Privacidad en los servicios de la industria del autómovil

CARLOS RODRÍGUEZ CASAL
Universidad Pública de Navarra

INTRODUCCIÓN

La industria del automóvil está introduciendo las comunicaciones y el procesado de la localización para mejorar la seguridad de los viajeros. Esta infraestructura es también utilizada para proporcionar servicios de apoyo a la conducción y de entretenimiento. Mientras algunos fabricantes de automóviles (como Fiat, General Motors o Mercedes Benz) desarrollan sus propios sistemas y servicios (Connect, OnStar y Tegaron respectivamente), están surgiendo proveedores que podrían instalar su plataforma en la fabricación de cualquier vehículo (por ejemplo Scoobi). Además, algunos de estos fabricantes están haciendo apuestas de futuro, por ejemplo Mercedes Benz con Infofueling, que utilizaría redes de área local para su conexión inalámbrica.

El funcionamiento de estos sistemas, típicamente englobados en el término «telematics», difiere según el fabricante, pero la idea subyacente es común a todos ellos: determinar la posición del vehículo, comunicar con un centro de información y facilitar información a los pasajeros.

La posición se podría obtener utilizando diferentes técnicas de localización, lo más típico es utilizar GPS, pero también caben otras posibilidades como E-OTD o Identificación de Celda mediando acuerdo con un operador de telefonía móvil. Esta información se transmite a una central de servicio utilizando para ello una conexión de telefonía móvil. La llamada suele realizarse desde un terminal «manos libres», y la conexión puede ser una sencilla conexión GSM o responder a un protocolo más sofisticado como UMTS. También podrían utilizarse otras tecnologías, por ejemplo la Comisión de Comunicaciones del Gobierno de EEUU reservó en 1991 la banda de 5.9 GHz para realizar este tipo de servicio utilizando conexiones inalámbricas de área local (IEEE 802.11a). A los conductores, y demás ocupantes, se les puede facilitar información de tráfico, aparcamiento, navegación (guiado a través de carreteras), información meteorológica y diversos servicios como reservas de hotel o teatro, música y, pensando en entretener a los pasajeros, películas o juegos.

En función de los servicios a prestar, el interfaz del usuario será diferente, si bien es común la existencia de un terminal manos libres con un conversor texto-voz, acompañado o no de un joistick, un teclado, una pantalla y, de gran importancia, un botón de conexión en caso de emergencia. Esta conexión de emergencia debería funcionar independientemente de que el coche estu-

[1] Directiva 95/46/EC.

[2] Directiva 97/66/EC.

[3] LOCUS (IST-1999-14093), Deliverable D2 Addendum on Institutional Issues, Septiembre 2001.

[4] Carlos Rodríguez Casal y María Loza Corera, «Protección de la Privacidad. Aproximación al Opt-in/Opt-out», Spanish Journal «Revista de Contratación Electrónica», Enero 2002. ISSN: 1576-2033.

viese en marcha o parado, encendido o apagado, e independientemente de que el sistema de comunicación esté activo o no, siendo también conveniente su activación inmediata en caso de colisión.

Una de las características más conflictivas de estos sistemas es el procesado de la posición del vehículo. El coche deja de ser un lugar privado que permite evadirse de la vida cotidiana, para convertirse en un centro de proceso controlado y vigilado desde fuera (mediante el procesado de los datos transmitidos), siendo posible incluir un sistema de «caja negra», similar al utilizado en los aviones, que registraría no sólo la posición, sino también las velocidades, servicios utilizados y la cronología de todo lo acontecido en el vehículo.

A continuación se analiza en primer lugar el régimen aplicable a los datos de localización. Le sigue el análisis de los servicios de emergencia y el procesado de datos médicos. A continuación se detallan otros sistemas en los cuales se podría violar la privacidad de los individuos como las cajas negras o los controladores de tráfico, cerrando la presentación de conclusiones y la lista de acrónimos.

PROTECCIÓN DE LOS DATOS DE LOCALIZACIÓN

Al procesar la posición del vehículo hay que tener en cuenta que los desplazamientos del automóvil suelen coincidir con los movimientos de su propietario. Si así ocurre, el procesado de los datos de localización ha de considerarse procesado de información de carácter personal, y ha de seguir la legislación existente al respecto.

En la Unión Europea y con el marco regulatorio actual, ha de seguirse la Directiva 95/46/EC[1] sobre protección del individuo. Pero en la UE existe también una propuesta de Directiva sobre el procesado de los datos de localización y esta Directiva, una vez aprobada, se le aplicará o no en función del tipo de servicios prestados.

En Junio de 2000 se propuso un marco regulador que siguiendo el espíritu de la cumbre de Lisboa, regulaba en 6 Directivas la conclusión del proceso de liberalización de las telecomunicaciones. Entre estas Propuestas de Directiva se encontraba la Propuesta 385 sobre protección de datos (directiva que una vez aprobada sustituiría a la Directiva 97/66[2]). En Diciembre de 2001 tanto el Consejo Europeo como el Parlamento Europeo dieron el visto bueno final al nuevo paquete regulador, pero se excluyó la conflictiva Directiva sobre protección de datos. Entre otros problemas se discutía la necesidad de eliminar los datos de localización (algo que el autor ya ha defendido ante la Comisión Europea[3]) y la regulación que se debería de dar al correo comercial no solicitado (algo sobre lo que el autor ya se ha posicionado[4] y que será abordado posteriormente).

La mayor modificación que introduce esta propuesta de Directiva respecto a la vigente es en cuanto a la distinción entre datos de tráfico de comunicaciones y datos de localización, así como la posibilidad de facilitar los datos de localización del usuario a las autoridades de emergencia aún cuándo éste no haya dado su consentimiento. Al respecto cabe señalar que la Propuesta 392 proponía en su artículo 22 (artículo 26 tras su enmienda y aprobación) la obligatoriedad de que, siempre que, «sea técnicamente posible», se facilite la posición a las autoridades de emergencia.

Una situación análoga se da en EEUU donde en 1999 el Congreso aprobó el Acta «Wireless Communications and Public Safety Act», enmendando el artículo 222 del Acta de Telecomunicaciones. Por esta enmienda no se aplicarán las reglas de privacidad al procesado de datos de localización en dos situaciones: por de notificación automática de accidente de tráfico y para facilitar información a un centro de atención de emergencias.

El problema que se ha obviado hasta aquí es que la legislación sobre localización se está desarrollando pensando en el procesado de tal información por operadores de telefonía móvil, pero no son los únicos que realizan tal procesado. A continuación se utiliza la legislación Europea para explicar este aserto.

Tanto la Directiva 97/66 como la Propuesta que podría sustituirla (COM (2000) 385), se aplican únicamente en la prestación de «servicios de comunicaciones electrónicas disponibles al público en las redes públicas de la Comunidad»[5]. De esta forma dependiendo de los servicios prestados el sistema sería afectado por la legislación o no. Por ejemplo, el autor entiende que a un sistema similar a OnStar, con casi dos millones de usuarios y ofreciendo servicio de telefonía, sí se le aplicaría esta Directiva y por tanto tendría que facilitar los datos a las autoridades de emergencia. Es cierto que la red utilizada por OnStar no es una red propia sino alquilada, pero la regulación tanto se ha de aplicar a operadores «reales» como a operadores «virtuales». Sin embargo, otro ejemplo, un sistema del tipo Connect, no sería afectado por esta Directiva al procesar los datos de localización. El motivo es que Connect no es una red de telecomunicación que obtiene la localización, sino que Connect se basa en tomar datos sobre la posición por medio de un GPS y transmitir esta información por medio de un SMS a una centralita donde se atiende a los usuarios. Connect no es una red de telecomunicación sino un usuario de una red de telecomunicación, por eso no se vería afectado por la propuesta de Directiva. Dicho sea de paso, el uso que hace Connect de la red no es a priori el más óptimo. Como se ha indicado, Connect utiliza SMSs para enviar la posición del vehículo y a partir de este mensaje comienza la atención al usuario, pero los SMSs no tienen prioridad en la red y en caso de saturación, serán los primeros en sufrir retardos, lo cual en casos de emergencia puede ser decisivo sobre la vida de las personas.

Si la directiva específica a los datos de localización no se aplica a un servicio proporcionado en el sector «telematics», podrían darse en este sector todos los problemas que se intentan evitar con la propuesta de protección de datos que se está debatiendo. Podría parecer extraño, pero no resulta descabellado pensar que diferentes compañías estén interesadas en procesar o conservar la localización con fines diferentes a la prestación de un servicio concreto. Por ejemplo «Virgin Mobile», un operador virtual en Reino Unido, ha reconocido recientemente tener almacenada información relativa a los movimientos de sus clientes desde noviembre de 1999 y no tener intenciones de borrarla[6].

LOCALIZACIÓN Y SERVICIOS DE EMERGENCIA. DATOS MÉDICOS

En 1996 la Comisión de Comunicaciones de Estados Unidos (FCC) publicó un mandato que obliga a los operadores móviles a calcular la localización de los móviles y a facilitar la posición obtenida en caso de realizar una llamada a los servicios de emergencia[7] (el norteamericano 911). En la UE en el «Communications Review» de 1999 se puso como objetivo para procesar la localización el año 2003, y pocos meses después se presentó el nuevo marco regulador que considera el traspaso de los datos de localización a las autoridades de emergencia (impulsando simultáneamente el uso del número de emergencia en la UE, el 112). Sin embargo, mientras en Estados Unidos se ha tratado de un mandato en el que se detallan precisiones, plazos y penetración (y que ha sido controvertido e incumplido), en la UE se ha intentado alcanzar un consenso entre las partes implicadas. Así, se constituyó el grupo CGALIES[8] («Coordination Group on Access to Location Information to Emergency Services») y la Comisión hasta el momento se ha limitado a imponer a los operadores la transferencia de la información de la

[5] Art. 3 Directiva 97/66/EC y Art. 3 de la Proposal COM(2000) 385.

[6] The Guardian 27 Octubre 2001.

[7] FCC Report and Order a Further Notice of Proposed Rulemaking CC Docket No.94-102, (12-6-1996).

[8] www.telematica.de/cgalies (Enero 2002).

[9] Art.22 de la Propuesta COM (2000) 392.

[10] www.itu.int (Enero 2002).

[11] Recomentación 97-5 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos.

ubicación a las autoridades del 112 allí «donde sea técnicamente posible»[9] (sin especificar cómo debe hacerse la transferencia). Curiosa expresión que tras las enmiendas del Parlamento Europeo ha sido aprobada como: «hasta donde sea técnicamente posible», expresión igualmente curiosa.

En los casos de llamadas de emergencia se facilitará la posición y las autoridades enviarán a los servicios que estimen oportunos (básicamente ambulancias, bomberos o policía) al punto exacto donde sea preciso. Si el aviso de la emergencia se realiza desde el sistema del automóvil, caben dos posibilidades. Por un lado disponer de unos servicios de atención propia, por otro lado redireccionar la llamada a un centro público de atención de emergencias (como el 911 en Norteamérica, el 112 en la Unión Europea o el 000 en Australia). Con la primera opción podrían entrar a formar parte de los servicios nuevos implicados, participando terceras entidades tales como empresas aseguradoras o servicios privados de atención médica.

En el caso de un teléfono móvil lo más común es que el teléfono vaya asociado a una persona. En el caso de un vehículo (que es lo que ahora nos interesa analizar) también es común que un vehículo se asocie a un único individuo y por ello en caso de emergencia, resultaría muy útil conocer el historial médico de esa persona.

Así, un conductor consciente de las ventajas que le podría aportar el facilitar su historial médico, podría poner todos los medios a su alcance para aunar información de su salud y de su familia para que esté disponible en caso de emergencia. ¿Quién podría ser depositario de tal información?

Podría ser el operador de telefonía el que tuviese los datos, al fin y al cabo la mayoría de los sistemas actuales basan sus comunicaciones en insertar la tarjeta SIM de un teléfono móvil (un duplicado de la tarjeta) en el sistema del vehículo. Pero también es cierto que hay sistemas en la actualidad que obtienen la posición por medio de un GPS y la transmiten por medio de un SMS sin que el operador conozca el contenido de tal SMS, de ahí que quepa considerar a quien presta los servicios al vehículo pudiese ser responsable de la información médica.

Cabe imaginar también la situación en que un vehículo tenga asociada una dirección IP y que de esa dirección se acceda a una base de datos, o incluso yendo más lejos, que los datos médicos estuviesen almacenados en la base de datos ENUM[10] donde junto a los datos de localización de una persona, se podría almacenar un documento con el historial médico. La idea, a priori, suena devastadora, pero no deja de ser una posibilidad.

Dando aquí por sentado la conveniencia de que se facilite el historial médico en caso de emergencia, resulta conveniente abordar la necesidad de que exista una gran protección a los datos del historial médico. No hace mucho tiempo, la prensa estadounidense publicaba que la conocida cadena de farmacias «CVS» estaba vendiendo información de las prescripciones médicas de sus clientes a empresas farmacéuticas (y poco después la cadena farmacéutica publicaba que dejaba de hacerlo). Una situación así parecería imposible en la UE, donde la ya mencionada Directiva sobre privacidad (95/46) protege a los ciudadanos en todos los campos. Respecto al procesado de datos médicos esta Directiva en su artículo 8 prohibe el procesado regulando sus excepciones (básicamente por consentimiento del sujeto o interés vital del mismo). También existe una Recomendación (texto no vinculante pero de gran interés por la atención prestada por los países miembros) que regula la recogida y tratamiento automatizado de datos respetando la intimidad y derechos de los afectados, tratando también de asegurar la seguridad y correcta conservación de los datos[11].

En Estados Unidos es preciso legislar en cada materia por separado y res-

pecto al procesado de los datos médicos, estará pronto en vigor la largamente debatida HIPAA («Health Insurance Portability and Accountability»), que aprobada en 2001 protegerá la información médica personal e impondrá a nivel federal medidas restrictivas al uso y divulgación de información médica en cualquier soporte. Este acta entrará en vigor en Abril de 2003.

LA CAJA NEGRA Y OTRAS FUENTES DE INFORMACIÓN PERSONAL

Aunque muchos compradores de vehículos no lo sabían, ya desde los principios de los noventa General Motors ha estado introduciendo un sistema que puede asimilarse al de «caja negra» de un avión. La idea subyacente es almacenar información del comportamiento del vehículo en caso de accidente para mejorar las prestaciones del vehículo en versiones y modelos posteriores. Si en un principio estos sistemas eran sencillos, en 1999 ya registraban 16 parámetros, incluyendo la velocidad y el estado de los pedales de freno y aceleración.

Aunque General Motors tiene como objetivo incluir «la caja negra» en todos sus vehículos en el año 2004, y aunque otros fabricantes, como Ford u Honda, ya han empezado a introducir sistemas similares, la mayoría de sus propietarios no son conscientes de la existencia de este dispositivo.

Estas cajas negras son un elemento clave para resolver la responsabilidad en caso de accidente y con tal fin han sido utilizadas ante los tribunales. También las empresas aseguradoras muestran un gran interés por el contenido de estas cajas.

Otro potencial control a la posición de un vehículo son los lectores de matrículas. Los lectores de matrículas se utilizan para controlar el tráfico, para controlar el acceso a garajes y así determinar el importe a pagar, o para vigilar qué vehículos se aproximan a áreas de seguridad, como centrales nucleares, aeropuertos o edificios del gobierno.

Para controlar el tráfico caben distintas posibilidades, que suelen agruparse en puntuales, continuas y espaciales. Las puntuales son las más inocuas a la privacidad, son aquellas que determinan el tráfico utilizando sensores acústicos o sensores bajo el asfalto, radar, infrarrojos, o cámaras en puntos conflictivos (a priori, no parece que estas cámaras supongan un atentado a la privacidad).

Los métodos continuos se basan en el seguimiento ininterrumpido de determinados vehículos. Podrían utilizarse vehículos especialmente adaptados para realizar tal seguimiento o cabría utilizar la infraestructura de comunicaciones de sistemas telematics para proporcionar información a las centrales de tráfico. Esto podría hacerse, bien informando a los sujetos de que son seguidos, bien facilitando la información de forma anónima, esto es, la central del sistema telematics, al tiempo que atiende a sus clientes determina el número de sus vehículos en determinadas zonas consideradas conflictivas y facilita la información numérica, sin identificar a los usuarios, a la entidad que está analizando el tráfico. También cabría utilizar flotas de vehículos (taxis, autobuses, camiones, vehículos de alquiler,...) para realizar la estimación del tráfico. Al respecto cabe señalar que ya es común en la actualidad que las empresas de alquiler de automóviles realicen el seguimiento de sus vehículos utilizando GPS, lo que puede hacer aparecer más conflictos. Por ejemplo, en el Estado de Connecticut, en Estados Unidos, la empresa de alquiler «Acme Rent a Car» realizaba el seguimiento de sus vehículos por satélite y sancionaba a sus clientes por exceder los límites de velocidad, las denuncias puestas por los clientes han llevado a que los tribunales hayan dictado su cese.

Volviendo a la detección de tráfico, la tercera y última posibilidad, los sis-

[12] Directive 2000/31/EC.

[13] Directive 2000/46/EC.

[14] Directive 2000/12/EC.

temas espaciales, son aquellos que se basan en la lectura de matrículas o de etiquetas puestas en los cristales frontales de los vehículos para realizar el pago automático en peajes. Estas tarjetas, frecuentemente conocidas como Zpass, se están popularizando y existen pruebas piloto para comprobar su utilidad para el pago en gasolineras o en servicios del tipo «drive in» (como Mc Donalds, Dunkin' Donuts, aparcamientos o gasolineras). El almacenamiento y uso de los datos adquiridos mediante la lectura de estas etiquetas, debería seguir medidas estrictas.

Tras la mención del control de las etiquetas de los vehículos como medio de pago, cabe indicar aquí el gran campo que telematics podría abordar precisamente como medio de pago. Se ha indicado la posibilidad de hacer reservas vía un operador que atiende el servicio. Por ejemplo en el caso de Fiat y su servicio telematics Connect, es la empresa «Targa» la que se encarga de atender a sus clientes y facilitarles información, asistencia y hacer reservas. La forma de hacer reservas es mediante una tarjeta de crédito, pero cabrían otras posibilidades. Cabe pensar que las reservas de hotel, las entradas del cine, los servicios de entretenimiento disfrutados en el vehículo y otros muchos gastos corran a cuenta del proveedor del sistema del automóvil (del proveedor de telematics). El cobro al usuario se le podría facturar de diversas formas, comprendiendo entre los opuestos sistemas de prepago y de crédito: el cobro instantáneo, el cobro en los siguientes días y la acumulación a un pago mensual.

En el momento en que Telematics preste tales servicios, se le aplicarán también las normas correspondientes a la actividad que decida desarrollar. Así cabe señalar como posibles campos implicados el comercio electrónico, el procesado de datos personales o la regulación de entidades de crédito. Por poner algunos ejemplos, en la Unión Europea le afectarían la Directiva de Comercio Electrónico[12], la Directiva de las entidades de dinero electrónico y su ejercicio[13] o la Directiva relativa a la actividad de las entidades de Crédito[14].

CONCLUSIONES

En este trabajo se han analizado diversas amenazas a la privacidad del individuo. La primera de ellas es el procesado de la localización del automóvil. El procesado de los datos de localización está siendo regulado a nivel de comunicaciones personales, pero no en cuanto al procesado de la localización de vehículos. La UE, en su debate abierto en torno a la Directiva de Protección de Datos debería de tener en cuenta esta coyuntura y poner todos los medios a su alcance para proteger la privacidad de los ciudadanos.

También se ha tratado la relación entre datos de localización y servicios de emergencia. Desde aquí se insta a facilitar la convergencia de datos médicos con los servicios de comunicaciones, no sólo personales, sino también del automóvil, por las grandes mejoras que esto supondría en la calidad de la atención a los pacientes.

Las medidas que se adopten para asegurar el respeto a la privacidad han de ser extensibles a cualquier forma de intromisión, no sólo por parte del proveedor de un servicio telematics, sino también por todas las partes que pudiesen tener acceso a datos por la manipulación de cajas negras, control de tráfico o prestación de cualquier servicio.

Cabe señalar, por último, que si la protección de datos no es forzosa por ley serán pocas las respetables empresas que de forma voluntaria los protejan, y serán muchos los usuarios que tendrán que renunciar a su privacidad para no perder las ventajas y seguridad de los nuevos servicios.

ACRÓNIMOS

CGALIES	Coordination Group on Access to Location Information for Emergency Services
E-OTD	Enhanced-Observed Time Difference
GPS	Global Possitioning System
HIPAA	Health Insurance Portability and Accountability
IP	Internet Protocol
SIM	Subscriber Identity Module
SMS	Short Message Service
UMTS	Universal Mobile Telecommunications Service