Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

Transparencia, ciberseguridad e identidad digital en el entorno 5G

Clara Rodríguez Ilárraz[1]

Universidad CEU San Pablo
Madrid

España

ORCID: 0009-0004-1080-4544

Ricardo J. Palomo Zurdo[2]

Universidad CEU San Pablo
Madrid

España

ORCID: 0000-0002-4243-6684

RECIBIDO: 31 de mayo de 2023
ACEPTADO:24 de noviembre de 2023

RESUMEN: El espíritu de la Directiva europea 2022/2555, conocida como NIS 2, en materia de ciberseguridad y del Real Decreto-ley 7/2022, de 29 de marzo, conocido como Ley de Ciberseguridad 5G, es que se promueva la creación e implementación de normas comunes, correspondientemente certificadas, en el ámbito de la ciberseguridad, en aras de favorecer la transparencia y la resiliencia del Mercado Único Digital Europeo. En este sentido, el sector de los prestadores de servicios de confianza, cuya normativa está siendo actualmente objeto de debate (denominada eIDAS 2), es el mejor ejemplo del uso de la estandarización en la que podría llamarse sociedad digital. En este trabajo se analiza la relación jurídica entre la ciberseguridad, la identidad digital y la transparencia, debido al nuevo escenario que implica la irrupción de la era de la Quinta Generación (TIC-5G) de telecomunicaciones y la convergencia de las tecnologías que la integran.

PALABRAS CLAVE: Ciberseguridad, transparencia, resiliencia, identidad digital, 5G.

[1] Investigadora en formación del programa de Derecho y Economía de la Escuela Internacional de Doctorado CEU (CEINDO).

[2] Catedrático en Universidad CEU San Pablo, Madrid.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

Transparency, Cybersecurity and Digital Identity in the 5G Context

ABSTRACT: The purpose of the European Directive 2022/2555, known as NIS 2, on cybersecurity, and the Spanish Royal Decree-Law 7/2022, of March 29, known as the 5G Cybersecurity Law, is to encourage the creation and implementation of common standards, correspondingly certified, in the field of cybersecurity, in order to enhance the transparency and resilience of the European Digital Single Market. In this regard, the sector of trust services providers, whose regulations are currently being discussed (referred to as eIDAS 2), is the prime example of the use of standardization in what could be termed the digital society. This paper analyzes the legal relationship between cybersecurity, digital identity, and transparency, in the light of the new scenario that emerges with the advent of the Fifth Generation (ICT-5G) of telecommunications and the convergence of the technologies that it encompasses.

KEYWORDS: Cybersecurity, transparency, resilience, digital identity, 5G.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

1.- Introducción

La cuarta revolución industrial, caracterizada por la aplicación intensiva de la ciencia informática, de la innovación de base tecnológica y la convergencia de nuevas tecnologías disruptivas como el 5G, está transformando la sociedad, crecientemente digitalizada. Inclusive, cabría preguntarse si no se ha iniciado ya una quinta revolución industrial con una clara tendencia hacia la creación de sociedades inteligentes, con un fuerte componente de transparencia, así como de sostenibilidad, si bien, la mera sostenibilidad, entendida como la reducción o eliminación de los efectos negativos de la actividad humana sobre el medioambiente, mejoraría con una economía circular, que lograría «un impacto positivo sobre el medioambiente, incrementando el valor, la productividad y la calidad de los recursos materiales» (PALOMO ZURDO, R., RODRÍGUEZ-MARTÍN, A. y GONZÁLEZ-SÁNCHEZ, F. 2020: 240).

La evolución exponencial de la tecnología parece adelantarse al legislador europeo en materia digital, que nació con el inicio del Mercado Único Digital Europeo (MUDE) en el año 2015, fruto del proceso de liberalización nacional y europeo del sector de las telecomunicaciones, con la consiguiente supresión de todas las barreras nacionales digitales, como las tarifas de itinerancia, la antigua imposibilidad de portabilidad transfronteriza de los servicios en línea o el geobloqueo.

Actualmente la Sociedad Digital europea está regulada aún desde una perspectiva de centralización propia de las generaciones anteriores a la Quinta Generación (5G), implantándose, a partir de ahora, un modelo descentralizado, con los menores intermediarios posibles, e interconectado de forma permanente y cada vez más global, que implica que no se puede tener en cuenta de forma aislada la ciberseguridad, sin tener en consideración también la seguridad física o la configuración de la identidad digital de ciudadanos, empresas e instituciones y también, de las "cosas" conectadas. Para ello, es necesario la creación de un entorno 5G gobernado por el principio de transparencia.

El modelo descentralizado 5G y la siguiente, la Sexta Generación (6G), (i) pretende aliviar el exceso de almacenamiento de los datos que generamos, gracias a la tecnología de la computación en el borde o *edge computing*, esto es, en los dispositivos o *hardware* que se encuentran a una mayor aproximación al usuario, en unión con el conocido almacenamiento en la nube o *cloud computing*, para garantizar una baja latencia, en convergencia con otras tecnologías, (ii) la interconexión entre personas, objetos y cuerpos en tiempo real, de forma ininterrumpida (*IoT/IoC*, por sus siglas en inglés) y (iii) la eficiencia y el ahorro energético en el uso de las redes y del espectro radioeléctrico.

Puede afirmarse que tres son los conceptos con los que mayormente se define el 5G. En primer lugar: el de virtualización de la red, que permite el uso de redes y la distribución de servicios por capas (*network slicing*), según las prioridades de servicio que se establezcan. En segundo lugar: la computación en el borde (*edge computing)* y, en tercer lugar, la descentralización de las comunicaciones, con mejora de la seguridad de las redes, apostándose por la certificación.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

1.1.- La transparencia en el entorno de la tecnología 5G

La transparencia en sus múltiples facetas se ha convertido en uno de los valores fundamentales de las democracias del siglo XXI y en uno de los principios más reclamados por la ciudadanía (MARTÍN DELGADO 2021: 14). Debe tenerse en cuenta que, en la Sociedad Digital, no debe hablarse de usuarios, en lugar de ciudadanía. Y precisamente para la regulación de un entorno garantista virtual, es necesaria la aplicación holística del principio de transparencia.

En este sentido, el Reglamento 2022/868 relativo a la gobernanza europea de datos, conocido como Reglamento de Gobernanza de Datos[3], plantea la transparencia como premisa fundamental para la integración de la actividad de las administraciones públicas, con el sector privado. Y «a fin de aumentar la transparencia [...] debe fomentarse el establecimiento de mecanismos de certificación», de acuerdo con el Considerando 100 del Reglamento General de Protección de Datos (RGPD)[4].

Por tanto: la transparencia no solo implica la obligación y el derecho de información, o de acceso a una información pública, sino también la creación de mecanismos de certificación y normalización. Así, la funcionalidad añadida de la certificación consiste en que «adquiere una importancia transversal porque goza de presunción *iuris tantum*» (VIGURI CORDERO, J.A. 2018: 10), disminuyendo -e incluso-, pudiendo llegar a evitar, la imposición de sanciones. La certificación resulta interesante para los agentes del mercado digital, además, porque les dota de un elemento diferenciador que les otorga una mayor competitividad.

El principio de transparencia pertenece a los Derechos de Libertad, como señala la Carta de Derechos Digitales española (2022: 9, 10)[5], aunque la vía de la certificación parezca imponer mayores barreras, especialmente a las Pequeñas y Medianas Empresas (PYMEs). Por ello, el Gobierno de España, en el Marco Estratégico en Política de PYME 2030 (2019: 73)[6] ya preveía «ofrecer un sistema de incentivos a las PYMEs que están certificadas con arreglo al Sistema de Gestión y Auditoría Medioambientales (EMAS), ISO 14000 o ISO 50001, y ayudar a las microempresas y las pequeñas empresas a aprovechar sistemas simplificados del tipo EMAS, como «EMAS-EASY». Además, en la Sociedad Digital, también debe tenerse en cuenta el principio de transparencia algorítmica, tal y como pone de relieve COTINO HUESO (2023: 19). Es esencial para el control de los sesgos de la tecnología y favorece la

[3] Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

[4] 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 (RGPD).

[5] "Carta de Derechos Digitales", Gobierno de España, 2019.

[6] "Marco Estratégico en Política de PYME 2030", Gobierno de España, 2019. Disponible en: https://industria.gob.es/es-es/Servicios/MarcoEstrategicoPYME/Marco%20Estrat%C3%Aggico%20PYME.pdf

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

transmisión y facilitación de información y conocimiento para toda la ciudadanía (COTINO HUESO (2023: 20).

Por todo ello, el progreso de la sociedad digital, al menos desde la consideración del legislador europeo, no puede entenderse sin control de sesgos o de discriminación de ningún tipo, ni tampoco sin interoperabilidad entre los distintos sistemas, especialmente en un entorno 5G conectado ininterrumpidamente. Desde el punto de vista técnico, la seguridad y privacidad desde el diseño y por defecto es necesaria, así como el establecimiento y cumplimiento de estándares normalizados y certificables, en aras de fomentar la transparencia y, por tanto, el crecimiento y la confianza en la Sociedad Digital europea.

En un entorno descentralizado 5G, el uso de la cadena de bloques o *DLT*[7], el *Blockchain*, o sus nuevas variantes acíclicas, denominadas *DAG*[8], por sus acrónimos en inglés, para el almacenamiento y rastreo de la información, incrementaría el nivel de seguridad en términos de disponibilidad, confidencialidad e integridad de los datos (CORTES VELES, J.J. 2021: 8). De hecho, ya es una realidad gracias a la Infraestructura europea de Servicios *Blockchain* (*EBSI*)[9]. De acuerdo con PALOMO ZURDO, «la tecnología Blockchain promete ser la mayor revolución tecnológica global después de la aparición de Internet» (2020: 18).

1.2.- Ciberseguridad en el entorno de la tecnología 5G

Actualmente en Europa está vigente la Directiva 2016/1148[10], denominada NIS 1, que ha sido traspuesta al ordenamiento jurídico español a través del Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de la información. En enero del año 2020 la Comisión Europea anunció la revisión de la NIS 1 y, en el año 2022, se aprobó y publicó la NIS 2[11], que entrará en vigor a partir del 18 de octubre de 2024.

Las novedades que incorpora la Directiva NIS 2 son: (i) que las medidas para la gestión de riesgos de ciberseguridad deben basarse en un planteamiento que abarque todos los riesgos y tenga por objetivo proteger también el entorno físico de dichos sistemas (Considerando 79 NIS 2); (ii) que se mantienen, como *lex specialis*, la normativa específica para entidades financieras[12], denominada Reglamento DORA, y

[7] Distributed Ledger Technology (DLT).

[8] Directed Acyclic Graph (DAG).

[9] *Vid*. Infraestructura Europea de Servicios Blockchain (EBSI). Más información disponible en: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

[10] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

[11] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (NIS 2).

[12] Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero (Reglamento DORA).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

la de los prestadores de servicios de confianza, cuyo Reglamento es el que está siendo actualmente revisado, denominado Reglamento eIDAS[13]; (iii) que se extiende el alcance de la norma a los propios prestadores de servicios de confianza, estableciendo la propuesta del eIDAS 2 (2021: 5)[14] que pretende «reducir la fragmentación en la aplicación de los requisitos generales en materia de ciberseguridad». Se extiende su alcance también a las medianas y grandes empresas que operan dentro de los sectores de actividad recogidos en sus anexos, así como a las pequeñas empresas y microempresas que tengan un papel clave para la sociedad, la economía o determinados sectores; (iv) se regulan los proveedores de plataformas de servicios de redes sociales; (v) se incluyen, los que se espera que sean, los futuros centros de seguridad o *SOC*, por sus siglas en inglés, 5G, que son los proveedores de gestión de servicios TIC (de empresa a empresa); (vi) se integran en el sector de infraestructuras digitales a los proveedores de servicios de centro de datos, los proveedores de redes públicas de comunicaciones electrónicas y los proveedores de servicios de comunicaciones electrónicas disponibles para el público y (vii) se distingue entre entidades esenciales e importantes.

Además de la anterior regulación, las infraestructuras críticas se rigen por una normativa distinta a la NIS 1, que es la Directiva 2022/2557 relativa a la resiliencia de las entidades críticas, que todavía no se ha traspuesto al ordenamiento jurídico español aplicándose, hasta que llegue ese momento, la Ley 8/2011 por la que se establecen medidas para la protección de infraestructuras críticas.

Por su parte, la Ley de Ciberseguridad 5G (LC5G) prevé especificaciones que se abordan en este trabajo, estando la normativa propia del sector de infraestructuras digitales (centros de datos, entre otros), del sector de infraestructuras críticas, del sector de servicios de TIC de empresa a empresa y la propia del sector de telecomunicaciones, de los operadores 5G y de los proveedores de servicios de confianza, entrelazada en materia de ciberseguridad. Todo ello en aras de promover una mayor transparencia y confianza, resultando de vital importancia la salvaguarda de las cadenas de suministro y la implementación de mecanismos de información coordinada entre las distintas autoridades competentes en materia de supervisión de la ciberseguridad en los entornos 5G.

1.3.- La Identidad Digital y las certificaciones de la tecnología 5G

La propuesta eIDAS 2 en materia de identidad digital está orientada a la creación de un monedero digital de identidad europeo o *European Digital Identity Wallet* (*EDIW*, por su acrónimo en inglés), que deberá operar también en un entorno 5G descentralizado.

[13] Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS).

[14] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea (eIDAS 2).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

Cabe mencionar que la propuesta eIDAS 2 hace referencia directamente a la Directiva NIS 2, en su artículo 21.2, en el que establece que «el organismo de control verificará si el prestador de servicios de confianza y los servicios de confianza que presta cumplen los requisitos establecidos en el presente Reglamento, y [...] la conformidad del proveedor de servicios de confianza con los requisitos establecidos en el artículo 18 de la Directiva XXXX [SRI 2] (NIS 2), el organismo de control solicitará a las autoridades competentes en virtud de la citada Directiva que lleven a cabo actuaciones de control en ese sentido [...]». Ello implica que los prestadores de servicios de confianza, sujetos a una normativa estricta y estandarizada, deberán también tener en cuenta en su evaluación de la conformidad los requisitos técnicos en materia de ciberseguridad que se determinen con la trasposición de la Directiva NIS 2. En este trabajo se estudia el modelo de identidad digital que se está creando en Europa y que constituye el mejor ejemplo de cara a la implementación de los esquemas de certificación 5G, atendiendo todo ello a los aspectos relacionados con el principio de transparencia, que constituye el fundamento de la confianza (OLIVARES DELGADO, F. 2018:476).

La Directiva NIS 2 y el entorno 5G, así como el futuro Reglamento eIDAS 2, tienen en común que serán implementados a través de normas estandarizadas. Para no sobrecargar a las entidades, es aconsejable establecer criterios comunes entre las referidas normas.

2.- Normativa y operadores en el entorno de la tecnología 5G

La normativa aplicable a las redes 5G de forma específica está conformada, por el momento, por la Recomendación europea 2019/534 sobre ciberseguridad, de 26 de marzo de 2019[15] y el Real Decreto-Ley 7/2022, de 29 de marzo, sobre los requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de Quinta Generación (Ley de Ciberseguridad 5G o LC5G), que sobre las redes 5G establece en su Preámbulo que «son claves para cumplir con los ambiciosos objetivos de descarbonización y reducción de emisiones de gases de efecto invernadero asumidos en el ámbito europeo para el año 2030, ya que facilitan la aparición de nuevos servicios inteligentes máquina a máquina (redes eléctricas inteligentes, logística inteligente, ciudades inteligentes, sistemas de producción inteligente) y la sustitución de determinadas actividades a la implantación de nuevas fuentes de energía limpias y renovables».

Por su parte, la Ley General de Telecomunicaciones, 11/2022 (LGT22), viene a implementar, entre otras, la Directiva por la que se establece el Código Europeo de Comunicaciones Electrónicas (CECE)[16], que sobre el 5G afirma que «es probable que estas redes se desarrollen fuera de los edificios y en las carreteras, para el transporte, la energía, investigación y desarrollo, la sanidad en línea, la protección pública y el socorro en caso de catástrofes, el internet de las cosas, la comunicación

[15] Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, sobre Ciberseguridad de las redes 5G. Disponible en: https://www.boe.es/doue/2019/088/L00042-00047.pdf

[16] Directiva (UE) 2018/1972 por la que se establece el Código Europeo de las Comunicaciones Electrónicas (CECE).

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

máquina a máquina y los vehículos conectados, destacando su alta conectividad ininterrumpida y resaltando los riesgos de la conectividad transfronteriza». De hecho, en la *Memoria de Impacto Normativo* (Ministerio de Asuntos Económicos y Transformación Digital 2021: 15), sobre el anteproyecto de la referida LGT22, se afirma que «las redes 5G se sitúan como el motor de transformación digital de la sociedad y la economía, contribuyendo en la lucha contra la despoblación, la brecha digital y el cambio climático».

Por el momento no hay una sobrerregulación, pero sí que se introducen cambios significativos, especialmente en materia de modelos de almacenamiento, cooperación y clasificación de sectores y servicios, así como en materia de notificación y supervisión de ciberseguridad, lo que afectará directamente a las políticas y procedimientos de las empresas, tanto públicas como privadas, en aras de poder garantizar el principio de transparencia en el cumplimiento de sus obligaciones legales.

Concretamente, con las redes 5G se pasa de un modelo centralizado de comunicaciones, a un modelo descentralizado autogobernado por cada usuario y en el que convergen distintas tecnologías, como la inteligencia artificial y el *Blockchain* y este cambio de paradigma, desde la centralización a la descentralización, requiere un entorno digital confiable, seguro y, por tanto, transparente.

2.1.- La dimensión del principio de transparencia en los operadores, suministradores y usuarios corporativos 5G

La LC5G introduce en nuestra legislación nacional tres nuevas figuras: los operadores, los suministradores y los usuarios corporativos 5G.

En primer lugar, los operadores 5G, que se definen en el artículo 3.1.a) LC5G como «la persona física o jurídica que instala, despliega o explota redes públicas 5G o presta servicios 5G disponibles al público a través, total o parcialmente, de las redes 5G, disponga de red 5G propia o no, y ha notificado al Registro de operadores el inicio de su actividad o está inscrita en el Registro de operadores».

De esta definición resulta bastante llamativa la distinción entre red púbica y red propia, un fenómeno que no ha ocurrido hasta ahora. Ello se debe al avance de la tecnología espectral que permite, con una capacidad cada vez mayor, un uso más eficiente del espectro radioeléctrico, así como la determinación del uso de las frecuencias que se utilizan y la generación de redes virtuales.

La virtualización de las redes permite la creación de redes propias por parte de los operadores, las administraciones públicas, los suministradores y los usuarios corporativos 5G. Hay muchos usos potenciales dentro de una sola banda de frecuencias gracias a la virtualización de la red 5G.

El modelo 5G está basado en una infraestructura de uso común, en la que el *software* adquiere el protagonismo, incluso, para la configuración de la red y los servicios 5G. Concretamente, se aplica una técnica denominada *network slicing,* gracias a la

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

virtualización de la red, que implica que se puedan ampliar y personalizar los recursos de red de manera flexible para satisfacer las necesidades de los usuarios, cuya gestión requiere tanto de sistemas de *software* complejos, como de proveedores para la orquestación o automatización de los referidos recursos. La organización 3rd Generation Partnership Project (3GPP), que es una asociación de empresas de telecomunicaciones que tiene como fin desarrollar estándares para las tecnologías de la comunicación móvil, reconoce la gestión de la red por capas, lo cual permite una estructura vertical de la red, encontrándose el organismo europeo de estandarización ETSI trabajando en la normalización de los sistemas virtuales de red, su funcionamiento, seguridad y demás especificaciones técnicas, siguiendo también las previstas por el grupo 3GPP. El diseño de la red virtualizada por capas en entornos descentralizados demanda una actuación transparente como mecanismo para desencadenar cambios profundos en ámbitos distintos y mayor credibilidad en las organizaciones (WANDEN-BERGHE LOZANO, J. L. y FERNÁNDEZ DAZA, E. 2020:132), así como en la Administración Pública, que también deberá cumplir con el principio de transparencia y obtener las correspondientes certificaciones.

Además, cabe mencionar que la investigación científica señala que será necesario no solo la tecnología del *edge computing* y *network slicing*, sino también nuevas soluciones de gestión de la movilidad en las ciudades (Nowak, T.W., *et. al.* 2021:4), pues la aplicación del *network slicing* se está concibiendo de acuerdo con las características específicas de cada negocio, habiendo ya casos de uso reales, fundamentalmente, en los sectores de automoción, logística, energía, salud, educación, seguridad pública, medios de comunicación y ciudades inteligentes. En este contexto adquieren especial relevancia los acuerdos de calidad de servicio (*QoS*, por sus siglas en inglés), que determinarán la velocidad de las transmisiones por servicios o capas, junto con el uso de los productos y servicios TIC-5G. La transparencia respecto de estos acuerdos de calidad de servicio también se hace necesaria para evitar conflictos de competencia entre operadores y una deficiente prestación de servicios de telecomunicaciones 5G a los usuarios.

En segundo lugar, los suministradores 5G se definen en el punto *f)* del artículo 3.1 LC5G como «el fabricante, el representante autorizado, el importador, el distribuidor, el prestador de servicios logísticos o cualquier otra persona física o jurídica sujeta a obligaciones en relación con la fabricación de productos, su comercialización o su puesta en servicio en materia de equipos de telecomunicación, los suministradores de *hardware* y *software* y los proveedores de servicios auxiliares que intervengan en el funcionamiento u operación de redes 5G o en la prestación de servicios 5G», pudiendo ser personas físicas o jurídicas.

A los suministradores 5G no se les aplica, por norma general, la Directiva NIS 2 ya que no se encuentran dentro del sector de infraestructura digital. No obstante, por medio de la excepción prevista en el artículo art. 2.2, puntos *c) y d)* NIS 2, sí que cabría la posibilidad, de forma excepcional, la aplicación de la NIS 2 a alguna entidad suministradora 5G, en caso de «una perturbación del servicio prestado que pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública», o bien, cuando «una perturbación del servicio prestado pudiera

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo».

De acuerdo con la LC5G, las obligaciones de los suministradores 5G «serán objeto de concreción y desarrollo en el Esquema Nacional de Seguridad de redes y servicios 5G (artículo 13.2 LC5G)». Es importante señalar que, actualmente, mientras continúa vigente la NIS 1 y el Real Decreto-ley 12/2018 referidos anteriormente, el Esquema de Seguridad Nacional se regula en el Real Decreto 311/2022, de 3 de mayo y es aplicable a todo el sector público. Sin embargo, a partir de la entrada en vigor de la NIS 2, las administraciones públicas también quedan, algunas de ellas, incluidas en el ámbito de aplicación de la NIS 2, lo cual previsiblemente provocará una nueva modificación del Esquema Nacional de Seguridad (ENS).

El ENS-5G, o Esquema Nacional de Seguridad 5G, es aplicable, una vez realizado, a los operadores, suministradores y usuarios corporativos 5G, de acuerdo en los artículos 4 y 16 LC5G. Llama la atención que el ENS 5G no hace referencia al principio de transparencia, cuando el Esquema Nacional de Seguridad (ENS) lo recoge del artículo 129 de la Ley 39/2015, de 1 de octubre, que establece los principios de buena regulación, que son el de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia. De acuerdo con esto, es importante señalar que el principio de transparencia debe ser tenido en cuenta también como principio de buena regulación o de buen gobierno.

Por otro lado, cabe añadir que la autoridad competente para la aprobación del ENS 5G es el Gobierno, mediante Real Decreto, a propuesta del Ministerio de Asuntos Económicos y Transformación Digital, previo informe del Consejo de Seguridad Nacional. Su creación es fruto de la citada Recomendación 2019/534 sobre la ciberseguridad de las redes 5G que incluso determina la realización de un análisis de riesgos a nivel nacional. En relación con este asunto, cabe resaltar el análisis de riesgos de las redes 5G, realizado en octubre de 2019, por el Grupo de Cooperación NIS europeo que establece cinco escenarios de riesgos concretos en el entorno 5G: (a) aquellos generados por la aplicación de medidas de seguridad insuficientes, (b) aquellos relacionados con la cadena de suministro 5G y (c) otros relacionados con el *modus operandi* de los *hackers*, revistiendo especial importancia las técnicas de ingeniería social para la vulneración de la seguridad de los sistemas de información e infraestructuras críticas.

Asimismo, el ENS 5G también debe hacer referencia a los riesgos relacionados con la interdependencia de las redes 5G con otros sistemas o servicios, especialmente con los de carácter crítico y aquellos derivados del uso del *IoT* o internet de las cosas, y la conexión ininterrumpida. Precisamente estos riesgos analizados a nivel europeo se tendrán que concretar ahora en el correspondiente análisis de riesgos realizado por cada Estado miembro.

Además, el Gobierno, mediante acuerdo adoptado en Consejo de Ministros y previo informe del Consejo de Seguridad Nacional, podrá calificar a determinados suministradores 5G como de alto riesgo (artículo 14.1 LC5G) que no podrán utilizar en los elementos críticos de red ningún recurso o servicio, ni podrán acceder a una red pública 5G, especialmente, cuando se trate de estaciones radioeléctricas con las que se proporcione cobertura a centrales nucleares, centros vinculados a la Defensa

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

Nacional, etc. Si un suministrador de alto riesgo utiliza sus equipos únicamente en redes privadas 5G o para la prestación de servicios 5G en régimen de autoprestación, será calificado como suministrador de riesgo medio (artículo 14.6 LC5G).

Esta calificación es importante porque los suministradores 5G de riesgo medio y alto deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital, cada dos años, «una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos», de acuerdo con el artículo 13.5 LC5G.

Por lo tanto: el ENS 5G, aunque no mencione explícitamente el principio de transparencia, aboga por la objetividad de la información, así como por el principio de publicidad, pues ambos buscan garantizar la moralidad e imparcialidad de la Administración Pública en la designación de las empresas que van a ser consideradas suministradores de alto o medio riesgo (DUQUE BOTERO, J.D. 2020: 79).

En tercer lugar, los usuarios corporativos 5G, definidos como la «persona física o jurídica que instala, despliega o explota redes privadas 5G o presta servicios 5G a través, total o parcialmente, de las redes 5G, para fines profesionales o en autoprestación», pudiendo tener «otorgados derechos de uso del dominio radioeléctrico para la instalación de una red privada 5G o prestar servicios profesionales o en autoprestación», constituyen la figura más innovadora del sector digital. Los usuarios corporativos 5G, o bien tendrán otorgados derechos de uso del dominio público radioeléctrico para explotar una red privada, o bien prestarán servicios 5G, en régimen de autoprestación, pudiendo ser con fines profesionales. El uso privativo del espectro supone la utilización de determinadas frecuencias de forma exclusiva, por un número limitado de usuarios situados en un mismo ámbito físico de aplicación. Estos usuarios corporativos 5G en régimen de autoprestación deberán solicitar una licencia de uso privativo del espectro a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID), dependiente del Ministerio de Asuntos Económicos y Transformación Digital. Además, hagan uso o no del espectro de forma privativa, los usuarios corporativos 5G deben tener en cuenta las medidas generales de valoración de riesgos que son comunes al resto de los operadores 5G y la adopción de medidas específicas previstas en la LC5G, como: (i) el examen de las vulnerabilidades ligadas a la cadena de suministro de las redes y servicios 5G (art.22.2.*b)* LC5G), (ii) la evaluación de su grado de dependencia con los suministradores 5G y (iii) las medidas a adoptar en caso de interrupción del suministro.

De acuerdo con lo anterior, el principio de transparencia va a vertebrar, en realidad, el entorno 5G, en sus dos grandes dimensiones: la objetividad de la información, que debe ser relevante, exacta y clara y la percepción de la imagen divulgada, que ha de ser percibida como comprensible y completa por los usuarios. Tanto los operadores, como los suministradores y los usuarios corporativos 5G deben recabar la información objetiva prevista en la legislación, así como realizar las correspondientes auditorías y obtener las certificaciones necesarias para que todos ellos puedan ser percibidos por el supervisor como entidades que cumplen con la normativa. La cuestión es que un operador 5G puede ser al mismo tiempo un operador de telecomunicaciones, sujeto entonces al cumplimiento de la Directiva

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

NIS 2 y el ENS, así como también a la LC5G y al ENS 5G. Ello generaría multitud de certificaciones que, en realidad, están basadas en la implementación de normas que establecen numerosos criterios comunes e igualmente válidos para su implantación en un esquema de certificación por servicios, como ocurre con el esquema de certificación de los prestadores de servicios de confianza.

2.2.- Análisis de la problemática de la determinación de la responsabilidad en el entorno 5G

Además de la organización 3GPP referida, cuyas normas en materia de 5G han sido validadas internacionalmente (3GPP 5G-SRIT, 3GPP 5G-RIT y 5Gi), la Comisión y la industria europeas de fabricantes de TIC, operadores de telecomunicaciones, proveedores de servicios, PYMEs e instituciones de investigación, conforman una iniciativa conjunta desde el año 2018, denominada 5G-PPP (Public, Private, Partnership), que tiene como fin ofrecer estándares para las infraestructuras 5G en Europa. Los proyectos en curso son parte de las dos últimas fases (Fase 3.5: Proyectos 5G Core y CAM y Fase 3.6: Innovaciones 5G y más allá de 5G) y abordan las necesidades de cuatro convocatorias de propuestas diferentes en el marco del programa de trabajo H2020, que son: (a) H2020-ICT-41: Innovaciones 5G para verticales con servicios de terceros; (b) H2020-ICT-42: Innovación en tecnologías centrales 5G; (c) H2020-ICT-52: Conectividad inteligente más allá de 5G; (d) H2020-ICT-53: 5G para Movilidad Conectada y Automatizada. En el *White Paper* del grupo 5G-PPP sobre la arquitectura de seguridad inteligente de las redes 5G (5G-PPP 2022: 1), se concluye que el proyecto europeo INSPIRE-5Gplus ofrece una innovadora orquestación de seguridad definida por *software* y un marco de gestión que promueve el cambio hacia una seguridad totalmente automatizada e inteligente, ideal para los sistemas conectados y servicios omnipresentes 5G.

La gestión de la seguridad avanzada se construye partiendo de una arquitectura denominada *Zero-touch Service Management* (*ZSM*) que permite la automatización de tareas, la eficiencia en la prestación de los servicios y la mínima intervención manual. Los estándares de esta arquitectura están siendo objeto de elaboración por ETSI y suponen una automatización completa de extremo a extremo en las comunicaciones para garantizar agilidad y velocidad de los servicios ofrecidos por los proveedores de servicios digitales. El objetivo de esta automatización es habilitar redes autónomas capaces de autoconfigurarse y autorrepararse sin intervención humana adicional, tecnología que utiliza el proyecto europeo INSPIRE-5Gplus (ETSI. 2021: 1). La tecnología de cadena de bloques o *Blockchain* «ofrece transparencia al poder ligar todas las transacciones de redes virtuales, lo que a su vez ofrece inmutabilidad» (LLAMAS COVARRUBIAS. 2021: 37) que, como se analiza posteriormente, no resulta compatible con el ejercicio de algunos derechos de protección de datos, pero existen soluciones técnicas aplicables.

El sistema 5G, en su conjunto, se visualiza como una red virtual y automatizada de extremo a extremo, con una arquitectura basada en servicios y definida por *software* de redes (*SDN*, por su acrónimo en inglés), virtualización de las funciones de red (*NFV*), gestión del ciclo de vida para respaldar el sistema 5G y orquestación de recursos de operadores de red. En este entorno es indispensable la aplicación del llamado derecho de explicación, tal y como pone de relieve BONMATÍ SÁNCHEZ (2020: 355), pues la automatización inteligente en la toma de decisiones no podría

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

resultar plenamente transparente, sin el derecho de los usuarios a conocer el cómo y el por qué.

De hecho, en el entorno descentralizado que es aplicable al del 5G, se pueden identificar roles adiciones, como los agregadores de servicios en varias capas, el agregador de servicios de red, el agregador de infraestructura y el agregador de centro de datos, así como el agregador del espectro (5G-PPP. 2021: 12). Estos roles se pueden desempeñar mediante actividades de prestación de servicios, pudiendo operar en entornos transfronterizos o entornos mixtos de red públicos y privados, esperándose una alta interacción entre los roles propios de las tecnologías de la información y sistemas tradicionales y los roles de los operadores 5G, y otros como el proveedor del sistema a clientes verticales.

Ante esta casuística, todos ellos deberán ser calificados, según corresponda, como responsables, corresponsables, encargados del tratamiento, cedentes o cesionarios, pudiendo resultar extremadamente complicado discernir entre las responsabilidades de cada uno de los operadores y proveedores participantes en este entorno. La Agencia Española de Protección de Datos (AEPD) ya identificó que, en el entorno 5G, el reparto de responsabilidad entre fabricantes, operadores de red y proveedores de servicios «podría llevar a problemas de ambigüedad en cuanto a la responsabilidad por el tratamiento de los datos [..] de cada una de las partes, quedando diluida» (AEPD. 2020: 10).

Teniendo en cuenta estos hechos, parece inevitable que el 5G sea propicio para la generación de un gran volumen de todo tipo de datos, no solo personales que, en todo caso, deberán ser protegidos conforme a las garantías europeas. Además, la identidad digital es la huella que toda persona deja en su uso e interacción en los medios y plataformas digitales. Por ello, en la sociedad digital, la posibilidad de los ciudadanos de decidir sobre los atributos de identidad que comparten, o que crean, debería incluir también que estos pudieran hacer uso de un pseudónimo para identificarse en este entorno, tal y como defiende ADSUARA VARELA (2022: 53), debiéndose analizar caso por caso y, de forma especializada, cada conflicto que pueda suscitarse en este entorno, cada vez, más complejo, debiendo regir en todo ello el principio de transparencia que opera como principio de buen gobierno, de acuerdo con el referido artículo 129 de la Ley 39/2015.

2.3.- Análisis de riesgos, medidas de transparencia y responsabilidad proactiva en el entorno 5G

Para garantizar un entorno de transparencia o cumplimiento normativo, es necesario que las organizaciones y las empresas prevean políticas y procedimientos que contemplen la medición del riesgo y la criticidad de sus infraestructuras y servicios. En el entorno 5G, se consideran elementos críticos los relativos a las funciones del núcleo de la red, los sistemas de control y gestión y los servicios de apoyo, así como la red de acceso de aquellas zonas geográficas y ubicaciones que se determine (art. 6.3 LC5G).

La separación entre la seguridad de la infraestructura, o parte de ella, de la ciberseguridad, plantea problemas de supervisión y de notificación de incidentes. Gracias a la aplicación del principio de transparencia, se fomentaría la cooperación

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

entre los supervisores y los organismos competentes en materia de notificación de incidentes -denominados *CSIRTs/CERTs* o *SOCs*, por sus acrónimos en inglés-, además de la conformación de criterios entre las normativas de aplicación. La Directiva NIS 2 apuesta, en su Considerando 52, por las herramientas y aplicaciones de ciberseguridad de código abierto para facilitar la interoperabilidad entre las herramientas de seguridad, permitir la diversificación de los proveedores, propiciar un proceso de detección de vulnerabilidades a cargo de la comunidad, así como un proceso de verificación más transparente.

Sobre el análisis de riesgos, faltaría por determinar en el ENS 5G el uso de soluciones de autenticación y la introducción de políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado, de acuerdo con los puntos *j)* y *h)* del artículo 21.2 NIS 2. También, sobre las medidas de transparencia, cabe resaltar que no se recogen en la LC5G, pero sí en la NIS 2, en el referido Considerando 52, se destaca la transparencia como parte de la estrategia de seguridad. El sistema de código abierto (*OSS*, por sus siglas en inglés) anteriormente comentado, posibilita una explotación libre de la invención tecnológica por medio de distintas plataformas colaborativas. Una estrategia contraria a la de China, por ejemplo, que ha optado por el registro de patentes y la elaboración de documentos de estandarización que las incluyan para que su aplicación sea mayor, en comparación con la aplicación de las patentes europeas. Por otro lado, la adopción de medidas de responsabilidad proactiva constituye una cuestión central.

Actualmente, con la NIS 1, todavía en vigor, se distingue entre operadores de servicios esenciales y operadores de servicios digitales, una denominación que cambia profundamente con la NIS 2, que introduce nuevos sectores y subsectores, como se ha mencionado al comienzo de este trabajo y, además, la distinción entre entidades esenciales e importantes. Las medidas de responsabilidad proactiva constituyen una cuestión fundamental porque la NIS 2 establece un sistema de supervisión por parte de la Administración Pública a todas estas entidades esenciales e importantes, que deberán cumplir con lo previsto en la Directiva y en la normativa nacional de trasposición, con la diferencia de que las entidades esenciales serán supervisadas con anterioridad y posterioridad a ser consideradas como tal, mientras que las importantes únicamente podrán ser supervisadas *a posteriori*, debiendo ambos tipos de entidades realizar auditorías de cumplimiento en materia de seguridad (arts. 32 y 33 LC5G).

3.- La identidad digital autosoberana como ejemplo de transparencia

La identidad digital es uno de los pilares de la conectividad y la interoperabilidad entre sistemas y servicios, más aún en el entono 5G. El modo en que se implante la configuración descentralizada debe tender a ser más interoperable y segura, teniendo como fin la economía de los datos, en la que se basa el Mercado Único Digital Europeo (MUDE).

El concepto de identidad es muy amplio, pero en palabras de LLANEZA GONZÁLEZ (2021: 33), desde una perspectiva legal, puede definirse como «el derecho a existir en el mundo jurídico a partir de unos atributos de identificación que dan lugar a una serie de capacidades, que es el presupuesto para el reconocimiento y atribución del resto de los derechos y de la capacidad de ejercitarlos de un determinado modo».

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

Para ello, sostiene la referida autora, que es necesario que exista, por un lado, la capacidad de las personas de demostrar su identidad y, por otro lado, la capacidad de los proveedores de servicios, denominados Prestadores de Servicios de Confianza (PSC o TSP, en inglés), de identificar a sus clientes.

Hoy en día, la identidad legal ha evolucionado de una identificación documental, a una identificación informática, basada en atributos de la identidad. Existen corrientes que abogan por modelos de identidad autosoberana en los que el titular de los atributos gestiona los mismos sin intervención del Estado, desde el control y la privacidad de los datos personales *(*LLANEZA GONZÁLEZ, P. 2021: 60). Además, existe el modelo de identidad centralizada, el modelo de identidad federada y el modelo de identidad centrada en el usuario. A diferencia de los demás, el modelo autosoberano de identidad está relacionado con el principio de libertad de elección de atributos, que se propone tener en cuenta como principio digital, permitiendo a los usuarios crear su propio identificador, siendo el resto de la comunidad quienes se nutren de esa identidad, validando su información.

Todo ello debería estar basado en algoritmos verdes[17] y de código abierto, «debiendo existir una firme separación entre el concepto de identidad y sus afirmaciones o *claims*, de tal forma que pueda ejercitarse el derecho al olvido» (LLANEZA GONZÁLEZ, P. 2021: 82). Una afirmación o *claim* puede definirse como la descripción de un determinado atributo. Por ejemplo: el atributo de edad puede ir acompañado del *claim* minoría o mayoría de edad.

Desde la publicación del Reglamento (UE) 2021/953, de 14 de junio de 2021, sobre pasaporte digital Covid y la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, la nueva propuesta europea eIDAS 2 está orientada a la creación de un monedero digital de identidad europeo o *European Digital Identity Wallet* (*EDIW*, por sus siglas), que deberá operar también en un entorno 5G. Ello se realiza técnicamente a través de un identificador descentralizado, denominado *DID*, por sus siglas, que en sí mismo no es una identidad sino «una cadena alfanumérica aleatoria única bajo el control del usuario» (LLANEZA GONZÁLEZ, P. 2021: 84), pero no contiene ningún atributo de identidad, salvo que se autorice por el usuario a través de una credencial verificable, siempre emitida por entidades que hayan comprobado previamente la identidad del sujeto, pudiéndose acceder con este *DID* o identificador descentralizado desde cualquier parte. El modelo hace uso de métodos de identificación tales como las herramientas criptográficas, las firmas digitales o los datos biométricos.

En el panorama de los sectores de la Sociedad Digital, la NIS 2 distingue entre el sector de las Infraestructuras Digitales, el de Gestión de Servicios de TIC (de empresa a empresa) y el de los Proveedores de servicios digitales. Los Prestadores de Servicios de Confianza o PSCs comienzan a formar parte del sector de Infraestructuras Digitales a partir del momento de entrada en vigor de la NIS 2, algo que no sucede en estos momentos. Actualmente estos prestadores se regulan por

[17] Un algoritmo verde es el resultado de un proceso de programación que tiene como fin reducir el impacto ambiental de las aplicaciones informáticas.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

su propio reglamento europeo, eIDAS, que no prevé la aplicación de las normas de seguridad previstas en la NIS 1. El eIDAS 2, como se ha analizado anteriormente, hace referencia directa a la NIS 2 en el artículo 21.2 de su Propuesta.

El todavía vigente Reglamento eIDAS se implementa a través de un esquema de certificación, que también está siendo ahora revisado. Estos prestadores se dividen en: (i) aquellos dedicados a «la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios», (ii) «la creación verificación y validación de certificados electrónicos relativos a estos servicios», o (iii) «la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios» (art. 3.16 eIDAS). Con ánimo de evitar una fragmentación en la supervisión de estos servicios, así como múltiples certificaciones por País e incluso Comunidad Autónoma, el eIDAS vino a establecer una serie de criterios unificados y certificables, mediante un proceso de evaluación de la conformidad, desarrollado por la entidad de normalización europea, ETSI-ESI, número EN 319 403, que además permite el mutuo reconocimiento de las evaluaciones a nivel comunitario.

El esquema de certificación y supervisión aplicable a los PSCs puede considerarse un modelo para los sistemas descentralizados 5G, siendo la intención del legislador europeo, que los agentes que actúen en la Sociedad Digital, adopten una conciencia de cumplimiento, auditoría, certificación, interoperabilidad y supervisión, para ofrecer mayores garantías, transparencia y seguridad jurídica e informática a todos los usuarios. Además de lo anterior, el esquema de certificación eIDAS ya distingue también entre la certificación de servicios, por ejemplo, la norma de estandarización ETSI-ESI EN 319 401 establece los requisitos comunes y transversales para todos los PSCs, la ETSI-ESI EN 319 421 se aplica a los servicios de sellado de tiempo, la ETSI-ESI EN 319 451, a los servicios de entrega electrónica certificada, etc. Lo mismo podría ocurrir en materia de ciberseguridad, en cuyo esquema se pueden tener en cuenta los criterios ya aplicables de seguridad de la información a los PSCs e introducir, tras los requisitos comunes, nuevas normas de estandarización para los servicios 5G.

4.- La identidad digital europea y captación de datos en el entorno 5G

El dato es un concepto clave en la Sociedad Digital. Las cadenas de valor de datos se basan en actividades de creación, recopilación, agregación, organización o estructuración, tratamiento, análisis, comercialización, distribución de datos, utilización y reutilización de datos.

Desde la publicación de la Carta de los Derechos Fundamentales de la Unión Europea, en el año 2000, el Derecho a la Protección de Datos se independizó jurídicamente del derecho a la intimidad, erigiéndose como un derecho fundamental autónomo consagrado en su artículo 8. En el entorno 5G en el que la conectividad se produce en tiempo real, aumentan los riesgos y las implicaciones en la protección de datos, debiendo ello abarcar tanto los datos personales, como los metadatos y los datos no personales, que también son utilizados y tratados en la Sociedad Digital.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

El RGPD define el dato personal, en el artículo 4.1, como «toda información sobre una persona física identificada o identificable [...] cuya identidad pueda determinarse, directa o indirectamente [...]». Los metadatos, considerados datos sobre datos, revisten especial importancia para los agentes del mercado digital porque pueden incluir datos de números telefónicos, sitios web visitados o de georreferenciación.

La georreferenciación de las personas u objetos y con etiquetas que contienen determinados datos sobre las mismas, permiten su localización, incluso en movimiento. La propia AEPD señala, en su informe sobre *Introducción a las Tecnologías 5G* (2020: 12), que recomienda «implantar medidas de minimización de datos, en particular, con relación a la georreferenciación, teniendo en cuenta el principio de privacidad por defecto y desde el diseño de productos que utilicen servicios 5G».

El tratamiento de los metadatos debería estar actualmente regulado por medio de la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, conocido como Reglamento *e-privacy*, que sustituiría a la Directiva vigente 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, traspuesta a nuestro ordenamiento por medio de la Ley 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE), pero su texto ya conoce hasta ocho presidencias europeas, sin haberse concluido a día de hoy un acuerdo definitivo. El objetivo general del Reglamento *e-privacy* es que el contenido de las comunicaciones en línea y los metadatos asociados a dichas comunicaciones, tengan la misma protección que las telecomunicaciones tradicionales. Afectará tanto a los datos de las personas físicas como jurídicas, siendo el consentimiento de los usuarios uno de sus elementos centrales, y pudiendo llegar a ser considerado el futuro Reglamento E-Privacy como una lex *specialis* del RGPD. Si bien la aplicación del principio de transparencia puede resultar contradictoria con la intimidad, especialmente, con la confidencialidad, en realidad se trata de conceptos distintos, pues la obligación de confidencialidad, al igual que la de seguridad, es inherente a la información (Febles Pozo, N. 2021: 468).

Además, cabe resaltar que, de acuerdo con la AEPD, uno de los principales riesgos en materia de privacidad en los entornos 5G, es que «permitirán llegar a una individualización precisa de las personas, así como al desarrollo de servicios que permitirán la toma de decisiones automáticas sobre las mismas» (AEPD. 2020:10). Por ello, y precisamente ante posibles brechas de seguridad, o del quiebre de la confidencialidad en el entorno 5G, tanto la aplicación del principio de transparencia, como el de protección de datos, son cruciales para la trazabilidad de los sucesos, garantizándose así una mayor confiabilidad en el sistema 5G.

Asimismo, la tecnología 5G permitirá la captación y el tratamiento de datos biométricos en tiempo real. Por ejemplo, se podrían utilizar cámaras de alta resolución y sensores avanzados para capturar características biométricas con mayor precisión y rapidez. Además, la menor latencia podría mejorar la experiencia del usuario al autenticarse en línea a través de la biometría, lo que podría ser especialmente útil en aplicaciones que requieren un alto nivel de seguridad, como las transacciones financieras.

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

El panorama tecnológico abarca diversas tecnologías para la verificación de la identidad basadas en *hardware*, dispositivos móviles y biometría: opedID connect, FIDO2, uso de certificado u otros medios electrónicos. También se han diseñado protocolos de autenticación basados en la tecnología de identificación por radiofrecuencia (*RFid*, por sus acrónimoa en inglés) y que puede complementarse con tecnología de cadena de bloques o *DLT*. Desde el punto de vista normativo, parece que se pueden suscitar dudas sobre su compatibilidad con el RGPD, habida cuenta que, en apariencia, como se ha comentado anteriormente, la arquitectura de *Blockchain* y su propia naturaleza inmutable y descentralizada podrían impedir el ejercicio de algunos derechos, como el de supresión o derecho al olvido, o el de rectificación, además de difuminar las figuras de los responsables y encargados del tratamiento de los datos entre millones de ordenadores anónimos. Existen soluciones técnicas que abordan el problema de la protección de datos, por ejemplo, las cadenas de bloques puedan tener su propio mecanismo de actualización, quedando registrado el cambio, la trazabilidad del mismo, pero mostrándose en la versión más reciente.

Este sistema de cadena de bloques garantiza el anonimato de manera segura porque encripta los datos y restringe su acceso únicamente al titular de los mismos, aunque no puede ocultar la IP de los usuarios, que está considerada como un dato personal. Frente a esto también se han adoptado distintas soluciones técnicas como los servicios TOR (*The Onion Router*), I2P (*Invisible Internet Project*) y el protocolo Wraith (LLANEZA GONZÁLEZ, P. 2021: 9) que protegen la identidad de la IP. Otras soluciones pasan por que los usuarios puedan determinar si las transacciones que realizan se registren en un registro público o privado ya que resulta que la disociación de los datos personales del titular de los mismos no resulta tan fácil en un sistema *DLT*, tal y como pone de manifiesto la AEPD en el Dictamen 5/2015 sobre técnicas de anonimización. La referida disociación de datos se denomina doctrinalmente técnica de la privacidad diferencial, entendida como un sistema para compartir información de forma pública sobre un conjunto de datos a los que se les aplica técnicas de ruido matemático, lo que permite que se preserve el anonimato sin importar posibles ataques o accesos indebidos.

Existiendo soluciones técnicas que aborden la complejidad de los entornos interconectados en tiempo real, en aras de fomentar la aplicación del principio de transparencia, los sistemas de cadenas de bloques o acíclicos (*DAG*) son los que están mejor diseñados para garantizar los principios de la seguridad de la información: confidencialidad, integridad, autenticidad, disponibilidad, responsabilidad y no repudio.

5.- Conclusiones

El trabajo analiza la implementación de las normativas aplicables a la ciberseguridad e identidad digital en Europa y en España y su relación con el principio de transparencia. La comunicación en los entornos descentralizados 5G se producirá de forma ininterrumpida, en tiempo real y entre cuerpos y objetos (*IoT/IoC*), lo cual va a influir en determinados aspectos de la protección de datos que también son analizados. La aplicación del principio de transparencia, como principio de buen gobierno e inspirador de la creación de normas estandarizadas y certificables, se

DOI: https://doi.org/10.51915/ret.298

interrelaciona directamente con la configuración jurídica y práctica o técnica de la ciberseguridad y la identidad digital.

La cantidad de datos personales, no personales y metadatos que circularán por las redes y los dispositivos conectados en los entornos 5G, afectará a la intimidad de los usuarios. El concepto de intimidad en la Sociedad Digital se analiza desde el punto de vista objetivo, esto es, el de la protección de datos personales, como desde la perspectiva subjetiva del Derecho a la intimidad, que incluye el derecho a no ser reconocido o al pseudonimato, así como a la identidad digital, todo ello en un hábitat digital seguro y transparente.

Desde el punto de vista de la protección de datos, en primer lugar, en los entornos 5G se pueden recabar o generar tipos de datos que pueden resultar ser considerados personales, como ocurre con los metadatos, o tener implicaciones en la personalización de contenidos y decisiones automatizadas sobre las personas, uno de los principales riesgos de los entornos 5G y, en segundo lugar, que la utilización del sistema de cadena de bloques o *DLT* no tiene por qué ser contraria a lo previsto en el RGPD, siempre que se adopten las medidas de seguridad y privacidad desde el diseño y por defecto correspondientes. El verdadero comercio se realiza respecto de datos anonimizados, sobre otros datos, a los que ya no se les aplica la normativa de datos personales y de los que se puede extraer mucha información. La transparencia en este entorno facilitaría la trazabilidad de las brechas de seguridad y cualesquiera otros sucesos que pudieran acontecer.

En segundo lugar, desde el punto de vista subjetivo, la intimidad implica también valorar la identidad, constituyendo junto con la privacidad, las dos caras de una misma moneda: la de la dignidad humana, que puede estar acechada de forma perpetua, en un mundo digital, ininterrumpidamente conectado, por un fallo de seguridad, físico o cibernético. Hoy en día una gestión eficaz y eficiente de la ciberseguridad es una actividad fundamental, quedando un largo camino legislativo y de implementación por recorrer para garantizar e instaurar un entorno verdaderamente transparente y seguro.

El principio de transparencia incide y está directamente relacionado con el modo de configuración de la seguridad y la identidad digital descentralizadas en los entornos 5G. Entendido también como cumplimiento normativo a través de la certificación del cumplimiento de normas estandarizadas, así como una protección frente al sesgo de la tecnología. Unido el principio de transparencia al de responsabilidad proactiva, el legislador exige la estructuración de una supervisión clara y común, en términos generales, por parte de los organismos competentes, en materia de ciberseguridad y fortalecer así la ciberdefensa nacional.

En el entorno 5G hay, al menos, tres actores fundamentales, que son los operadores 5G, los suministradores 5G y los usuarios corporativos 5G. Deberá delimitarse la responsabilidad de cada uno de ellos y el resto de los agentes intervinientes en este entorno, asignándose caso por caso la misma, debido a su complejidad, y conforme a medidas objetivas de medición de riesgos y detección de vulnerabilidades. Todo ello regido por el principio de transparencia, como principio de buen gobierno aplicable en toda la cadena de suministro.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

La identidad digital está gestionada por el sector de los Prestadores de Servicios de Confianza (PSC), que constituyen el mejor precedente de uso de la estandarización de servicios y procesos, dentro del sector de Infraestructura Digital. La implantación de los sistemas y redes 5G van a exigir que el legislador comience por la creación de un Esquema Nacional de Ciberseguridad 5G (ENS 5G), iniciándose así la vía de la certificación y la formación especializada.

La responsabilidad proactiva de las entidades esenciales e importantes reguladas por la NIS 2 exige la supervisión de la ciberseguridad por parte de la Administración Pública a todas ellas, que deberán cumplir con lo previsto en la Directiva y en la normativa nacional de trasposición, con la analizada diferencia de que las entidades esenciales serán supervisadas *a priori* y *a posteriori*, mientras que las importantes únicamente podrán ser supervisadas *a posteriori*. Esto significa que, salvo un buen trabajo de recopilación de criterios, podrían los operadores y suministradores estar sujetos, tanto al cumplimiento de la NIS 2 y el Esquema Nacional de Seguridad (ENS), como al de la LC5G y el ENS-5G, si prestan servicios en los entornos 5G.

La solución que se propone tras el análisis realizado es la coordinación y colaboración entre las Administraciones Públicas supervisoras competentes para la unificación de criterios de esquemas de certificación, junto con las entidades que deben cumplir con la normativa en materia de ciberseguridad e identidad digital, para la creación de un esquema de certificación 5G similar al previsto por el Instituto Europeo de Telecomunicaciones (ETSI) para los Prestadores de Servicios de Confianza (PSCs). Asimismo, cabe resaltar que, entre los servicios prestados por los PSCs, no se prevé un servicio para la emisión de atestaciones de atributos, ni tampoco para su registro y almacenamiento, pudiendo resultar necesaria la creación de dichos servicios.

En definitiva, el principio de transparencia es crucial para la seguridad e identidad digital en los entornos 5G. No solo garantiza el cumplimiento normativo, sino que también protege contra sesgos tecnológicos. Por ello los avances normativos pretenden una supervisión unificada basada en normas estandarizadas para fortalecer, entre otros ámbitos, el de la ciberdefensa nacional.

Revista Española de la Transparencia
RET. ISSN 2444-2607
Núm. 18. Segundo semestre. Julio-diciembre 2023
www.revistatransparencia.com

Sección Estudios y Artículos
Transparencia, ciberseguridad e identidad digital…
por Clara Rodríguez Iláraz y Ricardo J. Palomo Zurdo
Págs. 359-380
DOI: https://doi.org/10.51915/ret.298

Bibliografía

5G-PPP. 2021. 5GPPP Architecture Working Group. View on 5G Architecture, en *5G-PPP.eu*. Disponible en: https://5g-ppp.eu/wp-content/uploads/2021/11/Architecture-WP-V4.0-final.pdf

Adsuara Varela, B. 2022. «El derecho al pseudonimato. Entre la identificación y el anonimato (IV)», en *La carta de Derechos Digitales.* (coord.) COTINO HUESO, L. (53-78).

Agencia Española de Protección de Datos (AEPD). 2020. «Introducción a las tecnologías 5G y sus riesgos para la privacidad», en *Aepd.es.* Disponible en: https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5g.pdf

Bonmatí Sánchez, J. 2020. La automatización inteligente de la toma de decisiones y el principio de transparencia: el derecho de explicación, en el Anuario Jurídico Secciones del ICAM 2020 (coord. RIBÓN SEISDEDOS, E. (355-366).

Cortés Vélez, J.J. 2021. «Derecho a la privacidad en la era de la digitalización y del *blockchain*», en *Práctica de tribunales: revista de derecho procesal civil y mercantil*, Nº 149.

Cotino Hueso, L. 2023. «Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida», en *Revista Española de Transparencia*, número 16, Primer Semestre (17-63).

Duque Botero, J.D. 2020. «Los principios de transparencia y publicidad como herramientas de lucha contra la corrupción en la contratación del Estado», en Revista Digital de Derecho Administrativo, nº 24 (79-101).

ETSI. 2021. «Zero Touch Network & Service Managamente (ZSM)», en *etsi.org*. Disponible en: https://www.etsi.org/technologies/zero-touch-network-service-management

Llamas Covarrubias, J.Z. 2021. «Transparencia y protección de datos personales en la cadena de bloques (*blockchain*)», en Estudios en Derecho a la información, nº 11 (27-63).

Llaneza González, P. 2021. «Identidad digital, actualizado a la Orden ETD/465/2021, de 6 de mayo (sobre métodos de identificación remota) y a la propuesta de Reglamento eIDAS2». Madrid: Editorial Wolters Kluwer.

López Jiménez, D. 2021. «Marcas Negras (en la era de la transparencia)», en *Revista de ciencias sociales*, Vol. 27, nº 4 (475-477).

Martín Delgado, I. 2021. «Transparencia y acceso a la información pública», en *Guía de Gobierno Abierto del Centro de Estudios Políticos y Constitucionales*. Disponible

DOI: https://doi.org/10.51915/ret.298

en: https://www.cepc.gob.es/sites/default/files/2022-06/a-942-guia-del-gobierno-abierto-int-corregido.pdf

Mercader Uguina, J.R. 2020. «Datos biométricos en los centros de trabajo», en *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales.*

Ministerio de Asuntos Económicos y Transformación Digital. 2021. *Memoria de impacto normativo sobre el anteproyecto de la Ley General de Telecomunicaciones, de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales*.

NIS Cooperation Group. 2019. EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks, en *Ec. Europa.EU*. Disponible en: HTTPS://EC.EUROPA.EU/COMMISSION/PRESSCORNER/DETAIL/EN/IP_19_6049

Nowak, T.W. y Sepczuk, M., et. al. 2021. «Verticals in 5G MEC-use cases and security challenges», en *IEE Acess.*

Palomo zurdo, R. 2018. «Blockchain: la descentralización del poder y su aplicación en la defensa», en *Revista del Instituto Español de Estudios Estratégicos (Revista IEEE),* nº. 70, (1-20). Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO70-2018_Blockchain_PalomoZurdo.pdf.

Palomo Zurdo, R., Rodríguez-Martín, A. y González-Sánchez, F. 2020. «Transparencia y Economía Circular: análisis y valoración de la gestión municipal de los residuos sólidos urbanos», *CIRIEC- España, Revista de economía pública, social y cooperativa* (233-272).

Viguri Cordero, J.A. 2018. «La certificación en el nuevo Reglamento europeo de Protección de Datos y anteproyecto de la Ley orgánica de Protección de Datos», en *Universidad Carlos III Madrid*, *Instituto de Derechos Humanos Bartolomé de las Casas.* Disponible en: https://redtiempodelosderechos.files.wordpress.com/2018/01/wp11-certificacion-protecciondedatos.pdf

Wanden-Berghe Lozano, J.L. y Fernández Daza, E. 2020. «*Blockchain*: Instrumento de transparencia y control del sector público», en Revista española de control externo, Vol. 22, nº Extra 64 (132-149).