Privacidad y seguridad de los datos personales en la arquitectura semántica del Smart Campus. Entre la regulación y la normalización

María Estrella Gutiérrez David
Universidad Rey Juan Carlos

Índice. 1. Introducción. 2. Estado del arte y consideraciones metodológicas previas en torno al Smart Campus. 3. Hacia una conceptualización del «Smart Campus». 4. La privacidad desde el diseño y por defecto en la arquitectura semántica del Smart Campus. 5. Evaluaciones de Impacto en Proyectos de Smart Campus. Especial referencia a tecnologías de identificación RFID y smart metering. 6. Normalización, certificación y seguridad de los datos en los Smart Campus. 7. Bibliografía. 8. Guías y opiniones de las autoridades de protección de datos. 9. Relación de Normas Técnicas comentadas.

Palabras clave. Comunidad Inteligente. Smart Campus. Privacidad. Datos Personales. Seguridad. RGPD. Nueva LOPD. Normalización.

Abstract. El presente capítulo analiza el reto de la privacidad y la seguridad de los datos personales en los proyectos de Smart Campus a través de dos vectores: la normativa de protección de datos (a saber, el RGPD y la reciente Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales) y la normalización técnica. Para ello, se toma como referencia metodológica la arquitectura semántica de la Smart City definida en la Norma Técnica UNE 178201:2016. La estructura de esta Norma permite analizar la integración de los principios de responsabilidad proactiva y de privacidad desde el diseño por defecto, la identificación de nuevas taxonomías de datos personales, tratamientos específicos a través de las tecnologías inteligentes y finalidades de los mismos, con especial atención a las evaluaciones de impacto y a un enfoque de las medidas de seguridad desde la perspectiva de la ISO 27001 y la ENS, aplicable este último a Universidades Públicas españolas.

Summary. 1. Presentation. 2. State of art and methodology approach on Smart Campus. 3. Conceptualising a «Smart Campus». 4. Privacy by design and by default in semantic architecture of Smart Campus. 5. Privacy Impact Assessment in Smart Campus Projects. Especial reference to RFID identification and smart metering technologies. 6. Standardisation, certification and security of personal data in Smart Campus. 7. References. Guidelines and opinions of Data Protection Authorities. 8. References. 9. List of Standards commented.

Key words. Smart Community. Smart Campus. Privacy. Personal Data. Security. GDPR. New Spanish Data Protection Legislation. Standardisation.

Abstract. This chapter analyses the challenge of privacy and security on personal data in relation to Smart Campus projects. This study will be conducted under a twofold approach: the legislation on personal data protection (namely, GDPR and the recently enacted Organic Law 3/2018, on Personal Data Protection and Guarantee of Digital Rights). Our methodological framework will be the semantic architecture of the Smart City defined by the Spanish Standard UNE 178201:2016. This Standard enables an appropriate analysis of Smart Campus for the purposes of embedding the principles of accountability, privacy by design and by default and identifying new taxonomies of data, specific data processing by means of smart technologies and purposes thereof, with a special focus on PIAS and security approach based on the international Standard ISO 27001 and the National Security Scheme (ENS) applicable to Spanish Public Universities.

1. INTRODUCCIÓN

Los productos y servicios basados en las llamadas «tecnologías inteligentes», y en particular, el Cloud Computing, Internet de las Cosas (IoT), Big Data, Inteligencia Artificial (AI), Blockchain, Realidad Aumentada (AR) o Computación Cuántica (Quantum Computing) han encontrado aplicación en muy diferentes dominios, como la transición energética y la sostenibilidad ambiental[1], la ordenación urbanística y la movilidad urbana[2], las *smart grids*[3], las finanzas (fintech)[4], los *smart contracts*[5], la economía colaborativa[6], la Administración electrónica[7] o la gobernanza pública.

1. Ortiz García, M. «El nuevo modelo energético renovable-distribuido, participativo y digital. Un acercamiento al autoconsumo compartido». Galera Rodrigo, S. y Gómez Zamora, M. (eds). *Políticas Locales de Clima y Energía: Teoría y Práctica, INAP*, Madrid, 2018, pp. 143-161.

2. García Rubio, F. *Sostenibilidad ambiental y competencias. Un análisis jurídico*. Dykinson, Madrid, 2015, pp. 193-198.

3. Bautista Muttoni, I. *EV-smart grid integration*, LGI Consulting, 2015, pp. 1-26.

4. Pascua Mateo, F. *Criptomonedas*. García Mexía, P. (Coord.) *Criptoderecho. La regulación de Blockchain*. Wolters kluwers, 2018, pp. 363-409.

5. Tur Fáudez, C. *Smart Contracts. Análisis jurídico*. Editorial Reus, Madrid, 2018.

6. Lucas Durán, M. «Problemática jurídica de la economía colaborativa: especial referencia a la fiscalidad de las plataformas», *Anuario Facultad de Derecho*, Universidad de Alcalá, 2017, pp. 131-172.

7. Franco Escobar, S. «Luces y sombras de la Administración electrónica para las smart cities». GARCÍA RUBIO, F. Las nuevas perspectivas de la ordenación urbanística y del paisaje: smart cities y rehabilitación. Perspectiva hispano-italiana, Fundación Democracia y Gobierno Local, 2017, pp. 259-278.

En particular, la aplicación integrada de estas tecnologías para la prestación servicios públicos ha encontrado un paradigma en las Smart Cities[8] y, más recientemente, también en los Smart Campus. De hecho, existe común acuerdo en considerar que el concepto de «Smart Campus» surge del concepto de Smart City, al aplicar los principios de las Ciudades Inteligentes a la organización y gestión del Campus universitario[9].

De la misma manera que abordar la conceptualización y aproximación jurídica a las Ciudades Inteligentes exige un «esfuerzo titánico» de integración entre normativas sectoriales y normalización técnica[10], tal esfuerzo es aún mayor si abordamos el análisis de otros sub-ecosistemas inteligentes, como los Smart Campus y, en concreto, uno de sus indicadores transversales como es la protección de la privacidad y de los datos personales.

A mayor abundamiento, al analizar la confluencia entre Derecho y Tecnología en el fenómeno de la Smart City, se observa que buena parte del impulso de las tecnologías inteligentes y la aplicación de la *smartness* al desarrollo de proyectos (Smart grids, Smart Metering, Smart Buildings, Smart Cities, Smart Communities, Smart Campus) ha venido de la mano del *soft-law* público-privado[11], a través de la «normalización»[12]. Ello es así porque dado su carácter voluntario, consensuado y documentado, las normas técnicas resultan más flexibles a la hora de abordar los continuos y rápidos avances tecnológicos que la norma jurídica[13].

Por todo lo anterior, ya desde el propio título de este capítulo, «Privacidad y seguridad de los datos personales en la arquitectura semántica del Smart Campus. Entre la regulación y la normalización» se pretenden dejar claros cuáles son los dos vectores normativos que van a conducir el análisis concreto de la privacidad en el contexto de proyectos de Smart Campus: por un lado, la normativa reguladora de protección de datos personales, en particular, el Reglamento Ge-

---

8. Véanse, por ejemplo, TALARI, S. et al. «A Review of Smart Cities Based on the Internet of Things Concept». Energies, 10 (2017); GOMEZ, M.L. «Smart Cities. Una aproximación desde la gobernanza pública y la innovación social». GALERA RODRIGO, S. y GÓMEZ ZAMORA, M. (eds). *Políticas Locales de Clima y Energía: Teoría y Práctica*, INAP, Madrid, 2018, pp. 449-46.

9. Cfr. ABUARQOUB, A.; ABUSAIMEH, H. «A Survey on Internet of Things Enabled Smart Campus Applications». *3rd. International Conference on Future Networks and Distributed Systems (ICFNDS)*, Cambridge, July 19-20 2017, p. 2.; WIDYA SARI, M.; & WAHYU CIPTADI, P.; HARDYANTO, R. «Study of Smart Campus Development Using Internet of Things Technology», *IAES International Conference on Electrical Engineering, Computer Science and Informatics*, IOP Conf. Series: Materials Science and Engineering 190 (2017), p. 2.

10. GOMEZ, M.L. «Smart Cities […]», Op. cit., pp.451-453.

11. SARMIENTO, D. *El soft law administrativo. Un estudio de los efectos jurídicos de las normas no vinculantes de la Administración*, Navarra, Thomson-Civitas, 2008, pp. 137-139.

12. El art. 8.5 de la Ley 21/1992, de 16 de julio, de Industria, define la «normalización» como «la actividad por la que se unifican criterios respecto a determinadas materias y se posibilita la utilización de un lenguaje común en un campo de actividad concreto.» Y, a su vez, el art. 8.3 del precitado cuerpo legal entiende por «norma», «la especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueba un Organismo reconocido, a nivel nacional o internacional, por su actividad normativa.»

13. AMUTIO GÓMEZ, M.A. *Normalización en seguridad de las Tecnologías de la Información, Ministerio de Administraciones Públicas*, 2ª Edición, 2007, pp. 4-5.

neral de Protección de Datos (en adelante, «RGPD»)[14] y la reciente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, «LOPD-GDD»); y por otro, la normalización técnica en dos áreas concretas, las «Smart Cities» llevada a cabo por el Comité Técnico CTN178, y la «Ciberseguridad y protección de datos personales» desarrollada por el Comité CTN 320 de AENOR.

Al considerar la Smart City como paradigma del Campus Inteligente, una primera constatación es que son extrapolables al Smart Campus las mismas preocupaciones y retos jurídicos que, en la privacidad y en el derecho a la autodeterminación informativa, plantea el desarrollo de aplicaciones y servicios basados en las tecnologías inteligentes[15].

En este sentido, en el caso de la Agencia Catalana de Protección de Datos («APDCAT»), o ya en el ámbito comparado, del extinto Grupo de Trabajo del Artículo 29 (GT29) o el *Information Commissioner Officer* inglés (en adelante «ICO»), debe destacarse la elaboración de guías específicas o documentos de trabajo donde se ha analizado el impacto en la privacidad de ciertas tecnologías características de las Smart Cities[16]. En el caso de la Agencia Española de Protección de Datos (en adelante, «AEPD»), el tratamiento de la privacidad en la Smart City no ha ido más allá de considerarlo como un aspecto general adicional a considerar en la aplicación del RGPD en el ámbito de la Administración Local[17].

---

14. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo 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 por el que se deroga la Directiva 95/46/CE.

15. Entre otros, KITCHIN, R. *Getting smarter about smart cities: Improving data privacy and data security*. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland, January 2016, pp. 25-38, que elabora una taxonomía concreta de amenazas para la privacidad en sus diferentes dimensiones (personal, corporal, espacial, comunicaciones personales y transacciones) a lo largo del ciclo de vida de los datos personales. D'ACQUISITO, G. et al. *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*. ENISA, December 2015, pp. 54-68. Véase también, GONZÁLEZ FÚSTER, G.; SCHERRER, A. *Big Data and smart devices and their impact on privacy*, European Parliament, Directorate General for Internal Policies, PE 536.455, 2015, p. 14.

16. APDCAT. *La protecció de dades de caràcter personal en les ciutats intel·ligents* («Smart Cities»), Barcelona, febrero de 2013, que hace un recorrido por aplicaciones y servicios específicos de una Smart City con impacto en la privacidad (redes y contadores inteligentes, IoT, identificadores NFC, RFID, Geolocalización, Wireless Sensor Netwok, Open Data) o tratamientos de datos específicos de datos personales como el perfilado (*profiling*). Desde el ámbito comunitario, véanse, entre otros GT29. *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, WP251rev.01, revisadas y actualizadas a 6 de febrero de 2018; *Dictamen 03/2017 sobre el tratamiento de los datos personales en el contexto de los sistemas de transporte inteligentes (STI) cooperativos*, WP252, 4 de octubre de 2017; *Opinion 8/2014 on the Recent Developments on the Internet of Things*. WP 223, 16 de septiembre de 2014; *Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template')*, WP209, febrero de 2013; *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, WP180, 11 de febrero de 2011; *Opinion 12/2011 on smart metering*, WP 183, 4 de abril de 2011. En el caso del Derecho comparado, por su carácter exhaustivo, debe destacarse ICO. *Big data, artificial intelligence, machine learning and data protection*, Version: 2.2, 4 de septiembre de 2017.

17. AEPD. *Guía Sectorial de Protección de Datos y Administración Local*, febrero 2018, pp. 7, 24-25. Así, por ejemplo, la AEPD señala que la implementación de las Smart Cities también puede conlle-

Ahora bien, con la aplicación efectiva del RGPD y de la LOPD-GDD urge la conceptualización y sistematización rigurosa de las implicaciones que, para la privacidad y seguridad, tiene la implementación progresiva de tecnologías inteligentes en un Campus universitario o, en su caso, el desarrollo completo de un proyecto de Smart Campus, en la medida en que la normativa actual supone un marco jurídico con nuevos principios que deben regir el tratamiento de datos personales de las organizaciones (entre otros, el de responsabilidad proactiva y los de *privacy by design* y *by default*), nuevas categorías de derechos para los afectados (usuarios del Smart Campus) y obligaciones para responsables (la institución) y sus encargados de tratamiento (e.g. en casos de externalización de determinados servicios TIC).

2. ESTADO DEL ARTE Y CONSIDERACIONES METODOLÓGICAS PREVIAS EN TORNO AL SMART CAMPUS

A la hora de abordar el objeto de este Capítulo se constata que no existe aún en la literatura científica trabajos específicos que conceptualicen y/o sistematicen los atributos e indicadores característicos del Smart Campus, más allá de ciertos de estudios de campo centrados fundamentalmente en la aplicación de determinadas tecnologías inteligentes.

Así, por ejemplo, debe destacarse el uso de sensores Wi-Fi, infrarrojos o de geo-posicionamiento *indoor* mediante ibeacons para medir el uso y la ocupación real de edificios o espacios concretos del Campus[18]; la implementación de identificadores RFID o NFC para la gestión del préstamo bibliotecario[19] o la eficiencia energética de los edificios que integran el Campus a través de *smart grids* y análisis big data[20].

---

var un tratamiento de distintas categorías de datos personales, pero sin identificar cuáles. Asimismo, deja claro que la puesta en marcha de un proyecto «Smart City», además de tener en cuenta los principios de protección de datos previstos en el RGPD, en particular, la limitación de la finalidad, el principio de minimización o el principio de privacidad por diseño, exigirá una Evaluación de Impacto e incluso una consulta previa a la AEPD. En sentido similar, véase FEMP. *Guía para la Adaptación al Reglamento General de Protección de Datos de las Administraciones Locales*. Comisión de Sociedad de la Información y Tecnologías. Grupo de Trabajo para la Implantación del Nuevo Reglamento General de Protección de Datos (RGPD) en las Administraciones Locales, 2018, p. 28, donde simplemente se alude a que la implementación de proyectos de Smart Cities exigirá la correspondiente evaluación de impacto en protección de datos.

18. Valks, B., Arkesteijn, M.; den Heijer, A. *Smart campus tools 2.0: An international comparison*. Delft University of Technology, 2018, p. 24 y ss. Los autores realizan un interesante estudio comparado de la aplicación de tecnologías inteligentes basadas en el uso de sensores, entre otras, en las Universidades de Leuven, Cambridge, Sheffield Hallam University, Technical University of Denmark, Aarhus University, Oxford Said Business School, Maastricht University, Tilburg University, University of Amsterdam, University of Utrecht.

19. Brian, A.L., Arockiam, L. And Malarchelvi, S.K. «An IoT Based Secured Smart Library System with NFC Based». *International Journal of Emerging Technology in Computer Science & Electronics* (IJETCSE), Volume 11, Issue 5 (2014), pp. 18-21.

20. De Angelis, E. et al. «The Brescia Smart Campus demonstrator. Renovation toward a zero-energy classroom building». *Procedia Engineering* 118 (2015), pp. 735-743.

Por tanto, desde el punto de vista metodológico, en primer lugar, el estudio del Smart Campus y de las implicaciones jurídicas en la privacidad exige delimitar conceptualmente su significado, sus atributos, sus requisitos e indicadores.

Para los propósitos de este Capítulo se ha abordado esta tarea a partir de las Normas Técnicas relativas a Smart Cities, y en particular, la Norma UNE 178201:2016. Conocer la arquitectura sobre la que se asienta un Smart Campus, sus políticas de privacidad y seguridad, su organización humana y logística, los roles, responsabilidades y autoridades en la organización, sus activos de información, sus procesos, y particularmente, el flujo y el ciclo de vida de los datos personales tratados, exige tal esfuerzo previo de conceptualización.

En segundo lugar, el análisis de las implicaciones jurídicas en la privacidad de los proyectos de Smart Campus debe abordarse no sólo teniendo en consideración la normativa de protección de datos referenciada, sino también el abundante *soft-law* generado a partir de las Opiniones, Guías y Directrices desarrolladas por las Autoridades de Protección de Datos en el ámbito interno y comparado y, en particular, las relativas a soluciones y aplicaciones específicas relacionadas con proyectos de Smart Cities (e.g. *Smart grids*, *Smart metering*, redes RFID, sistemas de transporte inteligentes cooperativos, etc.) Se trata de instrumentos que no resultan jurídicamente vinculantes, pero cuyo seguimiento se recomienda como mejores prácticas en el sector[21].

Siguiendo, por último, nuestra aproximación dual entre norma jurídica y norma técnica, el reto de la privacidad y la seguridad de los datos personales también exige una referencia especial a la normalización técnica en el desarrollo de proyectos específicos de comunidades inteligentes y sus especificaciones concretas en materia de protección de datos, en particular, de la UNE-EN ISO/IEC 27001, en la que se basa el Esquema Nacional de Seguridad (en adelante, «ENS»), aplicable a Universidades Públicas[22].

3. HACIA UNA CONCEPTUALIZACIÓN DEL «SMART CAMPUS»

Los Smart Campus se han desarrollado a partir de la digitalización de los campus universitarios tradicionales y son una industria emergente, con una implementación de distintas soluciones tecnológicas que ya han sido adoptadas por distintas universidades en el mundo[23].

No existe, sin embargo, en la doctrina una definición científica del concepto de Smart Campus, ni un estudio sistematizado de sus atributos, requisitos, indicadores o semántica y arquitectura de su ecosistema. Por ello, a la hora de delimitar la noción de Smart Campus, metodológicamente, el punto de partida no puede ser otro que la noción de Smart City.

---

21. Cfr. Gómara Hernández, J.L. *Protección de Datos: el RGPD en las Entidades Locales*. Claves Prácticas. Francis Lefebvre, 2018, pp. 22-24.

22. CCN-CERT, *Esquema Nacional de Seguridad - Preguntas Frecuentes*, p. 6.

23. Abuarqoub, A.; Abusaimeh, H. «A Survey on Internet of Things […]», Op. cit., p. 2.

Desde el ámbito institucional y de la doctrina iuspublicista, se ha tratado de conceptualizar la noción de «Smart City»[24]. También desde el ámbito del *soft-law*, distintas Normas Técnicas han definido el concepto de Smart City[25], y lo ha ampliado, además, al de «Destino Turístico Inteligente»[26].

Por su parte, Marina Caporale pone énfasis en la opción terminológica adoptada por el legislador italiano[27] que utiliza la expresión «Comunità Intelligenti», subrayando que con esta opción se ha buscado una «dimensión institucional de la *smartness*», en lugar de que la cualidad de la *smartness* se vincule exclusivamente a un único término, como puede ser el de «ciudad»[28].

A su vez, la Agencia para la Italia Digital define indistintamente el término «Smart City/Community (SC)» como «lugar y/o espacio territorial en el que el uso planificado y prudente de los recursos humanos y naturales, debidamente administrados con la asistencia de las tecnologías TIC ya disponibles, permite la creación de un ecosistema capaz de mejorar el uso de los recursos y de proporcionar servicios más integrados e inteligentes [...] Los ejes sobre los cuales se desarrollan las acciones de un SC son muchos: movilidad, medio ambiente y energía, calidad de construcción, economía y capacidad para atraer talento e

---

24. Desde el ámbito institución europeo, véase EUROPEAN PARLAMENT. *Mapping Smart Cities in the EU*, Directorate General for Internal Policies, Bruselas, 2014, pp. 21-25. El documento propone como definición autónoma de Smart City: «[...] ciudad que busca conducir los asuntos públicos a través de soluciones basadas en las TIC a partir de una colaboración multisectorial de base municipal». Entre nuestra doctrina administrativa, el concepto de Smart City ha sido abordado, entre otros, por PIÑAR MAÑAS, J.L. *Derecho, técnica e innovación en las llamadas Ciudades Inteligentes. Privacidad y Gobierno Abierto*. PIÑAR MAÑAS, J.L. (Dir.*) Smart Cities. Derecho y técnica para una ciudad más habitable*. Madrid: Reus, 2017, p. 18, quien recoge la definición incluida en el Plan Nacional de Ciudades Inteligentes de marzo de 2015; BARRIO, M., «La smart city: versión 2.0 del municipio», *Documentación Administrativa* 3, Nueva Época, Enero-Diciembre 2016, quien la define como «[a]quel municipio en el cual las inversiones contribuyen al desarrollo económico sostenible y a una alta calidad de vida con una adecuada gestión de los recursos naturales mediante un gobierno abierto.»

25. AENOR. *UNE 178201:2016. Ciudades inteligentes. Definición, atributos y requisitos*. Abril de 2016, p. 7. Esta Norma Técnica define la «Ciudad Inteligente» como «una ciudad justa y equitativa centrada en el ciudadano que mejora continuamente su sostenibilidad y resiliencia aprovechando el conocimiento y los recursos disponibles, especialmente las Tecnologías de la Información y la Comunicación (TIC), para mejorar la calidad de vida, la eficiencia de los servicios urbanos, la innovación y la competitividad sin comprometer las necesidades futuras en aspectos económicos, de gobernanza, sociales y medioambientales.»

26. AENOR. *UNE 178501: 2016. Sistema de Gestión de los Destinos Turísticos Inteligentes. Requisitos*. Abril 2016, pp. 14 y 16. Esta norma técnica ha sido sustituida recientemente por la nueva norma UNE 178501:2018, sobre «Sistema de gestión de los destinos turísticos inteligentes. Requisitos»; que, a su vez, se completa con la UNE 178502:2018, relativa a «Indicadores y herramientas de los destinos turísticos inteligentes».

27. Cfr. art. 20 de la Legge 17 dicembre 2012, n. 221 conversione, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese (Gazzetta Ufficiale n. 294 del 18 dicembre 2012 -Supplemento Ordinario n. 208).

28. CAPORALE, M. «El régimen de las Smart City en Italia». GARCÍA RUBIO, F. *Las nuevas perspectivas de la ordenación urbanística y del paisaje: smart cities y rehabilitación. Perspectiva hispano-italiana*, Fundación Democracia y Gobierno Local, 2017, pp. 207-208, quien, desde la perspectiva del Derecho italiano, acoge la definición elaborada por la Agencia para la Italia Digital para la expresión «Smart City/Smart Community».

inversión, seguridad de los ciudadanos e infraestructuras urbanas, participación e implicación ciudadana. Son condiciones indispensables la conectividad generalizada y la digitalización de las comunicaciones y servicios [cursiva nuestra].» De hecho, la propia Agencia italiana aclara que sus recomendaciones tienen el objetivo de «discutir y proponer un enfoque metodológico y de gobernanza para la plena implementación del paradigma del SC.»[29].

En este sentido, Pistore ha aplicado el concepto de «Smart Community» al de «Campus Inteligente», entendiendo por tal aquella comunidad (educativa) que hace un esfuerzo consciente en el uso de las tecnologías de la información para transformar la vida y el trabajo en su región de una forma cualitativa, más que cuantitativa[30].

No parece, por tanto, que exista obstáculo para afirmar que el Campus Inteligente es una de las posibles dimensiones institucionales de la *smartness* con sus atributos, requisitos y arquitectura propios, donde las tecnologías inteligentes permiten la creación de un ecosistema capaz de mejorar el uso de los recursos del espacio físico, social y relacional que es el Campus y de proporcionar servicios más integrados e inteligentes a la Comunidad universitaria[31].

De hecho, buena parte de los estudios relativos a soluciones tecnológicas específicas para el desarrollo de Smart Campus parten de la adaptación de algunos de los atributos asociados las Smart Cities. Así, por ejemplo, en el Proyecto de Smart Campus para la Universidad PGRI Yogyakarta en Indonesia el objetivo ha sido la implementación de un sistema de «Educación Inteligente»[32] que se define como: «e-Aprendizaje, Aprendizaje Personalizado, Clase Virtual; b) Parking Inteligente, que facilita información en tiempo real sobre la disponibilidad de plazas; c) Aula Inteligente, mediante un sistema que proporciona información sobre la ocupación del aula en tiempo real[33].

En coherencia con lo anterior, se ha caracterizado a este tipo de Comunidades Inteligentes por las siguientes notas: (i) Constituye una evolución avanzada del Campus digital; (ii) Implica una institución que implementa tecnologías avanzadas para controlar y monitorizar las instalaciones del Campus, proporcionando servicios de alta calidad a toda la comunidad universitaria; (iii) El uso de las tecnologías inteligentes conduce a una mejora continua en el proceso de toma de decisiones, en la capacidad de respuesta del Campus a los retos inter-

29. Agenzia per l'Italia digitale. *Architettura per le comunità intelligenti: visione concettuale e raccomandazioni alla Pubblica Amministrazione*, Versione 2.0 del 03/10/2012, pp. 6 y 10.

30. Pistore, M. *Smart Campus Creating services WITH and FOR people*. Open Science Conference, 14 de Agosto de 2013.

31. Cfr. Kumar kar, A.; Gupta, M.P. How to make a Smart Campus - Smart Campus Programme in IIT Delhi, Indian Institute of Technology Delhi, 2015, p. 3. Los autores afirman que «hasta cierto punto, los [Smart] campus pueden ser considerados como un micro modelo de «pequeñas ciudades», con cuestiones y preocupaciones similares propias de un ecosistema más pequeño».

32. Véase Figura 1 *infra*. Conforme a la Norma Técnica UNE 178201:2016, el ámbito clave de la Smart City correspondiente a la «Smart People», incluye entre sus atributos, la «Educación Inteligente», la «Inclusión Social», y la «Participación en la Comunidad».

33. Widya sari, M. «Study of Smart Campus Development… […]», pp. 2-3.

nos y externos, en el aprovechamiento eficiente de sus recursos, y en la experiencia de todos los actores que integran la comunidad universitaria desde el punto de vista del bienestar ambiental y social[34].

4. LA PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO EN LA ARQUITECTURA SEMÁNTICA DEL SMART CAMPUS

A la vista de lo anterior, es posible afirmar que la integración del concepto institucional de «Comunidad Inteligente», por un lado, así como de los atributos[35], requisitos[36] y arquitectura semántica de la «Ciudad Inteligente» definidos por la Norma UNE 178201:2016, por otro, permite elaborar una construcción metodológica y sistemática del concepto de Campus Inteligente, entendido como un sub-ecosistema de las Comunidades Inteligentes. Una vez definido el esquema metodológico de aproximación al Campus Inteligente, nuestro objeto de estudio pasa por analizar las implicaciones que en la privacidad y en la seguridad tienen esta clase de proyectos.

Aunque las Comunidades Inteligentes, como la Smart City o como los Smart Campus, no son un nuevo concepto tecnológico, sin embargo, la combinación de infraestructuras, aplicaciones y servicios ya existentes, con las tecnologías inteligentes, plantea nuevos retos en el área de la privacidad y la seguridad de los datos personales. La doctrina ha identificado dos clases de retos a tener en consideración: el volumen y categorías de datos personales objeto de tratamiento y la exposición a nuevas vulnerabilidades resultantes de la interoperabilidad de sistemas.

En cuanto al primer reto, en general, la integración de tecnologías inteligentes en el desarrollo de proyectos de Smart Campus, implica el tratamiento de una gran cantidad y categorías distintas de datos personales (identificativos, biométricos, de salud, de geo-posicionamiento, de comportamiento, entre otros)[37].

Pero es que, además, el big data, en combinación con el IoT, con la AI o el *machine learning*, permiten la aparición de nuevos tipos de datos personales. Así, junto a los datos proporcionados de forma consciente por el propio interesado normalmente, en virtud del consentimiento (descarga de una aplicación móvil implementada por el propio Campus) o en virtud de un contrato (contra-

34. Abuarqoub, A.; Abusaimeh, H. «A Survey on Internet of Things […], Op. cit., p. 2.

35. AEN/CTN 178. *UNE 178201:2016. Ciudades inteligentes. Definición, atributos y requisitos*. Abril de 2016, p. 7. La Norma identifica seis ámbitos clave: economía (*Smart Economy*), gobernanza (*Smart Governance*), entorno (*Smart Environment*), movilidad (*Smart Mobility*), personas (*Smart People*) y estilo de vida (*Smart Living*).

36. Según la UNE 178201:2016, los requisitos son la base para construir los indicadores de la Smart City. Dichos requisitos son las TIC, la sostenibilidad ambiental, la productividad, la calidad de vida, la igualdad y la inclusión social y la infraestructura física.

37. Es más, algunos de esos datos personales (los biométricos, o los de salud) tienen consideración de categorías especiales de datos en el art. 9 RGPD y LOPD-GDD respectivamente.

tos de trabajo entre la Universidad y el personal laboral), debe llamarse la atención sobre la existencia de nuevas taxonomías resultantes de la aplicación de soluciones tecnológicas inteligentes. Es el caso de los «datos observados» (aquéllos registrados de forma automática, por ejemplo, la implementación de sensores para controles de asistencia a clase), los «datos derivados» (los generados a partir de la combinación de los anteriores, por ejemplo, el *scoring* del rendimiento académico de un alumno a partir del número de visitas al campus virtual a través de la plataforma Moodle[38]) o los «datos inferidos» (resultantes de las correlaciones de conjuntos de datos que, a partir de cálculo probabilístico permiten categorizar o generar perfiles)[39].

En cuanto al segundo reto, la interoperabilidad entre los distintos sistemas y procesos que conforman la arquitectura del Smart Campus (los existentes y los nuevos) implica un incremento de las vulnerabilidades del conjunto del sistema al abrirse nuevos vectores de ataques que antes no habían sido objeto de consideración, por lo que el riesgo para el conjunto del sistema será sensiblemente superior que el de los subsistemas interconectados individualmente considerados[40], como por ejemplo, un ataque de denegación de servicio (DDoS) o la ingeniería social.

Por lo anterior, la adecuada protección de los datos personales como atributo específico de las Comunidades Inteligentes, ya sea de una Smart City, ya sea de un Smart Campus, exige que cualquier proyecto de implementación de soluciones tecnológicas inteligentes debe regirse desde su misma concepción, y antes de su implementación, por los principios del art. 5 RGPD.

En concreto, deberán tenerse en cuenta los principios de privacidad por diseño (*by design*) y por defecto (*by default*)[41], pilares, a su vez, del principio de responsabilidad proactiva que impone el RGPD[42], en el desarrollo de sistemas o soluciones tecnológicas, especialmente cuando el proyecto de Smart Campus prevea la implementación de tecnologías que impliquen tratamientos de datos personales que, «por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas»[43], como pueden ser el Big Data o el IoT.

---

38. Vid. Kadoić, N.; Oreški, D. «Analysis of Student Behavior and Success Based on Logs in Moodle», *41st International Convention on Information and Communication Technology, electronics and microelectronics*, MIPRO 2018, Opatija [Croatia], 2018.

39. ICO. *Big data, artificial intelligence, machine learning and data protection*, Versión 2.2, 4 de septiembre de 2014, p. 12. Llaneza, P. «Dataísmo, transparencia y protección de datos». Rodríguez Marín, S. y Muñoz García, A. *Aspectos legales de la economía colaborativa y bajo demanda en las plataformas digitales*, Walters Kluwers, Madrid, 2018. pp. 203-304.

40. Bartoli, A.; Hernández-Serrano, M. S. et al. «On the Ineffectiveness of Today's Privacy Regulations for Secure Smart City Networks», 3rd. IEEE International Conference on Smart Grid Communications (SmartGridComm 2012), 5-8 November 2012, pp. 3-4.

41. Duaso Calés, R. «Los principios de protección de datos desde el diseño y protección de datos por defecto». Piñar Mañas, J.L., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid, Reus, 2016, pp. 301-304. AEPD. *Guía Sectorial de Protección de Datos y Administración Local*, febrero 2018, pp. 25-26.

42. Vid. Considerando 78 y art. 25 RGPD.

43. Cfr. art. 35.1 RGPD.

El concepto de *privacy by design* tiene su aplicación en el mismo momento de creación o implementación de una nueva tecnología, con el objetivo de que la privacidad esté integrada en el conjunto del sistema (vgr. en este caso, en la arquitectura del Smart Campus) o en la solución tecnológica (vgr. sensores RFID o plataforma IoT externa del municipio asociado que intercambia información con una Plataforma Inteligente del Campus[44]). En otras palabras, la protección de datos ha de estar presente en las primeras fases de concepción del proyecto un antes de iniciar las sucesivas etapas de desarrollo, con el objeto de mitigar al máximo la posibilidad de materialización de las amenazas (riesgo), o en su caso, eliminarlas.

En el caso del *privacy by default*, este principio garantiza que el sistema, por su propia arquitectura basada en la privacidad, sólo va a tratar aquellos datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento, garantizando, a su vez, las cuatro dimensiones de la seguridad de los datos personales (disponibilidad, autenticidad, integridad y confidencialidad) previstas en el RGPD, a las que el ENS añade la trazabilidad[45].

Para llevar a cabo una aproximación holística a las implicaciones jurídicas en la privacidad y en la seguridad de los proyectos de Smart Campus, es preciso determinar previamente y de forma sistematizada cuáles son los atributos, requisitos y arquitectura semántica de esta clase de comunidades inteligentes a partir de la estructura de la Norma UNE 178201:2016.

En primer lugar, es necesario identificar los atributos específicos del Smart Campus. Para ello, en la **figura 1** se han adaptado al Smart Campus los ámbitos clave de la Smart City identificados por la UNE 178201:2016.

Figura 1. ***Ámbitos clave (atributos) de un Smart Campus***

<table>
<tr><th>Smart Economy</th><th>Smart Governance</th><th>Smart Environment</th><th>Smart Mobility</th><th>Smart People</th><th>Smart Living</th></tr>
<tr><td>Eficiencia</td><td>Buen Gobierno Universitario</td><td rowspan="2">Infraestructuras universitarias eficientes</td><td>Infraestructuras inteligentes</td><td>Educación Inteligente</td><td rowspan="2">Bienestar ambiental</td></tr>
<tr><td>Innovación</td><td>Transparencia: reutilización y acceso a información pública universitaria</td><td>Transporte (inter-campus) inteligente</td><td>Inclusión social</td></tr>
</table>

44. Cfr. Anexo C de la Norma Técnica *CTN 178. UNE 178104:2017. Sistemas Integrales de Gestión de la Ciudad Inteligente. Requisitos de interoperabilidad para una Plataforma de Ciudad Inteligente.* Diciembre 2017.

45. Vid. CCN-CERT. *Guía de seguridad (CCN-STIC-803). Esquema Nacional de Seguridad. Valoración de los sistemas*. Enero 2011.

Sostenibilidad Económica del Campus	Gobierno Electrónico	Sostenibilidad ambiental del Campus	Infraestructuras y conectividad TIC	Participación en la comunidad universitaria	Bienestar social
Transferencia de nuevos modelos de negocio	Protección de datos personales				

Fuente: elaboración propia a partir de UNE 178201:2016.

Al observar los ámbitos clave «adaptados» de las Smart City para los Campus Inteligentes, vemos cómo el ámbito clave definido por la *Smart Governance* o Gobernanza Inteligente comprende «mecanismos para garantizar un entorno justo y equitativo, transparente, una gestión óptima de los servicios (Gobierno electrónico) y la protección de la información entendida como un derecho fundamental de la ciudadanía». Por tanto, a semejanza de la Smart City, entre los atributos del Campus Inteligente, debe incluirse la protección de datos personales[46], obviamente, desde los inicios del proyecto, desde el diseño.

Siguiendo de nuevo a la UNE 178201:2016 es preciso constatar que, mientras que los atributos definen los ámbitos clave de la Comunidad Inteligente, los requisitos son la base para construir indicadores que permiten medir el grado de evolución de la Comunidad Inteligente en los ámbitos clave previamente definidos.

Una vez más, los seis atributos de la Smart City son plenamente aplicables al Smart Campus: (i) Tecnologías de la Información y la Comunicación (TIC); (ii) Sostenibilidad Ambiental; (iii) Productividad; (iv) Calidad de vida; (v) Igualdad e inclusión social; (vi) Infraestructura física. Cada uno de estos requisitos interactúa con los ámbitos clave y sus atributos.

En el caso concreto de las TIC, este requisito comprende todos los indicadores relacionados con el tratamiento de la información (lo que incluye los datos personales), conexión a Internet, proveedores de acceso a la red, de telefonía, de cloud, etc., así como todos los indicadores TIC que son transversales a todos los ámbitos del Campus, como son la «privacidad y la seguridad de las comunicaciones»[47].

Por último, definir una semántica de Campus Inteligente permite establecer una estructura común o arquitectura que sea válida a lo largo del tiempo, e independiente del tamaño, ubicación o peculiaridades.

En la **Figura 2** *infra* se describe la arquitectura del Campus Inteligente, a partir de la semántica de la Ciudad Inteligente prevista en la UNE 178201:2016.

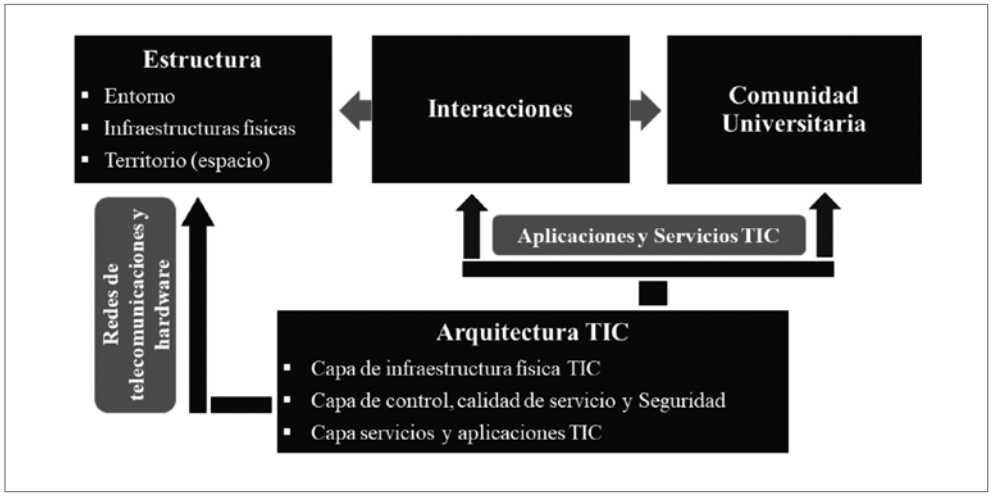
46. Junto a los atributos del Buen Gobierno, la Transparencia (reutilización, open data y derecho de acceso a la información pública), el Gobierno electrónico (con tecnologías esenciales como el Open Data, el Big Data, el IoT), la «protección de la información» implica «preservar el derecho fundamental de los ciudadanos a la protección de la información, disponer y decidir sobre las informaciones que se refieran a él y a la confidencialidad de la misma». Cfr. UNE 178201:2016, pp. 8-9.

47. Cfr. Idem, p. 11.

En un primer nivel, vemos cómo las «Interacciones» son las actividades que la «Sociedad» (comunidad universitaria) efectúa con las «Estructuras físicas» no humanas existentes en el Smart Campus y que pueden analizarse y medirse como flujos de información. A su vez, el sistema «Sociedad» engloba a las personas en un sentido amplio como integrantes de la Comunidad universitaria (alumnos, profesores, personal de administración y servicios, etc.) y al gobierno, que se refiere a la estructura institucional-administrativa del Campus y responsable de las políticas que facilitan el desarrollo del Campus.

En un segundo nivel, la «Arquitectura TIC» comprende el conjunto de componentes, hardware, redes, servicios y aplicaciones que interactúan entre sí y cuyo funcionamiento es esencial para el desarrollo correcto del Smart Campus. Dentro de la arquitectura del Smart Campus, las redes de telecomunicaciones y el hardware pertenecen a la infraestructura física, pero las aplicaciones y servicios TIC son la base del correcto funcionamiento del resto de los sistemas, Comunidad Universitaria y Relaciones.

Figura 2. ***Arquitectura semántica del Campus Inteligente***



Fuente: Elaboración propia a partir de UNE 178201:2016

Pues bien, siguiendo de nuevo la Norma UNE referenciada, «los principios básicos que debe cumplir la arquitectura TIC es que esté basada en estándares, sea flexible, escalable y tolerante a fallos», lo que incluye también «garantizar la seguridad, la protección de la información (privacidad) y un conjunto de servicios avanzados». Este modelo permite a los usuarios del Campus (personas, máquinas inteligentes y procesos) establecer relaciones de comunicación entre sí (comunicaciones usuario–usuario, usuario–máquina y máquina–máquina)[48].

48. Idem, pp. 15-16.

Se aprecia así como, al igual que la Smart City, el Smart Campus interrelaciona dispositivos, aplicaciones y personas para proporcional nuevas experiencias o servicios y mejorar la eficiencia operacional. Asimismo, además de la eficiencia y la sostenibilidad económica y ambiental, el Smart Camus posibilita la eficiencia y sostenibilidad social en tres ámbitos concretos: bienestar inteligente para los miembros de la Comunidad, aprendizaje inteligente para los alumnos y docentes, y seguridad inteligente[49].

Desde el punto de vista de la normativa de protección de datos, la protección de la privacidad a través de la «capa de control, calidad de servicio y seguridad», viene determinada por:

(i) La **aplicación de los principios en materia de protección de datos** (art. 5 RGPD) a la hora de configurar un proyecto de Smart Campus o de implementar tecnologías inteligentes de forma progresiva. Al considerar la implantación de tecnologías inteligentes, resultan de especial relevancia el principio de limitación de la finalidad, con especial atención a la compatibilidad entre la finalidad inicial y los fines ulteriores del tratamiento, así como el principio de minimización.

(ii) La **adecuación de los tratamientos de datos personales a través de soluciones inteligentes a la correspondiente base jurídica que legitime tales tratamientos**, de conformidad con lo dispuesto en el art. 6 RGPD. En el contexto de proyectos de Smart Campus, las bases legítimas habituales para el tratamiento de datos personales mediante tecnologías inteligentes serían el consentimiento del afectado (art. 6.1.a), el cumplimiento de una misión realizada en interés público (e.g. mantenimiento de la seguridad física y lógica del Smart Campus), o el interés legítimo del responsable (e.g. gestión ambientalmente sostenible del Smart Campus), siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales[50].

(iii) La garantía del **ejercicio de los derechos de los afectados** frente al responsable del tratamiento (la institución). Así, por ejemplo, el derecho a la información del afectado con relación a los datos que son objeto de tratamiento (arts. 13-14 RGPD), de una «forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo» (art. 12 RGPD), con independencia de que los datos se hayan obtenido del propio interesado (por ejemplo, a través de un formulario electrónico para solicitud de una beca) o se hayan obtenido por otros medios como sería el caso de los datos observados (e.g. a través de video-vigilancia o sensores RFID). Otros derechos que garantizan los arts. 15-22 RGPD son el derecho de acceso del interesado, el derecho de supresión y rectificación,

49. NEDWICK, R. «Smart campus - merging smart city and smart home in education for digital natives». *Dotmagazine*, February 2018.

50. Vid. VALKS, B., ARKESTEIJN, M.; den HEIJER, A. *Smart campus tools 2.0* […], p. 213.

el derecho a la limitación del tratamiento, el derecho a la portabilidad de los datos y el derecho de oposición, especialmente, con relación a decisiones individuales automatizadas, incluida la elaboración de perfiles. A los que debe unirse el bloqueo de datos que prevé el art. 32 LOPD-GDD.

(iv) El **cumplimiento de las obligaciones previstas en el RGPD y en la LOPD-GDD** por parte del responsable de tratamiento (la institución universitaria) y sus encargados de tratamiento, en particular, el Registro de Actividades de Tratamiento (RAT), que además es de publicidad obligatoria en el Portal de Transparencia de la institución si se trata de una Universidad Pública[51]; la designación de un Delegado de Protección de Datos (DPO) de acuerdo con lo dispuesto en el art. 34.1.b) LOPD-GDD; o la elaboración de contratos de encargo de tratamiento entre la institución universitaria y encargados, imponiéndose un deber de diligencia por parte del responsable a la hora de seleccionar encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas al encargo encomendado (art. 28.1 RGPD).

5. EVALUACIONES DE IMPACTO EN PROYECTOS DE SMART CAMPUS. ESPECIAL REFERENCIA A TECNOLOGÍAS DE IDENTIFICACIÓN RFID Y *SMART METERING*

Por su especial incidencia el objeto de estudio de este Capítulo, uno de los aspectos más relevantes de la nueva normativa de protección de datos a considerar son las Evaluaciones de Impacto relativas a la Protección de Datos Personales (en adelante, «EIPD»).

Todo tratamiento de datos personales asociado a la implantación de un proyecto de Smart Campus o, en su caso, de soluciones tecnológicas inteligentes aplicadas a la gestión del Campus Universitario, implica que haya de considerarse el riesgo, en la medida en que la «aproximación basada en el riesgo» es un criterio fundamental en torno al cual gira el RGPD, y elemento central del principio de responsabilidad proactiva y de privacidad desde el diseño[52].

---

51. Cfr. art. 31.2 con relación al art. 77.1.i) y la Disposición final undécima LOPD-GDD que introduce una modificación en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, al incluir el art. 6 bis. en los siguientes términos: «Registro de actividades de tratamiento. Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica».» En dicho Registro deberán quedar reflejados, entre otros aspectos, las actividades de tratamientos de datos personales que impliquen el uso de soluciones inteligentes, la finalidad específica y concreta de tales tratamientos, su base jurídica, las categorías de afectados y datos personales tratados, la existencia de cesiones, y en su caso, transferencias internacionales, así como las medidas técnicas y organizativas adoptadas por el responsable (que en el caso de las Universidades Públicas deberán remitir al ENS).

52. Gayo, R. «Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control». Piñar Mañas, J.L., *Reglamento Gene-*

El art. 35.1. RGPD establece la obligatoriedad de las EIPD en los siguientes términos: «Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un *alto riesgo para los derechos y libertades de las personas físicas*, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales [cursiva nuestra]».

En el contexto de dicha obligación, una EIPD es una herramienta *flexible, escalable y de carácter preventivo* que debe realizar el responsable del tratamiento (en este caso, la institución Universitaria) y que consiste en un proceso o metodología que permite identificar y analizar *ex ante* los riesgos o impactos que un producto, servicio o proyecto puede implicar no sólo para la protección de datos sino también en los derechos y libertades de los sujetos afectados[53] antes de que éstos se materialicen, con el fin de determinar las medidas técnicas y organizativas que mitiguen o eliminen tales riesgos o impactos negativos[54].

En este sentido, el extinto GT29 ha señalado que una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento en coherencia con el principio de responsabilidad proactiva[55].

Aunque el RGPD prevé que las EIPD se lleven a cabo «antes del tratamiento»; sin embargo, también resulta procedente dicha Evaluación cuando en una operación iniciada con anterioridad a la aplicación del RGPD se hayan producido cambios en los riesgos que el tratamiento implica en relación con el momento en que el tratamiento se puso en marcha.[56].

---

ral de Protección de Datos. Hacia un nuevo modelo europeo de privacidad. Madrid, Reus, 2016, pp. 352 y 355.

53. Adviértase que la referencia a la afectación de «los derechos y libertades» de los interesados atañe principalmente a los derechos a la protección de datos y a la intimidad, pero también puede implicar otros derechos fundamentales como el derecho al honor y a la propia imagen, la libertad de expresión, la libertad de pensamiento, la libertad de circulación y movimiento, la prohibición de discriminación, la integridad física y moral, el derecho a la libertad y la libertad de conciencia y de religión, u otros derechos y libertades (e.g. el derecho al trabajo). Cfr. GT29. *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*, WP248 rev.01, revisadas y actualizadas a 4 de octubre de 2017, p. 7.

54. AEPD. *Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetos al RGPD*, febrero 2018, p. 4; ICO. *Data Protection Impact Assessments* (DPIAs), 2018; PUJOL, J. *El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's*, Tirant lo Blanch, Valencia, 2018, pp. 13-19.

55. GT29. *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*, WP248 rev.01, revisadas y actualizadas a 4 de octubre de 2017

56. Por ejemplo, como consecuencia, de que se hayan empezado a aplicar tecnologías inteligentes a ese tratamiento, de que los datos se estén usando para finalidades distintas o adicionales a las que se decidieron en su momento, o de que se estén recogiendo nuevas categorías de datos, o datos diferentes, de los que en principio se utilizaban para el tratamiento (e.g. datos biométricos, de geoposicionamiento, tags identificadores). Vid. AEPD. *Guía Práctica para las Evaluaciones de Impacto […],* Op. cit., p. 2.

Al conceptualizar y determinar el concepto de riesgo, debe advertirse que no existe una definición formal del término en el GDPR. Sin embargo, los Considerandos 75 y 76 vinculan el riesgo con: (i) cualquier daño y perjuicio físico, material o moral efectivo en los derechos y libertades de los afectados, y en particular, cualquier «daño potencial» que pueda producirse; (ii) la probabilidad de que el daño se materialice y su gravedad para los derechos y libertades del interesado de acuerdo con la naturaleza, el alcance, el contexto y los fines del tratamiento de datos[57].

Asimismo, de conformidad con el art. 35.1 RGPD[58], una EIPD podrá abordar una única operación de tratamiento de datos o una serie de operaciones de tratamiento que entrañen altos riesgos similares, en «términos de naturaleza, alcance, contexto, fines y riesgos», o incluso diferentes tratamientos, siempre que los mismos no presenten incompatibilidades entre sí[59].

Así, por ejemplo, una Universidad con una red de Campus ubicados en distintas localizaciones (en la propia ciudad, a nivel supramunicipal, a nivel internacional) o con distintas bibliotecas ubicadas en diferentes emplazamientos, podrá realizar respectivamente una única EIPD de los tratamientos de videovigilancia de todos sus Campus o de los tratamientos relativos a la gestión del préstamo bibliotecario e interbibliotecario a través de identificadores RFID.

Con carácter general, se ha estimado que la implantación y desarrollo de Proyectos de Smart Cities exigen la correspondiente EIPD —e incluso la correspondiente consulta previa a la AEPD de conformidad con el art. 36 RGPD—, «valorando el volumen de la información que se pretende procesar y el número y tipo de fuentes desde las que se pretende obtener dicha información o incluso el tiempo durante el que se pretende conservar esta información»[60].

Mutatis mutandi, la implantación de un Proyecto de Smart Campus o, en su caso, de soluciones tecnológicas inteligentes («tratamientos en desarrollo»), así como las soluciones ya implantadas («tratamientos en producción»)[61] requerirán,

57. ICO. *Data Protection Impact Assessments (DPIAs)*, 2018.

58. El Considerando 92 añade que «[h]ay circunstancias en las que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyectan introducir una aplicación o un entorno de tratamiento común […] para una actividad horizontal de uso generalizado».

59. GT29. *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*, WP248 rev.01, revisadas y actualizadas a 4 de octubre de 2017, p. 8.

60. AEPD. Guía Sectorial de Protección de Datos y Administración Local, febrero 2018, pp. 24-25.

61. PUJOL, J. *El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's*, Tirant lo Blanch, Valencia, 2018, p. 20. Con relación a las EIPD, el autor distingue entre los «tratamientos en desarrollo», que hacen referencia al examen o evaluación previa de los tratamientos a realizar de cara a la futura implantación de un producto o servicio; y los «tratamientos en producción» que comprenden aquellos tratamientos que ya se vienen llevando a cabo por la organización. Debe pensarse que, con anterioridad al RGPD, la realización de EIPDs no era obligatoria, por lo que muchos tratamientos anteriores a la entrada en vigor al RGPD entrarían dentro de los supuestos que exigirían adecuación normativa al RGPD y exigirían realizar el correspondiente análisis de riesgos de esos tratamientos, conforme al nuevo marco normativo.

en su caso, la correspondiente EIPD cuando, de conformidad con el art. 35.3 RGPD y el art. 28.2 LOPD-GDD, la institución responsable vaya a realizar algunos de los siguientes tratamientos.

Figura 3. ***Tratamientos de alto riesgo y EIPD en Smart Campus***

<table>
<tr><th>Art. 35.3 RGPD</th><th>Art. 28.2 LOPD-GDD</th><th>Aplicación ad hoc en Smart Campus</th></tr>
<tr><td rowspan="3">Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar</td><td>Evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su localización o sus movimientos.</td><td>Tratamientos que impliquen el enriquecimiento de datos, mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades no compatibles con la finalidad inicial mediante uso o combinación de tecnologías inteligentes.</td></tr>
<tr><td>Privación a los afectados de sus derechos y libertades o impedir el control sobre sus datos personales</td><td rowspan="2">Tratamientos que impliquen combinación de datos personales procedentes de dos o más operaciones de tratamiento de datos realizadas para distintos fines o por responsables del tratamientos distintos de una manera que exceda las expectativas razonables del interesado mediante uso o combinación de tecnologías inteligentes.</td></tr>
<tr><td>Tratamientos que puedan generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas económicas, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.</td></tr>
</table>

Tratamiento a gran escala de las categorías especiales de datos.	Datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de personas con discapacidad.	Gestión y asistencia administrativa a personas con discapacidad o con necesidades educativas especiales.
	Tratamientos no meramente incidentales o accesorios de categorías especiales de datos o de datos relacionados con la comisión de infracciones penales o administrativas.	Tratamiento de datos biométricos de reconocimiento facial como medio de control de asistencia y realización de pruebas en docencia semipresencial en docencia on-line o semipresencial.
Observación sistemática a gran escala de una zona de acceso público.	Tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.	Aplicación de Big Data, Video-vigilancia del Campus.
En general, tratamiento que utilice nuevas tecnologías y que, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.	Aplica directamente RGPD.	Aplicación de soluciones tecnológicas especialmente invasivas (identificadores RFID, geolocalización, vigilancia electrónica mediante la monitorización del comportamiento de personas a través del análisis de la navegación por Internet, Big Data, IoT, Video-vigilancia del Campus).
Otros tratamientos que entrañen alto riesgo (lista no exhaustiva RGPD).	Transferencia de datos personales, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.	Contratación de servicios de Cloud ubicados en servidores en terceros países.
		Tutoriales online, Moocs a través de servicios de redes sociales (e.g. Youtube).
	Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.	A determinar en la propia EIPD*.

* Por ejemplo, «tratamientos invisibles» de datos que no hayan sido obtenidos directamente del afectado en circunstancias en las que el responsable considere que el cumplimiento del deber de información al afectado resulte imposible o exija un esfuerzo desproporcionado conforme al art. 14.5.b) RGPD. Vid. ICO. Data Protection Impact Assessments (DPIAs), 2018.

Fuente: Elaboración propia a partir de RGPD, LOPD-GDD, GT29 (WP248 rev.01), ICO (2018).

En primer lugar, como ha aclarado el GT29, se trata de un listado que tiene carácter enunciativo que no limitativo[62].

A su vez, la Autoridad inglesa de protección de datos ha interpretado el significado del término «nuevas tecnologías» que puedan implicar un «alto riesgo» empleado por el art. 35.1 RGPD. Más que con la tecnología que novedosa para el usuario, el ICO identifica la expresión «nuevas tecnologías» con la idea de «tecnologías innovadoras», en el sentido de «nuevas formas de obtención y uso de los datos personales» cuyo despliegue puede tener consecuencias personales y sociales desconocidas[63].

Asimismo, a efectos de determinar si el concepto de tratamiento se realiza «a gran escala»[64], el GT29 ha proporcionado algunos criterios orientativos que puedan ser aplicables al Campus Inteligente: a) el número de interesados afectados, bien como cifra concreta (número de alumnos matriculados y antiguos alumnos cuyos datos estuvieran bloqueados o pudieran tratarse para finalidades concretos, personal docente y administración y servicios) o como proporción de la población correspondiente (e.g. con relación al número de afectados en otras Universidades); b) el volumen de datos o la variedad de elementos de datos distintos que se procesan de forma no ocasional; c) la duración, o permanencia, de la actividad de tratamiento de datos (e.g. durante toda la gestión del expediente académico con relación a la duración del Grado y, en su caso, Posgrado); d) el alcance geográfico de la actividad de tratamiento (e.g. Campus Inteligente Internacional).

En distintas Recomendaciones y documentos, tanto la Comisión Europea como el GT29 han venido establecido la necesidad de la correspondiente EIPD con relación a los tratamientos de datos personales derivados de la implementación de aplicaciones basadas en tecnologías inteligentes y que, por tanto, constituyen un marco de referencia a tener en cuenta en la implementación de Proyectos de Smart Campus.

En este sentido, se han analizado los aspectos más relevantes de una EIPD relativa a la implementación de aplicaciones basadas en tags identificadores RFID, que según hemos visto se están desplegando en distintos proyectos de Campus Inteligentes. Se debe partir de la premisa de que este tipo de aplicaciones pueden tratar distintas categorías de datos (identificativos, biométricos, de geo-posicionamiento, de comportamiento o credenciales como el nombre de usuario, contraseña o número de EMI del smartphone del usuario)[65], y por tal

62. Vid. GT29. *Directrices sobre la evaluación de impacto* […], Op. cit., p. 10.

63. Como ejemplos de tales tecnologías innovadoras, se incluyen la AI, el *machine learning* (aprendizaje automático) y el *deep learning*, las tecnologías inteligentes (incluyendo los wereables) o algunas aplicaciones de IoT dependiendo del tipo de tratamiento aplicado.

64. Vid. GT29. *Directrices sobre la evaluación de impacto* […], Op. cit., p. 11.

65. Véase, en este sentido, la solución tecnológica para Bibliotecas Inteligentes basada en IoT, Sistema de Posicionamiento Indoor Local (LPS), e identificadores Near Filed Communication (NFC) a través de la red local inalámbrica (WLAN) de la propia Biblioteca, que explican BRIAN, A.L., AROCKIAM, L. AND MALARCHELVI, S.K. «An IoT Based Secured Smart Librar […], Op. cit., p. 2. Al describir las funcionalidades de esta solución, los autores identifican de forma específica las distintas categorías de datos personales que serían objeto de tratamiento.

motivo, la Comisión considera que existe un riesgo potencial de que esta tecnología pueda ser utiliza para monitorizar a los afectados[66] o que se usen las etiquetas (tags) por un tercero para fines para los que no estaban destinadas[67].

El GT29 propone un modelo de EIPD para esta clase de aplicaciones RFID que se articula en dos fases. Una primera fase de evaluación previa consistiría en evaluar si se requiere o no una EIPD y, en su caso, optar entre una EIPD «de gran escala» o «de pequeña escala». La fase propiamente dicha de evaluación de riesgos que se desglosaría en cuatro pasos: 1) Caracterización de la aplicación mediante el análisis de las categorías de datos objeto de tratamiento, los flujos de datos y ciclo de vida de los mismos (obtención, almacenamiento, combinación, cesiones o transferencias); 2) Identificación de los riesgos para los datos personales, mediante la evaluación de las amenazas, su probabilidad y su impacto en los derechos y libertades de los afectados y en el cumplimiento de la normativa europea; 3) Identificación y recomendación de controles de seguridad, en respuesta a riesgos previamente identificados. 4) Documentación de los resultados de la EIPD y establecimiento de una resolución sobre las condiciones de ejecución de las aplicaciones RFID bajo revisión e información sobre riesgos residuales[68].

Con el fin de conseguir una mejora de la eficiencia energética del Campus, en caso de que se implementara una redes y contadores inteligentes para analizar y gestionar el consumo energético de los distintos despachos y oficinas del Campus, habría que tener presente que tales mediciones permitirían realizar «perfiles energéticos» individualizados cuando esos despachos u oficinas estén ocupados por una persona concreta.

En este sentido, la implementación de un sistema de contadores inteligentes implica el tratamiento de las siguientes categorías de datos: a) número de identificación único del contador inteligente y/o número de referencia único del inmueble (en ausencia de estos datos, el contador puede identificarse por su gráfico de carga energética único); b) Metadatos relativos a la configuración del contador inteligente; c) Descripción del mensaje transmitido, por ejemplo una lectura de contador o un aviso de manipulación; d) Sello con fecha y hora; e) Contenido del mensaje que incluye lectura de minutería del contador, avisos (e.g. activación de alarma del contador), información sobre la red relativa a la tensión, los fallos de alimentación y la calidad de la potencia, y gráficos de carga con distintos niveles de detalle[69].

---

66. Comisión Europea. *Recomendación de 12 de mayo de 2009 sobre la implementación de los principios de privacidad y protección de datos en aplicaciones basadas en identificación por radiofrecuencia*, 2009/387/EC, Considerando 5.

67. GT29. *Dictamen 9/2011 relativo a la Propuesta Revisada de la Industria para un Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad en las Aplicaciones Basadas en la Identificación por Radiofrecuencia (RFID)*, p. 6.

68. Idem, p. 9.

69. GT29. *Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force*, WP209, febrero de 2013, p. 5.

Ahora bien, existen riesgos de que esos datos de consumo fuesen objeto de tratamientos que no son necesarios para lograr la finalidad (eficiencia energética) si de tales de tales perfiles energéticos se infirieran aspectos relativos al rendimiento en el trabajo de los afectados sobre cuya base se tomasen decisiones que produjeran efectos jurídicos (e.g. no conceder a un docente una ayuda o financiación para un proyecto de investigación). Precisamente, partiendo de la premisa de que la base jurídica que justifica el tratamiento de esta clase de datos podría ser el interés legítimo del responsable del tratamiento (art. 6.1.f RGPD), el GT29 estima que la aplicación de la correspondiente EIPD permitirá justificar la adecuada ponderación entre los legítimos intereses del responsable y de la propia Comunidad Universitaria en una mayor eficiencia del suministro y el consumo de energía y los derechos y libertades del interesado, sin que esta base jurídica pueda justificar cualquier otra finalidad distinta del tratamiento (e.g. monitorización e inferencia del rendimiento en el trabajo)[70].

5. NORMALIZACIÓN, CERTIFICACIÓN Y SEGURIDAD DE LOS DATOS EN LOS SMART CAMPUS

Como se ha venido repitiendo en estas páginas, a falta de un grupo normativo sectorial que regule de forma sistematizada la «intrincada problemática» de la Smart City[71], la «normalización» o «estandarización» constituye uno de los pilares fundamentales para el despliegue de las ciudades inteligentes[72].

Así, por ejemplo, no es infrecuente que en la contratación pública de soluciones específicas para el desarrollo de proyectos de Smart Cities[73] se exija en los Pliegos, como requisito previo de solvencia, la oportuna tenencia de certificaciones en ISO 9001 (sistemas de gestión de calidad)[74], o en el Esquema Nacional de Seguridad (ENS)[75], este último inspirado en la familia de estándares ISO 27000 y, más concretamente, en la ISO 27001[76]; o bien que el adjudicatario

70. Idem, pp. 9-10.

71. Barrio, M., «La smart city: versión 2.0 del municipio», Op.cit.

72. Marcos Paramio, T. «El modelo de normalización español de Ciudades Inteligentes (UNE, CTN 178) y su impacto internacional», *III Congreso Ciudades Inteligentes*, 27/10/2017.

73. Cfr. Suárez Ojeda, M. «Smart Cities: un nuevo reto para el Derecho Público», Piñar Mañas, J.L. (Dir). *Smart Cities. Derecho y técnica para una ciudad más habitable*. Madrid: Reus, 2017, p. 86.

74. RED.es. *Exp. 055/18-SP. Condiciones específicas del Pliego de Cláusulas Administrativas Particulares que regirán la realización del contrato de «desarrollo de la iniciativa Smart Island Mallorca» licitado mediante procedimiento abierto*. Cláusula 3.2.

75. Ayuntamiento de Cullera. *Expediente 645/18. Pliego de Cláusulas Técnicas para la Contratación de los servicios de voz, comunicaciones móviles, de acceso a Internet, máquinas virtuales y Esquema Nacional de Seguridad*. Cláusulas 4 y 7.

76. En este sentido, el Anexo V del correspondientes del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), incluye un modelo de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos. En concreto, el Anexo V dispone que: «Cláusula administrativa particular. En cumplimiento con lo dispuesto en el artículo 115.4 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público [actual art. 122.5

garantice en todo momento la calidad de los productos, por lo que la entidad contratante se reserva el derecho a realizar un proceso de certificación de los productos entregados en el marco del correspondiente expediente de contratación[77].

Más aún, con relación a las medidas de seguridad en materia de protección de datos en el ámbito del sector público institucional, las Universidades Públicas que, en su caso, desarrollen un proyecto de Smart Campus o implementen progresivamente soluciones tecnológicas inteligentes a la gestión y gobiernos del Campus, deberán tener en cuenta las previsiones incluidas en la Disposición Adicional Primera de la LOPD-GDD que, entre otras obligaciones impone la adecuación de las medidas de seguridad al ENS en los casos en los que un tercero preste un servicio en régimen de contrato.

La normalización y certificación en materia de soluciones tecnológicas inteligentes y en materia de privacidad está, de hecho, en la agenda de las políticas públicas. En su *Estrategia para el Mercado Único Digital de Europa* (2015), la Comisión Europea ha destacado el papel relevante de la normalización en el marco de las 16 acciones clave que integran la hoja de ruta establecida en dicha estrategia[78].

En este sentido, AENOR ha identificado una serie de áreas de estandarización clave para el mercado digital estructurado, entre las que deben destacarse: ciudades inteligentes; gobierno y gestión de las TIC; Administración electrónica; ciberseguridad; IoT; Big Data; Cloud Computing; eficiencia energética; o Blockchain[79]. Áreas todas ellas, con impacto disruptivo en la privacidad.

LCSP 2017], y en el artículo 18 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, servicios, equipos, sistemas, aplicaciones o sus componentes, cumplen con lo indicado en la medida op.pl.5 sobre *componentes certificados*, recogida en el apartado 4.1.5 del anexo II del citado Real Decreto 3/2010, de 8 de enero [cursiva nuestra].» Asimismo, en el párrafo segundo del Anexo V del ENS prevé que cuando estos productos de seguridad, servicios, equipos, sistemas, aplicaciones o sus componentes «sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal [RLOPD]». A su vez, es importante tener en cuenta que la Disposición Derogatoria Única de la nueva LOPD-GDD no ha derogado el RLOPD y, por tanto, siguen siendo de aplicación las medidas de seguridad previstas en dicha disposición reglamentaria en todo lo que no se oponga a la nueva Ley Orgánica.

77. Vid. RED.es. *Exp.: 163/15-AE. Pliego de prescripciones técnicas que regirán la realización del contrato de «Desarrollo de la Iniciativa Martos Smart City» (Procedimiento abierto)*. Cláusula 2.1.7.6.

78. Comisión Europea. *Una Estrategia para el Mercado Único Digital de Europa*. COM/2015/0192 final, Bruselas, 6 de mayo de 2015. En particular, debe destacarse la acción relativa a la «adopción de un plan prioritario de normas sobre TIC y la ampliación del marco europeo de interoperabilidad para los servicios públicos», estableciendo como sectores prioritarios las comunicaciones inalámbricas 5G, la informatización de los procesos de fabricación (Industry 4.0) y construcción, servicios basados en los datos, servicios en nube, ciberseguridad, sanidad electrónica, transporte, redes y contadores inteligentes o pagos móviles.

79. UNE. Normalización Española. «Apoyo de la Normalización para la Economía Digital». *UNE. Revista de la Normalización Española*, Núm. 6 (2018). Disponible en https://www.une.org/normalizacion_documentos/Normalizacion_economia_digital.pdf

Pues bien, en este contexto, debe subrayarse que la normalización y a los estándares definidos por los esquemas de certificación han cobrado una importancia especial en la actual normativa de protección de datos.

El RGPD aborda la cuestión de la normalización en el ámbito de la privacidad al reconocer la importancia de los códigos de conducta y la certificación en sus arts. 40 a 42.

Más allá de que una de las cuestiones discutidas por la doctrina jurídica es si la normalización debe o no garantizar el mismo nivel de protección que el RGPD o si debe ir más allá que el nivel legal establecido[80], lo cierto es que la certificación aplicada a la protección de datos personales es un instrumento que puede servir para no sólo para demostrar el cumplimiento de los responsables de tratamiento, de conformidad con el «principio de responsabilidad proactiva» consagrado por el Reglamento, sino también para generar confianza y conseguir una protección efectiva del derecho a la protección de datos del interesado y de otros derechos y libertades que puedan verse afectados por el tratamiento de datos personales[81].

Así, por ejemplo, con relación a los contratos de encargo de tratamiento, que puedan generarse en la implementación de proyectos de Campus Inteligentes, debe tenerse en cuenta lo establecido por el Considerando 81 RGPD: «La adhesión del encargado a un código de conducta aprobado o a un *mecanismo de certificación* aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable [cursiva nuestra].»

Por su parte, al abordar las medidas de responsabilidad proactiva de responsables y encargados de tratamiento en proyectos de Smart Campus, el art. 28.2 h) LOPD-GDD deja claro que podrán tenerse en cuenta instrumentos como los códigos de conducta y estándares definidos por esquemas de certificación a la hora de determinar las medidas técnicas y organizativas apropiadas para garantizar y acreditar que el tratamiento es conforme con la RGPD, con la propia ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable[82].

Asimismo, tanto el enfoque de análisis de riesgos como la adopción de las medidas técnicas y organizativas por parte de los responsables de tratamiento en un Smart Campus deben entenderse en el contexto de lo dispuesto en el art. 32.1 RGPD, teniendo en cuenta que ni el RGPD, ni la LOPD-GDD establecen cuáles son las medidas de seguridad concretas aplicables a la realidad de la or-

80. Grafenstein, M. (von). *The principle of purpose limitation*, Nomos Verlagsgesellschaft mbH, 2018, p. 621.

81. Fernández Sánchez, C.M.; Recio Gayo, M. «Certificación en protección de datos personales». Piñar Mañas, J.L., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid, Reus, 2016, pp. 413-414.

82. Téngase en cuenta que, entre las infracciones graves que tipifica la Ley Orgánica se encuentran, por ejemplo, la «utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado» (art. 73)

ganización, más allá de mencionar la seudoniminización y el cifrado de datos personales[83].

En el contexto de las Smart Cities, se ha vinculado directamente las obligaciones derivadas del art. 32 RGPD con la aplicación de la serie ISO/IEC 27000[84]. A este respecto, debe tenerse en cuenta que, junto a las normas técnicas en materia de Ciudades Inteligentes[85], el Comité CTN 320 de «Ciberseguridad y protección de datos personales» ha aprobado un total de 26 Normas Técnicas, de las cuales 18 están actualmente en vigor.

En la **Figura 4** siguiente se identifican algunas de las Normas Técnicas más significativas para la aplicación de soluciones tecnológicas, entre las cuales, como norma principal de la serie destaca la UNE-EN ISO/IEC 27001:2017.

La ISO 27001:2017 es una norma certificable que especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información (SGSI). La Norma también incluye los requisitos para la apreciación y el tratamiento de los riesgos de la seguridad de la información asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información, para cualquier tipo de organización, con independencia de su tamaño o naturaleza, pública o privada[86].

---

83. Dispone el art. 32.1 RGPD: «Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo».

84. VOJKOVIC, G. «Will the GDPR slow down development of Smart Cities?», 41st International Convention on Information and Communication Technology, electronics and microelectronics, MIPRO 2018, Opatija [Croatia], 2018, p. 1497, quien vincula directamente las obligaciones derivadas del art. 32 RGPD con la aplicación de la serie ISO/IEC 27000.

85. Actualmente, el CTN 178 ha aprobado 27 normas técnicas relativas a las diferentes áreas temáticas incluidas en el ámbito de las Ciudades Inteligentes. Véanse, entre otras, UNE 178109:2018. Ciudades Inteligentes. Estación inteligente y conexión con la plataforma de ciudad inteligente; UNE 178104:2017. Sistemas Integrales de Gestión de la Ciudad Inteligente. Requisitos de interoperabilidad para una Plataforma de Ciudad Inteligente; UNE 178108:2017. Ciudades Inteligentes. Requisitos de los edificios inteligentes para su consideración como nodo IoT según Norma UNE 178104; UNE 178105:2017. Accesibilidad Universal en las Ciudades Inteligentes. UNE 178401:2017. Ciudades inteligentes. Alumbrado exterior. Grados de funcionalidad, zonificación y arquitectura de gestión. UNE 178202:2016. Ciudades inteligentes. Indicadores de gestión en base a cuadros de mando de gestión de ciudad; UNE 178301:2015. Ciudades Inteligentes. Datos Abiertos (Open Data); UNE 178303:2015. Ciudades inteligentes. Gestión de activos de la ciudad. Especificaciones. Completa dicho listado, la Norma UNE 66182:2015, «Guía para la evaluación integral del gobierno municipal y el desarrollo como ciudad inteligente», que tiene como referencia, a su vez, el conjunto de documentos técnicos y normativos elaborados por el CTN 178 «Ciudades Inteligentes». El objeto de esta Norma es proporcionar a los gobiernos municipales una «metodología asequible y práctica para fijar y ganar en confiabilidad y facilitar la integración en sus servicios de la perspectiva de la ciudad inteligente», incorporando un método de evaluación con actividades a realizar e indicadores a considerar.

86. De hecho, en la 9ª Sesión Abierta de la AEPD, de 25 de mayo de 2017, entre las herramientas para la implementación del principio de proactividad del responsable basado en un enfoque del riesgo, se incluye la seguridad gestionada (SGSI), que comprende la implementación de las medidas de seguridad basadas en el Esquema Nacional de Seguridad o en la ISO 27001.

Figura 4. ***Normas del Comité CTN 320 «Ciberseguridad y protección de datos personales»***

Norma Técnica	Objeto
UNE-EN ISO/IEC 27001:2017	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015).
UNE-EN ISO/IEC 27002:2017	Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015).
UNE-ISO/IEC 27000:2014	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.
UNE 71504:2008	Metodología de análisis y gestión de riesgos para los sistemas de información.
UNE-ISO/IEC 27000:2012	Tecnologías de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.
UNE-EN ISO/IEC 27038:2016	Tecnología de la información. Técnicas de seguridad. Especificación para la redacción digital (ISO/IEC 27038:2014).
UNE-EN ISO/IEC 27041:2016	Tecnología de la información. Técnicas de seguridad. Directrices para garantizar la idoneidad y adecuación del método de investigación de incidentes (ISO/IEC 27041:2015).
UNE-EN ISO/IEC 27040:2016	Tecnología de la información. Técnicas de seguridad. Seguridad en el almacenamiento (ISO/IEC 27040:2015).
UNE-EN ISO/IEC 27043:2016	Tecnología de la información. Técnicas de seguridad. Principios y procesos de investigación de incidentes (ISO/IEC 27043:2015)
UNE-ISO/IEC TR 15446:2013 IN	Tecnologías de la información. Técnicas de seguridad. Guía para la producción de perfiles de protección y objetivos de seguridad.

Fuente: elaboración propia

En su Anexo A, la UNE-EN ISO/IEC 27001:2017 enumera los objetivos de control y 114 controles para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI con relación al tratamiento de los riesgos de la seguridad de la información. Estos controles han sido, a su vez, desarrollados, por la ISO 27002:2005. A, pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho Anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Así, por ejemplo, en la implementación de soluciones tecnológicas inteligentes en el contexto de un Smart Campus, las medidas de seguridad incluirían, entre otras, el control de acceso a sistemas y aplicaciones (A.9.4), cuyo objetivo

específico es prevenir el acceso no autorizado a los sistemas y aplicaciones y, por ende, a los datos personales que son objeto de tratamiento.

En la **figura 5** siguiente se establece una correlación entre las posibles amenazas y los riesgos asociados al uso de tecnologías inteligentes (por ejemplo, el uso de identificadores RFID) y las medidas de seguridad relacionadas con los controles de acceso a aplicar para mitigar o eliminar esos riesgos. La tabla incluye una equivalencia entre las medidas de seguridad previstas en la ISO 27001: 2017, y la ISO 27002:2017, así como en el Anexo II del ENS[87].

Figura 5. Amenazas, riesgos asociados y controles ISO y ENS

<table>
<tr><th colspan="2">AEPD</th><th colspan="3">UNE-EN ISO/IEC 27001:2017 — ENS</th></tr>
<tr><th rowspan="2">Taxonomía de Amenazas</th><th rowspan="2">Riesgo asociado</th><th colspan="3">A.9.4. Control de acceso a sistemas y aplicaciones — ENS [OP.ACC] Control de acceso</th></tr>
<tr><td colspan="3">Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones</td></tr>
<tr><td rowspan="2">Deficiencias organizativas en la gestión del control de accesos</td><td rowspan="2">Acceso no autorizado por parte de terceros (violación de la confidencialidad)</td><td>A.9.4.1</td><td rowspan="2">Restricción del acceso a la información</td><td rowspan="2">Control
Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.</td></tr>
<tr><td>[OP.ACC.2]</td></tr>
<tr><td rowspan="2">Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.</td><td rowspan="2">Modificación de datos no autorizada por parte de terceros (violación de la integridad)</td><td>A.9.4.2</td><td>Procedimientos seguros de inicio de sesión</td><td rowspan="2">Control
Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.</td></tr>
<tr><td>[OP.ACC.6] OP.ACC.7]</td><td>Acceso Local (Local Logon) y Acceso Remoto</td></tr>
</table>

87. Esta equivalencia se ha elaborado a partir de CCN-CERT. *Guía de Seguridad de las TIC CCN-STIC 825. Esquema Nacional de Seguridad. Certificaciones 27001*. Noviembre 2013.

Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.	Uso ilegítimo de datos (vulneración de los derechos y libertades)	A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
		[OP.ACC.5]	Mecanismo de autenticación	

Fuente: Elaboración propia a partir de AEPD, ISO 27001-27002 y ENS

7. BIBLIOGRAFÍA

ABUARQOUB, A.; ABUSAIMEH, H. «A Survey on Internet of Things Enabled Smart Campus Applications». *3rd. International Conference on Future Networks and Distributed Systems* (ICFNDS), Cambridge, July 19-20 2017. DOI: 10.1145/3102304.3109810.

ALOTAIBI, S.; ALHUSSAINI, *A. Smart campus project*, King Fahd University of Petroleum and Minerals, 2014. Disponible en http://www.ccse.kfupm.edu.sa/~akhayyat/files/coe485-132/final/smart.campus-final-report.pdf

AMUTIO GÓMEZ, M.A. *Normalización en seguridad de las Tecnologías de la Información,* Ministerio de Administraciones Públicas, 2ª Edición, 2007.

BARRIO, M., «La smart city: versión 2.0 del municipio», *Documentación Administrativa* 3, Nueva Época, Enero-Diciembre 2016.

BARTOLI, A.; HERNÁNDEZ-SERRANO, M. S. et al. «On the Ineffectiveness of Today's Privacy Regulations for Secure Smart City Networks», *3rd. IEEE International Conference on Smart Grid Communications (SmartGridComm 2012)*, 5-8 November 2012.

BRIAN, A.L., AROCKIAM, L. AND MALARCHELVI, S.K. «An IoT Based Secured Smart Library System with NFC Based». International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Volume 11, Issue 5 (2014).

CAMPOS ACUÑA, C. (Dir.). *Aplicación Práctica y Adaptación de la Protección de Datos en el Ámbito Local. Novedades tras el Reglamento Europeo*. El Consultor de los Ayuntamientos. Wolters Kluwer, 2018.

D'ACQUISITO, G. et al. *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*. ENISA, December 2015. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-dataprotection

DELOITTE CONSULTING. *Estudio y Guía Metodológica sobre Ciudades Inteligentes*, ONTSI, Ministerio de Industria, Energía y Turismo, noviembre 2015.

EUROPEAN PARLAMENT. *Mapping Smart Cities in the EU*, Directorate General for Internal Policies, Bruselas: 2014 Disponible en: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf

FEMP. *Guía para la Adaptación al Reglamento General de Protección de Datos de las Administraciones Locales*. Comisión de Sociedad de la Información y Tecnologías. Grupo de Trabajo para la Implantación del Nuevo Reglamento General de Protección de Datos (RGPD) en las Administraciones Locales, 2018. Disponible en https://www.dcd.es/ebooks/RGPD-administraciones-locales.pdf.

FERNÁNDEZ HERGUETA, R. «El sector público y el uso de la blockchain». En: PREUKSCHAT, A. (coord.) *Blockchain. La revolución industrial de Internet*. Barcelona: Gestión 2000, 2017.

GARCÍA RUBIO, F. *Sostenibilidad ambiental y competencias locales. Un análisis jurídico*. Madrid: Dykinson, 2015.

— *Las nuevas perspectivas de la ordenación urbanística y del paisaje: smart cities y rehabilitación*. Perspectiva hispano-italiana, Fundación Democracia y Gobierno Local, 2017.

GOH, B. «Securing the Smart City», *Kennedy School Review*, núm. 16, 2016. Disponible en http://ksr.hkspublications.org/2016/09/07/securing-the-smart-city/ (consulta: 18 octubre 2017).

GÓMARA HERNÁNDEZ, J.L. *Protección de Datos: el RGPD en las Entidades Locales*. Claves Prácticas. Francis Lefebvre, 2018.

GONZÁLEZ FÚSTER, G.; SCHERRER, A. *Big Data and smart devices and their impact on privacy*, European Parliament, Directorate General for Internal Policies, PE 536.455, 2015.

GRAFENSTEIN, M. (von). *The principle of purpose limitation*, Nomos Verlagsgesellschaft mbH, 2018.

KADOIĆ, N.; OREŠKI, D. «Analysis of Student Behavior and Success Based on Logs in Moodle», *41st International Convention on Information and Communication Technology*, electronics and microelectronics, MIPRO 2018, Opatija [Croatia], 2018.

KITCHIN, R. *Getting smarter about smart cities: Improving data privacy and data security*. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland, January 2016. http://www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Report_J anuary_2016.pdf

KUMAR KAR, A.; GUPTA, M.P. *How to make a Smart Campus - Smart Campus Programme in IIT Delhi*, Indian Institute of Technology Delhi, 2015.

MARCOS PARAMIO, T. «El modelo de normalización español de Ciudades Inteligentes (UNE, CTN 178) y su impacto internacional», *III Congreso Ciudades Inteligentes*, 27/10/2017. Disponible en https://www.esmartcity.es/comunicaciones/comunicacion-modelo-normalizacion-espanol-ciudades-inteligentes

— *Las Normas para las Ciudades Inteligentes. Informe de situación*, octubre 2015. Disponible en http://www.agendadigital.gob.es/planes-actuaciones/

Bibliotecaciudadesinteligentes/Material%20complementario/normas_ciudades_inteligentes.pdf

MILENKOVIĆ, M.; VOJKOVIC, G. «GDPR in Access Control and Time and Attendance Systems Using Biometric Data», *41st International Convention on Information and Communication Technology*, electronics and microelectronics, MIPRO 2018, Opatija [Croatia], 2018.

NEDWICK, R. «Smart campus - merging smart city and smart home in education for digital natives», *Dotmagazine*, February 2018. Disponible en https://www.dotmagazine.online/new-work-and-digital-education/ICT4D/smart-campus-merging-smart-city-and-smart-home-in-education-for-digital-natives.

OZUPAK, Y.; CETINTAS, G.; KAYGUSUZ, A., «A smart campus integrated with smart grid», *International Artificial Intelligence and Data Processing Symposium (IDAP)*, 2017.

PIÑAR MAÑAS, J.L. (Dir). *Smart Cities. Derecho y técnica para una ciudad más habitable*. Madrid: Reus, 2017.

— *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid, Reus, 2016.

PISTORE, M. *Smart Campus Creating services WITH and FOR people*. Open Science Conference, 14 de agosto de 2013. Disponible en http://www.open-science-conference.eu/wp-content/uploads/2013/08/14_Marco_Pistore_-_Smart_Campus__Services_with_and_for_People.pdf

SARMIENTO, D. *El soft law administrativo. Un estudio de los efectos jurídicos de las normas no vinculantes de la Administración*. Navarra: Thomson Civitas, 2008.

TALARI, S.; SHAFIE-KHAH, M. «A Review of Smart Cities Based on the Internet of Things Concept». *Energies* (10), 2017. doi:10.3390/en10040421

VALKS, B., ARKESTEIJN, M.; den HEIJER, A. *Smart campus tools 2.0: An international comparison*. Delft University of Technology, 2018. Disponible en https://pure.tudelft.nl/portal/files/44031971/SCT_book_2018_ebook.pdf

VOJKOVIC, G. «Will the GDPR slow down development of Smart Cities?», *41st International Convention on Information and Communication Technology, Electronics and Microelectronics,* MIPRO 2018, Opatija [Croatia], 2018.

WIDYA SARI, M.; & WAHYU CIPTADI, P.; HARDYANTO, R. «Study of Smart Campus Development Using Internet of Things Technology», *IAES International Conference on Electrical Engineering, Computer Science and Informatics*, IOP Conf. Series: Materials Science and Engineering 190 (2017). DOI: 10.1088/1757-899X/190/1/012032.

8. GUÍAS E INFORMES DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Adaptación al Reglamento General por parte de las Administraciones Públicas* [en línea], 2018 [ref. 8 de marzo

de 2018]. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/Adaptacion_RGPD_AAPP.pdf

— *El Delegado de Protección de Datos en las Administraciones Públicas*. Disponible en: https://www.aepd.es/media/docs/funciones-dpd-en-aapp.pdf

— *El Esquema Nacional de Seguridad recoge las medidas debe aplicar el sector público para cumplir con los requisitos del RGPD en este ámbito*, 12 de diciembre de 2017. Disponible en https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_12_12-ides-idphp.php

— *Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD*. Disponible en: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

— *Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetos al RGPD*, febrero 2018. Disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf

— *Guía Sectorial de Protección de Datos y Administración Local*, febrero 2018. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_Proteccion_datos_Administracion_Local.pdf

Agencia Española de Protección de Datos; Autoritat Catalana de Protecció de Dades; Agencia Vasca de Protección de Datos. *Guía para el cumplimiento del deber de informar*, marzo 2017. Disponible en https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf

— *Guía del Reglamento de Protección de Datos para Responsables de Tratamiento*. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

Autoritat Catalana de Protecció de Dades. *Evaluación de impacto relativa a la protección de datos. Guía Práctica*, enero de 2018 - versión 2.0. [ref. de 8 de marzo de 2018]. Disponible en http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-EVALUACION-DE-IMPACTO-CAST-2.0.pdf.

— *La protecció de dades de caràcter personal en les ciutats intel·ligents* («Smart Cities»), Barcelona, febrero de 2013.

Information Commissioner Office. *Big data, artificial intelligence, machine learning and data protection*, Versión 2.2, 4 de septiembre de 2014, Disponible en https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

— *Data Protection Impact Assessments (DPIAs)*, 2018. Disponible en https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/.

GRUPO DE TRABAJO DEL ARTÍCULO 29. *Directrices sobre los delegados de protección de datos (DPD)*, 16/ES WP 243 rev.01, 13 de diciembre de 2016 [revisión 5 de abril de 2017].

— *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, WP251rev.01, revisadas y actualizadas a 6 de febrero de 2018.

— *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*, WP 248 rev.01, 4 de abril de 2017 [revisadas 4 de octubre de 2017].

— *Dictamen 03/2017 sobre el tratamiento de los datos personales en el contexto de los sistemas de transporte inteligentes (STI) cooperativos*, WP252, 4 de octubre de 2017.

— *Opinion 8/2014 on the on Recent Developments on the Internet of Things.* WP223, 16 de septiembre de 2014.

— *Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force, WP209*, febrero de 2013.

— *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, WP180, 11 de febrero de 2011.

— *Opinion 12/2011 on smart metering*, WP 183, 4 de abril de 2011.

9. RELACIÓN DE NORMAS TÉCNICAS COMENTADAS

AEN/CTN 178. UNE 178201:2016. *Ciudades inteligentes. Definición, atributos y requisitos*. Abril de 2016.

CTN 71. UNE-EN ISO/IEC 27001. *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos*. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015). Mayo 2017.

CTN 178. UNE 178104:2017. *Sistemas Integrales de Gestión de la Ciudad Inteligente. Requisitos de interoperabilidad para una Plataforma de Ciudad Inteligente*. Diciembre 2017.

ÍNDICE