las informaciones que permiten la identificación de un objeto, enfocando los sistemas de información globales requeridos para permitir el desarrollo mundial de las aplicaciones concernidas.

Por otra parte, hemos decidido limitar el enfoque a las tecnologías de identificación sin contacto, que presentan las más importantes perspectivas de desarrollo para los próximos diez años, debido a la significativa reducción de los precios que su rápida generalización debería conllevar. El posicionamiento reciente de los actores en torno a una norma susceptible de sustituir el código de barras por estas tecnologías, añadiéndoles funcionalidades inteligentes, abre camino a corto plazo para aplicaciones de masa, con el fin de satisfacer mercados que pueden ser civiles o militares, públicos o privados.

Los marcadores, lectores y softwares de la tecnología RFID constituyen, en su conjunto, un sistema de identificación por radiofrecuencia en el que participan, en primer lugar, los actores bien establecidos de la economía digital mundial (principalmente IBM, Philips, VeriSign, Gemplus). Otras empresas del sector de la oferta se desarrollan rápidamente, en Francia, en particular, en torno al polo tecnológico de Sophia-Antipolis (pero no exclusivamente). La tecnología RFID va de par con el desarrollo sin precedente de los intercambios comerciales internacionales; en términos de flujos de datos digitales relativos al comercio internacional, es el equivalente material de los flujos financieros y, en consecuencia, *a priori* no existe límite alguno para su desarrollo futuro; por último, permite ahorros sustanciales al evitar errores humanos en logística y al limitar las “oportunidades” de fraude de cualquier origen.

## **PARTE I – IDENTIFICACIÓN DIGITAL DE LOS OBJETOS Y DESAFÍOS INDUSTRIALES**

### **1.1. Las tecnologías RFID y los actores de la oferta**

#### **1.1.1. Definición, hoja de ruta tecnológica, aplicaciones industriales**

La tecnología RFID (*Radio Frequency Identification*) – a veces también se habla de *smart tags* (etiquetas inteligentes) – se encuentra en la intersección de la tecnología del código de barras y la del microchip sin contacto. Del código de barras toma, modernizándolo, el principio de dotar a todo objeto de un código de identificación susceptible de ser leído por una máquina. Del microchip sin contacto retoma la posibilidad de leer informaciones o incluso de ordenar que se efectúe un tratamiento a distancia. Por lo tanto, y a pesar de algunos puntos débiles<sup>1</sup> que aún persisten, la tecnología RFID se presta muy bien a una automatización total de la cadena logística, tanto más cuanto que el objeto puede estar en movimiento y en cualquier posición. El principio de la tecnología RFID no tiene nada de innovador, puesto que podemos considerar que el pase *Navigo* de la RATP (red de transporte urbano de París) o los terminales de telepeaje de las autopistas lo utilizan ya.

Sin embargo, la superioridad de la RFID con respecto al código de barras, que debe pasar frente a una ventana de lectura o ser escaneado por un lector móvil (como en las cajas de los supermercados), consiste en la sustitución de las técnicas de lectura móvil por técnicas electromagnéticas. La etiqueta RFID, que puede ser insertada en el espesor de un embalaje o incluso impresa en el mismo, sólo se distingue de la tarjeta con microchip sin contacto por la ausencia del soporte “tarjeta plástica”, puesto que el principio físico es el mismo: un microprocesador, dotado de una antena e “iluminado” en condiciones adecuadas por un campo electromagnético, emite las informaciones que lleva consigo y puede incluso efectuar tratamientos.

Podemos distinguir:

- las etiquetas de sólo lectura o pasivas: en este caso, el fabricante ha impreso en la etiqueta ciertos datos (código de identificación único e infalsificable) que no pueden ser modificados ni completados; los usuarios sólo pueden leer el número de serie inscrito en el chip;
- las etiquetas de lectura / escritura o activas: en este caso, la etiqueta cuenta con una capacidad memoria en la que se puede escribir, completar, leer e incluso borrar informaciones; el número de ciclos de lectura es ilimitado.

Las tecnologías RFID también pueden clasificarse en cuatro categorías según las bandas de frecuencia en las que funcionan:

- los chips BF (frecuencia inferior a 135 kHz), con una distancia de lectura de unos cuantos centímetros;

---

<sup>1</sup> La RFID no funciona correctamente en presencia de masas que reflejan las ondas electromagnéticas (por ejemplo, embalajes metálicos o que contienen agua).

- los chips HF (frecuencia de 13,56 MHz), con una distancia de lectura de algunas decenas de centímetros; la mayoría de chips pasivos utilizan esta banda de frecuencia;
- los chips UHF (868-950 MHz), con una distancia de lectura del orden de un metro;
- los chips UHF a 2,45 GHz (misma banda que las normas Bluetooth y Wi-Fi).

### 1.1.2. El proceso de normalización EPC

Los retos de la normalización son considerables puesto que a fin de cuentas es la que garantizará la interoperatividad entre etiquetas, lectores y sistemas de tratamiento de las informaciones y, de manera más general, el funcionamiento adecuado del conjunto, en el contexto de una economía mundializada donde ya no hay fronteras para la circulación de los bienes. La normalización también resulta importante para efectos de series y, por ende, en la reducción de costes que permite. Distinguimos tres niveles en los que se sitúan estos retos:

- a nivel de los protocolos de intercambio entre la RFID y su entorno;
- a nivel de las frecuencias radioeléctricas que permiten los intercambios entre la RFID y su entorno;
- a nivel de la codificación de los propios objetos identificados por medio de la RFID.

En cuanto al primer punto, la ISO ya ha desarrollado normas (14 443, 15 693, familia de las normas 18 000<sup>2</sup>) que todavía están lejos de haber logrado la unanimidad. Los estándares propietarios siguen siendo numerosos, sin hablar de aquellos elaborados por otras coaliciones de intereses, como el muy reciente *EPCglobal UHF generation 2*<sup>3</sup>.

En lo que se refiere a las frecuencias, existe un serio problema en la banda UHF, *a priori* la más interesante en términos de potencial de utilización de la RFID. Las frecuencias utilizadas en Estados Unidos (915 MHz), están reservadas en Europa y Japón a las redes de telefonía móvil de segunda generación, lo que restringe de manera importante la potencia con la que pueden utilizarse y, en consecuencia, su alcance. Por su parte, la Unión Europea ha escogido la frecuencia de 868 MHz. Como es difícil que estas redes desaparezcan antes de un buen número de años, será necesario iniciar negociaciones internacionales sobre este punto si se quiere lograr una interoperatividad entre los sistemas americanos y los del resto del mundo.

---

<sup>2</sup> ISO 18 000-2 en la banda 125-135 kHz, futura norma ISO 18 000-3 que debería sustituir las normas ISO 14 443 (A/B) y 15 693, en la banda 13,56 MHz, futura norma ISO 18 000-6 en la banda 860-9340 MHz y futura norma ISO 18 000-4 en la banda 2,45 GHz.

<sup>3</sup> Acerca de EPCglobal Inc., véase § 1.2.1.

### 1.1.3. Los actores de la oferta de tecnologías RFID para la identificación de objetos

Los industriales presentes en el campo de la RFID son:

- los grandes fabricantes de componentes electrónicos: Hitachi, Infineon, NEC, Philips Semiconductors, STMicroelectronics, Texas Instruments, etc.;
- los grandes creadores de sistemas, capaces de diseñar, desarrollar, implantar e incluso explotar los sistemas que utilizan las RFID y que se basan ampliamente en las tecnologías de la información (gestión de bases de datos, redes, ...); IBM se ha posicionado en este nicho de manera muy clara, pero también encontramos otras empresas, como Accenture, Bearing Point, CSC, Unisys o VeriSign;
- los proveedores de software, como Microsoft, Oracle o SAP;
- algunos industriales de la telefonía móvil, como Nokia;
- por último, *last but not least*, los seleccionados para encargarse de la gestión de los EPC, como EPCglobal Inc.

En lo que se refiere al aspecto manufactura de la RFID propiamente dicho, podemos simplemente añadir que hoy en día el mayor reto consiste en reducir drásticamente su coste actual (a aproximadamente 0,05 €, contra 0,30 € de hoy), que los usuarios potenciales comparan de manera desfavorable con el coste casi nulo de un código de barras. Habida cuenta de la dificultad de jugar, más allá del efecto de serie, con el coste de los microprocesadores, los esfuerzos de los industriales se enfocan esencialmente en el coste de las antenas y del *packaging*. Por esta razón, han surgido en este nicho pequeñas sociedades innovadoras, como IER y Tagsys, o ASK, en Sophia-Antipolis, que ha desarrollado procesos que permiten imprimir la antena con un simple chorro de tinta sobre cualquier tipo de soporte. Cabe señalar que las perspectivas de mercado son colosales: se habla de 10 a 20 mil millones de objetos *RFIDizados* hacia 2008.

**La gestión de los códigos es un asunto infinitamente más importante por las consecuencias que conlleva y por los desafíos de poder que implica.** La entidad americana sin fines de lucro EPCglobal Inc.<sup>4</sup>, *joint venture* entre EAN International<sup>5</sup> y el *Uniform Code Council* (UCC<sup>6</sup>) americano, se ha posicionado de manera muy clara en el nicho, considerable, del etiquetado de paletas y cajas de cartón, y tiene la intención de administrar los *Electronic Product Codes* (EPC) a nivel mundial y prestar un servicio de

---

<sup>4</sup> <http://www.epcglobalinc.org/>. En su *Consejo de Gobierno* encontramos a representantes de firmas como Carrefour, Cisco Systems, Coca-Cola, Gillette, HP, Metro, Nestlé, Procter & Gamble o Wal-Mart.

<sup>5</sup> Organización internacional que representa a 101 organizaciones de 103 países (Gencode EAN France, por Francia), basada en Bruselas. Creada en 1977 bajo el estatuto de asociación con fines no lucrativos, tiene por objeto desarrollar normas que permitan una administración de cadenas logísticas globales y multiempresas. EAN International fija la estructura de los códigos de barras fuera de Estados Unidos (EAN = *European Article Number*) (<http://www.ean-int.org/>).

<sup>6</sup> Organismo técnico creado en Estados Unidos hace unos treinta años, el *Uniform Code Council* desarrolla normas y soluciones para mejorar la gestión de la cadena logística global. UCC fija la estructura de los códigos de barras en Estados Unidos (<http://www.uc-council.org/>).

interconexión a los servidores que contengan informaciones relativas a objetos identificados por códigos EPC. EPCglobal Inc. ha manifestado su deseo de vincular todos los objetos a internet y suministrar un servicio de transacciones básicas a través de su *EPCglobal Network*, como la localización de informaciones relativas a un objeto específico, la localización de un objeto dado, la localización de determinado objeto en la cadena logística, así como servicios de trazabilidad con valor añadido, entre otros. EPCglobal Inc. afirma que sólo tiene en la mira el mercado de *B to B (business to business)* y no el de *B to C (business to consumer)*. En todo caso, salta a la vista el poder que podría conferirle ese papel central en la circulación de las mercancías a través del mundo. Es pertinente añadir que EPCglobal ha encomendado la gestión de su red (*EPCglobal Network*) a la sociedad americana VeriSign que, entre otras actividades, administra los nombres de dominio (DNS) en internet.

## **1.2. La relación estratégica entre el ONS y el DNS y los principales actores de la demanda**

Mucho tiempo reconocida por el papel desempeñado en el funcionamiento de la infraestructura crítica subyacente al sistema DNS y en internet, la sociedad VeriSign desarrolla su infraestructura y su experiencia para apoyar el servidor raíz del servicio de asignación de nombre de objeto de EPCglobal Network (ONS: *Object Naming System*).

ONS es uno de los servicios que permite la realización de “procesos comerciales de valor superior en la red EPCGlobal Network”. La oferta de VeriSign está basada en la tecnología EPC Starter Service (SM), que permite la identificación y la cuantificación del valor de las informaciones de seguimiento y localización de los productos marcados RFID, creadas en cada punto de la cadena de producción, encaminamiento y distribución de los objetos, y a todo lo largo de su vida mientras su identificación no haya sido desactivada de manera voluntaria o fortuita.

### **1.2.1. La relación estratégica entre el ONS y el DNS**

La simbiosis entre internet e identificación de objetos físicos no era forzosa; sencillamente, en poco tiempo esta fusión se volvió lógica en el contexto actual, donde internet es el vínculo invasor que crea la complementariedad entre todas las actividades hasta ahora relacionadas, pero también distintas.

Los chips RFID son descendientes directos del código de barras. Por lo tanto, su uso hubiera podido circunscribirse a la esfera propia de la logística, como fue el caso de las etiquetas de barras durante los últimos 30 años.

Pero sus fervientes adeptos<sup>7</sup> se percataron de inmediato de las fantásticas posibilidades de proliferación que se creaban al apoyarse en las bases de datos en línea, y en particular en las tecnologías IP de internet, para hacer del proceso un proceso “sin

---

<sup>7</sup> Esencialmente los laboratorios del MIT.  
*Centre de traduction Minéfi – 2388-05-ES – 28/12/2005*

costura”, dotando con ello la arquitectura de los intercambios de una impresionante eficacia por un coste adicional en infraestructura insignificante.

Y muy rápidamente, el paralelismo de las situaciones ha llevado a desarrollar copias exactas en las soluciones inventadas para el direccionamiento de internet, el DNS (*Domain Name System*).

- El direccionamiento: ¿un fenómeno irreversible y apremiante?

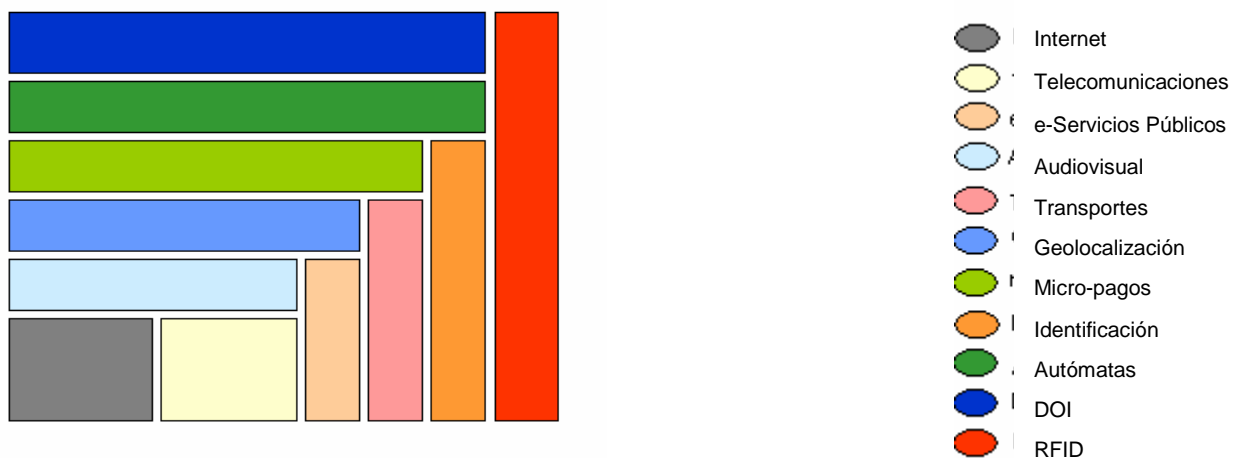
Desde hace algunos años, so pretexto de trazabilidad, cunde en el mundo la fiebre de asignar una dirección, de preferencia permanente, no sólo a los objetos físicos, los individuos, los vehículos en las carreteras y los animales, sino también a todos los objetos virtuales, ya sea que se trate de mensajes de tipo e-mail o SMS, de documentos administrativos, de fragmentos de música digitalizados o de esclavos secundarios de softwares (*applets*, *servlets* y demás agentes llamados “inteligentes”) que recorren, incansablemente, las redes intercambiando microinformaciones para servirnos mejor e incluso, muchas veces, para espiarnos mejor.

Pero, ciertamente, la batalla entre las tecnologías, las normas o los industriales enfrascados en esta lucha de influencia entre los diversos mundos en red, todavía no está ganada.

- Las luchas fratricidas de los mundos en red

Porque, desde ahora, esos múltiples mundos en red<sup>8</sup>, que van de las telecomunicaciones a los autómatas, pasando por la identificación de las personas, y para los cuales el discurso recurrente imagina fácilmente que en el futuro convergerán en una fusión idílica para beneficio del usuario, de hecho están enzarzados en una velada lucha fratricida, ya que todos han decidido apropiarse el mundo IP, **pero** cada uno deformándolo a su manera y adaptándolo a sus propios imperativos específicos.

Para simplificar, la cartografía provisional de estos mundos podría ser la siguiente:



<sup>8</sup> Ver la presentación en el anexo 4.7.

Puede predecirse que esas antiguas fronteras entre mundos que actúan todo el tiempo tratando de fagocitarse mutuamente no van a seguir intactas. La competencia entre DNS, ONS y DOI (*Digital Object Identifier*) se anuncia particularmente feroz.

#### - Las profundas similitudes entre ONS y DNS

No es sorprendente encontrar similitudes entre el primer modo de direccionamiento imaginado para internet, el DNS, y el direccionamiento en cada uno de los otros mundos, puesto que las necesidades son del mismo tipo.

Sin embargo, gracias a la conjunción de varios factores, el mundo ONS ha sido el más rápido para mantenerse lo más cerca posible de la arquitectura DNS.

En primer lugar, los actores que pueden tener un peso suficiente en las decisiones son fundamentalmente los mismos: el gobierno estadounidense con el *Department of Defense* (DoD) y el *Department of Commerce* (DoC), los grandes industriales como IBM, además de un actor que se ha vuelto imprescindible en el planeta internet en muy poco tiempo: VeriSign.

En ambos esquemas, DNS y ONS, el gobierno norteamericano confió discretamente el servidor raíz a VeriSign, sin que, aparentemente, se haya pedido la opinión de los demás actores. Cabe señalar que es poco probable que las condiciones de esta atribución se clarifiquen algún día, dado que la *Executive Order* (orden ejecutiva) americana del 16/10/2001 clasifica como "*Confidential Defense*" las arquitecturas esenciales de internet.

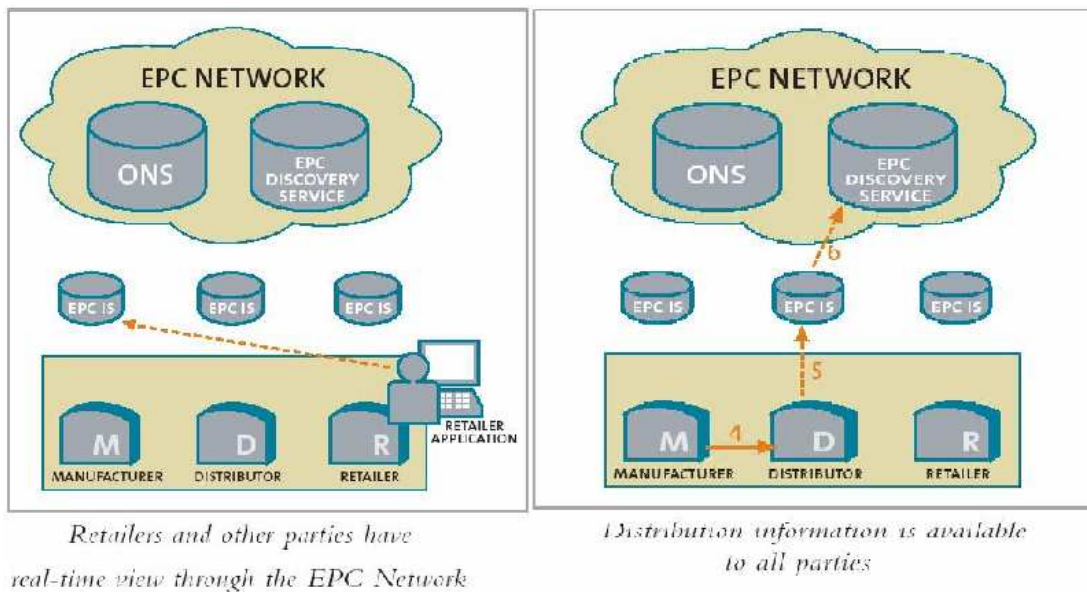
Desde nuestro punto de vista, la principal diferencia estriba en los servidores de segundo nivel. En el DNS se ha conservado la segmentación geográfica que permite a cada Estado mantener bajo su control al operador de direcciones correspondiente a su territorio geográfico.

En lo que respecta a las normas de EPC Global y del ONS, esa segmentación geográfica desaparece por completo. Los servidores secundarios pertenecen a grandes industriales, empresas multinacionales sobre las que los Estados no tienen ningún medio de control, como es bien sabido. Dada esta situación, por lo menos se puede deducir que ya no tendrán caso los debates de la ONU para saber cuál es el lugar que los Estados deberían ocupar en la gobernanza eficiente de internet.

Como los flujos, el número de objetos por identificar, el número de subcontratistas y de almacenes de distribución rebasa muy ampliamente el número de sitios internet, por lo que no resulta muy atrevido afirmar que el ONS (o al menos sus actores primordiales) podría fagocitar el internet que conocemos en poco tiempo, volviendo así ilusorias las modestas tentativas del GAC (*Gouvernement Advisory Committee*) y de la Cumbre Mundial de la Sociedad de la Información (SMSI).

Los esquemas siguientes ilustran los tres niveles de la arquitectura:

- en el primer nivel: un servidor raíz (ONS), con su *whois* (llamado aquí Discovery Service)
- en el segundo nivel: los servidores propios de los profesionales (fabricantes, mayoristas, etc)
- en el nivel tercero y último: el acceso de los usuarios finales entre los que se encuentra, en particular, la gran distribución (gráficos y textos de VeriSign).



Lo que pudiera parecer cuestionable y eventualmente podría frenar el auge de este modelo es el riesgo de inteligencia económica que esta arquitectura favorece. Nada garantiza que los industriales dejarán que cada uno de los actores de los diferentes “mundos” interrogue libremente sus propias bases y coteje los datos económicos y comportamentales que el modelo deja entrever.

Resulta sorprendente constatar que, en apariencia seducidos por las indiscutibles ventajas que permite vislumbrar la gestión “sin costura” de los flujos físicos, los industriales europeos participantes en los consejos de pilotaje o de vigilancia de EAN y de EPC Global se hayan mostrado tan discretos acerca de los riesgos indudables que este tipo de arquitectura centralizada hace pesar sobre informaciones vitales para su competitividad, su desarrollo y su saber hacer.

De la misma manera, los diversos foros, profesionales como el IETF o más institucionales como la SMSI, se focalizan insistentemente sobre ciertas estructuras (la ICANN...), pero olvidan sistemáticamente mencionar el lugar cada vez mayor, e incluso impropio, que ocupan ciertos actores privados de la esfera Internet.

En nuestra opinión, ya es hora de que las autoridades europeas, que escrutan con atención el mundo de la informática (el caso Microsoft es un ejemplo de ello) extiendan su vigilancia a los “mundos” vecinos, entre los que se encuentra el de Internet, y evalúen en

qué condiciones la sociedad VeriSign extiende las mallas de sus redes sobre los sectores más sensibles de la gestión de los mundos en red.

En todo caso, en las condiciones actuales nos parece importante alertar al gobierno acerca de estas desviaciones que potencialmente podrían ser muy dañinas para la integridad económica de sectores completos de la economía.

¿Por qué, por ejemplo, habría que poner, *en tiempo real*, todos los datos de intercambios de la industria francesa (incluso los del lujo, la aviación, la industria farmacéutica, etc.) a la disposición centralizada de una sola empresa cuya deontología en la materia no ha sido comprobada?

En efecto, tratándose en particular de internet, esta misma empresa ya es juez y parte puesto que se encarga, con base en un contrato firmado con el gobierno norteamericano, del mantenimiento de los servidores raíz al tiempo que, por otra parte, administra comercialmente varias decenas de millones de direcciones con la extensión .com (y otras .net) y tiene además a su cargo la certificación y la confidencialidad de los enlaces encriptados (¡incluso de ciertos servicios esenciales de la administración francesa!).

#### 1.2.2. Los actores de la demanda, sus exigencias y su influencia sobre el desarrollo del mercado

Considerando la atractividad de su bajo coste y su gran valor añadido en la hoja de ruta generalmente admitida por los profesionales de los marcadores y lectores RFID, la identificación por radio frecuencia y la red EPCglobal en proceso de constitución tienen suficiente potencial para imponer una banalización total de esta tecnología en todos los eslabones de la cadena logística de los objetos, pero también de los desplazamientos y comportamiento de las unidades vivas pertenecientes al reino animal y vegetal: animales vivos en el marco de la vigilancia sanitaria obligatoria, humanos en cuanto a su comportamiento de (ciber) viajeros, de consumidores (incluso de sistemas de salud y de seguridad) y de ciudadanos...

Por ejemplo, en Corea, país que ha realizado una inversión de 100 M€ en 4 años para dotarse de un programa "*Ubiquitous-sensor Plan*" y convertirse así en uno de los líderes de la RFID hacia 2010, una cadena de grandes tiendas ofrece al consumidor un seguimiento, desde su sitio internet, del itinerario recorrido por la vaca que está saboreando.

Los motivos para adoptar la RFID son de índole económica. Esta tecnología permitiría reducir los costes de inventario y los de la mano de obra utilizada para el suministro; permitiría igualmente disminuir las pérdidas por robo en los anaqueles y piratería. Los ahorros conseguidos en la cadena logística de la gran distribución serían del orden del 6 al 7% (estudio AT Kearney citado en el informe de la DREE; véase la bibliografía).

El coste de utilización del estándar EPC debería incrementarse con la remuneración de las patentes de la sociedad norteamericana Intermec sobre las tecnologías RFID; según EPC Global, el encarecimiento debido al pago de *royalties* representaría entre el 5 y el 10% del precio del chip electrónico. Todos los demás constructores han cedido gratuitamente

patentes para que el estándar EPC esté libre de remuneración por concepto de la propiedad intelectual.

En el estado actual de las cosas, el coste de un chip RFID sigue siendo superior al del código de barras, pero no es comparable directamente si se tienen en cuenta las posibilidades complementarias de recolección, almacenamiento y utilización de datos suplementarios. Además, se esperan importantes reducciones de coste gracias a la producción masiva y, por otro lado, a ciertas innovaciones tecnológicas como la impresión.

Ciertamente, los primeros actores de la demanda van a influenciar la política normativa mundial. Tendrán peso principalmente: la gran distribución, con Wal-Mart y Marks & Spencer; las condiciones de acceso a los mercados de suministro del departamento de la defensa norteamericano (DoD) y de sus agencias para el mercado de los objetos; las especificaciones del Grid del sistema global de información del DoD en lo que se refiere a las tecnologías sin contacto *Wireless Global Information Grid (WGIG)*; sin olvidar a las industrias de consumo masivo (en particular Coca Cola, Gillette, Nestlé, Whirlpool Europe), la distribución de productos petroleros (Exxon Mobil), así como los transportes (RATP, gerentes de peaje en las autopistas...). La sociedad Metro en Alemania distribuye tarjetas de fidelización con chips RFID, que también ya se utilizan en el marco del flete exprés (DHL) o de la medición de calidad de los servicios postales internacionales (Posteurop).

Uno de los actores más influyentes desde el punto de vista logístico, habida cuenta del número de sus proveedores y de la calidad y cantidad de los productos suministrados, es el DoD, el cual ha optado por una estrategia integrada de identificación digital de los objetos y aprobado la banda de frecuencias de 860-960 Mhz para los marcadores pasivos (*passive RFID tags*). Según su normativa interna, que puede ser consultada en su sitio Internet [www.dodrfid.org](http://www.dodrfid.org), estos marcadores respetarán las especificaciones de los marcadores pasivos de clase 0 y 1 del consorcio EPCGlobal. Se aplicarán sobre cualquier envío y sobre todas las unidades de paletas. El 1° de enero de 2007 serán complementados por un sistema mucho más fino de marcación del objeto, en el marco del concepto básico de identificación universal (*UID Registry concept*) cuyo gráfico se presenta en el anexo n° 4.1.

El 30 de julio de 2004, el Subsecretario de la Defensa norteamericano hizo explícita la política de identificación por radiofrecuencia basada en marcadores activos, cuyo objetivo es brindar una visibilidad global de las entidades móviles. Este servicio debe ser sostenido por una infraestructura de red internet que funcione con base en el esquema siguiente: los datos procedentes de los marcadores RFID serán encaminados hacia los servidores llamados de visibilidad regional para ser enviados después a la red global de transporte de información. Una estructura central asegurará las relaciones con los servidores regionales, incluido el de la red de direccionamiento secreto del protocolo internet (*ITV server on the Secret Internet Protocol Router Network – SIPRNET*). Corresponderá a este servidor asegurar la interoperatividad de esos datos así centralizados con el sistema global de apoyo a las fuerzas armadas, el sistema de control y mando, así como los demás sistemas de información clasificados (véanse los anexos n° 4.2 y 4.3).

Aún cuando una auditoría de la agencia norteamericana encargada de controlar la contabilidad federal (*General Accounting Office: GAO*) formula dudas sobre la capacidad, e incluso la voluntad, de las diferentes entidades de las fuerzas armadas estadounidenses de adoptar un sistema tan centralizado y global, los recursos presupuestarios fueron implementados a marchas forzadas.

Otro de los principales factores de influencia sobre el mercado será la posición de las instancias chinas de normalización en el ámbito de la RFID. Habrá que tener en cuenta no solamente los mercados de exportación, resultado en particular de la deslocalización de actores internacionales hacia ese país, sino también el desarrollo del mercado interior chino. Si bien la tecnología RFID es neutra en sí misma, dentro de los límites del impacto toxicológico y ecotoxicológico generado por las materias empleadas (nanotecnologías, según el calendario de la hoja de ruta), plantea sin embargo graves cuestiones de sociedad además de los “frenos” de tipo técnico (disponibilidad y armonización de las frecuencias) y económico (rapidez de la reducción de costes) al generalizarse en el corto plazo.

La polémica suscitada por el hecho de que, en el marco de la generalización del sistema Navigo, haya que pagar más caros los cupones semanales y mensuales de la RATP (Red Autónoma de Transportes Parisinos) para poder conservar el anonimato, ilustra **la incertidumbre en cuanto a la aceptación por parte de la sociedad** con respecto a la facilidad de uso que la tecnología aporta. ¿Hay que pagar para mantener el anonimato en los transportes? Esta es una pregunta a la que la Comisión Nacional de Informática y Libertades (CNIL) responde negativamente. La emergencia de este tipo de debate es inducida por la banalización de las tecnologías sin contacto. ¿Debe prevalecer la necesidad económica? Si es así, ¿con qué consecuencias? **Aquí es particularmente tangible la frágil distinción entre la identificación de las personas y la de los objetos.**

## **PARTE II – IDENTIFICACIÓN DIGITAL DE LAS PERSONAS Y EQUILIBRIOS INSTITUCIONALES**

Al hablar de las personas físicas, utilizaremos exclusivamente el término de **identificación**. En efecto, aunque la reciente ley sobre la bioética autoriza, en ciertos casos, la posibilidad de patentar fases de secuenciación del genoma humano en calidad de proceso innovador, en el estado actual de las cosas no se puede hablar de una verdadera identidad digital humana.

No obstante, empieza a plantearse globalmente la cuestión de la identidad digital humana, más allá de elementos ya clásicos como la digitalización del apellido, el nombre, la fecha de nacimiento, el domicilio y la firma, como también de su número de inscripción en el registro nacional de identificación de las personas físicas o en algún registro internacional (por ejemplo, en el sistema de información llamado Schengen II – SIS II).

En agosto de 2004, las autoridades japonesas aceptaron la clonación de embriones humanos con fines de investigación médica; las bases de datos digitales genéticos podrían constituir un elemento de identidad digital de estos embriones. Los bancos de datos biométricos humanos, incluyendo su dimensión comercial, tienen asegurado un verdadero auge en el futuro, lo que hace que se planteen las cuestiones relativas al anonimato y el consentimiento.

En la actualidad, la presión ejercida por las exigencias de la seguridad, el orden público y la lucha contra el terrorismo hace que se desarrollen otros elementos constitutivos de la identidad digital humana: la imagen digital del rostro, del iris, la huella digital, las imágenes digitales médicas totales o parciales del cuerpo humano, incluida la impresión cerebral (*brain fingerprint*, que ya se utiliza judicialmente en Estados Unidos en el marco de procesos criminales). En Francia, el expediente médico único, creado por ley, debería acelerar la evolución hacia la definición y el uso público y privado de la identidad digital humana.

Calificamos aquí de *accesorias* las identidades digitales relativas a los objetos comunicantes y a los servicios digitales, en la medida en que la finalidad que implica los más importantes desafíos se concentra en la recogida, por cualesquiera medios lícitos o ilegales, de datos digitales personales o impersonales, a partir de los cuales se puede proceder a la identificación de una persona física, - y de su comportamiento.

Sin embargo, estas informaciones – y su tratamiento –, procedentes en su mayoría de la economía transaccional (libre o de mercado), directa o indirectamente constituyen en sí mismas un considerable yacimiento de valor y, en consecuencia, sin duda justifican que las autoridades encargadas de la industria y de la sociedad de la información sean capaces de conocer y anticipar las evoluciones posibles para cumplir su misión de manera satisfactoria. Por lo tanto, desde el punto de vista industrial resultan fundamentales.

Las disposiciones legislativas vigentes en Francia contemplan el tratamiento de datos de carácter personal, pero aparentemente están atrasadas en cuanto a las posibilidades de fusión de informaciones digitales de tal forma que, debidamente organizadas, permitan utilizar un conjunto de datos, cada uno de los cuales tomado de

manera aislada no quede comprendido en el campo de aplicación de la ley, pero cuya agregación permita lograr, según la finalidad buscada en realidad, no solamente la identificación sino también la elaboración de un perfil de estado y de comportamiento.

La existencia de estas informaciones agregadas, al igual que la finalidad y los usos reales de esta agregación, escapan así al control ejercido por los miembros y los agentes de la CNIL.

Lo anterior muestra que, de hecho, el espíritu de la ley es fácilmente eludible, especialmente cuando las obligaciones que incumben a los responsables del tratamiento no pueden ser aplicadas ni, *a fortiori*, controladas debido a la extraterritorialidad de las acciones que la violan.

## **2.1. Recordatorio de las disposiciones jurídicas francesas; alcance y límites**

La ley n° 2004-801 del 6 de agosto de 2004 sobre la protección de las personas físicas con respecto al tratamiento de datos de carácter personal, que modifica la ley n° 78-17 del 6 de enero de 1978 relativa a la informática, los ficheros y las libertades, transpone en particular las disposiciones de la directiva europea sobre la privacidad y las comunicaciones electrónicas del 12 de julio de 2002.

Su artículo 1° define con precisión los datos de carácter personal y la manera como debe procederse para decidir el carácter identificable o no de una persona.

Por ejemplo, “constituye un dato de carácter personal toda información relativa a una persona física identificada o identificable, directa o indirectamente, mediante un número de identificación o uno o varios elementos que le son propios”.

“Para determinar si una persona es identificable, deben tenerse en cuenta todos los medios susceptibles de permitir su identificación, con que cuenta o a los que puede tener acceso, el responsable del tratamiento, o cualquier otra persona”.

La definición legal de tratamiento es neutra con respecto a las tecnologías empleadas, puesto que “constituye un tratamiento de datos de carácter personal toda operación o conjunto de operaciones, *efectuadas o no mediante procedimientos automatizados*, aplicadas a datos personales como la recogida, el registro, la organización, la conservación, la adaptación o la modificación, la extracción, la consulta, el uso, la comunicación por transmisión, difusión o cualquier otra forma que permita el acceso a los mismos, la alineación (cotejo) o la interconexión, así como el bloqueo, la supresión o la destrucción”.

La definición anterior tiene en cuenta la combinación de elementos separados con miras a la identificación y con la finalidad de establecer un perfil, u otra, particularmente al usar los términos de alineación e interconexión.

Cabe señalar que la legislación comunitaria es más precisa que la francesa en cuanto a la lista de los datos que pueden contribuir a la identificación de una persona. De conformidad con el reglamento (CE) n° 45/2001 del 18 de diciembre de 2000, “se

considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación **o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social**".

La posibilidad de aplicar la ley francesa a los responsables del tratamiento se limita necesariamente a que éstos estén establecidos en el territorio francés, o a que utilicen medios de tratamiento situados dentro del mismo territorio, excluyendo los tratamientos utilizados por uno de los estados miembros de la Unión Europea exclusivamente con fines de tránsito.

Entre las obligaciones que fija la ley a los responsables del tratamiento figura la de informar previamente a las personas cuyos datos de carácter personal se prevé transferir en hacia un Estado no miembro de la Unión Europea.

Señala en particular que "el responsable del tratamiento o su representante debe informar de manera clara y completa a cualquier persona usuaria de las redes de comunicaciones electrónicas de:

- la finalidad de toda acción tendiente a acceder, mediante transmisión electrónica, a informaciones almacenadas en su equipo terminal de conexión, o a registrar informaciones en su equipo terminal de conexión por el mismo procedimiento;
- los medios con los que cuenta el interesado para oponerse a ello."

Asimismo, la ley prevé el derecho que toda persona física tiene a:

- oponerse, por motivos legítimos, a que sus datos de carácter personal sean objeto de un tratamiento;
- oponerse, sin gastos para ella, a que el responsable actual del tratamiento o el responsable de un tratamiento futuro utilice los datos relativos a su persona con fines de prospección comercial.

Así pues, la identificación de las personas *a sus espaldas* es manifiestamente ilegal, está debidamente sancionada y sujeta a disposiciones penales en contra de las personas físicas o morales infractoras que violen las disposiciones legales previstas y sancionadas en los artículos 226-16 a 226-24 del código penal.

#### 2.1.1. Los nuevos medios para la CNIL, insuficientes con respecto a las necesidades nacidas de la nuevas amenazas

Durante la presentación del informe anual de la CNIL el 22 de junio de 2004, su presidente, Sr. Alex Turck, destacaba el fortalecimiento de la capacidad de esta Comisión en tres ámbitos, a saber, la posibilidad de realizar verificaciones documentales y físicas aún en

contra de la voluntad de los organismos controlados; la facultad de dictar sanciones pecuniarias por un importe de hasta 300 000 €; y, por último, la capacidad de desempeñar plenamente su nuevo papel de asesora en las negociaciones internacionales llevadas a cabo por el gobierno o de autorizar códigos de conducta o softwares que contribuyan a la protección de datos personales.

Cabe señalar que el tratamiento de los datos biométricos necesarios para la autenticación o la verificación de la identidad de las personas está sujeto a una autorización por decreto aprobado por el *Conseil d'Etat* con base en la opinión fundada y publicada por la CNIL.

Sin embargo, la aplicación plena y total de la ley parece depender de un cambio drástico del comportamiento de los actores responsables, en el sentido de una mayor toma de conciencia y una mayor responsabilidad. En efecto, la CNIL estima solamente en un 30% el porcentaje de declaraciones de las PYMES. En cuanto a las 700 000 asociaciones registradas, desde 1994 sólo han sido declarados 7 000 ficheros de miembros... Y además, se trata de personas morales debidamente identificadas por el registro mercantil o por su declaración ante la administración. Ahora bien, ¿todos los actores de los tratamientos de ficheros digitalizados pueden ser debidamente identificados a partir del territorio francés y son identificables durante un tiempo suficientemente largo para poder ejercer de manera eficaz el derecho de rectificación?

De los cuatro ejes principales de la nueva CNIL definidos por su presidente, es decir, “comunicación, correspondiente, control y coerción”, el que debe ser reforzado de manera considerable, a priori como a posteriori, es el de las inspecciones, en su aspecto cualitativo, mediante una fuerte inversión en la comprensión de las técnicas, principalmente extraterritoriales, de agregación de datos múltiples y, en el cuantitativo, para mantener la proporción con respecto a los desarrollos potencialmente exponenciales a los que desde ahora nos lleva el auge de la sociedad de la información.

#### 2.1.2. Tratamientos automáticos, fusión de ficheros y realidad del consentimiento previo

Puesto que se considera que el consentimiento debe darse por cada tipo de dato, ¿cómo garantizar a los individuos el respeto de la vida privada ante tratamientos cuya finalidad es fusionar los ficheros? Ciertamente la ley considera el cotejo o la interconexión como un tratamiento de datos de carácter personal, pero su aplicabilidad se enfrenta a dificultades significativas, que no pueden ser subestimadas ante la multiplicidad de actores potenciales (responsables actuales y futuros, subcontratación por comunicación a terceras personas) tanto menos sometidos al riesgo de sanción o de condena cuanto que la posibilidad de deslocalización es real.

Cierto número de datos de carácter personal son recogidos, almacenados y tratados a partir de una identificación automatizada; *a priori*, se considera que el usuario conoce y acepta en cada caso este procedimiento. Por ejemplo, la recogida automática de datos puede realizarse a través de un pórtico detector, del uso del GPRS, del GSM o de antenas RFID. Sin embargo, nada deja suponer que exista una aceptación previa en cuanto

a la *finalidad* de un fichero que agrega datos constitutivos de la identidad, e incluso del comportamiento individual, cuya recolección se efectúa por cuenta de terceros...

El artículo 19 del reglamento (CE) citado arriba toma en cuenta los riesgos que corren las personas en cuanto al respeto de la vida privada por el simple tratamiento automatizado de los datos. Estos riesgos son tan conocidos que sólo circunstancias particulares pueden autorizar el uso de este tipo de tratamiento en el caso de decisiones que produzcan efectos jurídicos.

Así, “el interesado tiene derecho a no ser sometido a una decisión que tenga efectos jurídicos sobre él o que le afecte de manera significativa, y que **esté basada únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, fiabilidad o conducta**, salvo cuando tal decisión esté expresamente autorizada en virtud de la legislación nacional o comunitaria o, si fuera necesario, por el Supervisor Europeo de Protección de Datos”.

Recordemos aquí que de los 9 casos comunicados en 2003 por la CNIL, una sola denuncia ante la Fiscalía está relacionada con una operación de recogida ilícita y desleal de datos personales realizada a partir de anuarios, sin que las personas afectadas hayan podido ejercer eventualmente su derecho de oposición, caso “tecnológicamente” sencillo como pocos... Las mallas de la red parecen en consecuencia demasiado grandes frente a las prácticas.

### 2.1.3. Nuevos riesgos tecnológicos contra la aplicabilidad de la ley

Cuando la sociedad Cisco Systems, actor dominante a nivel mundial en el mercado de los enrutadores utilizados por internet, adquirió de la sociedad californiana P-Cube la tecnología de las plataformas que permiten a los operadores de telefonía IP (VoIP) identificar a sus “abonados”, - es decir, a usuarios de servicios gratuitos como en el caso de la oferta de Skype, o de clientes que pagan el servicio -, anunció su intención de ofrecer, a sus propios clientes operadores, **nuevas capacidades para controlar y administrar servicios como la voz sobre IP, juegos interactivos, video a pedido y P2P, o para crear ofertas específicas.**

Esto significa que con la maduración de los usos de internet que implica la generalización progresiva de la alta y la muy alta velocidad, las prácticas personales, privadas o transaccionales, serán sometidas *de facto* a un crecimiento exponencial de los registros automáticos de datos personales y, por lo tanto, a un aumento inmoderado del número de combinaciones materialmente realizables de los ficheros digitales correspondientes, tanto en el tiempo como en el espacio.

Frente a la cuestión actual sobre la gobernanza mundial de internet con fines de interés general, ¿cómo hacer aplicar en la Unión Europea, y en Francia, las obligaciones *para suprimir y convertir en anónimos* los datos de tráfico necesarios para el establecimiento de la comunicación y la facturación? (véase el art. 37 del reglamento CE citado).

En particular, el giro cada vez más acelerado del tráfico de voz, de las redes clásicas de telecomunicaciones hacia el IP total y, por otra parte, la multiplicación de operadores de comunicaciones que dan servicio en IP gracias a la reducción de barreras tecnológicas y financieras, crean una situación inédita en la que la aplicación de la ley necesitará no sólo una inversión importante en la eficacia de los modelos de control, sino también en la financiación de la consecución de un nivel adecuado. En su defecto, toda la arquitectura de la confianza ganada con mucha paciencia se debilitará por mucho tiempo.

Además, la “gratuidad” de los softwares descargados, y a veces incluso de las comunicaciones por IP, ya no permite referirse a los criterios clásicos de responsabilidad de los operadores como en una economía transaccional clásica basada en el contrato (de abonado), lo que dificulta cada vez más la búsqueda de la responsabilidad en caso de infracciones a la ley, es decir, si se recaban datos con fines ilícitos o de transferencia en tiempo real, para su tratamiento, hacia países “terceros” cuyo nivel de protección de los datos personales es considerado insuficiente por la Comisión Europea toda vez que, en ellos, el tratamiento no está sujeto a las obligaciones de declaración o acuerdo previos que protegen a la persona.

Basta con recordar que la sociedad Skype, basada en Luxemburgo y creada por los fundadores de Kazaa, desde el inicio de sus actividades ha registrado la descarga de su software gratuito por 7 millones de personas, administra 1,2 millones de llamadas diarias sin ser propietaria de ninguna red, no gasta prácticamente nada en publicidad para su servicio y sólo tiene 50 empleados (*Wall Street Journal Europe*, 25 de agosto de 2004), condiciones económicas y tecnológicas que caracterizan el umbral más bajo, casi podríamos decir inexistente, para poder entrar en el mercado.

La rapidez con que el modelo de voz sobre IP se sustituye al de las redes clásicas de telecomunicación desde ahora se refleja en las anticipaciones de los analistas financieros que constatan la contracción de los beneficios realizados por los gigantes de la industria de las telecomunicaciones. Por ejemplo, AT&T ha sufrido una baja del 18% de sus beneficios en tres años; la estimación del valor de la acción se degrada hasta alcanzar, a veces, el de los “bonos basura” (*junk bond*).

Además de los problemas planteados por la descarga gratuita de softwares, desde el punto de vista de la responsabilidad en la recogida y el tratamiento de informaciones soporte de identidad o de identificación, la cuestión del comportamiento previo se plantea aún con más agudeza cuando se trata de procesadores embarcados para los que el constructor no ha previsto la opción “optar por salirse” (*opt-out*). Del otro lado del Atlántico se utiliza el mote de “*built-in digital handcuffs*” para referirse a este tipo de chip. Hasta donde sabemos, no existen procesadores “libres”, a semejanza de los softwares libres.

Los chips electrónicos que se utilizan en las líneas de fabricación de los microordenadores, desde finales de 2004 deben incluir las especificaciones adoptadas por el Grupo TCPA (Trusted Computing Platform Alliance) del que forman parte Microsoft e Intel. Estas especificaciones comportan excelentes argumentos en términos de seguridad y protección de los derechos de propiedad intelectual. El reverso de la medalla de esta innovación es la imposibilidad de escoger entre ejercer o no el derecho de negarse a que se recojan automáticamente datos.

El departamento de informática de la Academia de Ciencias de China anunció en septiembre de 2002 la construcción del procesador “dragon chip”, basado en la arquitectura RISC (y no CISC), que utiliza una forma “achinada” de Linux, oficialmente por razones de seguridad de los sistemas de información en el ámbito de las aplicaciones militares.

En uno y otro de estos casos, las especificaciones técnicas deberán ser estudiadas a la luz de la aplicabilidad de la ley.

#### 2.1.4. Del ejercicio del derecho de rectificación

La arquitectura jurídica global de las obligaciones, sanciones y penas, se fundamenta en la noción de responsable del tratamiento, definido como cualquier entidad organizacional que, de manera independiente o conjuntamente con otras, determine los fines y los medios del tratamiento de datos de carácter personal.

En potencia, esta definición se aplica simultáneamente a tantas entidades que el ejercicio del derecho de consentimiento previo del interesado, de retractación de dicho consentimiento incluso de manera temporal, o de rectificación en el más amplio sentido del término, se vuelve - y de hecho ya lo es – prácticamente inaplicable. ¿Cómo identificar con seguridad al o a los responsable(s) del tratamiento? ¿Dónde se encuentran exactamente? El tiempo que cada persona concernida debería dedicar a comprobar que sus datos de carácter personal digitalizados están debidamente protegidos de fines ilícitos o de un uso sin su consentimiento previo es infinito, habida cuenta de las dudas que pesan sobre la adecuada conclusión de sus búsquedas o demandas.

La “gratuidad” del derecho de rectificación, elevada en la práctica legislativa al rango de principio, se vuelve entonces teoría pura.

¿Cómo puede, en estas condiciones, imponerse el respeto de la ley sobre la información previa y, posteriormente, la aplicación del nuevo artículo 43 de la ley nº 78-17 modificada antes citada, según el cual “toda persona física que compruebe su identidad puede exigir al responsable del tratamiento que, según el caso, sean rectificadas, completadas, actualizadas, bloqueadas o eliminadas las informaciones de carácter personal inexactas, equívocas o caducas, o cuya recogida, utilización, comunicación o conservación está prohibida”?

Y con mayor razón, ¿cómo comprobar eficazmente que el responsable del tratamiento ha cumplido las **formalidades necesarias** cuando un dato ha sido comunicado a terceros, para poder notificar las operaciones realizadas en el marco del derecho de rectificación y de su ejercicio (párrafo 4)?

### 2.2. El poder público es responsable del marco fijado para la trazabilidad digital de las personas, a todos los niveles de subsidiariedad

Cuando se realiza bajo la responsabilidad de las autoridades públicas, la fusión de ficheros de datos digitales de carácter personal puede plantear algunos cuestionamientos

relativos al control democrático de una finalidad de tratamiento que se revelase abusiva con respecto a las disposiciones legales.

En efecto, las mismas tecnologías que permiten a los gobiernos difundir programas y servicios, interactivos o no, mediante las aplicaciones múltiples de la administración electrónica nacional, regional o local, en “manos poco delicadas” pueden ser desviadas de sus propósitos iniciales con fines de vigilancia y observación de los ciudadanos, y ello fuera del control de los jueces a través de un proceso o de cualquier disposición legal.

A este respecto y en lo que a Francia se refiere, el abogado Etienne Wery, en un artículo publicado el 11 de agosto de 2004 en Internet, revela que el Consejo Constitucional no tuvo que pronunciarse sobre la cuestión de saber si el hecho de que la creación de un fichero policiaco conteniendo datos sensibles ya no esté subordinada a un decreto aprobado por el *Conseil d'Etat* – con base en la opinión positiva de la CNIL – era conforme o no con la constitución, toda vez que el asunto no le fue sometido; este hecho *parece* traducir un consenso, al menos coyuntural, de la clase política francesa sobre el tema.

Paralelamente, con la generalización de los modelos de administración electrónica, las autoridades que utilizan datos digitales de carácter personal para identificar o ayudar a la identificación y autenticación de las personas, deben absolutamente ser protegidas de toda intrusión en sus sistemas de información.

Deben preservar sus redes de información de las tentativas llamadas *cognitive hacking*, cuyas modalidades pretenden introducir una o varias fuentes de desinformación, particularmente en los elementos de identificación utilizados en el marco de las aplicaciones de gobierno electrónico, con miras a modificar, a sus espaldas, el comportamiento de los agentes públicos y de los actores concernidos.

Ya sea que se trate de entidades públicas o privadas, una de las amenazas que gravitan sobre la gestión y el ciclo de vida de los objetos tangibles, visibles o invisibles para el ojo humano, y para objetos intangibles, es la usurpación de una identidad digital. Esta usurpación puede tener lugar durante la fase de rastreo por radiofrecuencia (etiquetas radio inteligentes que pueden sustituir a los códigos de barras pasivos y estáticos), o mediante el uso de un software (“tatuaje” electrónico con fines de identificación y reconocimiento).

Estas cuestiones todavía no han sido resueltas técnicamente a nivel de las normas internacionales.

Por ejemplo, el tema de la usurpación de identidad de dominio en una dirección de correo electrónico, muy practicada en los envíos de correo basura (*spams*) aunque existan otros medios, forma parte de una consulta abierta hasta febrero de 2005 en el marco de un grupo de trabajo del IETF, con la apelación de protocolo llamado “Marid” intitulado “Sender ID: authenticating e-mail”. No obstante, parece imposible lograr una normalización coactiva antes de mucho tiempo (eventualmente varios años)...

Frente a la amplitud de este fenómeno mundial, los internautas han adoptado el neologismo inglés “*Phishing*”, contracción de los términos *Fishing* y *Phreaking*, que designa el fraude informático, para denominar un correo electrónico enviado por un remitente que deliberadamente se hace pasar por una sociedad o cualquier otro tipo de entidad supuestamente de confianza, con el fin de recoger informaciones sensibles de los equipos de los destinatarios.

¿Hacia qué punto de equilibrio tender, entre el síndrome de “Big brother” de la “electrónica total” y el modelo que se considera ideal, descentralizado, respetuoso de la calidad de los datos personales relacionados con la vida privada de los ciudadanos, su salud, su patrimonio, sus ingresos y su familia? La autorregulación de los actores privados no ha generado la confianza necesaria, mientras que el intervencionismo de los Estados sigue siendo objeto de paradójicas expectativas a favor de una mayor seguridad, pero también con más libertad... cuando no es una desconfianza radical hacia la acción pública en los países que se separan progresivamente de la economía planificada.

Pero lo cierto es que, en todos los casos, si no existe la voluntad de realizar concretamente lo debido, los autores del informe sobre la Hiper-República entregado en enero de 2003 al Secretario de Estado encargado de la Reforma del Estado por Pierre de La Coste, consideran en su conclusión que “no es imposible que se realice la pesadilla orwelliana, aunque no en la forma prevista por el autor”.

“Porque los grandes grupos que tendrán en su poder las llaves de las tecnologías de la información no tendrán ningún empacho en liberalizar los accesos y cruzar, en lugar de los Estados, todas las informaciones personales que recaben, ni en brincarse las barreras jurídicas irrisorias que éstos intenten oponerles, particularmente en Francia. Lejos de ser un aliado del Estado, *Big brother* será su peor enemigo”.

Se ha abierto en Francia un nuevo campo de aplicación de la ley en el contexto de la reforma del sistema de salud y del seguro médico, que merece un examen particular.

### 2.2.1. Protección de la identidad digital en salud: contexto y alcance

Como herramientas de ayuda a la protección de los datos para los responsables del tratamiento, las tecnologías de seguridad de los sistemas de información son utilizadas por numerosos actores privados, encabezados por los actores del intercambio monetario pero también, en un futuro próximo, por los profesionales de la salud.

La instauración del expediente médico personalizado, creado por el artículo 3 de la ley n°2004-810 del 13 de agosto de 2004 relativa al seguro médico, constituirá a este respecto un desafío particular tanto para la definición de los elementos constitutivos de los datos personales como para su digitalización, recogida, tratamiento y utilización. Y esto concierne a toda la población francesa cubierta por el seguro médico, es decir, prácticamente a 60 millones de personas.

Creado y hospedado por un profesional autorizado del alojamiento web de datos de salud de carácter personal, el expediente médico personalizado tendrá un acceso restringido y no permitirá su consulta, en particular, al sector de la medicina del trabajo ni en el marco de la conclusión de contratos de protección complementaria en materia de cobertura de gastos médicos. Un decreto aprobado por el *Conseil d’Etat* después de haber escuchado la opinión de la CNIL determinará las condiciones en las que podrá utilizarse un identificador para la apertura y la gestión del expediente médico personal.

Un GIP (Grupo de interés público) denominado *Institut des données de santé* (Instituto de los datos de salud), creado por el artículo 64 de la misma ley, tiene por misión asegurar la coherencia y velar por la calidad de los sistemas de información utilizados para

la gestión del riesgo enfermedad; velará, además, porque se ponga a disposición de sus miembros datos procedentes de los sistemas de información de sus mismos miembros con fines de gestión del riesgo de enfermedad o relativos a cuestiones y preocupaciones de sanidad pública.

Con la constitución de este expediente médico digital se franqueará un nuevo paso hacia la identidad digital humana. Esta maravillosa posibilidad técnica, que augura ahorros sustanciales por la ganancia de eficacia en el servicio a los asegurados, deberá estar rodeada de las precauciones habituales y habrán de preverse sanciones para los infractores ajustadas a los riesgos de abuso que puede engendrar. Desarrollaremos este punto más adelante, en el marco de la reglamentación europea relativa a los datos biométricos personales digitalizados. En este tema, la opinión de la CNIL comportará una responsabilidad societal considerable.

El derecho comunitario se apoya en el artículo 286 del tratado constitutivo de la Comunidad Europea, según el cual los actos comunitarios relativos a la protección de las personas físicas con respecto del tratamiento de datos con carácter personal y a la libre circulación de esos datos, son aplicables a las instituciones y órganos establecidos por el tratado o sobre la base del mismo.

Las disposiciones de “puerto seguro” llamadas de *safe harbour* relativas al nivel de protección de los datos de carácter personal exportados hacia países no miembros de la Unión Europea, han sido reforzadas por la decisión de la Comisión adoptada el 27 de diciembre de 2001 referente a las cláusulas contractuales tipo para la transferencia de esos datos hacia los encargados del tratamiento establecidos en países terceros en virtud de la directiva 95/46/CE.

En particular, recuerdan que el exportador de datos “responsable del tratamiento de los datos personales transferidos”, es quien está obligado a la reparación en caso de recurso judicial, quedando entendido que el derecho de apelar contra el importador constituye una excepción. También en este caso cabe interrogarse acerca de la aplicabilidad del principio de gratuidad de los recursos judiciales en los largos y complejos juicios a nivel internacional, además de la dificultad que implican la trazabilidad y el establecimiento de pruebas técnicas.

La interpretación que la sociedad Microsoft hace de estas disposiciones de *safe harbour* consiste en escribir, en su convenio de confidencialidad (disponible en versión española: <http://privacy2.msn.com/es-us/fullnotice.aspx>), que “Microsoft se atiene al acuerdo de Safe Harbor establecido por el Departamento de Comercio de los Estados Unidos en relación con la recopilación, el uso y la retención de datos procedentes de la Unión Europea”. Y añade que (en MSN) “no utilizamos ni revelamos sin su expreso consentimiento información personal confidencial como la relativa a la raza, religión o tendencia política”, lo que supone sin embargo que eventualmente podría hacerlo.

El derecho comunitario ha sido completado recientemente en lo que se refiere a la protección de los datos personales para responder a las exigencias contrastadas de la sociedad civil, que pide un respeto mayor y garantizado de su derecho a la protección de la

vida privada y, al mismo tiempo, confianza en las instituciones para garantizar el orden público, en particular frente a acciones terroristas.

La directiva sobre la privacidad y las comunicaciones electrónicas antes citada, cuyo objeto es actualizar la directiva del 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, tiene en cuenta la introducción, en la Unión Europea, de nuevas tecnologías digitales, así como de los nuevos servicios de comunicación electrónica aportados por la generalización progresiva del uso de internet y su estela de posibilidades inéditas de recopilación y tratamiento de datos relativos a la persona y a su vida privada.

Mide bien los riesgos al considerar que **“los denominados «programas espía» (spyware), web bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios” (considerando 24)**. Estima que “sólo debe permitirse la utilización de tales dispositivos para fines legítimos y con el conocimiento de los usuarios afectados”.

Reconoce también que este tipo de dispositivos, como los denominados “chivatos” (*cookies*), pueden constituir un elemento de gran utilidad por ejemplo para verificar la identidad de los usuarios que participan en una transacción en línea, pero su uso sólo debe ser autorizado a condición de que se facilite al usuario información clara y precisa al respecto y se respete su “derecho a impedir” (la instalación de tales dispositivos).

También admite el hecho de que los datos de posición geográfica del equipo terminal móvil del usuario suelen ser presentados de manera más precisa que lo estrictamente necesario para la transmisión de una comunicación, y que estos datos pueden utilizarse para ofrecer servicios personalizados de valor añadido, como información sobre tráfico y orientaciones individualizadas a los conductores. También en este caso, la directiva recomienda que el proveedor obtenga el consentimiento previo (art. 9), con la posibilidad, por un procedimiento gratuito y sencillo, de rechazar temporalmente el tratamiento de los datos de localización incluso cuando se ha consentido a ello anteriormente.

De entre las recientes disposiciones de la legislación comunitaria, tres merecen ser mencionadas: el nombramiento del Supervisor Europeo de Protección de Datos (22 de diciembre de 2003), la Agencia Europea para la seguridad de las redes y la información (creada por decisión del Consejo y del Parlamento Europeo el 20 de noviembre de 2003) y el proyecto de sistema de información sobre visados, a raíz de las conclusiones del Consejo JAI (Justicia y Asuntos de Interior) del 5 y 6 de junio de 2003, que integra datos biométricos.

En los tres casos, la voluntad manifiesta del legislador europeo parece concordar con las expectativas de la sociedad civil. No obstante, es preciso advertir la dificultad que implica la toma de decisión final así como los retrasos, a veces considerables, observados en la instauración, e incluso la aplicación aparentemente mínima, de los textos comunitarios finalmente adoptados.

## 2.2.2. El Supervisor Europeo de Protección de Datos

La institución del Supervisor Europeo de Protección de Datos tiene su origen en el artículo 41 del reglamento adoptado el 18 de diciembre de 2000. El tratado CE había previsto que, antes del 1º de enero de 1999, una decisión tripartita, tomada con base en el procedimiento señalado en su artículo 251, constituiría un órgano independiente de supervisión encargado de vigilar la aplicación de la obligación de proteger los datos que tienen las instituciones contempladas en el mismo Tratado.

El estatuto y las condiciones generales de ejercicio de las funciones correspondientes sólo fueron objeto de una decisión del Parlamento Europeo, del Consejo y de la Comisión hasta el 1º de julio de 2002, y ha debido esperarse hasta el 17 de enero de 2004 para que se publicara la decisión del Parlamento Europeo y del Consejo por la que se nombra a la autoridad de control independiente prevista por el artículo 286 del Tratado CE, que da paso al nombramiento del holandés Johan Hustinx y de su adjunto español, Joaquín Bayo Delgado, para un período de 5 años.

En total, el retraso entre la intención del legislador europeo y la puesta en obra efectiva fue de cinco años; mientras tanto, en la Unión Europea y en el mundo desarrollado tuvo lugar la revolución de Internet.

Para el futuro, el artículo I-51 del título VI del proyecto de tratado constitucional de la Unión Europea intitulado “Vida democrática de la Unión”, afirma el derecho de toda persona a la protección de los datos personales que la conciernen, y sitúa en el plano de la legislación europea las reglas relativas al respeto de ese derecho por parte de las instituciones, órganos y agencias de la Unión, que debe estar sujeto al control de una autoridad independiente.

Entre las cinco misiones a corto plazo presentadas ante el Parlamento polaco el 26 de mayo de 2004, el Supervisor europeo no se refiere a la evaluación del impacto de la evolución de las tecnologías de la información sobre la protección de los datos. Menciona, simplemente, que una de sus atribuciones importantes consiste en hacer un seguimiento de los hechos nuevos de interés, en la medida en que tengan repercusiones sobre la protección de los datos de carácter personal. A pesar de tomarla textualmente del artículo 46, párrafo e) del reglamento fundador, el Supervisor omite completar su declaración con el final de dicho párrafo, que reza: “en particular de la evolución de las tecnologías de la información y la comunicación”.

No obstante, en el plan de acción de su institución, reconoce plenamente la incidencia que tiene la lucha contra el terrorismo tal como la llevan a cabo los Estados Unidos y la Unión Europea. Por esta razón, ha tomado la iniciativa de entrar en contacto con el coordinador de la lucha contra el terrorismo en la Unión Europea, Sr. Gijs de Vries y, más allá de los convenios denominados de “*safe harbour*” para la seguridad de los flujos transfronterizos de datos, podría tener que dar opiniones y consejos sobre la muy sensible cuestión de la comunicación de datos relativos a los pasajeros aéreos, habida cuenta de la divergencia de las posiciones tomadas por el Parlamento Europeo y, posteriormente, por la Comisión Europea sobre su decisión, que no ha suscitado la unanimidad.

Será necesario esperar los primeros informes de actividad de esta nueva institución europea para evaluar los resultados obtenidos con relación a las misiones confiadas.

Con sus 15 empleados de tiempo completo y su funcionamiento en doble red con los delegados de cada institución comunitaria y, por otra parte, su cooperación con los representantes de los Estados miembros dentro del grupo de trabajo denominado “del artículo 29” (de la directiva de 1995), esta institución ciertamente tiene el potencial requerido para implementar la vigilancia tecnológica necesaria y que figura, *expressis verbis*, en su texto fundador. Pero falta que reconozca la importancia estratégica de esta vigilancia, cosa que en realidad no aparece claramente en su único comunicado público, disponible en su sitio Internet.

### 2.2.3. La Agencia Europea de Seguridad de las Redes y la Información (ENISA)

Concebida a raíz de los eventos del 11 de septiembre de 2001, en el contexto de la banalización de los ataques lógicos a través de internet y como respuesta a las presiones de los actores del comercio electrónico, la Agencia Europea de Seguridad de las Redes y la Información tenía como primera intención hacerse cargo de importantes misiones de interés general comunitario.

El 18 de febrero de 2003, el Consejo Europeo decidió pronunciarse a favor de la propuesta de la Comisión consistente en crear un grupo de trabajo sobre la ciberseguridad. Invitaba a los Estados miembros a desarrollar la formación y la sensibilización, sobre todo entre los jóvenes, respecto de las problemáticas de seguridad planteadas por los sistemas de información.

La Agencia, jurídica y financieramente operacional desde enero de 2004 (24,3 millones de euros durante 5 años), cuenta finalmente con un consejo de administración integrado por un representante de cada Estado miembro, de conformidad con el acuerdo tomado por el Parlamento Europeo y el Consejo el 20 de noviembre de 2003. Henri Serres, Director Central de Seguridad y Sistemas de Información, es el representante de Francia.

La ENISA fue creada para aconsejar y asistir a la Comisión y a los Estados miembros en el conocimiento de las amenazas que pesan sobre la seguridad de los sistemas de información y en su diálogo con la industria, ya sea que se trate de infraestructuras o de datos digitales considerados sensibles, de carácter personal o no.

Más concretamente, su cometido consiste en identificar los problemas relativos a los equipos y programas que se ofrecen en el mercado interior; recoger y analizar los datos sobre los incidentes de seguridad ocurridos en la Unión Europea y explicitar los riesgos emergentes; promover los métodos apropiados de evaluación y gestión de riesgos para reforzar la capacidad de enfrentar las amenazas relacionadas con la seguridad de la información; y, por último, acrecentar la sensibilización y la cooperación entre los diferentes actores del sector, desarrollando la colaboración entre instancias públicas y privadas, entre otras tareas.

Hasta la fecha, no se ha mencionado de manera explícita que los nuevos riesgos que pudiesen obstaculizar la legislación sobre la protección de datos personales,

susceptibles de ocurrir por los recientes desarrollos tecnológicos durante la interconexión y el uso de las redes y sistemas de información, formen parte del campo de acción de la ENISA. Sin embargo, nada en los textos permite excluir su competencia en esta cuestión.

También en este caso será conveniente esperar los primeros informes de actividad de la ENISA para saber si esta agencia pretende tratar, y en qué medida, el complejo tema de los potenciales y las amenazas de la identificación digital de las personas y la identidad digital de los objetos y servicios, desde el punto de vista del respeto de la legislación europea sobre los datos personales, entendida ésta como uno de los elementos capitales de la confianza de los ciudadanos europeos en la oferta de bienes y servicios de la sociedad de la información en Europa.

El posicionamiento actual, en su fase de arranque, parece ser el de un organismo de observación, dado que las medidas que deben ser puestas en obra incumben a cada Estado miembro. El uso del programa comunitario Modinis 2003-2005 de seguimiento del plan de acción e-Europa podría constituir un medio para hacer que se tome en consideración la estrecha relación entre la confianza y el respeto de los datos personales en la búsqueda de un nivel eficiente de seguridad de los sistemas de información.

#### 2.2.4. Riesgos específicos inherentes a la centralización de los datos digitales de carácter personal.

Acerca de la centralización de datos, cabe señalar que el grupo de trabajo sobre la protección de datos, denominado grupo del artículo 29, se pronunció sobre el uso de datos biométricos el 1º de agosto de 2003. Adoptando un enfoque muy equilibrado con respecto a los potenciales y riesgos, insiste sin embargo sobre los peligros particulares de todo sistema centralizado de imágenes e identificadores digitales.

Recuerda que varias autoridades nacionales se han pronunciado a favor del almacenamiento de datos utilizando medios pertenecientes a la propia persona, como una tarjeta con chip, una tarjeta bancaria o un teléfono móvil, pero admite que es imposible realizar un reconocimiento sin un sistema dotado de la imagen digital a partir de la cual pueda realizarse la verificación.

El grupo de trabajo subraya que en ciertos casos la biometría puede permitir un *mayor* respeto de la vida privada y la intimidad cuando este tipo de información hace superfluo el cotejo con otros datos de identificación, como el apellido, el nombre o la dirección.

No obstante, insiste sobre la ilusión de confianza total que podría asociarse con estos identificadores digitales, tanto por la disminución de vigilancia del respeto de la vida privada derivada del uso banalizado desde la infancia (acceso al comedor escolar, al préstamo de libros en las bibliotecas, por ejemplo), aunque también, y de manera más grave, por la casi imposibilidad de aportar la prueba de una falla material, cuyas consecuencias podrían causar importantes perjuicios y, llegado el caso, dificultades considerables para asumir una defensa legal.

¿Cómo podrían los ciudadanos de la Unión Europea ser capaces de detectar un eventual error y ejercer su derecho a la rectificación? ¿Cuánto les costaría realmente? ¿En qué consistirían las eventuales reparaciones por el (los) daño(s) sufrido(s), si se diera el caso? ¿Y cuál sería el plazo para conseguir la información y la notificación de la rectificación?

El grupo del artículo 29 concluye manifestando su fuerte preferencia por los sistemas basados en datos biométricos cuya recogida, digitalización y finalidad del tratamiento no se efectúe a espaldas de los interesados y a partir de rastros que hayan podido dejar sin darse cuenta (huellas digitales, ADN...), que no se centralicen en un sistema único, que no conduzcan automáticamente a la interconexión con otros sistemas y ficheros por el solo hecho de su arquitectura técnica y, por último, que faciliten el ejercicio, por parte de las personas concernidas, del control de los tratamientos realizados con base en sus datos personales digitalizados.

El 2 de diciembre de 2004 el Parlamento Europeo adoptó una resolución legislativa parlamentaria sobre el proyecto de reglamento del Consejo, estableciendo normas para los dispositivos de seguridad y los elementos biométricos integrados en los pasaportes de los ciudadanos europeos, en el sentido de las recomendaciones del grupo del artículo 29. Adoptó una enmienda al artículo 1º del reglamento, según la cual **“No se establece ninguna base centralizada de los pasaportes y documentos de viaje de la Unión Europea que contenga datos biométricos y de otro tipo, de todos los titulares de un pasaporte de la UE.”**

## **CONCLUSIÓN**

El informe ha permitido mostrar la emergencia de una tecnología de identificación de entidades digitales, cuyo desarrollo más rápido tiene lugar actualmente en el ámbito de la logística, como complemento de las tecnologías del código de barras.

La hoja de ruta tecnológica de los chips RFID, la aceleración del equipamiento de los actores en sistemas de información que permiten desarrollar de manera eficaz el conocimiento de sus existencias y flujos, como también el conocimiento de las rutas de tránsito y de los comportamientos, abren importantes perspectivas de mercado, de mucho mayor trascendencia que la simple sustitución, a cierto plazo, del sistema código de barras por otro sistema totalmente digitalizado y sin contacto, mundialmente interoperable.

El acercamiento, o incluso la identidad, de los actores más significativos de las infraestructuras del Sistema de Nombres de Dominio (DNS) de internet con los del Sistema de Nombres de Objetos (ONS), hace temer desviaciones incontrolables en términos de captura de información de tipo comercial, económico, financiero, tecnológico y, en resumidas cuentas, estratégico.

La toma de conciencia sobre una concentración de los poderes de intervención en torno a unos cuantos actores, que refuerza el liderazgo norteamericano en el control de los sistemas de información, todavía es poca, o incluso inexistente, tanto entre los actores del mercado como entre las autoridades públicas, en Francia y en la Unión Europea.

Francia y la Unión Europea todavía están buscando un punto de equilibrio institucional por cuanto se refiere a la protección de datos de carácter personal digital y de los usos ilícitos de datos que permiten la identificación de la persona y su comportamiento.

La multiplicación de situaciones que permiten la recogida de datos y las oportunidades de tratamiento por interoperatividad y exportación hacia “terceros”, el establecimiento de relaciones más o menos formales desde el punto de vista contractual entre actores privados y profesionales de internet, así como el fuerte desarrollo de la administración electrónica, crean un verdadero dilema para la sociedad civil, cuyas expectativas, a veces contradictorias, no ayudan a los poderes públicos a escoger con facilidad las políticas más adecuadas.

Ya existen instrumentos apremiantes para marcar los límites y sancionar los usos delictuosos. No obstante, la insuficiente vigilancia tecnológica y el retraso en la adopción de modos coercitivos apropiados para hacer que los actores respeten la ley más allá de las diligencias debidas, crean un contexto desfavorable al libre arbitrio y a la confianza que se necesita para la generalización de la sociedad de la información en beneficio del mayor número posible de personas.

Queda por explorar una serie de recomendaciones para atenuar las debilidades identificadas que, más allá de los simples consejos, propone integrar en el programa de acción del CGTI la definición de un pliego de condiciones para la evaluación dinámica y el control de las evoluciones tecnológicas en Francia y en esta materia.

El informe previsto en el programa de 2004 sobre la identidad digital podrá servir como exposición de motivos para ese pliego de condiciones. Presentará la problemática de la identificación desde tres ángulos: la creación, el tratamiento y el uso de datos personales; la trazabilidad de los objetos durante todo el ciclo de vida del producto; y, por último, la trazabilidad de los servicios. Tratará de las aplicaciones lícitas así como aquellas que pueden practicarse de manera voluntariamente oculta, ya sea que entren o no en el marco de la licitud.

## **RECOMENDACIONES**

1. Efectuar un análisis profundo de las amenazas que presentan las tecnologías RFID, tanto de las que afectan a las personas, como a las empresas o a la soberanía nacional, principalmente en lo que respecta a su facilidad de uso.
2. Sensibilizar a los actores de la oferta y de la demanda en materia de RFID con respecto a las oportunidades y las amenazas que presenta esta tecnología.
3. Implementar los medios pedagógicos correspondientes (coloquios, foros, artículos, ...), de tal manera que se suscite la confianza del gran público y se dé a los poderes públicos las herramientas necesarias para preservar la soberanía nacional.
4. Adaptar la oferta de servicios en materia de RFID a la luz de las lecciones aprendidas.
5. Favorecer las iniciativas profesionales, ya sea que surjan de los fabricantes o de los usuarios, con miras al desarrollo de aplicaciones RFID que infundan en el consumidor y el ciudadano una confianza nacida del entendimiento.
6. Evaluar la aplicabilidad de la ley garantizando la protección de los datos de carácter personal desde el punto de vista de la tecnología de identificación digital por radiofrecuencia.
7. Favorecer la participación de Francia en las instancias de normalización y foros internacionales en materia de tecnología RFID, de instancias alternativas de atribución de nombre y de direccionamiento.
8. Invertir en la investigación sobre los efectos económicos y sociales de las tecnologías RFID y de los sistemas de información que sirven de base para las aplicaciones con alcances societales.

---

*Comité de Inspection*

---

## **LAS TECNOLOGÍAS DE IDENTIFICACIÓN POR RADIOFRECUENCIA (RFID): RETOS INDUSTRIALES Y CUESTIONES SOCIETALES**

---

**Informe presentado por**

**Françoise ROURE, Inspector general  
Jean-Claude GORICHON, Inspector general  
Emmanuel SARTORIUS, Ingeniero general**

**A N E X O S**

**Informe N° II-B.9 - 2004  
Enero de 2005**

## ÍNDICE de los ANEXOS

---

- ANEXO 1 : Siglas y acrónimos
- ANEXO 2 : Bibliografía
- ANEXO 3 : Sitios Internet
- ANEXO 4 : Documentos anexados

# ***A N E X O 1***

---

## Siglas y acrónimos

---

CISC	: Complex Instruction Set Computer
CNIL	: Comisión Nacional de Informática y Libertades
DNS	: Domain Name System
DoC	: Department of Commerce
DoD	: Department of Defense
DOI	: Digital Object Identifier
EAN	: European Article Number
ENISA	: Agencia Europea para la Seguridad de las Redes y la Información (en inglés: European Network Information Security Agency)
GAC	: Government Advisory Committee
GAO	: General Accounting Office
GIP	: Grupo de Interés Público
GPRS	: General Packet Radio Service
GSM	: Global System for Mobile communications
IETF	: Internet Engineering Task Force
IP	: Internet Protocol
JAI	: Justicia y Asunto de Interior (Consejo)
ONS	: Object Naming System
RFID	: Radio Frequency Identification
RISC	: Reduced Instruction Set Computer
UID	: Universal Identity
WGIG	: Wireless Global Information Grid

# ***A N E X O 2***



## Bibliografía

---

### Disposiciones jurídicas citadas en el informe:

#### ***Derecho francés***

Ley n°2004-801 del 6 de agosto de 2004 relativa a la protección de las personas físicas con respecto del tratamiento de datos de carácter personal, que modifica la ley n°78-17 del 6 de enero de 1978 relativa a la informática, los ficheros y las libertades.

Código penal, artículos 226-16 a 226-24, sección V, "De los atentados contra los derechos de las personas resultantes de los ficheros o de tratamientos informáticos".

Ley n°2004-810 del 13 de agosto de 2004 relativa a l seguro médico, "expediente médico personalizado", art. 3 y "uso de los datos de salud" art. 64.

#### ***Derecho de la Unión Europea***

Reglamento (CE) n°45/2001 del Parlamento Europeo y del Consejo, del 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, y a la libre circulación de esos datos (DOCE del 12 de enero de 2001).

Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (DOCE del 23 de noviembre de 1995).

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de intimidad en el sector de las comunicaciones electrónicas (DOCE del 31 de julio de 2002).

Decisión de la Comisión n°2002/16/CE del 27 de diciembre de 2001 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la directiva 95/46/CE.

Decisión n°1247/2002/CE del Parlamento Europeo, de l Consejo y de la Comisión, del 1° de julio de 2002, relativa al estatuto y a las condiciones generales de ejercicio de las funciones de Supervisor Europeo de Protección de Datos (DOCE del 12 de julio de 2002).

Decisión n°2004/55/CE del Parlamento Europeo y del Consejo, del 22 de diciembre de 2003 por la que se nombra a la Autoridad de vigilancia independiente prevista por el artículo 286 del Tratado CE (Supervisor Europeo de Protección de Datos) (DOCE del 17 de enero de 2004).

Resolución del Consejo (2003/C 48/01) del 18 de febrero de 2003 sobre un enfoque europeo orientado hacia una cultura de seguridad de las redes y de la información (DOCE C 048, 28 de febrero de 2003).

Resolución legislativa parlamentaria del 2 de diciembre de 2004 sobre el proyecto de reglamento del Consejo que establece las normas para los dispositivos de seguridad y los elementos biométricos integrados en los pasaportes de ciudadanos de la Unión Europea (P6\_TA-PROV (2004) 0073 A6-0028/2004).

Propuesta de decisión del Consejo relativa a la creación del sistema de información de visados (VIS) (COM (2004) 99 final).

Carta europea de los derechos fundamentales, art. 8 (futuro II-8 del proyecto de Constitución), adoptada por la Cumbre Europea de Niza, junio de 2002.

Artículo 29 – Data protection Working Party, « Working document on biometrics », 1268/02/EN WP 80, 01/08/2003, 11 p.

### ***Derecho internacional***

Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal o Convención 108 del Consejo de Europa, adoptada en 1981, ratificada por 31 Estados miembros del Consejo de la Unión Europea, art. 8 en particular.

### ***Informes***

*La RFID dans la distribution : une technologie prometteuse mais limitée à la sphère logistique ? Synthèse Amérique du Nord, Asie, Europe occidentale* (La RFID en la distribución: ¿una tecnología prometedor pero limitada a la esfera logística? Síntesis América del Norte, Asia, Europa occidental). Ministerio de Economía, Finanzas e Industria , DREE 5 C, abril de 2004, 21 p.

*L'Hyper République. Bâtir l'administration en réseau autour du citoyen* (La Hiper-República. Construir la administración en red en torno al ciudadano). Informe entregado a Henri Plagnol, Secretario de Estado para la Reforma del Estado, por Pierre de La Coste. Relator Vincent Bénard. 8 de enero de 2003.

### ***Especificaciones técnicas***

Department of Defense standard practice. Military marking for shipment and storage. (Point 4.9 RFID), 29 de octubre de 2004.

### ***Artículos***

Anne Debet, comisaria miembro de la CNIL, *L'Europe de la sécurité* (La Europa de la seguridad), 23 de julio de 2004. Tribune in <http://www.cnil.fr>.

Brett Glass : « Microsoft's Palladium : security for whom ? 24 de junio de 2004, in [http://www.extremetech.com/print\\_article/0,3998,a=28481,00.asp](http://www.extremetech.com/print_article/0,3998,a=28481,00.asp).

Etienne Wery : *La France transpose enfin la directive vie privée de 1995 ! La loi du 6 août 2004 est publiée au JO (Por fin Francia transpone la directiva sobre la privacidad de 1995! La ley del 6 de agosto de 2004 se publica en el DO)*, 11 de agosto de 2004, in [http://www.droit-technologie.org/1\\_2.asp?actu\\_id=971](http://www.droit-technologie.org/1_2.asp?actu_id=971).

# ***A N E X O 3***



## Sitios Internet

---

<http://www.dodrfid.org>

<http://www.EPCglobalUS.org>

<http://www.verisign.com>

<http://www.edps.eu.int> Sitio del Supervisor Europeo de Protección de Datos.

[http://europa.eu.int/comm/internal\\_market/privacy/links1\\_fr.htm](http://europa.eu.int/comm/internal_market/privacy/links1_fr.htm) Sitio de la Comisión Europea sobre los enlaces útiles relacionados con la política de protección de datos personales.

<http://privacy2.msn.com/fr-fr/fullnotice.aspx> Sitio de Microsoft relativo al marco y a los compromisos de respeto de los datos personales digitalizados recogidos por los sitios y los servicios MSN (por ejemplo MSN Hotmail, MSN Money o MSN Health...).

<http://www.ietf.org/internet-drafts/draft-ietf-marid-core-03.txt> Sitio del IETF relativo al documento de trabajo sobre la autenticación de los dominios de la dirección de remitentes de correo electrónico. 2004, 10 p.

<http://english.peopledaily.com.cn>. rúbrica Ciencia / Educación, 29 de septiembre de 2002, en particular.

# ***ANEXO 4***

---

## Documentos anexados

---

- 4.1 **UID *registry concept* : representación gráfica DoD y calendario provisional**
- 4.2 ***Military marking for shipment and storage*. MIL-STD6129P w/Change 3 29, DoD, octubre de 2004**
- 4.3 ***Radio Frequency Identification (RFID) Policy*, The Under Secretary of Defense, DoD, 30 de julio de 2004**
- 4.4 **“*Verisign to run EPC Directory*”, RFID Journal, 13 de enero de 2004**
- 4.5 ***Demain, une autre gouvernance de l'INTERNET* (Mañana, otra gobernanza de INTERNET), presentación .ppt, J-C. Gorichon, 4 de enero de 2005**
- 4.6 **Posición del IEEE contra el uso de identificadores universales (UID)**
- 4.7 ***Verisign : the EPC Network : Enhancing the Supply Chain (White paper) 2004***

# ***ANEXO 4.1***

---

**UID registry concept : representación gráfica DoD y calendario previsional**

# ***A N E X O 4.2***

---

***Military marking for shipment and storage.***  
**MIL-STD6129P w/Change 3, DoD**  
**29 de octubre de 2004**

# ***A N E X O 4.3***

---

***Radio Frequency Identification (RFID) Policy,  
The Under Secretary of Defense, DoD  
30 de julio de 2004***

# ***A N E X O 4.4***

---

***“Verisign to run EPC Directory”, RFID Journal  
13 de enero de 2004***

# ***A N E X O 4.5***

---

***Demain, une autre gouvernance de l'INTERNET,***  
**presentación .ppt, J-C. Gorichon**  
**4 de enero de 2005**

# ***ANEXO 4.6***

---

**Posición del IEEE contra el uso de identificadores universales (UID)**

# ***A N E X O 4.7***

---

***Verisign : the EPC Network : Enhancing the Supply Chain (White paper) 2004***