Legislación, ética y seguridad para la preservación de la privacidad de la información espacio-temporal

Benjamín Ramos Álvarez, Ana Isabel González-Tablas Ferreres,
Arturo Ribagorda Garnacho y Julio César Hernández Castro

{benja1,aigonzal,arturo,jcesar}@inf.uc3m.es

Av. de la Universidad, 30. 28911-Leganés
Universidad Carlos III de Madrid, España

Resumen. En diferentes países, y por motivos variados, en los últimos años ha cobrado mucha importancia la protección de los datos de carácter personal y la preservación de la privacidad de los individuos. Cada vez son más los servicios en los que se involucran datos que pueden comprometer la vida privada, e incluso íntima, de las personas, y dichos datos pueden ser accedidos y tratados desde una amplia gama de nuevos equipos y dispositivos móviles. En este documento se expone el estado de la cuestión relativo a la legislación, los principios y derechos, los códigos de conducta, las técnicas y los estándares cuyo objetivo común es preservar la privacidad. En particular se aborda la privacidad de la información espacio-temporal (IET) de una persona, y se indaga en las diferentes reglamentaciones que constituyen el marco jurídico adecuado para preservarla.

Palabras Clave: datos de carácter personal; información espacio-temporal; privacidad; intimidad; ética; servicios de seguridad.

1. Introducción.

En la actualidad, la coincidencia de diferentes avances tecnológicos, como son la telefonía móvil, la interconexión de redes y los servicios de localización, propicia el desarrollo de nuevos servicios telemáticos en los que se obtiene, envía y almacena información relativa a individuos. Por tratarse de datos de carácter personal, los legisladores se ven obligados a revisar aquellas parcelas del derecho encaminadas a preservar la privacidad de las personas y al respeto de su intimidad. Como en estos nuevos servicios se hallan involucrados usuarios de diferentes profesiones, han de revisarse, o formularse como nuevos, los códigos de conducta en pro de un correcto uso de tales datos desde el punto de vista ético. Obviamente, las características de los datos y su variada gestión obliga a la elección de los mecanismos de seguridad más adecuados para su correcta protección.

En España, según el artículo 3 apartado a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, "*datos de carácter personal es cualquier información concerniente a personas físicas identificadas o identificables*". En la Comunidad Europea, según el artículo 2, apartado Definiciones, de la Directiva 1995/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, "*datos personales: toda información sobre una persona física identificada o identificable (el interesado); 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*" (Directiva 1995/46/CE).

En este grupo pueden incluirse los datos de la localización física de un individuo, y tales datos son ya una posibilidad real tras la aparición y rápida evolución de una gran variedad de dispositivos móviles. La mayoría de estos servicios de valor añadido basan su oferta en la posibilidad de proveer al usuario localizado una cierta información útil en un momento determinado, por ejemplo cuando se encuentra dentro de un área definida. Téngase en cuenta que en el par persona-dispositivo, la relación de pertenencia del dispositivo a una persona supone que al ser localizado el dispositivo es encontrado realmente el usuario, es decir ha de asumirse la inequívoca propiedad del aparato por parte de la persona.

El objetivo de este documento es exponer el estado de la cuestión relativo a la legislación, los principios y derechos, los códigos de conducta, las técnicas y los estándares cuyo objetivo común es preservar la privacidad. En particular se aborda la privacidad de la información espacio-temporal (IET) de una persona, y se indaga en las diferentes reglamentaciones que constituyen el marco jurídico adecuado para preservarla.

2. Ética.

En el Diccionario de la Lengua Española (RAE, 2001) se define **Ética** como "*conjunto de normas morales que rigen la conducta humana*" y se entiende que **ética profesional** consiste en llevar tales normas al ejercicio de la profesión de una persona. La Ética, como parte de la filosofía, trata de la moral y de las obligaciones del hombre. Por tanto, si a un sujeto se le atribuye un "proceder ético" se entiende que se trata de un individuo "recto", que su conducta es conforme a la moral. Partiendo de esta nueva acepción de ética, el comportamiento de una actuación se puede calificar de bueno o malo, como así dice el Diccionario sobre **Moral** "*Perteneciente o relativo a las acciones o caracteres de las personas, desde el punto de vista de la bondad o malicia*". Bajo esta óptica, la moralidad de una acto no concierne al orden jurídico, sino al fuero interno o al respeto humano. Otro concepto relacionado con ética y moral es la **Deontología** que se define como "*Ciencia o tratado de los deberes*" y a menudo, asociado con la conducta de un trabajador, se le recuerda el código

deontológico de su profesión, como guía o conjunto de normas a tener en cuenta en su quehacer.

Los códigos de ética, tal como se conocen en el mundo de las empresas, son sistemas de reglas establecidos con el propósito general de guiar el comportamiento de los integrantes de la organización y de aquellos con los cuales ésta actúa habitualmente, tales como vendedores, clientes y proveedores. Este conjunto de reglas o políticas depende en gran medida de la profesión que cada uno desempeñe, aunque siempre con la recomendación de que el límite de lo que cada uno pueda hacer público excluye el caso de que se dañe deliberadamente la imagen de otras personas.

2.1. Ética informática.

Cabe preguntarse cómo influyen las nuevas tecnologías en el comportamiento de las personas, si surgen problemas éticos vinculados con las TIC, cómo afecta la interacción sociedad-tecnología al tratamiento de los datos personales, resumiendo ¿tiene sentido una Ética de las tecnologías de la información y de la computación? Ya en 1968, Donn Parker, analizando algunos crímenes relacionados con la computación en USA, se encontró con numerosos casos de intromisión en la privacidad de ciudadanos por agencias del gobierno. Walter Maner, en un curso desarrollado en 1980, pone de manifiesto que el principal foco de interés se halla en la ética médica, publicando ese mismo año su "Starter Kit in Computer Ethics".

Más tarde, James Moor publica en 1985 "What is Computer Ethics?", en el que pone de manifiesto que el problema surge porque existe un vacío en políticas relativas a la forma en que deberían ser utilizadas tales tecnologías. Ello implica que no se sabe qué reglas seguir cuando se trata de realizar elecciones referidas a la nueva problemática tanto por parte de las personas como por la sociedad. Numerosos estudiosos de la ética asociada a las nuevas tecnologías acuden al clásico "Ética Informática"[1], de Deborah Johnson, que en 1985 postulaba que con la ética tradicional no pueden abordarse cuestiones planteadas con la introducción de las TIC.

Veamos, a manera de ilustración, dos códigos de ética de asociaciones de profesionales de la ingeniería informática. El primero, de 1990, es el "IEEE Code of Ethics" del "Institute of Electrical and Electronics Engineers" de los Estados Unidos (IEEE), que dice así:

"Nosotros, los miembros del IEEE (Institute of Electronic and Electrical Engineers) en reconocimiento de la importancia de nuestras tecnologías al afectar la calidad de vida en todas partes del mundo, y en aceptación de una obligación personal para nuestra profesión, sus miembros y las comunidades que servimos, por la presente nos comprometemos a la más alta conducta ética y profesional y acordamos:

---

1 "Ética Informática" da título a la traducción de "Computer Ethics" que en 1996 realizó al español el profesor Dr. Porfirio Barroso Asenjo, Ed. Universidad Complutense de Madrid.

1. *aceptar la responsabilidad en la toma de decisiones de ingeniería consistente con la seguridad, la salud y el bienestar del público, y revelar rápidamente los factores que puedan dañar al público o al medio ambiente;*
2. *evitar conflictos de interés, reales o percibidos, si es posible, y revelarlos a las partes afectadas cuando existan;*
3. *ser honesto y realista al plantear reclamos o estimativos basados en datos disponibles;*
4. *rechazar el soborno en todas sus formas;*
5. *mejorar el entendimiento de la tecnología, su aplicación apropiada, y sus consecuencias potenciales;*
6. *mantener y mejorar nuestra competencia técnica y acometer labores tecnológicas para otros sólo si se está calificado, mediante el entrenamiento o la experiencia, o después de una revelación completa de las limitaciones pertinentes;*
7. *solicitar, aceptar y ofrecer crítica honesta del trabajo técnico, reconocer y corregir errores, y acreditar apropiadamente las contribuciones de otros;*
8. *tratar imparcialmente a todas las personas respecto de factores tales como raza, religión, género, discapacidades, edad o país de origen;*
9. *evitar dañar a otros, su propiedad, reputación o empleo mediante acciones falsas o destructivas;*
10. *asistir a los colegas y colaboradores en su desarrollo profesional y apoyarlos en el seguimiento de este código de ética."*

El segundo código, de 1992, es el "ACM Code of Ethics and Professional Conduct" de la "Association for Computing Machinery" (ACM), y dice así:

"*Como miembro de ACM, yo:*

1. *contribuiré al bienestar de la sociedad y de los seres humanos*
2. *evitaré dañar a otros*
3. *seré honesto y sincero*
4. *seré justo y no realizaré acciones discriminatorias*
5. *honraré los derechos de propiedad incluyendo los derechos de autor y las patentes*
6. *daré el crédito apropiado a la propiedad intelectual*
7. *respetaré la privacidad de los demás*
8. *honraré la confidencialidad."*

3. Privacidad.

Siguiendo en el Diccionario de la Lengua Española (RAE, 2001), se define **privacidad** como "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*". El libro de estilo del diario El País señala que *privacidad* es un barbarismo y recomienda emplear *intimidad*, *vida privada* o *confidencialidad*, según los casos (El País, 2002). El Manual de Español Urgente de la agencia de noticias EFE prescribe evitar la palabra, que considera innecesaria, y recomienda que

se utilice en su lugar *intimidad*, *en privado*, *vida privada* o *independencia* (Agencia EFE, 2005). Otras consideraciones sobre el uso de la palabra privacidad, sobre todo en el periodismo, sugieren sea sustituida por *intimidad, vida privada o aislamiento* (Rojo, 2002).

El desarrollo de las Tecnologías de la Información y su grado de integración en nuestra sociedad facilita en gran medida el tratamiento de datos de carácter personal, tratamiento que en ocasiones supone una amenaza para la privacidad de los individuos. Por ello, se han desarrollado durante la última década varios reglamentos que protegen este derecho.

Si la reglamentación de esta materia es imprescindible para lograr una protección efectiva de la privacidad, no menos importante es la consideración de los mecanismos técnicos que permitan llevarla a cabo. Como la cuestión sigue siendo la protección de datos, aunque ahora se trate de nuevos datos, a la hora de elegir los mecanismos y protocolos apropiados, se tratará de adecuar los ya existentes, sean o no estándares.

3.1. Privacidad e Intimidad.

La privacidad, en su conjunto, representa el ámbito de la persona formado por su vida familiar, sus aficiones, sus bienes particulares y sus actividades personales, alejadas de su faceta profesional o pública. Todos estos aspectos, además de los íntimos, constituyen un esfera de la vida que se tiene derecho a proteger de intromisión. Referido a la privacidad, podemos matizar: por un lado, será el derecho que posee una persona de poder excluir a las demás personas del conocimiento de su vida personal, es decir, sus sentimientos, sus emociones, sus datos biográficos y personales y su imagen. Por otro lado, además, será la facultad de determinar en qué medida esas dimensiones de la vida personal pueden ser legítimamente comunicadas o conocidas por otras personas.

Intimidad, según una de las acepciones incluidas en (RAE, 2001) es la "*zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia*". La palabra se emplea para referirse al ambiente o la situación en que un individuo disfruta de la soledad o de la compañía de un reducido círculo de personas próximas, de forma reservada, especialmente para realizar determinadas acciones que requieren aislamiento. Claramente se deduce que el ámbito de la intimidad forma parte de la privacidad, pero no al contrario. Tanto la intimidad como la privacidad son reservadas, pero de distinta forma. Para las cosas íntimas hay personas que son reservadas incluso con los seres más próximos, pues se hallan en lo más profundo de nuestro interior, mientras que la privacidad es preservada de la mirada de quienes no forman parte de nuestro entorno personal, constituido por los familiares, y a veces por nuestros amigos personales. Éstos pertenecen a nuestra vida privada, pero sólo algunos son íntimos.

A la hora de tipificar estos nuevos datos cabe preguntarse ¿dónde situar el umbral que marca el primero de los datos privados que dejan de ser íntimos? Seguramente que ese punto de separación será relativo, la división entre unos datos y otros lo fijarán las políticas que pacten los proveedores de servicios de IET con los usuarios, sin bajar el listón obligatorio impuesto por la normativa legal y la ética. Respecto de la Información Espacio-Temporal podría, igualmente, distinguirse entre

datos de carácter personal -los que específicamente marca la ley y que han de ajustarse por ello al reglamento correspondiente-, **datos privados** -los acordados entre proveedores y usuarios y, por tanto, han de ser preservados según las políticas pactadas entre ambos- y **datos íntimos** -no deberían ser accesibles nunca y, más aún, no deberían existir almacenados-.

3.2. Privacidad: principios y derechos.

El derecho a la privacidad se establece en el ámbito de la Comunidad Europea en el Tratado de 2004 por el que se establece una Constitución para Europa, y en el ámbito nacional en la Constitución Española de 1978, en cuyo artículo 18, relativo a los Derechos Fundamentales y las Libertades Públicas, se establece lo siguiente:

1. *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
3. *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
4. *La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

En España, además de la LOPD, el Reglamento de Medidas de Seguridad establece medidas técnicas y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados que contengan datos de carácter personal y las entidades y recursos que intervengan en su tratamiento (Real Decreto, 994/1999)[2]. La Ley 32/2003 General de Telecomunicaciones, la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSICE), y el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios también establecen medidas para la proteger la privacidad en los ámbitos a los que se refieren.

El equivalente a estas normas en el ámbito europeo lo ha supuesto la Directiva 1995/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas o Directiva sobre la privacidad y las comunicaciones electrónicas. La primera ha sido traspuesta en la LOPD en 1999 y la segunda lo ha sido principalmente en la Ley 32/2003, la Ley 34/2002 y el Real Decreto 24/2005.

En la LOPD se pueden distinguir dos bloques fundamentales en los que se establecen los principios de la protección de datos y los derechos de las personas.

---

2 En la actualidad se está pendiente de la publicación en el B.O.E. de un nuevo Reglamento de medidas de seguridad, que sin duda abordará muchas de las consideraciones que se exponen en este artículo.

Además, esta ley impone una serie de obligaciones a las empresas, instituciones y profesionales, y en general a todas las personas jurídicas o físicas que operen ficheros de datos de carácter personal. Estas obligaciones son, entre otras, la inscripción de los ficheros en el Registro General de la Protección de Datos, la elaboración de un Documento de Seguridad, la implantación de medidas de seguridad y la realización de auditorías periódicas. Asimismo, se deben cumplir y garantizar respectivamente los principios y derechos que a continuación se resumen:

Principios:

1. **De consentimiento:** El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado salvo en aquellos supuestos en los que exista una excepción legal.
2. **De información de la recogida (también es un derecho):** Los interesados a los que se les soliciten datos personales deberán ser informados previamente de modo expreso, preciso e inequívoco del posible tratamiento de sus datos, de su finalidad y de los destinatarios de la información, de si es obligatorio o no comunicar dichos datos y de las consecuencias de comunicarlos o no, así como de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.
3. **De calidad de los datos o de finalidad:** Los datos de carácter personal recabados deben ser proporcionales (adecuados, pertinentes y no excesivos) al fin para el que se recogen. La veracidad y actualidad de dichos datos debe garantizarse y éstos serán cancelados tras cumplirse el fin para el que se recabaron. Los datos de carácter personal sólo podrán utilizarse con el fin para el que se recabaron, o con fines históricos, estadísticos o científicos.
4. **De seguridad:** El encargado del tratamiento de los datos deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de éstos y eviten su alteración, pérdida y tratamiento o acceso no autorizado.
5. **De secreto:** Todos aquellos que intervengan en el tratamiento de los datos de carácter personal están obligados a guardar secreto con respecto a éstos, incluso después de finalizado el tratamiento.
6. **De cesión a terceros:** Los datos de carácter personal sólo podrán ser comunicados o cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario con el previo consentimiento del interesado.

Derechos:

1. **De consulta:** Cualquier persona podrá conocer la existencia de tratamientos de datos de carácter personal, su finalidad y el responsable del tratamiento dirigiéndose al Registro General de Protección de Datos.
2. **De acceso:** El interesado puede recabar información de sus datos de carácter personal sometidos a tratamiento, su origen, y las comunicaciones a terceros que se hayan realizado o se prevean realizar.

3. **De rectificación y cancelación:** El interesado puede instar al responsable del fichero a cumplir con la obligación de mantener la exactitud de los datos cuando resulten completos o inexactos, así como a rectificar o cancelar éstos cuando resulten incompletos o inexactos, o sean inadecuados para la finalidad recogida.
4. **De oposición:** El interesado podrá oponerse al tratamiento de sus datos de carácter personal siempre que no exista una ley que disponga lo contrario.
5. **De impugnación:** El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad.

4. Privacidad de la Información Espacio-Temporal (PIET). Legislación y Ética.

Como se ha dicho antes, la información de localización de entidades en un momento determinado puede considerarse como un dato de carácter personal pues el conocimiento de esta información podría suponer una amenaza a la privacidad de los individuos. La localización en ciertos momentos (información espacio-temporal o IET) puede incluso considerarse un dato de carácter íntimo, sobre todo cuando aquélla puede asociarse a la identidad del individuo o a perfiles que le puedan identificar. Su obtención de forma periódica (seguimiento y monitorización de entidades) puede permitir la construcción de patrones de comportamiento del individuo que pueden potencialmente identificarle, así como permitir la determinación de hábitos de consumo, preferencias, aspectos de su personalidad y costumbres de su vida privada. Por estas razones, el desarrollo de las tecnologías de estimación de la posición y la aparición de los servicios basados en la localización ha provocado un aumento de la preocupación sobre la privacidad de la información espacio-temporal y cómo preservarla en diversos ámbitos (académico, gubernamental, social, moral).

La protección de la Privacidad de la IET (PIET) en España está contemplada en las leyes citadas con anterioridad por concluirse que se trata de un dato de carácter personal. Sin embargo, es sólo en el reciente Real Decreto 424/2005 donde se hace referencia explícita a la información de localización, trasponiendo parte de la Directiva 2002/54/CE. En el citado Real Decreto se diferencia los datos de tráfico de los datos de localización con respecto a la provisión de servicios de valor añadido, conceptos que se definen de la siguiente manera:

- ***Datos de tráfico:*** *cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de su facturación.*
- ***Datos de localización:*** *cualquier dato tratado en redes de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público.*

- ***Tratamiento de datos:*** *operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*
- ***Servicio con valor añadido:*** *todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vaya más allá de lo necesario para la transmisión de una comunicación o su facturación.*

En el artículo 70 del Real Decreto 424/2005 se dispone que sólo podrán tratarse los datos de localización distintos de los de tráfico si éstos se hacen anónimos o previo consentimiento del afectado, en la medida y tiempo necesarios para la prestación de un servicio de valor añadido. La norma también dispone que los sujetos obligados (aquellos que requieren el tratamiento de los datos) deberán informar al afectado del tipo de datos que se recaba, de su finalidad, de la duración del tratamiento, de si se transmitirán a un tercero y solicitarán el consentimiento del afectado. De todas formas, se comenta que se entenderá que existe consentimiento expreso si el usuario se ha dirigido al sujeto obligado para la prestación de un servicio de valor añadido que requiere el tratamiento de sus datos de localización. El usuario contará con la posibilidad de retirar en cualquier momento su consentimiento así como rechazar su tratamiento de forma temporal fácilmente.

Se puede observar que existe una coherencia entre lo regulado en el artículo 70 del Real Decreto 424/2005 con los principios de PIET ya regulados en la LOPD, pero que se realiza un mayor énfasis en los Principios de consentimiento, de información, de finalidad, de cesión y en el derecho de oposición. A veces incluso se realiza un refinamiento del principio, como ocurre con el principio de consentimiento, donde también se permite el tratamiento de los datos de localización si estos datos son anónimos o si se ha solicitado un servicio de valor añadido que los necesite independientemente de si el usuario ha otorgado su consentimiento expreso.

Los principios de privacidad expuestos han sido adaptados al contexto específico de los Servicios Basados en la Localización (LBS), en los ámbitos empresarial y académico. El organismo *Location Interoperability Forum* (LIF), que reúne a empresas como Lucent, Alternis, Ericsson, Motorola, Nokia y a entidades normalizadoras como la ETSI, ha desarrollado un documento donde se describen los principios que deberían contemplarse para preservar la PIET (LIF, 2001). Otros autores han discutido y analizado cuáles deberían ser éstos, por ejemplo en (Langheinrich, 2001) y (Minch, 2004). Desde ambas vertientes también se hace un énfasis en algunos de los principios reflejados en la legislación, en particular los de consentimiento, de información, de finalidad, de seguridad, de cesión y al derecho de oposición.

En cuanto a la ética, las entidades implicadas suelen acudir a los códigos desarrollados por instituciones normalizadoras o de prestigio para disponer de guías de comportamiento o códigos de conducta para sus empleados y para las relaciones de unas entidades con otras. Como resumen, podría decirse que el acatamiento de la legislación, más las políticas de las empresas y el código deontológico de los profesionales, sería la mejor presentación para una eficaz preservación de la privacidad e intimidad de los personas.

5. Privacidad y Servicios de Seguridad.

En Seguridad de la Información se define **confidencialidad** como la "*propiedad de la información que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados*" (ISO/IEC 7498-2, 1988). En la misma norma se establece que el **control de acceso** es "*el servicio de seguridad que previene el uso de un recurso salvo en los casos y de la manera autorizada*". Estos servicios de seguridad, así como cuestiones relacionadas con ellos, se puede consultar en numerosas obras, como (Menezes, Oorschot & Vanstone, 2001) y (Stallings, 2002).

El **anonimato** es un objetivo de seguridad que recientemente ha atraído una mayor atención entre académicos y legisladores. En (Pfitzmann & Köhntopp, 2005) los autores definen el anonimato de un sujeto como "*el estado de ser no identificable dentro de un conjunto de sujetos, el conjunto de anonimato; el conjunto de anonimato está compuesto por todos los posibles sujetos*". El **pseudoanonimato** es un mecanismo relacionado habitualmente con el anonimato. Pfitzmann y Köhntopp definen también el pseudoanonimato de un sujeto como "*el estado de usar un pseudónimo como identificador*", mientras que la norma (ISO/IEC 15408, 2005) lo define como: "*propiedad que garantiza que un usuario pueda utilizar un recurso o servicio sin desvelar su identidad, pero todavía pueda ser responsabilizado sobre este uso*".

De las definiciones expuestas se puede deducir que los mecanismos de seguridad existentes para proporcionar los servicios de confidencialidad, control de acceso y anonimato son apropiados para preservar la privacidad de los individuos y en particular la Privacidad de la Información Espacio-Temporal (PIET). Las técnicas y estándares para preservar la PIET harán uso de estos mecanismos.

6. Técnicas y estándares de seguridad para preservar la PIET.

En la literatura se encuentran diversos modelos y mecanismos cuyo objetivo es preservar la privacidad de la información espacio-temporal (PIET) de los sujetos. A grandes rasgos se pueden clasificar en tres grupos, dependiendo del mecanismo principal que utilizan, aunque algunas propuestas contemplan varios de ellos. Un primer grupo de proposiciones para preservar la PIET se basaría en la utilización de políticas para gestionar los permisos para localizar a una entidad y determinar bajo qué condiciones y modos esta información es accedida (Leonhardt & Magee, 1998), (Snekkenes, 2001), (Langheinrich, 2002), (Myles, Friday & Davies, 2003), (IETF, 2003) y (Gajparia, Mitchell & Yeun, 2004).

La mayoría de estas propuestas asume que existe una entidad intermediaria entre los servicios de localización (LCS) que localizan al sujeto y los servicios basados en la localización (LBS) deseosos de utilizar esta información. Las entidades intermediarias controlan el flujo de la IET entre los LCS y los LBS basándose en las políticas o preferencias, definidas habitualmente por la entidad responsable del sujeto. A veces el rol de entidad intermediaria lo asume el propio LCS (Leonhardt & Magee, 1998). Las condiciones a determinar en las políticas dependen de cada propuesta.

Habitualmente, las políticas que se proponen siempre permiten especificar qué entidades pueden acceder a la IET, como se hace en los sistemas tradicionales de control de acceso, pero es también habitual proporcionar mecanismos para especificar la granularidad de la IET o la granularidad con la que se revela la identidad del sujeto contemplando por ejemplo su identidad real, un pseudónimo a largo o a corto plazo, un rol o de forma anónima. Algunos modelos aducen, además, que las políticas permitan también especificar bajo qué condiciones espacio-temporales del sujeto la IET podrá ser accedida. Todas o parte de estas posibilidades se ofrecen en (Leonhardt & Magee, 1998), (Snekkenes, 2001), (Myles, Friday & Davies, 2003), (IETF, 2003) y (Hengartner & Steenkiste, 2004).

En otras de las propuestas que utilizan políticas para preservar la PIET se estipula que éstas faciliten el control del uso de la IET, su retención, almacenamiento o distribución una vez ésta ha sido comunicada. En algunos casos esta comprobación se realiza en el momento del acceso a la información mediante la comparación de las preferencias establecidas por los usuarios y las políticas de privacidad establecidas por los LBS (Myles, Friday & Davies, 2003). En otros casos se propone que las preferencias del usuario se asocien a la IET de forma segura, es decir, que la IET y sus preferencias estén encapsuladas en un objeto que preserve su integridad y a veces su confidencialidad, dejando en manos de entidades reguladoras -Agencias de Protección de Datos- el cumplimiento de estas políticas asociadas (IETF, 2003), (Gajparia, Mitchell & Yeun, 2003) y (Gajparia, Mitchell & Yeun, 2004). Algunos de los mecanismos para preservar la integridad de la IET asociada al sujeto y a las preferencias contemplados en estas últimas propuestas, consideran la generación de firmas digitales y sobres seguros.

Otro grupo de modelos se basa en la emisión de certificados de atributos que acreditan los permisos otorgados a cierta entidad para obtener, almacenar, utilizar e incluso a veces ceder la localización de otra, como ocurre en las propuestas de (Hengartner & Steenkiste, 2004) y (Hauser & Kabatnik, 2001), en esta última los permisos se asocian a la clave pública de la entidad que solicita la localización, el sujeto localizado es identificado bajo un pseudónimo, que es una clave pública conocida sólo por él y por el servicio de localización, y cada uno de los solicitantes autorizados recibe este pseudónimo modificado para indicar el sujeto en las solicitudes. En (Hengartner & Steenkiste, 2004) se utilizan certificados SPKI/SDSI (según la RFC99) para expresar las autorizaciones. En la idea de (Rodden, Friday, Muller & Dix, 2002) se utiliza el mismo concepto pero los certificados se reducen al conocimiento del pseudónimo bajo el que el usuario se ha registrado en el servicio de localización.

Un último grupo de técnicas propone utilizar servicios e infraestructuras intermediarias entre los servicios de localización y los servicios basados en la localización para proporcionar IET anónima (Federrath, Jerichow & Pfitzmann, 1996), (Beresford & Stajano, 2003). La propuesta en (Gruteser & Grunwald, 2003) utiliza técnicas estadísticas para controlar la granularidad con la que la IET es revelada para conseguir el suficiente anonimato.

7. Propuesta para preservar la PIET.

La técnica que proponemos para preservar la PIET permite que los sistemas que las utilicen sean conformes a la legislación existente y proporcionen a los usuarios instrumentos para adaptar el comportamiento del sistema de acuerdo a las preferencias de cada uno de forma flexible. Se basa en la utilización de dos mecanismos de seguridad complementarios: políticas de autorización y certificados de atributos. La técnica propuesta considera la existencia de una entidad confiable que se encargará de tomar las decisiones de autorización o denegación para obtener y comunicar la IET referente a un individuo a un servicio basado en la localización que así lo solicite.

Las políticas de privacidad ideadas podrán determinar la autorización o la denegación de la petición de acuerdo con los siguientes parámetros:

- La identidad del solicitante de la IET y del receptor de ésta si fuera distinto.
- El tratamiento previsto para la IET, información que debe ser comunicada por el solicitante en la petición. El tratamiento estará comprendido por la finalidad prevista de la IET (comercial, de seguridad, emergencias, navegación, etc.), su almacenamiento y su posible distribución.
- La situación espacio-temporal del individuo sobre el que se solicita la IET.

Los certificados de autorización ideados son equivalentes a las políticas de privacidad de autorización positiva, pero al tener una fecha de expiración complementan a las políticas permitiendo a los usuarios gestionar su privacidad de manera más flexible.

Por otro lado, la técnica que proponemos para preservar la PIET protege, además de la privacidad, la integridad y autenticidad de la IET. Para ello se utilizan mecanismos de certificación digital. La entidad confiable comunica la IET referente a los individuos dentro de un certificado espacio-temporal que contiene los siguientes campos:

- Versión del formato del certificado espacio-temporal.
- Número de serie.
- Instante de emisión.
- Periodo de validez.
- Identificación de la entidad emisora.
- Sujeto del certificado o entidad a la que hace referencia la IET.
- Información Espacio-Temporal (IET), incluyendo su resolución y las entidades implicadas con su obtención.
- Tratamiento autorizado para esta IET (finalidad, almacenamiento y distribución).
- Usuarios autorizados para tratar la IET.
- Firma digital sobre todo lo anterior.

Los servicios en los que la entidad beneficiada de la información de localización es la entidad localizable podrían estar enfocados en la seguridad, mensajería, navegación, directorios locales, etc., todos ellos basados en la posición del usuario.

Por otro lado, los servicios en los que la entidad beneficiada de la información es un tercero podrían enfocarse en la publicidad, en la seguridad, en la atención de emergencias, etc.

8. Conclusiones.

Se ha comenzado exponiendo la aparición relativamente reciente en la Sociedad de la Información de unos nuevos datos relativos a las personas, los que constituyen la Información Espacio-Temporal, que son susceptibles de comprometer la privacidad y la intimidad de los individuos. Ambos conceptos, privacidad e intimidad, se han estudiado y analizado partiendo de diferentes fuentes de referencia. Se ha reflexionado sobre la conducta, el comportamiento y los códigos éticos de los profesionales implicados. Por último, se exponen las Técnicas propuestas para preservar la PIET, detallando un modelo basado en Políticas.

Las futuras líneas a seguir van a estar motivadas, por un lado, por las nuevas ofertas de valor añadido que ofrecerán los Servicios Basados en la Localización y, por otro, por las nuevas demandas de proteger la privacidad e intimidad de los usuarios. Es decir, se demanda u ofrece un nuevo servicio, y ello obliga a ajustar la reglamentación (o a legislar nuevas leyes), mejorar los hábitos de conducta y actualizar las Técnicas (o a desarrollar otras nuevas) para mantener la confianza y seguridad de los ciudadanos.

Este artículo se enmarca dentro del Proyecto de Investigación CERTILOC, Servicio de CERTIficacion digital de la LOCalizacion, Ref. SEG2004-02604, concedido en el marco del Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica 2004-2007. Ministerio de Educación y Ciencia. España.

Referencias

Agencia EFE. (2005). Departamento de Español Urgente: Vademécum, *http//:www.efe.es*.

Beresford A. R. & Stajano F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing, 2*(1).

Burmester M., Desmedt Y., Wright R. N. & Yasinsac A. (2004). Accountable privacy. *The Twelfth International Workshop on Security Protocols*.

Chaum D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM, 24*(2), 84-90.

Constitución Española. (1978). Constitución Española de 27 de diciembre de 1978, modificada por reforma de 27 de agosto de 1992.

Constitución para Europa. (2004). Tratado por el que se establece una Constitución para Europa, 29 de octubre de 2004.

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

Directiva 2002/58/CE. (2002). Directiva del Parlamento Europeo y del Consejo de 12 de Julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

El País. (2002). Libro de estilo. *Ed. Santillana, Madrid*.

Federrath H., Jerichow A. & Pfitzmann A. (1996). MIXes in Mobile Communication Systems: Location Management with Privacy. *Information Hiding*.

Gajparia A., Mitchell C. J. & Yeun C. Y. (2003). Using constraints to protect personal location information. *Proceedings of VTC 2003 Fall. IEEE Semiannual Vehicular Technology Conference*.

Gajparia A., Mitchell C. J., & Yeun C. Y. (2004). Information Preference Authority: Supporting user privacy in location based services. *Proceedings of the 9th Nordic Workshop on Secure IT-systems*.

Gruteser M. & Grunwald D. (2003). Anonymous usage of location-based services through spatial and temporal cloaking. *ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys)*.

Hauser C. & Kabatnik M. (2001). Towards privacy support in a global location service. *Proceedings of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001)*.

Hengartner U. & Steenkiste P. (2004). Implementing access location information. *The Ninth ACM Symposium Models and Technologies (SACMAT'04)*.

IETF. (2003). Geographic Location/Privacy WG (geopriv). Charter. *Available at: http://www.ietf.org/html.charters/geopriv-charter.html*.

ISO/IEC 7498-2. (1988). Information processing systems - Open systems interconnection - Basic reference model - Part 2: Security arquitecture, 1988.

Langheinrich M. (2001). Privacy by design - principles of privacy-aware ubiquitous systems. *UbiComp '01: Proceedings of the 3rd international conference on Ubiquitous Computin*. Springer-Verlag, 273-291.

Langheinrich M. (2002). A privacy awareness system for ubiquitous computing environments. *Proceedings of Ubicomp*, 237-245.

Leonhardt U. & Magee J. (1998). Security considerations for a distributed location service. *Journal of Network and System Management*, 51-70.

Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico.

Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

LIF, Location Interoperatibility Forum. (2001). LIF Privacy Guidelines. *The 3rd ACM conference on Electronic Commerce, Tampa, Florida, USA.*

Menezes A., Oorschot P. van & Vanstone S. (2001). Handbook of Applied Cryptography. CRC Press.

Minch R. P. (2004). Privacy issues in location-aware mobile devices. *The 37th Hawaii International Conference on System Sciences*.

Myles G., Friday A. & N. Davies. (2003). Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing, 2*(1).

Pfitzmann A. & Köhntopp M. (2005). Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology. *Draft, versión 0.22*.

RAE, Real Academia Española. (2001). *Diccionario de la Lengua Española*.

Real Decreto 424/2005 de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Rodden T., Friday A., Muller H. & Dix A. (2002). A lightweight approach to managing privacy in location-based services. *Technical Report Equator-02-058*. University of Nottingham, Lancaster University, and University of Bristol.

Snekkenes E. (2001). Concepts for personal location privacy policies. *The 3rd ACM conference on Electronic Commerce.* ACM Press.

Stallings W. (2002). Cryptography and Network Security: Principles and Practice, 3rd Edition. Prentice Hall.