IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

Smart cities, movilidad inteligente y protección de los datos personales*

Alessandro Mantelero
Profesor agregado de Derecho privado
Nexa Center for Internet and Society (Politecnico di Torino)

Fecha de presentación: octubre, 2015
Fecha de aceptación: noviembre, 2015
Fecha de publicación: diciembre, 2015

Resumen
En este artículo el autor afronta las cuestiones relativas a la protección de datos en el contexto de amplios proyectos de movilidad territorial. En la primera parte, se describen brevemente los sistemas de movilidad inteligente y los problemas que de ellos se derivan, con especial atención a su incidencia sobre la dimensión individual y colectiva de la protección de datos. La segunda parte del artículo analiza cómo se han afrontado estos aspectos en Italia en el ámbito de un proyecto piloto concreto que ha involucrado a entes de transporte, gobiernos locales y a la academia.

Palabras clave
transportes, movilidad inteligente, protección de datos personales, big data, privacy by design, smart cities

Tema
protección de datos personales

Smart cities, smart mobility and personal data protection

Abstract
In this paper, the author addresses the issues related to data protection in the context of large territorial smart mobility plans. The first part of the paper introduces smart mobility systems and discusses the new problems that arise from these applications, which have an impact both on individual privacy and collective data protection. The second part analyses how these issues have been addressed in a specific leading smart mobility project realised in Italy, which has involved transport companies, local government and academic research.

Keywords
transport, smart mobility, data protection, big data, privacy by design, smart cities

Topic
data protection

* Traducción de María-José Pifarré de Moner, profesora agregada de la Universitat Oberta de Catalunya.

Introducción

La enorme cantidad de información recogida a través de los dispositivos *online* y *offline*, así como los escenarios futuros del Internet de las cosas (*Internet of Things*)[1] y de la robótica, crean serias dudas acerca del posible uso de los datos para monitorizar individuos y grupos.[2] Hay que tener en cuenta también que estas tecnologías a menudo crean situaciones de desequilibrio, ya que los individuos no tienen conocimiento de los elementos fundamentales del tratamiento de sus datos y de sus consecuencias,[3] ni son plenamente capaces de negociar su información. Por último, en el contexto de los *Big Data* la recogida de información puede llevarse a cabo para perseguir fines no definidos con antelación y derivados de las correlaciones que emergen del flujo de los datos, que son distintos de los fines iniciales de la recogida.[4]

Por estos motivos, el desarrollo de las *smart cities* y de los ecosistemas digitales inteligentes no debería caracterizarse por un enfoque meramente *data-driven* centrado en la eficiencia, sino que es necesario tomar también en consideración sus posibles efectos sociales y los riesgos que emergen de la creación de ambientes íntimamente interconectados.

En este sentido, ya son varios los autores que han subrayado la importancia de definir un marco jurídico y ético que regule el uso de los datos personales en la era de los *Big Data* y de las *smart cities*,[5] aunque en muchos casos se trata de contribuciones que adoptan una perspectiva meramente teórica. Esta perspectiva, a pesar de ser fundamental para construir un futuro marco jurídico que responda a las distintas problemáticas que aquí brevemente señalamos, se debería integrar además con estudios empíricos. Hay que destacar que el análisis empírico es coherente con la naturaleza de la tutela de los datos personales y de la *privacy*, ya que se trata de aspectos que varían en función del contexto cultural y jurídico.[6]

También se hace necesario tomar en consideración que, en referencia a determinados contextos, la ponderación entre los diversos intereses contrapuestos no se puede llevar a cabo únicamente en términos generales y abstractos. Así, por ejemplo, si distintos ordenamientos jurídicos admiten que el interés general en la eficiencia de la movilidad y el desarrollo de las ciudades inteligentes puede justificar formas limitadas de localización de los usuarios, esta valoración general deberá acompañarse necesariamente de una valoración del impacto general que comportan las soluciones específicas que se adopten, y más en concreto, de las que se generen para la protección de los datos.

Las ciudades inteligentes, por tanto, no representan un mero contexto tecnológico, sino que deben convertirse en un ambiente inclusivo y participativo en el que ciudadanos, administraciones públicas y empresas operen conjuntamente para mejorar la eficiencia a nivel local a través de procesos inclusivos y participativos. En términos de protección de datos, esto implica la adopción de un nuevo paradigma centrado en la valoración del riesgo y en el refuerzo del papel de vigilancia de las autoridades de protección de datos.[7]

Por este motivo, es necesario llevar a cabo estudios empíricos dirigidos a indagar acerca de las dificultades y los obstáculos que se interponen frente a la actuación de un proceso con muchas partes interesadas, dirigido a ofrecer soluciones innovadoras que sitúen al ciudadano en el centro del proceso. Estos análisis, además, facilitarían la definición de *best practices* para las comunidades de ciudadanos y para los innovadores en relación con aplicaciones tecnológicas determinadas.

Desde este punto de vista, los sistemas públicos de movilidad local pueden constituir un interesante caso de estudio y un posible laboratorio para la experimentación de enfoques *multi-stakeholder,* basados en una pluralidad de partes interesadas. Y ello precisamente por el papel central que la movilidad pública desempeña en la vida urbana, por la presencia de caracteres comunes que caracterizan a los sistemas de movilidad de los diversos contextos urbanos y por las posibilidades de mejora de los servicios a través de soluciones innovadoras basadas en las TIC.

1. V. Article 29 Data Protection Working Party (2014a).
2. V. Brown (2013); Mantelero y Vaciago (2014, pág. 175 y sig).
3. V. también Acquisti *et al*. (2015, pág. 509 y sig).
4. V. Bollier (2010).
5. V. Schwartz (2010); Wright (2011, pág. 199 y sig.).
6. V. Westin (1970, pág. 183 y sig.); Bygrave (2002, pág. 327); Nissenbaum (2010); Altman (1977, pág. 66 y sig.).
7. V. Mantelero (2014, pág. 643 y sig.).

Sin embargo, si bien los sistemas de movilidad inteligente por una parte producen efectos sobre la interoperabilidad entre los servicios de transporte en una determinada área, por la otra crean interrogantes en lo que a su impacto sobre la *privacy* individual y colectiva se refiere. Las principales preocupaciones se derivan, concretamente, de la capacidad de estos sistemas para identificar y localizar a los usuarios a través de una monitorización que podría ser invasiva, especialmente cuando la información sobre la movilidad se asociara a datos provenientes de otras fuentes.

Por estos motivos, el empleo de las *smart technologies* en el contexto de la movilidad representa un interesante campo de investigación en el que es posible poner en acto soluciones empíricas dirigidas a crear ambientes *privacy-oriented*. Desde este punto de vista, el presente artículo examinará en primer lugar los sistemas de movilidad inteligente en general, valorando su impacto sobre las dimensiones individual y colectiva de la protección de datos, para posteriormente detenerse en cómo se han afrontado estos aspectos mediante soluciones de *privacy by design* en uno de los principales proyectos de movilidad inteligente llevados a cabo en Italia.

1. Soluciones innovadoras para la movilidad inteligente y su impacto sobre la dimensión individual y colectiva de la protección de datos

La movilidad representa un factor clave para el desarrollo social y económico. Sin embargo, para que se convierta en un factor de cohesión territorial y crecimiento de las áreas urbanas, es necesaria una adecuada planificación de los transportes. Es necesario poner de relieve que la movilidad se ve necesariamente condicionada por las dinámicas sociales, que cambian a lo largo del tiempo y que en parte dependen de otros factores de cambio, como la planificación urbana, las inversiones industriales y comerciales o la disponibilidad de servicios públicos. Por último, la infraestructura de los transportes a menudo representa un nuevo plano que se superpone al ya existente ambiente antropomorfizado y, por este motivo, su realización puede resultar difícil y onerosa.

Partiendo de las características que brevemente se han mencionado, es posible comprender el papel que las TIC pueden desempeñar en la gestión de la demanda y en la prestación de servicios de movilidad a través de sistemas de análisis del tráfico, de un mapeo constante de los recorridos, del análisis de la demanda y de la creación de sistemas eficientes de gestión y venta de billetes. El hecho de que la implementación de todos estos aspectos innovadores necesite de la recogida y elaboración de la información inherente a la movilidad hace que las soluciones inteligentes en el ámbito de los transportes necesiten, y a la vez creen, un gran ecosistema de datos que implica a varios sujetos (usuarios, administraciones locales, entes de transportes y proveedores de servicios).

En concreto, son varios los beneficios que pueden conseguir los diferentes sujetos involucrados. En primer lugar, las administraciones locales utilizan la información de movilidad para hacer más eficaz la oferta de los servicios de transporte, para optimizar la utilización de fondos destinados a subvencionar el transporte público local y para crear sistemas integrados y multimodales. En segundo lugar, las empresas de transportes se benefician de una distribución más equitativa de los recursos públicos y pueden utilizar los datos de movilidad para planificar sus servicios y modelos de negocio. Los usuarios, por último, tienen la posibilidad de acceder a su propia información de movilidad, de disfrutar de sistemas inteligentes de venta de billetes más eficaces y, en muchos casos, de utilizar sistemas de pago electrónicos y *online*. A nivel colectivo, además, los ciudadanos y las administraciones locales tienen acceso a la información sobre movilidad en forma agregada, lo que hace más fácil definir estrategias de reducción de la congestión del tráfico, apoyar la planificación urbanística, potenciar los servicios de uso compartido (por ejemplo los servicios de *bike sharing* o *car sharing* combinados con el uso de medios públicos de transporte) y crear nuevos servicios comerciales (por ejemplo, programas de fidelización para los abonados, formas publicitarias basadas en la posición en tiempo real del usuario).

Por el contrario, un uso indebido y no *privacy-oriented* de los datos de movilidad puede modificar un contexto centrado en un uso positivo de la innovación y transformarlo en un ambiente inteligente distópico, en el que los gobiernos monitoricen los hábitos de movilidad y las interacciones sociales de los ciudadanos, las empresas de transporte aprovechen la información sobre movilidad para desplegar prácticas comerciales incorrectas o que vulneren la libre competencia y las empresas privadas envíen publicidad no deseada a los usuarios o realicen análisis de mercado de manera oculta.

La mitigación del impacto potencial sobre la protección de los datos, ya sea en términos individuales o en términos colectivos, representa, en consecuencia, la piedra angular de las estrategias inteligentes de transporte basadas en la utilización de información sobre la movilidad de personas físicas identificadas o identificables. Sin embargo, no es posible eliminar estos potenciales riesgos recurriendo simplemente al empleo de datos anónimos —que por otra parte no tendrían la capacidad de proporcionar un conjunto de datos lo suficientemente detallados[8] ni permitirían adoptar soluciones eficaces de pago y de detección de fraudes— porque la anonimización ofrece una tutela limitada debido a que en el contexto de los *Big Data* el riesgo de reidentificación continúa siendo, hasta la fecha, importante.[9]

2. La arquitectura de los flujos de datos y la protección de los datos

En varios países, entre los cuales se encuentra Italia, el transporte público se halla subvencionado tanto a nivel nacional como regional para garantizar unos niveles mínimos de servicio en aquellas áreas en las que el modelo comercial no es capaz de generar ingresos suficientes. Tal empleo de fondos públicos, sin embargo, se debe gestionar de manera eficiente teniendo en cuenta el número efectivo de pasajeros transportados, las líneas cubiertas por el servicio y la frecuencia de uso de tales líneas. En este contexto, los sistemas inteligentes de billetaje representan una solución técnica de apoyo a un servicio de transporte multimodal integrado y dirigido a monitorizar un uso eficaz de este, lo cual permite subvencionar a las empresas de transporte locales con fondos públicos adecuados y proporcionados al uso de los servicios.

En términos de flujos de datos, la adopción de un sistema integrado de billetaje electrónico genera dos flujos diferentes de información: uno relativo a los pagos efectuados por parte de los usuarios del servicio de transporte y otro inherente a los datos de movilidad. Dado que se trata de modalidades de información que se tratan con finalidades distintas, requieren la adopción de soluciones diferentes en materia de protección de datos. Por estas razones, en el caso de estudio que examinaremos a continuación los datos inherentes a los contratos de transporte suscritos por el usuario y los pagos a estos correspondientes se han separado de la información sobre la movilidad referida a estos mismos usuarios, lo cual únicamente permite la posibilidad de sincronizar estas distintas fuentes de información de manera excepcional (por ejemplo, para la detección de fraudes, la gestión del crédito electrónico para los transportes o la gestión de las subvenciones públicas).

Un examen del uso de los datos y de las operaciones a los que estos se han sometido pone de manifiesto que la «propiedad» de la información puede convertirse en un aspecto crucial en la realización de los ecosistemas de información de apoyo a las *smart cities* y, más específicamente, a la movilidad inteligente, a causa de las distintas empresas implicadas en estos proyectos y del papel desempeñado por las administraciones públicas locales.[10] Si por una parte, efectivamente, los distintos actores desearían ejercer el control de los datos como propietarios de estos, no se puede olvidar que la información personal no puede considerarse una mercancía, ya que representa aspectos específicos del individuo, y la protección de los datos personales coadyuva tanto a la prevención de formas de ilegítima intromisión en la vida privada de las personas como a prácticas discriminatorias.

Además, hay que tener presente que el régimen jurídico de la circulación de datos personales complica este panorama desde el momento en que en este régimen, elementos próximos a la noción de propiedad (por ejemplo, la transferencia de los datos a terceros o la explotación económica de los datos) coexisten con el reconocimiento a la persona individual de una especie de control sobre los datos destinado a perdurar a pesar de que se haya realizado ya la comunicación de la información a terceros.[11]

En este contexto teórico proprio del modelo europeo, los sistemas inteligentes de movilidad no pueden, por tanto,

8. Los datos anónimos se pueden utilizar para conocer la frecuencia de uso de las líneas de transporte, pero son necesarios datos referidos a sujetos identificados o datos pseudoanonimizados para realizar un mapa de flujos de pasajeros a través de itinerarios que comprenden líneas distintas, y estos flujos representan la información más preciosa para la planificación de la movilidad.
9. V. Narayanan *et al*. (2015); Narayanan, Felten (2014); Mayer-Schönberger, Cukier (2013, pág. 154 y sig.); Schwartz, Solove (2011, pág. 1841 y sig.); United States General Accounting Office (2011, pág. 68 y sig.); Ohm (2010, pág. 1701 y sig.); Golle (2006); Sweeney (2000).
10. V. también European Cities and Regions Networking for Innovative Transport Solutions (2013).
11. V. art. 12, 13 e 14, Directiva 95/46/CE.

adoptar un enfoque basado en la propiedad de los datos, y la información generada por los pasajeros y obtenida mediante el uso de los sistemas electrónicos de billetaje no puede considerarse propiedad de los entes públicos que tienen la competencia sobre el transporte, ni de las sociedades privadas de transporte ni, más en general, de los distintos sujetos implicados en los proyectos de movilidad. Tales datos, dado que conciernen a personas físicas identificadas o identificables,[12] son y continúan siendo, efectivamente, datos personales y, por esta razón, los sujetos a los que se refieren conservan algunos derechos sobre dicha información y deben participar adecuadamente en el proceso de su elaboración. Por tanto, es necesario que los usuarios reciban una clara comunicación en referencia al tratamiento de sus datos, proporcionen su consentimiento cuando la ley lo requiera y vean reconocidos sus derechos a la autodeterminación informativa.[13]

Cabe señalar, por último, que precisamente la presencia de datos personales o el riesgo de reidentificación de los sujetos, allí donde se recurra a datos anonimizados o pseudoanonimizados, debería inducir a las administraciones públicas a evaluar las oportunidades y las modalidades de extensión de políticas de *open data* a la información detallada inherente a la movilidad[14] En este sentido, parece oportuno adoptar un enfoque contextualizado, que considere la especificidad del *data set*, la naturaleza georeferencial de la información y, que cuando —como sería deseable— se recurra a datos anónimos o presudoanonimizados, considere los factores que puedan aumentar el riesgo de reidentificación (por ejemplo, la dimensión del *data set*, la amplitud del área geográfica, el número de usuarios implicados en el proyecto o la complejidad de los sistemas de transporte).

Un ejemplo de los efectos negativos de la carencia de un tal análisis preliminar lo proporciona el caso del proyecto de *bike-sharing* de la ciudad de Londres, en el que la administración local había hecho público el *data set* de los desplazamientos en bicicleta de los usuarios, que contenía información suficiente para describir los hábitos de movilidad de los ciclistas en todo Londres. Efectivamente, en el *data set* se habían incluido tanto los identificadores unívocos de los usuarios del servicio como la posición y la fecha y hora de inicio y fin de cada viaje, de manera que sobre la base de los itinerarios más frecuentes y la fecha y hora del viaje era posible identificar los lugares en los que los usuarios vivían y trabajaban, por lo que posteriormente esta información se podía utilizar para reidentificar a los usuarios.[15] Si bien el riesgo de reidentificación en una gran área metropolitana es inferior al que se corre en ámbitos de dimensiones inferiores, este caso nos muestra el papel central que desempeña la realización de una valoración preliminar del impacto potencial que las estrategias de *open data* pueden suponer para la protección de los datos.

A la luz de lo visto hasta el momento, hay que concluir que para evitar perjuicios para los derechos de los individuos a raíz de sus datos, las soluciones de *privacy by design* no deberían limitarse a la simple pseudoanonimización de los datos, sino que deberían también cubrir la representación de los trayectos de movilidad referidos a un pasajero específico, aunque se le haya hecho no identificable de manera nominativa. En este sentido, es deseable que la información relativa a los distintos segmentos de un mismo recorrido (por ejemplo, las distintas líneas de transporte utilizadas por un mismo viajero se memoricen de manera autónoma y separada, sin ligarlas a un usuario unívoco), aunque no esté identificado de manera nominativa. Efectivamente, esta solución hace mucho más difícil determinar comportamientos recurrentes en los recorridos de movilidad de los usuarios de los que inferir elementos útiles para reidentificarlo.

Tal como están las cosas por el momento, sin embargo, no parece necesario adoptar ulteriores y más complejas soluciones técnicas de protección (por ejemplo, de *differential privacy*)[16] ya que, en lo que se refiere a los datos de movilidad, la naturaleza de la información tratada, junto a la cantidad de tiempo y al esfuerzo necesario para realizar la reidentificación, nos hacen pensar que la solución antes descrita (recurso a formas de anonimización/pseudoanonimización y segmentación de los movimientos de los usuarios) permite alcanzar un nivel de protección proporcional a los riesgos y coherente con la relación entre costes y beneficios.

12. V. art. 2(a), Directiva 95/46/CE.
13. V. art. 12, 14, y 22, Directiva 95/46/CE.
14. V. *supra* nota 11.
15. V. Mirant (2014); Saddle (2014).
16. V. Dwork (2011); I. Mironov *et al.* (2009).

3. Un caso de estudio italiano: el sistema de la movilidad inteligente en Piamonte

El sistema multimodal de transporte integrado llevado a cabo por la Región del Piamonte, en el norte de Italia, constituye un caso de estudio de interés por diversas razones. En primer lugar, el centro y norte de Italia son las zonas en las que existe la red de transporte más amplia a nivel nacional, y Turín (capital regional del Piamonte) es la ciudad italiana con la mayor cobertura en términos de transporte público (615 km/100 km^2). En segundo lugar, el uso de tecnologías inteligentes para recoger y analizar información acerca de la movilidad representa el núcleo del modelo piamontés. En tercer lugar, el proyecto cubre toda la región, que cuenta con un área de 25 400 km^2, con aproximadamente 4,6 millones de habitantes (aproximadamente la población de la República de Irlanda), y comprende diversos contextos territoriales (el área metropolitana de Turín, ciudades de pequeña y mediana dimensión, zonas rurales y de montaña). Por último, el sistema implica a varias empresas de transporte que proporcionan servicios distintos tanto en términos de frecuencia (servicios 24/7, diarios, semanales, etc.) como de modalidades de transporte (tranvía, autobús, metro, autobuses extraurbanos, trenes regionales y trayectos de ferrocarril nacionales).

Por todo ello, el proyecto del Piamonte representa un *leading case* en el contexto italiano de los sistemas de transporte multinodales inteligentes en un contexto en el que hay proyectos similares en curso (en Milán, Roma y en la Región Emilia-Romaña), que sin embargo cubren áreas más limitadas o bien no se encuentran aún en una fase avanzada. Esta variedad de proyectos es consecuencia de la regulación del transporte público local en Italia, que otorga las competencias legislativas y administrativas en la materia a las regiones, que a su vez han adoptado normas específicas en lo que concierne a las concesiones de licencias, a los subsidios a las empresas y a las tarifas del transporte.

Este modelo, que se basa en subvenciones públicas y en procedimientos competitivos de concursos y adjudicaciones, tiene dos consecuencias principales en términos de gestión de la información sobre la movilidad y la protección de datos. En primer lugar, reduce las potenciales barreras de las empresas ante soluciones dirigidas a la interoperabilidad y a la realización de redes integradas, ya que en un régimen de exclusivas falta una competencia directa entre las empresas de transporte. Esto facilita la creación de un sistema regional de información sobre la movilidad que constituye un elemento esencial para planificar y gestionar las redes de transporte integradas. En segundo lugar, en un contexto caracterizado por los altos costes y las bajas ganancias, las subvenciones públicas juegan un papel ciertamente relevante y son un factor importante para inducir a las empresas de transporte a participar en proyectos de movilidad inteligente.

A pesar de ello, hay que poner de relieve que en un ámbito que se caracteriza por utilizar procedimientos de concurso competitivos y por atribuir exclusivas, la información detallada acerca de la movilidad proporcionada por las sociedades de transportes puede llegar a asumir una cierta relevancia competitiva y, en consecuencia, razones de protección del secreto industrial y de competencia inducen a las empresas de transporte a considerar atentamente cualquier forma de divulgación de estos datos. En este sentido, la iniciativa de la Región del Piamonte y el papel desempeñado por esta mediante sus propios entes instrumentales para la movilidad proporcionan garantías adecuadas a las empresas acerca del uso correcto de la información y el empleo de esta únicamente para los fines de eficiencia de los transportes, sin interferencias sobre las estrategias de negocio de cada empresa.

Desde el punto de vista organizativo y estructural, la tarjeta BIP es un elemento clave de la estructura del proyecto de *smart mobility* que estamos examinando.[17] Se trata de una tarjeta personal con tecnología *contactless* dotada de un microchip en el que se memorizan los datos contractuales referidos al titular de la tarjeta (número de identificación del usuario, tipo de usuario, naturaleza y duración del abono); los usuarios pueden recargar la tarjeta con distintos tipos de abonos proporcionados por las distintas sociedades de transporte del Piamonte. Además, es posible cargar en la tarjeta una cantidad limitada de dinero (el llamado crédito de transporte) y usar la tarjeta en la modalidad *pay as you go* para pagar distintos desplazamientos. El empleo de la tarjeta requiere únicamente una validación al inicio del viaje

17. BIP es el acrónimo de *Biglietto Integrato Piemonte* (Billete integrado Piamonte).

(*touch-in*) en caso de que el pasajero sea titular de un abono o utilice la tarjeta en el área urbana (en la que existe una tarifa única basada en el tiempo del viaje), mientras que se requiere también una validación al final del viaje (*touch-out*) en los casos en que se use la tarjeta en su modalidad *pay as you go* fuera de las áreas urbanas.

En lo que se refiere al modelo de elaboración de los datos, el sistema de movilidad inteligente realizado en el Piamonte adopta una esquema arquitectónico ordenado en tres niveles. El primer nivel lo constituyen las sociedades de transporte, que recogen datos personales de los usuarios según el esquema tradicional basado en el consentimiento informado y proporcionan las tarjetas BIP a los usuarios. El segundo nivel viene representado por los centros provinciales de control, que son estructuras funcionales cuya misión es agregar los flujos de información de movilidad provenientes de un determinado grupo de empresas de transporte que operan en la misma provincia o en el área metropolitana de Turín. Estos centros de control envían todos sus datos de movilidad al Centro de Servicios Regional, que representa un tercer y último nivel de la estructura arquitectónica de la gestión de los datos, cuyas funciones se otorgan a una sociedad privada controlada por la Región del Piamonte, la Ciudad de Turín y la Provincia de Turín. El Centro de Servicios Regionales analiza los datos de movilidad útiles a las finalidades del proyecto (planificación de servicios, gestión de las subvenciones públicas a las sociedades de transportes, detección de fraudes, etc.) y comunica datos agregados o información detallada a las sociedades de transporte que operan en el sistema de movilidad inteligente del Piamonte, además de a las administraciones públicas locales y a la Región del Piamonte.

3.1. Un modelo basado en la centralidad del interesado

Sobre la base de esta breve descripción del sistema de movilidad del Piamonte se pueden realizar algunas consideraciones sobre este esquema arquitectónico IoT (*Internet of Things*), actualmente más bien simple, pero que en el futuro podrá expandirse mediante nuevas soluciones TIC añadidas (por ejemplo, *mobile payment*, *mobile ticketing*, *pricing* dinámico, planificación en tiempo real del tráfico, etc.).

Más específicamente, la mayor simplicidad del modelo reduce los riesgos que caracterizan a los sistemas más articulados,[18] en los que la complejidad y la naturaleza oculta del tratamiento de los datos hacen de difícil realización una efectiva autodeterminación del sujeto al que los datos se refieren. Los usuarios de los servicios de movilidad tienen así la capacidad de saber tanto cuándo se generan esos datos de movilidad como qué tipologías de información se recogen, de manera que reciben información completa sobre el tratamiento en el momento en que solicitan la tarjeta BIP a partir de la cual se solicita el consentimiento al tratamiento de datos.

El potencial uso secundario de los datos de movilidad con fines comerciales, en cambio, solo está previsto para finalidades de promoción del transporte público local y se realiza sobre la base de un consentimiento específico al efecto proporcionado por el usuario del servicio. Tal limitación de los usos secundarios se introdujo con la finalidad de limitar el riesgo de potenciales abusos de los datos de movilidad por parte de terceros y también a causa de la preocupación de que las campañas de marketing pudieran tener un efecto negativo en la propensión de los usuarios a utilizar el nuevo sistema de movilidad inteligente.[19]

Respecto al marco normativo que se deriva de la regulación comunitaria, hay que poner de relieve que el modelo adoptado para la elaboración de los datos en el caso que estamos examinando no se beneficia de las disposiciones del artículo 7.b) y 7.f) de la Directiva 95/46/EC. Según el artículo 7.b), el tratamiento de datos también puede ser realizado sin el consentimiento del interesado cuando ello sea necesario para la ejecución de un contrato en el que sea parte el sujeto al que los datos se refieren. El alcance de esta base legal, en cualquier caso, se encuentra limitado por el principio de «necesidad», que exige un vínculo directo y objetivo entre el tratamiento de los datos y las finalidades del contrato. En el caso de datos sobre movilidad, un tal vínculo directo y objetivo no parece darse en referencia a todas las distintas finalidades del tratamiento realizado en el contexto de los

18. V. Article 29 Data Protection Working Party (2014a), pág. 6.
19. A excepción de las iniciativas de marketing llevadas a cabo de manera autónoma por cada una de las empresas de transportes utilizando los datos de movilidad de que disponen.

sistemas de movilidad inteligente. Además, el potencial uso secundario de tales datos con fines comerciales o de promoción de servicios distintos ha inducido a la Región del Piamonte a adoptar un enfoque general y uniforme basado en el modelo del consentimiento informado.

Consideraciones análogas se pueden realizar acerca del distinto fundamento jurídico del legítimo interés del artículo 7.f) de la Directiva 95/46/CE. Como en el caso del artículo 7.b), tal disposición exige la «necesidad» del tratamiento de datos y no se puede considerar que meros intereses económicos puedan prevalecer sobre la tutela de los datos personales.[20] En presencia de una vasta y profunda recogida de datos sobre movilidad, el interés del gobierno regional en la planificación de los transportes y la gestión de los fondos públicos parece, efectivamente, superar los límites del legítimo interés.[21] Hay que tener presente que la trasposición italiana de la Directiva 95/46/CE y su interpretación se orientan hacia una aplicación limitada del recurso al legítimo interés como base jurídica del tratamiento de datos.

Por todas estas razones y desde un punto de vista que se centra en el usuario, el sistema de movilidad inteligente del Piamonte ha adoptado un modelo basado en el consentimiento informado, considerado en gran medida coherente con la idea de una comunidad inteligente participativa e inclusiva. En el intento de adoptar una estrategia global *privacy-oriented*, el uso de la tarjeta BIP únicamente es obligatorio para los abonos, que son utilizados por muchos viajeros, mientras que la Región Piamonte ha mantenido diversas soluciones que permiten viajar en modo anónimo. De hecho, es posible utilizar billetes de papel, o billetes de *chip-on-paper* para viajes de un solo trayecto, que se pueden adquirir en metálico en las taquillas automáticas *self-service* o en los puntos de venta autorizados. En estos casos, sin embargo, los usuarios no se pueden beneficiar del sistema integrado de transportes regional, ya que estos billetes solo dan acceso a los servicios proporcionados por la sociedad de transportes que los ha emitido o, en algunos casos, a los servicios multimodales proporcionados por varias sociedades en un área determinada.

Una solución distinta, más parecida a la de la tarjeta BIP, se encuentra actualmente en fase de experimentación en una de las provincias del Piamonte. Prevé que los usuarios puedan obtener una tarjeta BIP no personal y anónima en la que pueden cargar una cantidad de dinero y usarla en modalidad *pay as you go* para pagar sus viajes.

En términos de flujos de datos inherentes al usuario, las tarjetas BIP no personales no generan un flujo de información acerca de los datos contractuales, sino solo un flujo de datos de movilidad, que está conectado al número de tarjeta. Sin embargo, en este caso, el número de la tarjeta no se puede vincular con la identidad de quien lo utiliza, ya que el sistema no recoge informaciones sobre su identidad.

A pesar de los límites del anonimato de los que hemos hablado, el empleo de una tarjeta anónima y no personal, utilizable por distintos viajeros en momentos distintos, y la adopción de las soluciones *by design* antes examinadas (por ejemplo, la segmentación de los recorridos de los usuarios) reducen al mínimo los riesgos de reidentificación de los usuarios a partir del análisis de sus hábitos de movilidad.

3.2. La estructura arquitectónica del tratamiento de datos del modelo del Piamonte

En coherencia con los principios fundamentales en materia de protección de datos personales y siguiendo un enfoque de *privacy by design*, el proyecto realizado en el Piamonte se ha concentrado principalmente en tres aspectos: 1) la distribución de las tareas entre los diversos sujetos implicados en el proyecto; 2) las modalidades de conservación y anonimización de los datos; 3) las modalidades de acceso a los datos recogidos.

En lo que concierne a la distribución de las tareas, el sistema implica a tres tipos distintos de sujetos (empresas de transporte, centros provinciales de control y el Centro de Servicios Regional), que asumen los siguientes roles: las empresas de transporte y el Centro de Servicios Regional actúan como responsables del tratamiento, mientras que los centros provinciales lo hacen como encargados del tratamiento por cuenta de las empresas de transporte. Esta distribución de tareas resulta coherente con el enfoque

20. V. también Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)*, M. Costeja González (2014, pág. 73-81); Article 29 Data Protection Working Party (2014a, pág. 15 y sig.); Article 29 Data Protection Working Party (2014b).
21. V. Article 29 Data Protection Working Party (2014a, pág. 16).

funcional de la Directiva 95/46/CE, que define el rol que han asumido los autores del tratamiento a raíz de las relaciones que han asumido con los datos, más que en virtud de la naturaleza de sus relaciones intersubjetivas o de las relaciones contractuales. Es precisamente el concreto poder decisivo ejercitado en materia de tratamiento de datos lo que se erige en criterio de distinción entre los distintos roles: el responsable del tratamiento es quien «determine los fines y los medios del tratamiento de datos personales», mientras que el encargado del tratamiento es quien «trate datos personales por cuenta del responsable del tratamiento».[22]

A la luz de tal distinción, las empresas de transporte y el Centro de Servicios Regional tienen que ser considerados los responsables del tratamiento, ya que persiguen fines específicos y autónomos en materia de tratamiento de datos de movilidad,[23] mientras que a los centros provinciales de control, que actúan por cuenta de las empresas de transporte y realizan meras operaciones de gestión de los datos con el fin de enviar un flujo único y estandarizado de datos al Centro de Servicios Regional, se les debe considerar encargados del tratamiento. Según este modelo, las sociedades de transporte deberán designar formalmente cuál será el centro provincial de control del que se servirán como encargado del tratamiento en relación a los datos que a este transfieran, y además deberán autorizar a ese centro a unir los datos de movilidad pertenecientes a esa sociedad concreta con aquellos proporcionados por otras sociedades de la misma provincia, de modo que permita al centro provincial enviar un único *dataset* al Centro de Servicios Regional.

Sobre la base de esta estructura arquitectónica y en aplicación del principio de minimización de los datos tratados,[24] hay que valorar si toda la información, tanto contractual como de movilidad, recogida por las empresas de transporte debe ser necesariamente transmitida al Centro de Servicios Regional. Con estos fines, la información de movilidad se tiene que transmitir necesariamente porque su análisis a escala regional constituye precisamente la finalidad principal del proyecto y del tratamiento de datos correspondiente. Son posibles restricciones en cuanto a los datos contractuales relativos al usuario, donde la comunicación se debe desarrollar dentro de los límites de lo estrictamente necesario para el cumplimiento de las funciones centralizadas a nivel regional, en especial la lucha contra el fraude.

Por ello, se han creado dos bases de datos regionales distintas, una que contiene las información contractual y otra que contiene los datos de movilidad,[25] de manera que en la primera base de datos se encuentra la información relativa al perfil del usuario y a los abonos de los que es titular, pero no la información sobre su identidad (nombre y apellido), ya que el sistema genera un identificativo de usuario unívoco aplicando una función de *hash* al código fiscal[26] del titular de la tarjeta BIP. La sustitución del nombre y apellidos con este nuevo identificativo impide que los operadores del Centro de Servicios Regional puedan realizar búsquedas en la base de datos de los datos contractuales con el nombre de los usuarios.[27]

No es posible interrogar a ambas bases de datos conjuntamente de modo que permita combinar los datos presentes en ellas, a no ser que se requiera por motivo de lucha contra el fraude: en este último caso, los operadores regionales podrán excepcionalmente asociar los datos memorizados en ambas bases de datos según el número de tarjeta BIP[28]

22. V. art. 2.d) y 2.e), Directiva 95/46/CE.
23. Específicamente, las empresas de transporte recogen los datos del usuario y los datos de movilidad para prestar los servicios de transporte y utilizan esta información para organizar sus propias actividades, mientras que el Centro de Servicios Regional recibe parte de estas informaciones y las emplea para la concesión de subsidios al transporte público, para prestar servicios específicos a los usuarios (por ejemplo, servicios de prevención del fraude o gestión de los abonos) y para la planificación de la movilidad regional.
24. V. art. 6, Directiva 95/46/CE.
25. V. en este sentido el informe de la autoridad de protección de datos personales holandesa, *Onderzoek van het College bescherming persoonsgegevens* (CBP) (2010).
26. En Italia el código fiscal identifica al ciudadano en todas sus relaciones con las administraciones públicas, no solo de naturaleza fiscal; lo emite la Agenzia delle Entrate (Agencia Tributaria) italiana, v. <http: //www1.agenziaentrate.gov.it/english/italian_taxation/tax_code.htm.> [fecha de consulta: 15 de septiembre de 2015]. En el ámbito del proyecto de movilidad del Piamonte, el número de código fiscal lo solicita la empresa de transporte en el momento de emisión de la tarjeta BIP, quien posteriormente lo remite al Centro de Servicios Regional.
27. V. también Dinant, Keuleers (2004, pág. 22 y sig.).
28. V., en este sentido, *Onderzoek van het College bescherming persoonsgegevens* (CBP) (2010).

siguiendo, sin embargo, un procedimiento específico que genera un *file log* a nivel de sistema con la finalidad de dejar huella de la operación.

El recurso a la pseudoanonimización y el limitado recurso a la unión de los datos contenidos en las dos bases de datos permiten, por tanto, reducir los riesgos de una monitorización ilegítima de la movilidad de los ciudadanos y además, en aplicación del principio de necesidad y habida cuenta las finalidades antifraude mencionadas, la posibilidad de unir los datos memorizados en las dos bases de datos se limita a la información de movilidad durante los tres días posteriores a aquellos en que se recogieron.[29] Pasados estos tres días, el acceso a los datos de movilidad y a los datos contractuales solo es posible para el titular de la tarjeta BIP, que puede ver los datos de su movilidad correspondientes a los dos meses inmediatamente anteriores. Pasados dos meses, toda la información de movilidad se transforma y anonimiza completamente, y los datos inherentes a los distintos segmentos de un mismo viaje (como por ejemplo las líneas utilizadas) se memorizan separadamente y no se podrán referir a un mismo pasajero anónimo. Durante dos meses, los datos de movilidad sí que podrán ser utilizados por el Centro de Servicios Regional a través del identificador unívoco atribuido mediante la antes mencionada función de *hash*, pero sin permitir que tales datos se puedan unir a los datos presentes en la base de datos de la información contractual.

Conclusiones

El análisis de los aspectos relativos a la protección de los datos personales en el contexto de proyectos de movilidad inteligente ha puesto en evidencia potenciales riesgos en materia de vigilancia individual y social que derivan de la amplitud y capilaridad de los datos recogidos. Por ello, se hace necesaria la adopción de soluciones técnicas y organizativas adecuadas dirigidas a evitar que los sistemas de movilidad inteligente se conviertan en una especie de instrumento de vigilancia territorial generalizada.

Desde este punto de vista, el caso que ha sido objeto de estudio muestra cómo el recurso a la transformación de los datos de forma anónima o a la pseudoanonimización puede reducir las potenciales implicaciones negativas del uso de los datos, haciendo más difícil que se realicen posibles reidentificaciones, la trazabilidad de los pasajeros o un acceso ilegítimo a la información.

Por lo tanto, uniendo soluciones estructurales y tecnológicas es posible conseguir un equilibrio entre intereses individuales y colectivos en el contexto de las *smart cities*. Además, este objetivo resulta más fácil de conseguir cuando son las administraciones locales, en este caso regionales, las que asumen un papel de coordinación que incluye también la planificación y la monitorización del tratamiento de los datos, además del uso y el acceso a la información generada por las soluciones tecnológicas aplicadas al territorio.

Por último, el análisis empírico ha confirmado la importancia y la consecuente necesidad de adoptar procedimientos de *data protection impact assessment* con la finalidad de mitigar las posibles consecuencias negativas, tanto sociales como individuales, que puedan derivarse de la amplia recogida de información que es instrumental a la actividad de las *smart cities*. Tal valoración preliminar permite introducir en fase de realización del proyecto oportunas soluciones de *privacy by design* dirigidas a reducir al mínimo los riesgos de uso ilegítimo de los datos y de potencial empleo de estos para finalidades de control individual o social.

29. V. también *Commission nationale de l'informatique et des libertés*. (2003).; *Onderzoek van het College bescherming persoonsgegevens* (CBP) (2010).

Bibliografía

ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. (2015). «Privacy and human behavior in the age of information». *Science*. Vol. 347, 6221, pág. 509-514. <http://dx.doi.org/10.1126/science.aaa1465>

ALTMAN, I. (1977). «Privacy Regulation: Culturally Universal or Culturally Specific?». *J. Soc. Issues*. Vol. 33, 3, pág. 66-84. <http://dx.doi.org/10.1111/j.1540-4560.1977.tb01883.x>

Article 29 Data Protection Working Party. (2014a). *Opinion 8/2014 on the on Recent Developments on the Internet of Things* [documento *online*] disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> [fecha de consulta: 15 de septiembre de 2015].

Article 29 Data Protection Working Party. (2014b). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* [documento *online*] disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> [fecha de consulta: 15 de septiembre de 2015].

BOLLIER, D. (2010). *The Promise and Perils of Big Data* [documento online]. Aspen Institute, disponible en <http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/The_Promise_and_Peril_of_Big_Data.pdf> [fecha de consulta: 15 de septiembre de 2015].

BROWN, I. (2013). *Future Identities: Changing identities in the UK-the next 10 years. DR5: How will surveillance and privacy technologies impact on the psychological notions of identity?* [artículo *online*] disponible en <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275755/13-507-surveillance-and-privacy-technologies-impact-on-identity.pdf> [fecha de consulta: 15 de septiembre de 2015].

BYGRAVE, L. A. (2002). *Data Protection Law. Approaching Its Rationale, Logic and Limits*. The Hague, Londres, Nueva York: Kluwer Law International.

Commission nationale de l'informatique et des libertés. (2003). *Délibération n°03-038 du 16 Septembre 2003 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives par les societes de transports collectifs dans le cadre d' applications billettiques* [documento *online*] disponible en <http://www.cnil.fr/documentation/deliberations/deliberation/delib/10/>[fecha de consulta: 15 de septiembre de 2015].

DINANT, J-C. ; KEULEERS, E. (2004). «Data protection: multi-application smart cards: the use of global unique identifiers for cross-profiling purposes - Part II: towards a privacy enhancing smart card engineering». *Computer Law & Security Review*. Vol. 20, 1, pág. 22-28. <http://dx.doi.org/10.1016/s0267-3649(04)00005-6>

DWORK, C. (2011). «The Promise of Differential Privacy. A Tutorial on Algorithmic Techniques». *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2011)*, disponible en <http://research.microsoft.com/apps/pubs/default.aspx?id=155617> [fecha de consulta: 15 de septiembre de 2015].

European Cities and Regions Networking for Innovative Transport Solutions. (2013). *The Move Towards Open Data in the Local Transport Domain* [documento *online*] disponibile en <http://www.polisnetwork.eu/uploads/Modules/PublicDocuments/polis-position-paper_-open-transport-data.pdf> [fecha de consulta: 15 de septiembre de 2015].

GOLLE, P. (2006). «Revisiting the uniqueness of simple demographics in the US population». En: Juels, A. (ed), *Proc. 5th ACM workshop on Privacy in electronic society*. Nueva York, NY: ACM, pág. 77 s. <http://dx.doi.org/10.1145/1179601.1179615>

MANTELERO, A. (2014). «The future of consumer data protection in the EU Rethinking the "notice and consent" paradigm in the new era of predictive analytics». *Computer Law and Security Review*. Vol. 30, 6, pág. 643-660.

MANTELERO, A.; VACIAGO, G. (2014). «Social media and big data». En: Akhgar, B., Staniforth, A. y Bosco, F.M. (eds), *Cyber Crime & Cyber Terrorism. Investigators' Handbook*. Waltham, MA: Elsevier. <http://dx.doi.org/10.1016/b978-0-12-800743-3.00015-3>

MAYER-SCHÖNBERGER, V.; CUKIER, K. (2013). *Big Data. A Revolution That Will Transform How We Live, Work and Think*. Londres: John Murray 2013.

MIRANT, L. (2014). «London's bike-share program unwittingly revealed its cyclists' movements for the world to see». *Quartz*, 16 April [artículo *online*] disponible en <http://qz.com/199209/londons-bike-share-program-unwittingly-revealed-its-cyclists-movements-for-the-world-to-see/> [fecha de consulta: 15 de septiembre de 2015].

MIRONOV, I [*et al.*] (2009). «Computational Differential Privacy». En: T. Beth, N. Cot, I. Ingemarsson (eds). *Advances in Cryptology. CRYPTO `09'*. Berlin: Springer, pág. 126 s., disponible en <http://people.seas.harvard.edu/~salil/research/CompDiffPriv-crypto.pdf> [fecha de consulta: 15 de septiembre de 2015].

NARAYANAN, A., FELTEN, E. W. (2014). *No silver bullet: De-identification still doesn't work* [artículo online] disponible en <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf> [fecha de consulta: 15 septiembre 2015].

NARAYANAN, A., HUEY, J.; FELTEN, E. W. (2015). *A Precautionary Approach to Big Data Privacy* [artículo *online*] disponible en <http://randomwalker.info/publications/precautionary.pdf> [fecha de consulta: 15 de septiembre de 2015].

NISSENBAUM, H. (2010) *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

OHM, P. (2010). «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization». *UCLA L. Rev.* Vol. 57, pág. 1701-1777.

Onderzoek van het College bescherming persoonsgegevens (CBP). (2010). *Verwerking van persoonsgegevens met betrekking tot de studenten OV-chipkaart bij GVB Exploitatie B.V.* [documento *online*] disponible en <https://cbpweb.nl/sites/default/files/downloads/mijn_privacy/rap_2010_ovchip_db_gvb.pdf> [fecha de consulta: 15 de septiembre de 2015].

SADDLE, J. (2014). «I Know Where You Were Last Summer: London's public bike data is telling everyone where you've been"» [comment in blog] disponible en <http://vartree.blogspot.co.uk/2014/04/i-know-where-you-were-last-summer.html> [fecha de consulta: 15 de septiembre de 2015].

SCHWARTZ, P. M. (2010). *Data Protection Law and the Ethical Use of Analytics* [artículo *online*] disponible en <http://www.huntonfiles.com/files/webupload/CIPL_Ethical_Undperinnings_of_Analytics_Paper.pdf> [fecha de consulta: 15 de septiembre de 2015].

SCHWARTZ, P. M., SOLOVE, D. J. (2011) «The PII Problem: Privacy and a New Concept of Personally Identifiable Information». *N.Y.U. L. Rev.* Vol. 86, pág. 1841-1894.

SWEENEY, L. (2000). *Simple Demographics Often Identify People Uniquely* [artículo *online*] Carnegie Mellon University, disponible en <http://dataprivacylab.org/projects/identifiability/paper1.pdf> [fecha de consulta: 15 de septiembre de 2015].

United States General Accounting Office (2011). *Record Linkage and Privacy. Issues in creating New Federal Research and Statistical Information*. Pág. 68 y sig. [documento *online*] disponible en <http://www.gao.gov/assets/210/201699.pdf> [fecha de consulta: 15 de septiembre de 2015].

WESTIN, A. F. (1970). *Privacy and Freedom*. New York, NY: Atheneum.

WRIGHT, D. (2011). «A framework for the ethical impact assessment of information technology». *Ethics Inf. Technol.* Vol. 13, pág. 199-226. <http://dx.doi.org/10.1007/s10676-010-9242-6>

Cita recomendada

MANTELERO, Alessandro (2015). "Smart cities, movilidad inteligente y protección de los datos personales". *IDP. Revista de Internet, Derecho y Política*. No. 21, págs. 37-49. UOC [Accessed: dd/mm/yy]
<http://journals.uoc.edu/index.php/idp/article/view/n21-mantelero/n21-mantelero-pdf-es>
<http://dx.doi.org/10.7238/idp.v0i21.2919>

Sobre el autor

Alessandro Mantelero
alessandro.mantelero@polito.it

Profesor agregado de Derecho Privado
Nexa Center for Internet and Society (Politecnico di Torino)
<http://staff.polito.it/alessandro.mantelero/about.html>

Politecnico di Torino
Nexa Center for Internet and Society
Corso Duca degli Abruzzi, 24
10129 Torino, Italia