AECIT
ASOCIACIÓN ESPAÑOLA DE
EXPERTOS CIENTÍFICOS EN TURISMO

REVISTA DE ANÁLISIS TURÍSTICO, nº 16, 2º semestre 2013, pp. 13-20

IDENTIFICACIÓN Y AUTENTIFICACIÓN DE CLIENTES EN ESTABLECIMIENTOS HOTELEROS. LA DIFÍCIL COMBINACIÓN ENTRE BIOMETRÍA Y HOTELERÍA

José Ramón Soler Fuensanta
Vicente Guasch Portas
Escuela Universitaria de Turismo del Consell de Ibiza

Revista de Análisis Turístico
ISSN impresión: 1885-2564; ISSN electrónico: 2254-0644
Depósito Legal: B-39009

www.aecit.org email: analisisturístico@aecit.org

IDENTIFICACIÓN Y AUTENTIFICACIÓN DE CLIENTES EN ESTABLECIMIENTOS HOTELEROS. LA DIFÍCIL COMBINACIÓN ENTRE BIOMETRÍA Y HOTELERÍA

José Ramón Soler Fuensanta
j.ramon.soler@ipsasoft.com
Escuela Universitaria de Turismo del Consell de Ibiza

Vicente Guasch Portas
v.guasch@hotmail.com
Escuela Universitaria de Turismo del Consell de Ibiza

resumen

Uno de los puntos más conflictivos en cualquier establecimiento hotelero es sin duda la correcta identificación de sus clientes. Dentro de las tecnologías más atrayentes para solucionar este problema está la biometría, ya probada en otros entornos con una eficacia y eficiencia más que sobresaliente. Sin embargo, problemas legales, que no técnicos, impiden una correcta y amplia implantación de estas tecnologías. El presente texto hace un repaso a los sistemas de identificación y autentificación de clientes en el sector hotelero haciendo hincapié en las tecnologías biométricas y los problemas legales derivados de su utilización.

Palabras clave: Biometría, LOPD, identificación, hoteles, hotelería, autentificación.

abstract

One of the most contentious points in any hotel establishment is undoubtedly the correct identification of their customers. Between the most compelling technologies to solve this problem we have the biometrics, already tested in other environments with an efficiency and effectiveness more than outstanding. However, legality and not technical problems inhibit the correct and widespread deployment of these technologies. This paper gives an overview of the identification and authentication systems for customers in the hospitality industry with an emphasis on biometric technologies and legal issues arising from their use.

Key words: Biometrics, LOPD, identification, hotels, hospitality, authentication.

ISSN impresión: 1885-2564
ISSN electrónico: 2254-0644

1. introducción

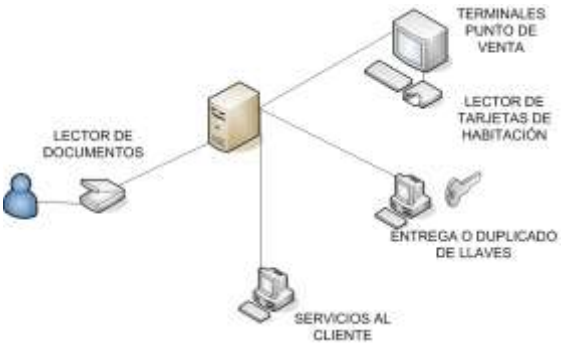
La introducción paulatina de las nuevas tecnologías en los establecimiento hoteleros ha significado sin duda una gran mejora en todos los sentidos. No solo ayudan en temas de gestión simplificando las tareas administrativas, facilitando el trabajo en el front-office y en el back-office, sino que también permiten tener un mejor control de las necesidades del cliente durante su estancia, y, en el caso de que éste lo permita, son una inestimable ayuda en temas de promoción, fidelización y marketing. Internet ha sido uno de los catalizadores de las necesidades del cliente y no se percibe un hotel sin página web en la que se permita la reserva de plazas. La visualización por parte de la dirección del hotel de páginas de control de reputación, como tripadvisor.com, son una cosa habitual, así como el uso de herramientas de yield Management. Sin embargo, temas más cercanos y no por ello menos importantes como la correcta identificación y autentificación del cliente siguen siendo una de las asignaturas pendientes en muchos hoteles. Debemos quizás hacer una distinción entre ambos conceptos. La identificación nos permite inicialmente saber quien es el cliente, y es él quien nos facilita esa información, aunque puede ser falsa. La autentificación nos permite determinar, con un alto grado de certeza, si el cliente es quien dice ser. Algunos han apostado por el uso de herramientas biométricas, lectores de huella digital fundamentalmente, para solucionar el problema de la suplantación de identidad. Sin embargo esta cuestión no ha sido completamente resuelta.

Las maneras de identificar/autentificar al cliente no varían de las utilizadas en un entorno de seguridad clásico. Estos esquemas se basan en:

- Algo que el usuario sabe (conocimiento). El ejemplo clásico es pedir la habitación. Tiene el inconveniente de que el cliente puede darnos una habitación errónea, bien por descuido o bien a propósito para evitar la carga de un servicio extra en su cuenta. Para minimizar este problema se suele pedir además el nombre del ocupante de la habitación, pero este nombre puede haberse obtenido de forma ilícita, o incluso con la connivencia del empleado que teóricamente realiza el control.
- Algo que el usuario tiene (propiedad). Generalmente la tarjeta de la puerta o una tarjeta de cliente. En este caso se pasa la tarjeta por un lector que identifica la habitación y como comprobación adicional se suele solicitar el número de habitación que no aparece impreso en la tarjeta. El punto débil se encuentra en que la tarjeta puede duplicarse, encontrarse o, en el caso de hoteles con All Inclusive, pasarse a otros usuarios.
- Algo inherente al usuario. Su principal problema es un coste mayor y, como veremos, los inconvenientes legales en su implantación. Se basan en:
  - Algo que el usuario es (aspecto fisiológico).
  - Algo que el usuario hace (aspecto de comportamiento).

Evidentemente una combinación de estos sistemas puede ser mucho más fiable que la utilización de uno solo de estos métodos de autentificación. Un esquema que funciona desde hace varios años en hoteles de nuestro país aprovecha el proceso de la llegada del cliente para diseñar un sistema de autentificación sencillo pero potente. A la llegada del cliente, y con la intención primera de rellenar automáticamente la ficha de policía, se pasa el DNI o pasaporte por un lector de pasaportes que, aparte de imprimir y guardar la ficha de policía, discrimina la foto y firma del cliente que se asignan al ocupante de la habitación correspondiente en su reserva. A partir de este momento cualquier actuación en el hotel (pedir duplicado de llaves, carga de extras a habitación, acceso a comedor, o simple control de acceso a ubicaciones destinadas a clientes del hotel), se realiza pasando la tarjeta por el lector correspondiente, que presenta, en el terminal punto de venta o de control, la foto del propietario de la tarjeta, o, en el caso de ser una tarjeta de habitación, la foto de todos sus ocupantes.

Gráfico 1. Sistema de identificación no biométrico.



Fuente: Elaboración propia.

Sin embargo, si vemos las tendencias del mercado, sobre todo en hoteles con un cierto factor de calidad, es la biometría la que está ganando más adeptos en temas de autentificación, dado que en este tipo de establecimientos la discusión de la asunción de un extra o no como propio por parte de un cliente significa mucho dinero. La principal ventaja de estos sistemas es la calidad y relativo abaratamiento de los lectores utilizados actualmente, la disponibilidad absoluta del factor de autentificación (nadie puede dejar su dedo en casa), y la eliminación del problema del repudio, es decir, que el cliente no puede alegar que dicho servicio no ha sido autorizado o consumido por él.

ISSN impresión: 1885-2564
ISSN electrónico: 2254-0644

2. los sistemas biométricos

La identificación/autentificación biométrica se basa en características inherentes de nuestra fisiología o de nuestro comportamiento. En particular un elemento biométrico es un buen candidato para su utilización en dispositivos de control si es:

- Universal. Existe en todas las personas.
- Único. En cada persona, por lo que permite distinguirla.
- Permanente. La propiedad del elemento biométrico no cambia con el tiempo. Esto no es estrictamente cierto dado que envejecemos y, consecuentemente cambia nuestra fisiología. Sin embargo, este cambio no es radical sino lo suficientemente lento como para considerarlo permanente.
- Medible fácilmente. De alguna manera que permita obtener una medida capaz de diferenciar a los diferentes individuos.

Las técnicas biométricas, como ya hemos comentado anteriormente, puede basarse en:

- *Aspectos fisiológicos*. Huellas digitales, análisis de la retina, reconocimiento facial, reconocimiento de voz, etc. Alguna de ellas más precisa que otras, pero más intrusivas y por lo tanto no tan bien aceptadas por los clientes. La huella digital, la geometría de la mano, la vascularización de ambas y el reconocimiento de voz son sistemas poco intrusivos, fáciles de usar y con una buena fiabilidad y estabilidad. El análisis de retina y la exploración del iris, aunque se consideran más seguros y sólidos, son generalmente peor aceptados por los usuarios, y no son en absoluto adecuados en sistemas hoteleros.
- *Aspectos basados en el comportamiento*. Dentro de estos, el análisis de la pulsación de las teclas, que controlan el tiempo que el usuario mantiene pulsada la tecla, la frecuencia de pulsación, el tiempo entre palabras, el tiempo después de puntos seguidos y apartes, así como los errores de escritura habituales y la comprobación de la firma manuscrita. Estos sistemas no son adecuados para su aplicación en el sector hotelero (pero pueden ser apropiados para otros usos como los sistemas de e-learning).

- Pero, ¿Cómo funciona un sistema de este tipo? En todos los sistemas de reconocimiento biométricos se siguen dos pasos:
- Registro. Es decir recopilación de datos biométricos mediante un sensor específico. Los datos recogidos por esos sensores son analizados y se extraen rasgos específicos para obtener lo que se denomina una "plantilla" biométrica, es decir una representación en forma de un conjunto de datos matemáticos. Esta fase es fundamental ya que se trabaja con los datos brutos, los algoritmos de extracción, los de protección (cifrado y hash) y las plantillas. En función de cómo se traten los datos brutos, la inscripción puede tener que realizarse siguiendo lo que establece el artículo 8 de la Directiva 95/46/CE[1].
- Comprobación. En este caso se realiza la lectura para la comparación con la base de datos de plantillas en funciones de identificación o verificación de la identidad.

[1] Artículo 8 Tratamiento de categorías especiales de datos.

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.
2. Lo dispuesto en el apartado 1 no se aplicará cuando:
a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o
b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o
c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o
d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una
fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que
mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o
e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario
para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.
3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.
4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.
5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.
Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.
6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.
7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Gráfico 2. Pasos en la identificación biométrica.

Fuente: Elaboración propia.

Debemos hacer una distinción clara entre identificación y autentificación. En el primer caso el sistema determina la identidad del cliente, en el segundo es el propio cliente el que se identifica, siendo el dispositivo biométrico el encargado de verificarla. Desde un punto de vista matemático, la identificación sería una búsqueda de uno a muchos (1:N). Al sistema se le presenta una plantilla obtenida a través del dispositivo sensor y el sistema busca entre todos los datos almacenados en la base de datos dando, como resultado aquellos clientes que presentan una aproximación suficiente en base a los parámetros obtenidos de la lectura. Evidentemente la búsqueda es un trabajo laborioso y puede presentar como resultado más de un individuo en el caso de bases de datos muy extensas (que no suele ser el caso de clientes de un hotel). La autentificación es un proceso más simple, una búsqueda (1:1) en la que el usuario ya se ha identificado y lo que se pretende es comprobar su identidad comparando su plantilla con la almacenada en el sistema. En función de la similitud que se exija en el lector biométrico se puede encontrar una proporción muy elevada de falsas aceptaciones, es decir reconocer como válida a una persona que no lo es, o falsos rechazos, es decir, el caso contrario, no reconocer a un usuario válido. Hay que recalcar que a pesar de que el ideal de un sistema biométrico es basarse en un elemento biométrico permanente, es difícil que eso ocurra ya que nuestra fisiología no lo es. Envejecemos o nos vemos alterados por el entorno con lo que es necesario introducir un cierto porcentaje de incertidumbre en la lectura. En la práctica se busca un equilibrio entre la probabilidad de falsa aceptación (False Accept Rate o FAR) y la de falso rechazo (False Reject Rate o FRR). Los rangos de FAR aceptados suelen variar entre 0,0001% y 0,1% en función de la criticidad en el reconocimiento. Por ejemplo un lector de huella dactilar típico de un ordenador de sobremesa trabaja con un FAR: 0.001% y un FRR: 0.1% utilizando tecnología Life Finger Detection (LFD). El uso de estas tecnologías, que distinguen entre una huella real y una imagen de esa huella, es necesario para evitar posibles fraudes.

Un aspecto a tener en cuenta es la forma en que se van a guardar y usar esas plantillas. En principio pueden guardarse en:

- La memoria del dispositivo biométrico.
- En una base de datos central.
- En tarjetas inteligentes o no que permanecen en poder del propietario de los datos.

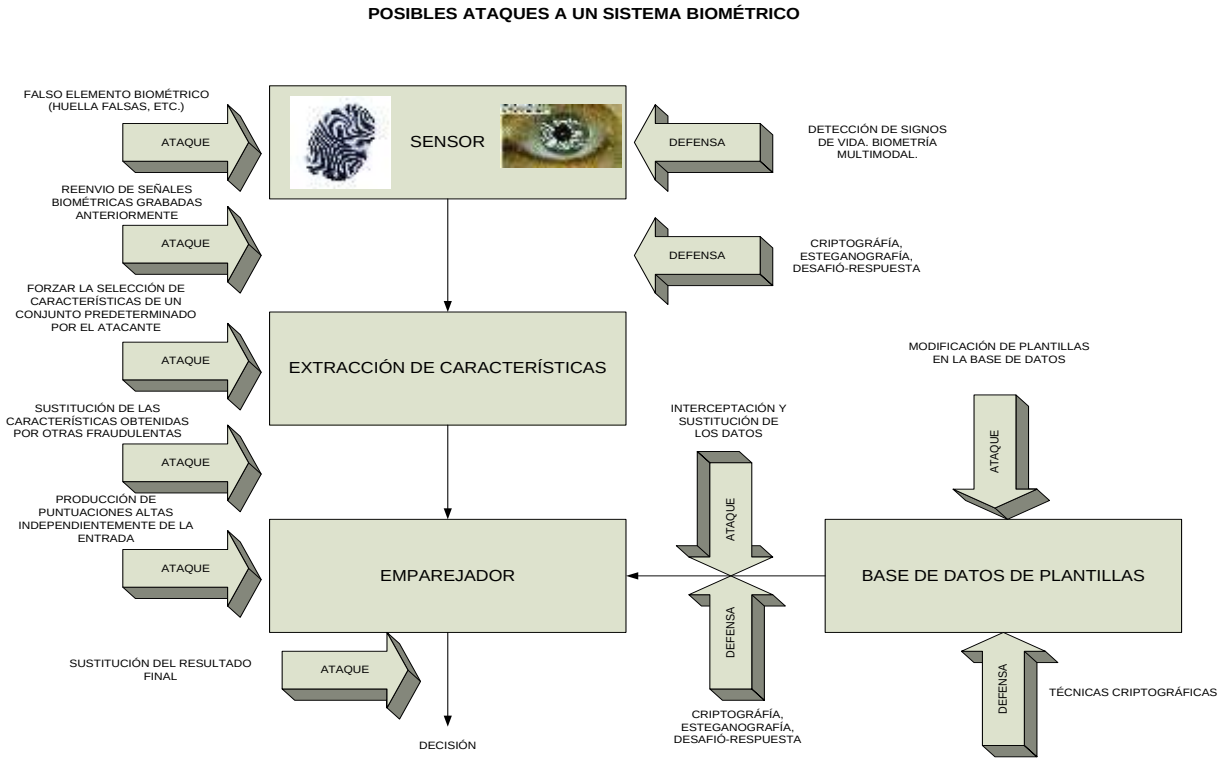
En ambientes hoteleros pueden utilizarse los tres, pero para su utilización en identificación del cliente para cargar extras a su reserva solo serían de utilidad los dos últimos ya que en caso de utilizar el primero obligaría a desplazar al cliente al lugar donde estuviese ubicado el lector, cosa en general no deseable por la molestia que representa. Sin embargo, el primer método sí es adecuado en temas de control de presencia y vigilancia laboral.

Una cuestión importante es que a efectos de autentificación no es necesario el almacenamiento de los datos brutos o las plantillas en una base de datos central, al contrario de lo que ocurre en un sistema cuya función sea la identificación. Esto es un punto a tener muy en cuenta ya que tiene ciertas implicaciones legales como veremos más adelante.

Pero, ¿Son absolutamente seguros los sistemas biométricos? La verdad es que no, dependen en muchos casos de su gestión y administración. Parafraseando a Mario Devargas, autor de un libro clásico sobre seguridad en redes de los años 90: "*La seguridad es realmente una cuestión de gestión, no un problema tecnológico*". Los puntos de ataque a un sistema biométrico son varios como podemos ver en el esquema siguiente, en el que se presentan también algunas técnicas para evitar esos ataques. Sin embargo, no hay que preocuparse demasiado. Un buen control administrativo, la utilización de herramientas criptográficas para cifrar y verificar las lecturas del sensor y almacenarlas en la base de datos y el uso de sistemas con tecnologías de detección de vida permite un grado de seguridad muy elevado.

ISSN impresión: 1885-2564
ISSN electrónico: 2254-0644

Gráfico 3. Ataques a un sistema biométrico



Fuente: Elaboración propia.

3. la autentificación mediante sistemas biométricos en hoteles

Volviendo al tema de la autentificación, y centrándose en un entorno hotelero, se pueden concretar los principales usos de los sistemas biométricos en tres:

- Apertura de puerta de la habitación del cliente. Por ejemplo el cliente utiliza su huella digital para acceder a la habitación.
- Control de extras realizados por el cliente. Por ejemplo el cliente desea cargar a su reserva el importe de la cena en el restaurante y utiliza su huella digital para verificación de su identidad.
- Control de acceso y presencia. Para control laboral.

Cada uno de estos sistemas presenta sus características propias, y, si bien lo lógico sería que el primer y segundo caso fuesen complementarios desde el punto de vista de gestión, no es tan evidente que se pueden utilizar conjuntamente por problemas legales. El tercer caso es el más obvio y conocido. El empleado usa el lector biométrico para "fichar" a la entrada del trabajo, evitando el problema de suplantación inherente a otros sistemas como el de fichas o tarjetas de personal, o el de la palabra de paso o clave. Es muy fácil en estos casos dar la tarjeta o la clave a un compañero para que sea éste quien fiche, burlando de esta manera al sistema y teniendo como única manera de verificación el control humano. Estos sistemas, si el recinto de trabajo lo permite por sus características, pueden ampliarse para controlar las entradas y salidas del personal simplemente asociando la identificación biométrica correcta a una cerradura. De esta manera no solo se controla cuando se entra, sino también cuando se sale y cuanto tiempo se está fuera dado que una vez entrado en el recinto estos sistemas, generalmente, no permiten la apertura de la puerta para volver a entrar si no se ha grabado mediante la lectura previa correspondiente la salida del recinto.

4. el problema legal

Hasta ahora hemos visto el aspecto técnico y de gestión de estos sistemas, sin embargo, no son los únicos aspectos a tener en cuenta. Sin duda la cuestión legal puede ser un problema y en nuestro caso viene dado por la legislación sobre protección de datos. Los datos biométricos son, tanto desde el puno de vista de la

legislación española[2], como de la europea[3] un dato personal. La Ley Orgánica 15/99, en adelante referenciada como LOPD, en su artículo tercero especifica muy claramente lo que se considera dato personal:

> *A los efectos de la presente Ley Orgánica se entenderá por:*
> *a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.*

Es evidente que el dato biométrico es una información concerniente a una persona identificada o identificable, y el problema en nuestro caso radica en que es absolutamente necesario que así sea. Por otra parte, la definición dada por la LOPD es la misma que la establecida en la Directiva 95/46/CE en su artículo segundo. Estamos pues ante un dato de carácter personal, pero, curiosamente, aunque el uso y almacenamiento de datos biométricos es de particular interés en la Unión Europea, en la que el Grupo de Trabajo sobre protección de datos del artículo 29 ha publicado varios documentos de trabajo sobre el tema, referidos a biometría en general (WP 80), reconocimiento facial en servicios en línea y móviles (WP 192), y opiniones sobre desarrollo en tecnología biométrica (WP 193), la Agencia de Protección de Datos Española ha sido más parca en sus trabajos y resoluciones. En realidad la LOPD no hace referencia expresa a los datos biométricos, aunque sí los define como datos personales porque cumplen los supuestos de la definición de este tipo de datos. En su informe jurídico 0368/2006 sobre el uso de huellas dactilares en un centro escolar define muy claramente que:

> *En este sentido debe indicarse que, si bien el procesamiento de los datos biométricos no revela nuevas características referentes al comportamiento de las personas sí permite, lógicamente, su identificación, por lo que resulta evidente que, en caso de procederse a su tratamiento dicho tratamiento deberá ajustarse a la Ley Orgánica 15/1999.*

Sin embargo, el Documento de Trabajo WP 80 antes mencionado, hace alguna matización:

> *Cuando los datos biométricos, como una plantilla, se almacenan de manera que el responsable del tratamiento o cualquier otra persona no pueden utilizar ningún medio razonablemente para identificar al interesado, dichos datos no se clasificarán como datos personales.*

En la cuestión formulada sobre si era legal establecer un sistema de control basado en la obtención de la huella dactilar de los alumnos para gestionar sus ausencias y retrasos, la Agencia Española, siguiendo las directrices del grupo de trabajo del artículo 29 de la Directiva 95/46/CE, consideró el uso de datos biométricos como medio para identificar a los alumnos como "*excesivo y desproporcionado*" para dicha finalidad.

Es curioso el hecho de que lo que pretende controlarse mediante dicha huella dactilar era la entrada y salida de los alumnos en el centro escolar. Decimos curioso ya que es el mismo caso que se pretende controlar en temas laborales y, como veremos, la Agencia sí lo admite. Sin embargo, el dictamen de la Agencia española no es único y otras Agencias europeas se han manifestado también al respecto. Podemos considerar por ejemplo la decisión desfavorable tomada por la autoridad portuguesa de protección de datos sobre la utilización de un sistema biométrico basado en la huella digital por parte de una universidad para controlar la asiduidad y puntualidad del personal no docente[4].

El mismo resultado, basado en el principio de proporcionalidad, se obtiene en el informe 0082/2010 de la Agencia Española, aunque éste nos afecta mucho más directamente. En este informe jurídico el solicitante pretende utilizar la biometría para identificar a los clientes asociando un código alfanumérico a la huella dactilar. En todos los casos es la proporcionalidad el criterio que prevalece:

> *Con arreglo al artículo 6 de la Directiva 95/46/CE, los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Además, los datos personales serán adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente (principio de fines).*
> *El cumplimiento de este principio implica en primer lugar una determinación clara de los fines para los que se recogen y tratan los datos biométricos. Por otra parte, hace falta evaluar el cumplimiento de la proporcionalidad y de la legitimidad, teniendo en cuenta los riesgos para la protección de los derechos y libertades fundamentales de las personas y especialmente si los fines perseguidos pueden alcanzarse o no de una manera menos*

[2] Ley Orgánica 15/99 de 13 de diciembre y Real Decreto 1720/2007 de 21 de diciembre.
[3] Directiva 95/46/CE.
[4] Véase en la página electrónica de la Autoridad portuguesa el "*Parecer nº 11/02*".

ISSN impresión: 1885-2564
ISSN electrónico: 2254-0644

intrusiva. La proporcionalidad ha sido el criterio principal en casi todas las decisiones adoptadas hasta ahora por las autoridades encargadas de la protección de datos sobre el tratamiento de datos biométricos.

A pesar de ello todos sabemos que, principalmente por desconocimiento, esto se sigue haciendo. Un ejemplo muy típico es el de los gimnasios en los que se suele utilizar la huella digital para permitir o denegar la entrada en función de si el cliente está o no al corriente de pago. Este ejemplo es directamente aplicable a nuestro segundo caso de estudio, es decir, la utilización de la biometría como control del servicio al cliente. Basándose en dicho informe podemos deducir que la utilización de la biometría como sistema para control de los diversos servicios realizados al cliente no es directamente posible debido a las restricciones legales que emanan del mismo. Indudablemente, si necesitamos saber a quien corresponden los servicios extras consumidos en el hotel y actualizar la cuenta de ese cliente, debe asociarse a un número de reserva, al número de habitación, o a un código de control que debe estar asociado a la persona que finalmente realizará el pago.

En el primer caso que hemos planteado, la utilización de un elemento biométrico, por ejemplo la huella digital como llave de la habitación del cliente, podemos deducir que podría utilizarse siempre que hubiese una identificación única del patrón biométrico con la cerradura pero no se almacenase ningún otro dato suplementario. Hemos de recalcar que eso, en la práctica, es extremadamente difícil sino imposible en entornos hoteleros. La disociación en estos casos es inviable dado que si bien pueden considerarse tratamientos distintos, existe siempre la posibilidad, por inferencia, de la obtención de los datos que pueden cruzarse a partir de la habitación y la fecha.

Sin embargo un caso asimilable y que sí es aceptado es el del control laboral. En varios informes jurídicos de la Agencia Española de Protección de Datos[5] sobre el tratamiento de la huella digital de los trabajadores para identificación de los mismos y el control del cumplimiento de su jornada de trabajo, la Agencia considera que el empleador está legitimado para tratar las huellas de los empleados sin consentimiento de éstos en aplicación del artículo 6.2 de la LOPD en que se especifica que no será preciso el consentimiento cuando los datos "*se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*". Añadiendo sin embargo que "*el fichero quedaba sometido a las demás disposiciones de la LOPD, en cuanto a su creación y funcionamiento, siendo necesario informar a los interesados de su existencia y de los demás extremos a que se refiere el artículo 5.1 de la Ley Orgánica.*". Al mismo resultado llegan las sentencias del Tribunal Superior de justicia de Murcia de fecha 25 de enero de 2010 y del Tribunal Supremo (Sala de lo Contencioso-Administrativo) de fecha de 2 de julio de 2007. Añadiendo además en el primer caso que el empresario no precisa del acuerdo de los representantes de los trabajadores para la implantación de un sistema de control de acceso biométrico.

¿Qué es pues lo aceptado por las Agencias de Protección de datos europeas? Este tema es importante ya que, como veremos, restringe las posibilidades técnicas en la solución del problema. En primer lugar tanto la legislación española como la europea prohíben el tratamiento ulterior de los datos para un fin que fuera incompatible con los fines para los que se recogieron dichos datos. Basándose en este principio el Grupo de Trabajo del art. 29 considera que:

.. el riesgo de reutilización de datos biométricos obtenidos a partir de rastros físicos dejados por personas sin darse cuenta (por ejemplo: huellas digitales) para fines incompatibles es relativamente bajo si los datos no están almacenados en bases de datos centralizadas, sino en poder de la persona y son inaccesibles para terceros.

Y entrando en lo que nos interesa:

.. el Grupo apoya el uso de sistemas biométricos que no memoricen rastros en un dispositivo de control de acceso ni los almacene en una base de datos central. Pero si está prevista la utilización de esos sistemas y, teniendo en cuenta el riesgo de la (re)utilización con distintos fines y los peligros específicos en caso de acceso no autorizado, el Grupo recomienda que los Estados miembros contemplen la posibilidad de presentarlos al control previo por parte de las autoridades encargadas de la protección de datos de conformidad con el artículo 20 de la Directiva 95/46/CE, ya que es probable que ese tipo de tratamiento comporte riesgos específicos para los derechos y libertades de los interesados.

Restringiendo más el tema nos avisa que:

Determinados datos biométricos podrán considerarse sensibles en el sentido del artículo 8 de la Directiva 95/46/CE y, en particular, los datos que revelen el origen racial o étnico o los datos relativos a la salud. Por ejemplo, en sistemas biométricos basados en el reconocimiento facial, se pueden tratar

[5] Puede consultarse, entre otros, el Informe Jurídico 0324/2009 de la AEPD.

> *los datos que revelan el origen racial o étnico. En esos casos, se aplicarán las garantías especiales contempladas en el artículo 8 además de los principios generales de protección de la Directiva.*
> *Esto no significa que todo tratamiento de datos biométricos vaya a incluir necesariamente datos sensibles. Si un tratamiento contiene datos sensibles es una cuestión de apreciación vinculada con la característica biométrica específica utilizada y la aplicación biométrica en sí. Es más probable que eso ocurra en caso de tratamiento de datos biométricos en forma de imágenes, porque en principio los datos brutos no se pueden reconstruir a partir de la plantilla.*

Resumiendo podemos afirmar que, desde un punto de vista estrictamente legal siguiendo la doctrina sobre protección de datos nos encontraríamos con que el sistema de reconocimiento biométrico debería tener disociada la identidad del usuario de su patrón biométrico, que éste debería estar guardado preferentemente en una tarjeta o dispositivo similar que estuviese en manos del propio usuario, y que siempre que fuese posible no debería guardarse el dato en bruto (la fotografía en caso de identificación facial) asociada al patrón biométrico y a los datos. Es decir, que eliminaríamos la principal virtud de estos sistemas, su valía como sistemas de autentificación en entornos con múltiples usuarios. Ya no entramos en tema de transferencias internacionales de datos[6] a un país que no tenga nivel adecuado de protección declarado por la Agencia Española de Protección de Datos o por decisión de la Comisión Europea, tema éste muy común en cadenas hoteleras y que necesitaría un extenso artículo por sí solo.

En cuanto al tema de la utilización de la biometría en temas de control laboral creemos también que tiene los días contados. La CNIL (*Commission Nationale de l'Informatique et des Libertés*), la Autoridad francesa en materia de protección de datos personales adoptó, el 27 de abril de 2006, una autorización única de puesta en marcha de dispositivos biométricos basada en el reconocimiento de la forma de la mano con la finalidad del control de acceso y horarios en los puestos de trabajo[7]. Sin embargo, actualmente la visión de la Comisión es que es desproporcionada la utilización de la biometría para los fines antes citados. Sin embargo, como medida transitoria permitirán la utilización a los organismos que ya lo tuvieran implantado durante un periodo de cinco años. Visto lo anterior y dado que se prevé en los próximos meses una normativa conjunta comunitaria que reemplace a las normativas nacionales, es muy posible que se adopte el punto de vista francés, más coherente desde nuestro punto de vista.

[6] Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

[7] Autorisation unique n° AU-007 - Délibération n°2012-322 du 20 septembre 2012 portant autorisation unique de mise en œuvre de traitements reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la restauration sur les lieux de travail

5. conclusión

Como vemos el uso de las tecnologías biométricas queda limitado por cuestiones legales, que no técnicas. Los sistemas biométricos son sencillos, tienen precios razonables y cuentan con la ventaja de utilizar algo que el cliente no puede olvidar ni perder. Sin embargo, un uso inadecuado de estos sistemas puede hacernos incurrir en un claro incumplimiento de las normas europeas y españolas sobre protección de datos. No creemos que la próxima reforma europea en materia de protección de datos permita una utilización con menos trabas legales. La opinión que mantienen la AEPD y el Grupo de Trabajo del art. 29 sobre este tema tampoco apunta a cambios sustanciales en un próximo futuro. Todo ello nos lleva a predecir que el uso de estas tecnologías en el sector hotelero, será, en lugar de lo habitual, lo anecdótico.

6. bibliografía

Devargas, M. (1993): *Network Security*. NCC Blackwell.

Simón Zorita, D. (2003): *Reconocimiento automático mediante patrones biométricos de huella dactilar*. Tesis doctoral de la Universidad Politécnica de Madrid.

Gomez-Barrero, M., Galbally, J., Tome-González, P. y Fierrez, J. (2012): "On the vulnerability of Iris-based Systems to a Software Attack based on a Genetic Algorithm". Documento del Biometric Recognition Group de la Universidad Autónoma de Madrid.

Fox, S. (2008): "Pathway to maturity". Info Security.

Jeza Alotaibi, S (2010): "Using biometrics authentication via fingerprint recognition in E-exams in E-learning environment". *The 4th Saudi International conference*. The University of Manchester. 30-31 Julio 2010.

Fecha de recepción del original: enero 2013
Fecha versión final: julio 2013

ISSN impresión: 1885-2564
ISSN electrónico: 2254-0644