

Claves 34

Serie Claves del Gobierno Local

Blockchain y Gobiernos locales

Coordinador: Gustavo Manuel DÍAZ GONZÁLEZ

Vincenç AGUADO I CUDOLÀ	Patricia GARCÍA MAJADO
Antonio David BERNING PRIETO	Andrea GARRIDO JUNCAL
Andrés BOIX PALOP	María HERNANDO RYDINGS
Antonio BUENO ARMIJO	José PEDREIRA MENÉNDEZ
Magdalena CORDERO VALDAVIDA	Manuel PEREIRO CÁRCELES
Gustavo Manuel DÍAZ GONZÁLEZ	Mariola PÉREZ RODRÍGUEZ
Roberto FERNÁNDEZ LLERA	Miguel Ángel PRESNO LINERA

La **Fundación Democracia y Gobierno Local** es una entidad sin ánimo de lucro constituida en mayo de 2002.

Su finalidad es contribuir y dar soporte a todo tipo de actuaciones y de iniciativas para el conocimiento, el estudio, la difusión y el asesoramiento en materia de régimen local. Al mismo tiempo, ha sido concebida como lugar de encuentro y de intercambio en el que las diputaciones provinciales, los cabildos y los consejos insulares puedan poner en común sus experiencias y coordinar esfuerzos para favorecer el desarrollo de sus funciones de cooperación y asistencia a las entidades locales.

Aspira a ser una institución de referencia para otras organizaciones nacionales e internacionales en el impulso de la calidad institucional de los Gobiernos locales, haciéndolos más eficientes en términos de prestación de servicios públicos, reforzando su legitimidad democrática y la confianza de los ciudadanos. En particular prestará atención a los Gobiernos locales intermedios y a su correcto encaje en el sistema local, así como a sus relaciones con el resto de niveles de Gobierno.

Entre sus **líneas estratégicas** se destacan:

- Liderar institucionalmente, en el marco actual de distribución territorial del poder del Estado, la puesta en valor de los Gobiernos locales, en general, y de los intermedios, en particular, reforzando su legitimidad democrática y la confianza de los ciudadanos.
- Reforzar el liderazgo político y directivo de los Gobiernos locales.
- Colaborar en la gestión del conocimiento en el ámbito de los Gobiernos locales: compartir conocimientos, favorecer la investigación, impulsar la comunicación.
- Realizar alianzas internacionales, para reforzar el valor institucional de los Gobiernos locales.

www.gobiernolocal.org



Blockchain y Gobiernos locales

Claves **34**

Serie Claves del Gobierno Local

Blockchain y Gobiernos locales

Coordinador: Gustavo Manuel DÍAZ GONZÁLEZ

Vincenç AGUADO I CUDOLÀ	Patricia GARCÍA MAJADO
Antonio David BERNING PRIETO	Andrea GARRIDO JUNCAL
Andrés BOIX PALOP	María HERNANDO RYDINGS
Antonio BUENO ARMIJO	José PEDREIRA MENÉNDEZ
Magdalena CORDERO VALDAVIDA	Manuel PEREIRO CÁRCELES
Gustavo Manuel DÍAZ GONZÁLEZ	Mariola PÉREZ RODRÍGUEZ
Roberto FERNÁNDEZ LLERA	Miguel Ángel PRESNO LINERA



FUNDACIÓN
DEMOCRACIA
Y GOBIERNO LOCAL

© FUNDACIÓN DEMOCRACIA Y GOBIERNO LOCAL
Rambla de Catalunya, 126 - 08008 Barcelona
c/ Fernando el Santo 27, bajo A - 28010 Madrid
www.gobiernolocal.org

Corrección y revisión de textos: María Teresa Hernández Gil

Producción: Gráficas Naciones S.L.

Depósito legal: M-6028-2022

ISBN: 978-84-120267-8-8

Queda rigurosamente prohibida, sin la autorización escrita del titular del copyright, bajo las sanciones establecidas en las leyes, la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares mediante alquiler o préstamos públicos.

- 9 **Blockchain y administraciones públicas: una visión panorámica**
GUSTAVO MANUEL DÍAZ GONZÁLEZ
- 83 **Ciudades inteligentes y tecnología de cadena de bloques: hacia un ejercicio compartido de funciones públicas**
VICENÇ AGUADO I CUDOLÀ
- 125 **Tecnología *blockchain* y entidades locales: nuevas formas de funcionamiento interno y de interacción con el ciudadano**
ANTONIO DAVID BERNING PRIETO
- 153 **Transparencia y protección de datos personales en el uso de la tecnología *blockchain*: especial consideración de su impacto en el ámbito local**
ANDRÉS BOIX PALOP Y MANUEL PEREIRO CÁRCELES
- 189 **Blockchain y contratación pública: análisis general e implicaciones en el ámbito local**
MARÍA HERNANDO RYDINGS
- 213 **Servicios locales y *blockchain***
ANDREA GARRIDO JUNCAL
- 237 **Democracia local y tecnología *blockchain***
PATRICIA GARCÍA MAJADO Y MIGUEL ÁNGEL PRESNO LINERA
- 275 **Subvenciones locales, *blockchain* y actuación administrativa automatizada**
ANTONIO BUENO ARMIJO
- 325 **Gestión tributaria: *blockchain* y otras nuevas tecnologías**
JOSÉ PEDREIRA MENÉNDEZ

347 **Tecnologías emergentes aplicadas al presupuesto, el control interno y la fiscalización externa del sector público local**
ROBERTO FERNÁNDEZ LLERA, MARIOLA PÉREZ RODRÍGUEZ
Y MAGDALENA CORDERO VALDAVIDA

***Blockchain* y administraciones públicas: una visión panorámica**

Gustavo Manuel Díaz González*

Profesor ayudante doctor de Derecho Administrativo.

Universidad de Oviedo

SUMARIO. 1. Introducción. 2. Fundamentos de la tecnología *blockchain*.

2.1. La conexión de las tecnologías de registro distribuido con el movimiento *cypherpunk*. 2.2. Principios de funcionamiento e implicaciones de la tecnología *blockchain*. 2.2.1. Distribución, descentralización, ¿desintermediación? 2.2.2. Encriptación y criptografía asimétrica: claves públicas, claves privadas y la garantía de la seguridad. 2.2.3. El consenso como base de la tecnología *blockchain*. 2.2.4. ¿Inmutabilidad de la cadena de bloques? 2.3. Tipos de redes *blockchain*. 2.4. Breve recapitulación: la controversia en torno a la tecnología *blockchain*. **3. La regulación de la tecnología *blockchain*.** 3.1. Los retos para el diseño de la disciplina jurídica aplicable a la tecnología *blockchain*. 3.1.1. Mutabilidad de la tecnología *blockchain*. 3.1.2. La supranacionalidad del fenómeno. 3.1.3. El desafío de los usos delictivos. 3.1.4. El (difícil) encaje de *blockchain* en los sistemas normativos vigentes. Breve referencia a la protección de datos de carácter personal (remisión). 3.2. La (pretendida) capacidad normativa del código (*code as law*). 3.3. Un repaso de los principales enfoques regulatorios aplicables a la tecnología *blockchain*. 3.3.1. Prohibicionismo y abstencionismo. 3.3.2. *Wait and see*. 3.3.3. La autorregulación regulada. 3.3.4. Los denominados *sandboxes* regulatorios. **4. *Blockchain* y administraciones públicas: aproximación general.** 4.1. Consi-

* Miembro del grupo de investigación “Derecho Administrativo (DA)” de la Universidad de Oviedo, dirigido por el prof. Dr. Alejandro Huergo Lora.

deraciones introductorias. 4.2. Breves reflexiones sobre las principales ventajas y los desafíos del empleo de las tecnologías de registro distribuido por parte de las administraciones públicas. 4.3. Casos de uso de la tecnología *blockchain* en el sector público (selección) **5. Bibliografía.**

1. Introducción

De un tiempo a esta parte viene insistiéndose desde ámbitos muy diversos en que las denominadas tecnologías de registro distribuido –y, singularmente, la tecnología *blockchain*– representan un muy relevante factor de transformación económica y social¹. Los principios de funcionamiento de las redes Bitcoin y Ethereum –como es ocioso recordar, dos de las más importantes criptomonedas del mercado actual– resultarían extrapolables a múltiples sectores de actividad y poseerían un potencial disruptivo de extraordinaria significación, cuyas implicaciones serían incluso equiparables a las de la aparición y popularización de internet, que habría, a su vez, de experimentar una profunda mutación². El empleo auxiliar de aquellas en el ejercicio de las potestades administrativas constituiría un punto de inflexión en su desarrollo, en cuanto que supondría la asimilación por parte de los poderes públicos de

1. Tal consideración de la tecnología *blockchain* es asumida no solo por un muy relevante sector doctrinal, sino también en el ámbito institucional. Desde esta última perspectiva, destaca, por ejemplo, el informe de la OECD titulado *Science, Technology and Innovation Outlook 2016* (107 y ss.), en el que se analizan diversos casos de uso de las tecnologías de registro distribuido, se alerta sobre las incertidumbres y dificultades a que puede dar lugar su implantación, tales como su impacto medioambiental o su posible utilización para fines ilícitos, y se califica de “impredecible” el impacto de las mismas en diversos sectores de actividad. En fechas más recientes, destaca, entre otros, el *main report* de junio de 2021, elaborado por la Asesoría Financiera en Innovación del Banco Europeo de Inversiones para la Comisión Europea y titulado *Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy*. En dicho informe se parte del potencial disruptivo de la inteligencia artificial y la tecnología *blockchain* en relación con un amplio abanico de sectores de actividad, así como del papel central que, consiguientemente, las mismas desarrollarán en la transición ecológica y digital y, en fin, de su efecto fortalecedor de la soberanía digital europea, para efectuar un detallado análisis de algunos retos específicos referentes a su implantación, tales como los déficits de inversión, los cuellos de botella en relación con la financiación de proyectos o sus implicaciones éticas y sociales.

2. En este sentido, como pone de manifiesto Pastor Sempere (2018), la implantación de la tecnología *blockchain* comportaría cambios muy relevantes en el ámbito de los sistemas de pago, en la medida en que, entre otros aspectos, favorecería una radical transformación de los servicios de intermediación bancaria, la automatización de numerosas categorías de operaciones financieras y la aparición y consolidación de nuevas unidades de valor, denominadas criptomonedas. Surgiría, en este contexto, una nueva internet, denominada “del valor”, en cuanto ya no solo apta para el almacenamiento y el intercambio de datos, sino también facilitadora de la consolidación de nuevos modelos de negocio en torno a “valores” progresivamente desvinculados de los activos físicos.

una comprensión de sus propias funciones diametralmente opuesta a la tradicional, permitiendo, al mismo tiempo, un avance aún hoy difícilmente imaginable tanto para los derechos y garantías de los ciudadanos –singularmente, aunque no solo, desde la perspectiva del derecho a la protección de datos de carácter personal– como desde el punto de vista de principios jurídicos tales como los de eficacia o transparencia.

Resulta en estos momentos muy difícil pronunciarse sobre si la anterior constituye una visión realista del fenómeno o si, por el contrario, los defensores de la tecnología *blockchain* exageran al describir sus virtudes con tanto entusiasmo. A nadie escapa que los intereses concurrentes son un elemento a considerar, pues resulta evidente que es mucho lo que está en juego. Y, sin embargo, parece igualmente cierto que los poderes públicos no pueden vivir de espaldas al desarrollo tecnológico, máxime cuando se trata de sistemas en expansión que los interpelan con vehemencia no solo en su condición de reguladores, sino también –e incluso en primer término– como potenciales participantes en la red. Siendo ello así, y resultando la *blockchain* una tecnología aún embrionaria, compete a la doctrina (no solo) jurídica, como con buen criterio ha defendido una de las principales especialistas europeas en la materia, el análisis de los retos que la misma plantea, así como de sus implicaciones, justamente en la fase previa a la generalización de su uso³, a fin de asistir, cabría añadir, a los agentes públicos en la toma de decisiones.

En este sentido, el presente volumen, centrado en el mundo local, persigue precisamente proporcionar una visión multisectorial en relación con el –hoy ya no solo posible, sino cierto– recurso a esta tecnología por parte del nivel administrativo más próximo al ciudadano. De esta forma, las diversas contribuciones de la obra tienen como principal objetivo facilitar al lector una primera aproximación a los usos más relevantes de la tecnología *blockchain* por parte de las entidades locales. La exposición combinará, así, la reflexión teórica y el análisis de experiencias reales, elementos a partir de los cuales se ensayará la formulación de propuestas sobre los desafíos presentes y futuros de *blockchain* en el ámbito local.

Con carácter preliminar, en el presente capítulo se abordará el análisis general del fenómeno, con específica referencia a su impacto en la actividad de las administraciones públicas. En este sentido, se partirá de una breve descripción

3. Finck (2019: 3 y 33). Debe destacarse que los especialistas en la materia continúan refiriéndose a *blockchain* como una tecnología aún precisada de un cierto tiempo para completar su proceso de maduración y desplegar todos sus efectos; en este sentido, particularmente, Herencia Antón (2021: 66).

de esta tecnología, sus bases ideológicas y principios de funcionamiento, y se expondrán las principales líneas argumentales del debate que la misma y las dudas acerca de su potencial eficacia y su sostenibilidad han suscitado (2). A continuación, se dará cuenta de los retos y de las estrategias regulatorias aplicables a la tecnología *blockchain*, aspecto esencial para la configuración de un marco normativo que, como es notorio, va desarrollándose paulatinamente, impulsado en buena medida por las instancias supranacionales (3). Ello nos permitirá reflexionar, en último lugar, acerca de las posibles transformaciones de la actividad administrativa resultantes de la implantación de la tecnología *blockchain*, así como ofrecer una visión panorámica en relación con algunos de los principales casos de uso desarrollados hasta la fecha (4).

2. Fundamentos de la tecnología *blockchain*

2.1. La conexión de las tecnologías de registro distribuido con el movimiento *cypherpunk*

Como habrá de exponerse seguidamente, *blockchain* no se basa en principios o elementos tecnológicos radicalmente nuevos, sino en la combinación de las denominadas redes entre pares o *peer-to-peer* (P2P) y el empleo de la criptografía asimétrica⁴. Idéntica continuidad se observa desde la perspectiva filosófica; en este sentido, diversos estudios han subrayado la íntima relación existente entre las bases ideológicas de la tecnología *blockchain* y una singular corriente surgida en el tránsito de la década de los ochenta a la de los noventa del siglo pasado: el movimiento *cypherpunk*⁵.

Dos personalidades sobresalen en el desarrollo de este pensamiento: Timothy C. May y Eric Hughes. El primero publicaría en 1988 el *Manifiesto Criptoanarquista*, redactado con un lenguaje que puede antojarse épico

4. En este sentido, *cfr.*, entre otros, García Mexía (2018b: 78-79), Dimitropoulos (2020: 1127) y Capiello (2021: 17).

5. Sobre la referida conexión, *in extenso*, González-Meneses (2017: 19 y ss.), Carrascosa Cobos *et al.* (2017) y Magnuson (2020: 16 y ss.). *Cfr.* asimismo Pollicino y De Gregorio (2021: 3 y ss.), que subrayan no solo el parcial retorno, en la etapa actual, al ideal criptoanarquista, sino también la frustración del mismo con la regulación de la red y los límites de la descentralización como principio de funcionamiento de la tecnología *blockchain* como aspectos conexos (extremos sobre los que, en todo caso, se volverá *infra*). Como excepción, sorprende, en fin, que otros análisis sobre el carácter utópico de la narrativa construida en torno a las tecnologías de registro distribuido no mencionen en ningún momento el referido movimiento ideológico; en este sentido, *cfr.* Kohl (2021).

y cómico a un tiempo –es conocido su encabezamiento: “Un espectro está surgiendo en el mundo moderno: el espectro de la criptoanarquía”–, y en el que se anunciaba la liberación de la ciudadanía respecto al yugo del Estado a partir de la consolidación de avances tecnológicos que permitirían una interacción entre los individuos sustraída a toda posibilidad de control institucional, garantizándose de esta forma elevados niveles de confidencialidad y, en último término, una plena autodeterminación individual. De nada serviría al Estado afanarse en poner límites a esta revolucionaria transformación, incluso pese a la posible legitimidad de sus razones:

“El Estado intentará, por supuesto, retardar o detener la diseminación de esta tecnología, citando preocupaciones de seguridad nacional, el uso de esta tecnología por traficantes de drogas y evasores de impuestos y miedos de desintegración social. Cualquiera de estas preocupaciones serán válidas; la criptoanarquía permitirá la comercialización libre de secretos nacionales y la comercialización de materiales ilícitos y robados. Un mercado computarizado anónimo permitirá incluso el establecimiento de horribles mercados de asesinatos y extorsiones. Varios elementos criminales y extranjeros serán usuarios activos de la CryptoNet. Pero esto no detendrá la extensión de la criptoanarquía”⁶.

Por su parte, Eric Hughes abundaría, en el *Manifiesto Cypherpunk* (1993)⁷, en las ventajas que las técnicas de encriptación traerían consigo desde la perspectiva de la autodeterminación informativa, en la medida en que permitirían limitar la información transmitida a terceros con ocasión de la realización de transacciones a la estrictamente necesaria a tal fin. Se garantizaría, en consecuencia, un elevado grado de privacidad, que en modo alguno habría de confundirse con el secreto. Tan solo a los ciudadanos competaría decidir sobre la gestión de su propia información, de forma que los mismos dejarían de depender en este punto de la intervención del Estado o de otras organizaciones. De ello derivaría un forzoso desplazamiento de la regulación institucional por la autonomía individual.

Los posicionamientos referidos representan una apuesta decidida por una retracción casi absoluta de la intervención estatal, inequívocamente vinculada a las tesis anarquistas tradicionales. Tal comprensión ha podido incluso ser descrita

6. Cita extraída de la traducción publicada en: <https://academy.bit2me.com/manifiesto-criptoanarquista/>.

7. Cfr: la traducción publicada en: <http://www.tugurium.com/docs/UnManifiestoCiphernk.php>.

como una suerte de defensa del retorno al nivel de descentralización propio del estado de naturaleza⁸. No es muy diferente, en el fondo, la promesa que, si se ha de dar crédito a un destacado sector entre los partidarios de *blockchain*, ofrece esta singular tecnología: sus principios de funcionamiento favorecerían una descentralización y una desintermediación totales, de las que resultarían no solo la transformación o la desaparición de numerosos sectores de actividad, sino también una redefinición del papel del Estado en las sociedades actuales⁹. Ahora bien, ¿cabe esperar una mutación de tan hondo calado a partir de la generalización del uso de la tecnología *blockchain*? ¿Cómo es posible que, exponiéndose la cuestión en estos términos, las administraciones públicas se planteen fomentar su implantación e incluso servirse de ella en el ejercicio de sus potestades?

2.2. Principios de funcionamiento e implicaciones de la tecnología *blockchain*

No resulta posible dar respuesta a las cuestiones con las que se cerraba el apartado anterior sin una previa explicación de los principios de funcionamiento de la tecnología *blockchain*. En este sentido, ha de considerarse que el detalle del mecanismo subyacente a las tecnologías de registro distribuido presenta una notable complejidad, razón por la que la exposición sucesiva poseerá un carácter meramente instrumental, en la medida en que perseguirá tan solo proporcionar las herramientas necesarias para el recto entendimiento del discurso ulterior. Se renuncia, por consiguiente, al análisis pormenorizado de todos y cada uno de los elementos tecnológicos que confluyen en la conformación de las redes *blockchain*. Para una visión en profundidad al respecto, es obligada la remisión a la bibliografía específica en la materia¹⁰.

En extrema síntesis, las redes *blockchain* se configuran sobre la base de cuatro elementos esenciales. En primer lugar, la *blockchain* prototípica –como habrá de exponerse seguidamente, la red pública sin permisos– es un libro mayor *distribuido*, lo que significa que el conjunto de nodos o servidores posee una copia auténtica de toda la información relativa a las transacciones realizadas en la misma, sin que, por consiguiente, exista una autoridad central encargada de su custodia y actualización (2.2.1). En segundo lugar, las redes *blockchain* se caracterizan por el empleo de una criptografía de tipo *asimétrico*, esto es, basada

8. En este sentido, *vid.* Magnuson (2020: 11 y ss.).

9. Son conocidos los planteamientos que cuestionan la necesidad misma del Estado a partir de la consolidación de la tecnología *blockchain*, rebatidos con solvencia por Atzori (2015: 1-37, especialmente 22 y ss.).

10. Por todos, ciñéndonos a las contribuciones publicadas en nuestro idioma, González-Meneses (2017), Morales Barroso (2018), Ponce de León (2018) y Herencia Antón (2021).

en un sistema de doble clave, pública y privada, que permite el intercambio de mensajes e información entre los usuarios intervinientes en las correspondientes transacciones con un elevado nivel de seguridad (2.2.2). En tercer lugar, la *blockchain* funciona sobre la base del *consenso* de los nodos o servidores, a los que se atribuye la función de validación de las transacciones que se integran en la cadena de bloques a través del empleo del mecanismo definido con carácter previo en la propia red, que, entre otros extremos, articula la forma de retribución de dicha labor (2.2.3). Discutible y discutido es, por último, si de lo anterior resulta el carácter *immutable* de esta tecnología (2.2.4).

2.2.1. Distribución, descentralización, ¿desintermediación?

El carácter distribuido de la *blockchain* representa uno de sus elementos definitorios esenciales; no es casual, en este sentido, que dicho rasgo se destaque en la propia denominación de la categoría de tecnologías a la que la misma pertenece (de registro *distribuido*). Tanto es así que esta característica se erige, de hecho, en presupuesto lógico de buena parte de sus restantes principios de funcionamiento –singularmente, del principio de descentralización–.

La distribución posee en el ámbito de la tecnología *blockchain* un significado distinto al ordinario, pues no implica división de la información entre los servidores o nodos, sino, como ha quedado dicho, la réplica del libro mayor en el que se registran todas las transacciones, incorporadas a la cadena de bloques, en los dispositivos de aquellos¹¹. Dicho con otras palabras, cada uno de los nodos posee una copia de toda la información almacenada en la cadena de bloques, que se descarga en el momento de la incorporación a la red, en el que se adquiere, asimismo, la condición de administrador de aquella. Los nodos son, a un tiempo, depositarios de una copia auténtica del libro mayor –lo que, entre otros aspectos, otorga a la información contenida en el mismo un elevado grado de seguridad, puesto que, en el supuesto de que uno de los nodos sufra un ataque informático, no existirá riesgo de pérdida de la información¹²– y responsables de la validación

11. *Cfr.* nuevamente Morales Barroso (2018: 47).

12. A este respecto, debe tenerse presente que también en los sistemas centralizados se recurre a copias de las bases de datos para evitar los daños ocasionados por posibles pérdidas o ataques. La peculiaridad de las redes *blockchain* en este punto viene representada por el hecho de que, mientras que en aquellos sistemas existe tan solo una única base de datos originaria, constituyendo las restantes meras réplicas secundarias, en estas, las copias de todos y cada uno de los nodos poseen carácter auténtico: sobre esta cuestión, *cfr.* Carullo (2021: 47). Otros autores han destacado el carácter más frágil, pero más eficiente de las bases de datos centralizadas por comparación con la cadena de bloques, que proporciona, como habrá

de las transacciones y, consiguientemente, de la actualización de aquel. Esta última tarea, conocida comúnmente como *minado*, es llevada a cabo a través de la aplicación del correspondiente mecanismo de consenso –concepto sobre el que se volverá más adelante¹³– y objeto de retribución mediante incentivos predefinidos en la red –por ejemplo, en el caso de Bitcoin, el primer nodo que consigue resolver el problema matemático con el que se cierra cada uno de los bloques de la cadena obtiene a cambio un número de criptomonedas determinado conforme a las reglas establecidas por Satoshi Nakamoto en su *Libro Blanco*¹⁴–.

Como viene de señalarse, íntimamente ligado al principio de distribución se encuentra el carácter descentralizado de la tecnología *blockchain*. Este segundo rasgo comporta la inexistencia de una autoridad central encargada del mantenimiento de la red, puesto que dicha labor es realizada de forma colaborativa por parte de los servidores o nodos. Así, el modelo *puro* o *ideal* de red *blockchain* se caracteriza por la corresponsabilidad en la gestión y, consiguientemente, por la igualdad tendencialmente plena de todos los servidores, principio al que remite uno de los elementos basilares de esta modalidad de tecnología: la conformación de una estructura reticular entre pares (red *peer-to-peer* o P2P).

Consecuencia de las dos características sumariamente referidas sería, en último lugar, la tendencia a la desintermediación en sectores en los que las instituciones de confianza han desempeñado tradicionalmente un papel fundamental, como es, singularmente, el bancario. Ello redundaría, entre otros aspectos, en un significativo abaratamiento de los costes de las transacciones, y forzaría a numerosos operadores a acometer un importante cambio de mentalidad, toda vez que la eventual oposición de resistencias terminaría por condenarlos a desaparecer¹⁵. Y no solo eso: de generalizarse la realización de operaciones económicas a través de redes *blockchain* de carácter público y no permissionado, se afirma, amén de la garantía de un control absoluto sobre la propia información, en la línea de lo auspiciado por los *cypherpunks*, se produciría una *democratización* de las relaciones económicas, puesto que las personas excluidas, que se contarían por “miles de millones” en todo el mundo, podrían “incorporarse pronto a la economía global”. De resultas de ello, la redistribución de la riqueza como horizonte sería sustituida por una distribución inicial más justa de la misma¹⁶.

de comprobarse, mayores niveles de seguridad, pero cuyo funcionamiento es más lento y costoso; en este sentido, véase particularmente Macchia (2021: 122).

13. Apartado 2.2.3.

14. Nakamoto (2008).

15. En este sentido, entre otros, Reed (2016: 75-76).

16. Tapscott y Tapscott (2017: 37-38).

Con respecto a esta última promesa, y sin perjuicio de que sobre la cuestión relativa a la capacidad de transformación real de la tecnología *blockchain* haya de volverse *infra*¹⁷, debe destacarse que, ciertamente, la Organización de las Naciones Unidas para la Alimentación y la Agricultura (FAO, por sus siglas en inglés) ha subrayado la posibilidad de recurrir a aquella en la lucha contra el hambre en el mundo¹⁸. Sin duda es pronto para evaluar tales iniciativas; con todo, no puede dejar de convenirse con quienes ven en esta lacra uno de los problemas que la tecnología *blockchain* no puede solucionar¹⁹.

En buena medida, ello es así porque los rasgos sucintamente descritos –distribución, descentralización, desintermediación– no son comunes al conjunto de redes *blockchain*: ante todo, la *blockchain* es una tecnología *flexible*, motivo por el cual no es correcto predicar de la totalidad de redes las características asociadas al principio de distribución en idéntico grado. Más aún: ni siquiera aquellas gestionadas con el máximo nivel posible de distribución, las conocidas como redes públicas sin permisos, son absolutamente descentralizadas. Antes de profundizar en estas cuestiones, sin embargo, ha de completarse la explicación en lo referente a los restantes principios de funcionamiento de la tecnología *blockchain*.

2.2.2. Encriptación y criptografía asimétrica: claves públicas, claves privadas y la garantía de la seguridad

Como se ha señalado previamente, la tecnología *blockchain* se caracteriza por la combinación de elementos tecnológicos preexistentes, en concreto, las redes P2P y la criptografía asimétrica. Esta segunda técnica comporta la utilización de un sistema de doble clave, pública y privada, directamente vinculadas entre sí a través de una función informática: en la red *blockchain*, la clave privada se genera aleatoriamente, y a partir de ella, en aplicación de la referida función, se calcula la clave pública. Esta última, claro está, es la que incorpora el mensaje que se da a conocer al conjunto de servidores o nodos, mientras que la privada se utiliza para el almacenamiento de la información que no se desea compartir

17. Apartado 2.4.

18. *Cfr.* la entrada “De la tecnología ‘blockchain’ en las cadenas de suministro de café a la Moda Azul: soluciones innovadoras para el Hambre Cero en la Cumbre Seeds and Chips”, en: <http://www.fao.org/news/story/es/item/1192773/icode/>.

19. Así lo considera, con buen criterio, Ramón Martínez Palomares, destacado especialista en la materia; a este respecto, puede consultarse su intervención en el *webinar* “*Blockchain* y Administraciones Públicas”, organizado por la Diputación de Alicante y la Fundación Democracia y Gobierno Local el pasado 1 de febrero de 2021, en: <https://www.youtube.com/watch?v=xY2DhOxKyK8>.

en la red —o que tan solo se desea compartir puntualmente—. Ello facilita una gestión autónoma de la propia identidad en la red, uno de los más relevantes usos que la tecnología *blockchain* posibilita y en el que, como se expondrá en sucesivos capítulos de esta obra, se están concentrando buena parte de los esfuerzos tanto en el ámbito de la investigación como en el regulatorio.

Junto al anterior, el principal interés que presenta la criptografía asimétrica es el relativo al grado de seguridad que la misma proporciona. De acuerdo con el actual estado de la técnica, la función a partir de cuyo uso se obtiene la clave pública es unidireccional, es decir, la operación consistente en la obtención de esta última a partir de la clave privada no es reversible, por lo que quien conozca la clave privada podrá saber cuál es la pública, pero no al revés²⁰. Ello comporta un elevado nivel de seguridad²¹ y representa el elemento que, junto al consenso de los nodos como mecanismo de validación de las transacciones, posibilita la sustitución de la confianza en el intermediario por la depositada en la propia red, aspecto sobre el que se volverá seguidamente.

Ahora bien, no puede dejar de destacarse que sobre dicho estado de cosas pende la amenaza del desarrollo de una función que permita la descryptación de la clave privada a partir de la pública. En este sentido, algunos especialistas vienen alertando sobre la efectiva posibilidad de que la tecnología alcance un grado de desarrollo tal que facilite no solo la obtención de la clave pública a partir de la privada, sino también la realización de la misma operación en sentido inverso. De hecho, de acuerdo con recientes informaciones aparecidas en prensa, nos hallaríamos cada vez más cerca del referido escenario²². Parece inevitable que, como señalan quienes han llamado la atención sobre la cuestión, llegado el caso, habría de interrumpirse temporalmente la realización de transacciones en la red, en tanto el problema no fuera solucionado²³.

Es importante subrayar lo anterior, por cuanto no son pocas las exposiciones en las que las redes *blockchain* se presentan como entornos digitales plenamente

20. En este sentido, Núñez Miller (2017: 209-210).

21. Grado o nivel de seguridad que posee dos manifestaciones diferentes, pero complementarias: por una parte, se garantiza la confidencialidad del mensaje remitido a través de la red *blockchain*; por otra, la integridad del mismo, esto es, la imposibilidad de alteración de su contenido antes de que sea recibido por su destinatario. Al respecto, *cfr.* Herencia Antón (2021: 70).

22. *Cfr.* la noticia: “La amenaza que puede destruir Bitcoin y todas las criptomonedas”, en *El Confidencial* de 17 de noviembre de 2021: https://www.elconfidencial.com/tecnologia/novaceno/2021-11-17/criptomonedas-perder-valor-ordenador-cuatico_3325197/.

23. Al respecto, *cfr.* nuevamente Núñez Miller (2017: 213-215).

seguros, sin posibilidad aparente para el desarrollo de actuaciones contrarias a los intereses de los usuarios. Sin embargo, en modo alguno puede considerarse que la anterior afirmación sea correcta, no solo por razón del riesgo al que viene de hacerse referencia, sino también por la existencia de otras amenazas para la seguridad de la red, particularmente las que se dan en escenarios de control de su funcionamiento por parte de una minoría de usuarios, extremo sobre el que se volverá *infra*²⁴. La confianza en las bondades de la tecnología *blockchain* no puede, en suma, hacernos olvidar los peligros asociados a la misma, sin que ello deba en ningún caso ser interpretado como un rechazo preventivo a su desarrollo e implantación.

2.2.3. El consenso como base de la tecnología *blockchain*

En diversos momentos de la exposición se ha mencionado el consenso como aspecto esencial del funcionamiento de la tecnología *blockchain*. Con ello se hace referencia al principio conforme al cual la construcción de la cadena de bloques —que, como ya sabemos, se produce a partir de la incorporación y de la validación de las transacciones en el libro mayor— requiere del acuerdo de la red en su conjunto. Dicha exigencia no es, en realidad, sino consecuencia lógica del carácter descentralizado de las tecnologías de registro distribuido: en la medida en que no existe una autoridad central encargada de garantizar la validez de las transacciones, estas han de ser aceptadas por los servidores o nodos, que se pronuncian al respecto indirectamente, incorporando nuevas transacciones a la cadena cuando la operación es válida o, en caso contrario, ignorándola mediante la consideración de una transacción diferente como eslabón último —lo que puede ocurrir, particularmente, en los supuestos de detección de un doble pago—. Como viene de decirse, este aspecto, unido al empleo de una criptografía de tipo asimétrico, se encuentra en la base de la traslación teórica de la confianza comúnmente depositada en los prestadores de servicios de intermediación hacia el conjunto de la red o, lo que es lo mismo, de la innecesariedad de confiar en un agente externo para el desarrollo de operaciones en los entornos *blockchain*. Con todo, ha de advertirse que esta característica, a la que usualmente se hace referencia con la expresión anglosajona *trustless trust*, resulta cuestionable ya desde una perspectiva general, por cuanto, como con buen tino se ha señalado, la pretendida confianza en el código no es, en el fondo, sino confianza en las personas encargadas de su elaboración²⁵.

24. Apartado 2.4.

25. En este sentido, Low y Mik (2020: 139).

Con independencia de lo anterior, en relación con el consenso como principio de funcionamiento de las redes *blockchain* deben efectuarse dos precisiones adicionales. En primer lugar, en contra de lo sugerido por muchos de los gurús de las tecnologías de registro distribuido, los usuarios o nodos no asumen poder de (co)decisión alguno en el desarrollo de la tarea de validación de las transacciones. El consenso que se encuentra en la base del funcionamiento de *blockchain* es de tipo algorítmico, en cuanto que la labor de validación es controlada en su práctica totalidad por la correspondiente función algorítmica, diseñada por los creadores de la red. La intervención de los nodos presenta, de esta forma, un elevado grado de automatización o predeterminación, de lo que resulta un significativo alejamiento con respecto al ideal de negociación o acuerdo entre iguales que evoca la noción de *consenso*²⁶.

En segundo lugar, y en íntima conexión con lo anterior, debe subrayarse que el consenso de los servidores no implica un pronunciamiento acerca de la legalidad de las transacciones, cuestión esta ajena al espacio digital y que, en su caso, habrá de resolverse en el mundo físico: de lo que se trata, por el contrario, es de verificar el cumplimiento de las reglas de funcionamiento de la propia red –por continuar con el ejemplo citado más arriba, que el pagador dispone en su cartera de criptoactivos suficientes para llevar a término la transacción controvertida–. Considerado cuanto viene de señalarse, la validación llevada a cabo por los nodos se traduce, en definitiva, en una participación de alcance muy limitado, en cuanto predefinida algorítmicamente y consistente en la comprobación automatizada de que se han observado determinadas condiciones técnicas²⁷.

Sentado lo anterior, ha de hacerse referencia a los mecanismos de consenso empleados en las redes *blockchain*²⁸. De todos ellos, destacan la denominada prueba de trabajo (*proof of work*), utilizada en la red Bitcoin, y la prueba de esfuerzo (*proof of stake*), que sirve de base al funcionamiento de la red Ethereum. Como sabemos, la actividad de minado llevada a cabo por los nodos o servidores integrantes de las respectivas redes es objeto de retribución conforme a las reglas establecidas en el correspondiente código. Los diferentes mecanismos de consenso permiten determinar a quién corresponde en cada caso la remuneración por razón de su participación, es decir, qué nodo ha llevado a cabo con éxito y en primer lugar la operación de validación de la última transacción de cada bloque. Cuestiones técnicas aparte, interesa en este momento reflexionar brevemente sobre las implicaciones de ambos

26. *Cfr.* nuevamente Low y Mik (2020: 140-142).

27. *Ibidem.*

28. Para una exposición general de los mismos, *cfr.* Ponce de León (2018: 51 y ss.).

modelos, que, como habrá de comprobarse seguidamente, plantean problemas específicos.

Por lo que hace al mecanismo de la prueba de trabajo, este determina la prioridad de los nodos cuyos equipos poseen una mayor capacidad computacional. Ello ha dado lugar, en el contexto de la red Bitcoin, a una auténtica carrera o competición entre los servidores, que en ocasiones se agrupan y acuerdan la creación de los conocidos como *mining pools* o fondos de minería, a fin de beneficiarse mutuamente de la capacidad computacional de los socios, y que incluso llegan a invertir elevadísimas sumas de dinero para la construcción de las denominadas *mining farms*, amplios espacios en los que se instalan dispositivos exclusivamente dedicados al minado de transacciones. Los estudiosos del fenómeno han señalado cómo, si bien la tecnología *blockchain* permite una deslocalización de estos centros y su ubicación en territorios con una alta disponibilidad de energías renovables, algunos inversores han optado por trasladar las instalaciones a países en los que el impacto medioambiental de esta actividad alcanza límites alarmantes. El crecimiento, que ya puede considerarse descontrolado e incluso exponencial, de la capacidad de computación de algunos actores, ha convertido en urgente la búsqueda de alternativas, máxime a la vista del escaso éxito que ha conocido el llamamiento de Nakamoto a un “pacto entre caballeros” con el fin de frenar la referida escalada por el bien de la propia red²⁹.

Las dudas que, desde la perspectiva de la sostenibilidad medioambiental, plantea esta tecnología, han motivado incluso el anuncio por parte de Elon Musk, en mayo de 2021, de que Tesla no aceptaría bitcoins como método de pago, noticia que tuvo un efecto devastador sobre la cotización de esta criptomoneda³⁰. Sin embargo, apenas dos meses después el magnate abriría de nuevo la puerta a su utilización, subrayando en todo caso que habrían de introducirse mejoras en relación con la cuestión que nos ocupa³¹. Estas declaraciones, claro está, han incidido antes sobre la recuperación del valor de bitcoin que sobre la (re)configuración del método de consenso³².

29. Sobre estas cuestiones, *cfr.*, por todos, Magnuson (2020: 122 y ss.).

30. “El bitcoin se desploma tras anunciar Musk que Tesla ya no acepta pagos con la criptomoneda”, en *El Economista*, 13 de mayo de 2021, noticia disponible en: <https://www.economista.es/mercados-cotizaciones/noticias/11212779/05/21/El-bitcoin-se-desploma-tras-anunciar-Musk-que-Tesla-ya-no-acepta-pagos-con-la-criptomoneda.html>.

31. “Tesla aceptará Bitcoin como forma de pago en el futuro, según afirma Musk”, en *CincoDías*, 22 de julio de 2021, noticia disponible en: https://cincodias.elpais.com/cincodias/2021/07/22/mercados/1626954992_738608.html.

32. “Elon Musk espolea al bitcoin tras anunciar que Tesla volverá a aceptarlo”, en *Bolsamanía*, 22 de julio de 2021, noticia disponible en: <https://www.bolsamania.com/>

La alternativa ofrecida por el sistema de la prueba de esfuerzo, mecanismo de consenso empleado en la red Ethereum, destaca, en este sentido, por poseer un impacto ambiental significativamente inferior. Ello es debido a que la *proof of stake* no privilegia a los nodos cuyos equipos poseen una mayor capacidad de computación, sino a aquellos que son titulares de un porcentaje más elevado de la categoría de criptoactivos que se utilizan en las transacciones llevadas a cabo en la red correspondiente, lo que, como se ha destacado, dota a su funcionamiento de un grado de determinismo superior al de otros mecanismos de consenso³³. De esta forma, el sistema ya no incentiva la inversión en equipos costosos y que consumen un elevado volumen de recursos energéticos, sino la involucración del servidor en la red. Así, el avance y la consolidación de esta no conducen forzosamente a una disyuntiva entre el progreso tecnológico y la protección del medio ambiente, como en cambio ocurre en el caso del sistema de la prueba de trabajo. Con todo, este mecanismo puede promover indirectamente la concentración del poder de decisión en manos de una minoría de nodos, situación de monopolio que puede llegar a resultar enormemente problemática desde diversas perspectivas, como habrá de comprobarse *infra*³⁴.

Abstracción hecha del específico problema de la sostenibilidad medioambiental de las redes basadas en la prueba de trabajo y de cuanto se ha señalado en relación con la falsa promesa de la que podría denominarse “cogobernanza de *blockchain*”, lo que interesa en este momento subrayar es que la técnica del consenso representa un elemento esencial, junto al empleo de la criptografía asimétrica, desde la perspectiva de la seguridad de la red: en la medida en que los nodos aceptan la validez de una determinada transacción, incorporando a la cadena operaciones sucesivas, se refuerza la estabilidad de aquella al aumentar exponencialmente los costes de su eventual modificación, lo que proporciona certidumbre a los sujetos intervinientes en relación con la misma. Ahora bien, ¿quiere ello decir que las transacciones que se integran en la cadena de bloques son realmente inmutables?

2.2.4. ¿Inmutabilidad de la cadena de bloques?

No son infrecuentes las referencias a las redes *blockchain* como entornos digitales en los que se registran transacciones de forma permanente, querién-

noticias/criptodivisas/elon-musk-espolea-al-bitcoin-tras-anunciar-que-tesla-volvera-a-aceptarlo--8043318.html.

33. Morales Barroso (2018: 57).

34. Apartado 2.4.

dose decir con ello que la cadena de bloques es inmutable. Tal forma de describir las redes *blockchain* traslada la idea de que, incorporada y validada una determinada operación en la cadena de bloques, y a diferencia de lo que ocurre con los archivos informáticos y las bases de datos tradicionales, su posterior corrección deviene imposible, lo que, si bien comportaría mejoras en términos de seguridad, plantearía asimismo dificultades específicas desde diversas perspectivas –por citar solo dos ejemplos, en relación con la observancia de algunas de las garantías previstas en la normativa sobre protección de datos personales o con la eventual declaración judicial de invalidez de un contrato ya ejecutado en la red–. El consenso de los nodos se impondría, de esta forma, sobre el propio sistema jurídico institucional, lo que incidiría negativamente sobre la eficacia tanto del derecho interno como de los ordenamientos supranacionales.

Sin perjuicio de que estas cuestiones hayan de ser tratadas específicamente más adelante, interesa en este momento subrayar que tal caracterización de las redes *blockchain* debe matizarse, por cuanto no resulta correcto afirmar la inmutabilidad absoluta de las transacciones registradas en la cadena de bloques, incluso una vez obtenido el consenso de los nodos. En este sentido, la experiencia de la red Ethereum es particularmente ilustrativa.

En extrema síntesis, los hechos fueron los siguientes³⁵. En el año 2016 la red Ethereum sufrió un hackeo que afectó a un elevado número de nodos y amenazó con provocar pérdidas multimillonarias. En dicho contexto, los participantes en la misma se vieron ante la disyuntiva de mantenerse fieles al ideal de la inmutabilidad de la red, lo que equivalía a una renuncia a toda posibilidad de recuperación de las criptomonedas sustraídas, o rectificar las transacciones ya validadas y, con ello, rehacer la cadena de bloques. La divergencia irreconciliable de opiniones sobre el particular motivó la escisión de un nutrido grupo de nodos y, con ella, la división en dos de la red, de forma que, en la actualidad, netamente diferenciada de la cadena que ha permanecido sin cambios, denominada Ethereum Classic, existe otra, que ha mantenido el nombre de Ethereum.

La conclusión que se impone con claridad a partir de lo anterior es que la introducción de modificaciones en la cadena de bloques que comporten una reconfiguración de la misma, transformación a la que comúnmente se hace referencia mediante el empleo de la expresión inglesa *hard fork* –diferente de

35. Para una exposición detallada del hackeo y la posterior escisión de Ethereum, hemos de remitirnos a Magnuson (2020: 61-66).

la mera revisión puntual de sus normas de funcionamiento o *soft fork*³⁶—, es una operación traumática, en cuanto no acorde, en principio, con la filosofía inspiradora de las redes *blockchain*, por lo que su realización, de admitirse, tiene lugar con carácter muy excepcional. Es sin duda discutible si, en el caso del hackeo de Ethereum, la opción correcta era la de asumir las pérdidas, mediante una defensa a ultranza de la seguridad, entendida como certidumbre, de las transacciones incorporadas a la cadena de bloques, o si, por el contrario, la gravedad de la situación permitía una flexibilización puntual del principio de inmutabilidad. Sin embargo, con independencia de la postura que en cada caso se adopte, lo cierto es que queda fuera de toda discusión que la tecnología *blockchain* no garantiza la inmutabilidad absoluta de las transacciones, de forma que el horizonte de la plena certidumbre empresarial, que parece estar detrás de la insistencia en este punto³⁷, no puede considerarse aún alcanzable.

Debe señalarse que el equívoco al respecto ha alcanzado al nivel regulatorio. En este sentido, la doctrina crítica con la caracterización de la *blockchain* como una tecnología que garantiza una inmutabilidad absoluta de las transacciones ha subrayado cómo dicha comprensión ha sido asumida por la legislación de Estados como Arizona. La cuestión es desde luego problemática, no solo por el lógico escepticismo al que puede dar lugar la consagración normativa de una característica de la tecnología que no se corresponde con los avances que esta posibilita, sino también por las dificultades interpretativas que resultan de la difuminación de los contornos aparentemente precisos de un concreto concepto a partir de su traslación al mundo jurídico³⁸. Ciertamente, es admisible en derecho la modulación del significado de determinadas nociones a partir de su juridificación; ello no puede resultar, sin embargo, de la falta de comprensión del ámbito de la realidad al que las mismas hacen referencia. Parece claro, en definitiva, que en este punto debe convenirse con quienes consideran que lo correcto sería aceptar las limitaciones de la tecnología *blockchain* y poner el foco en el análisis relativo a si la actual configuración de la misma aporta condiciones de seguridad satisfactorias desde la perspectiva de los correspondientes casos de uso³⁹.

36. En relación con la diferenciación entre *hard fork* y *soft fork*, con referencia a los papeles desempeñados en uno y otro caso por las diversas categorías de participantes en la red *blockchain*, véase Cappiello (2021: 21-22).

37. En este sentido, Herian (2020: 104, en nota al pie).

38. Al respecto, *vid.* Walch (2017: 1-2), que cuestiona la intención del legislador con respecto a esta cuestión.

39. En este sentido, Greenspan (2017).

2.3. Tipos de redes *blockchain*

Expuestos ya en apretada síntesis los principios de funcionamiento de *blockchain*, procede ahora culminar la descripción general de esta tecnología mediante una breve referencia a las características que presentan los diferentes tipos de redes. Ello permitirá no solo completar la explicación, ya apuntada, en relación con la flexibilidad de esta tecnología, sino también reflexionar acerca de las diversas posibilidades que ofrece su utilización por parte de las administraciones públicas. Esta última cuestión, en todo caso, habrá de ser abordada más adelante.

Las redes *blockchain* pueden clasificarse atendiendo a criterios diversos⁴⁰. En este sentido, un primer aspecto es el relativo a la forma de acceso, que permite diferenciar entre redes públicas, redes privadas y redes híbridas, federadas o de consorcio.

Las redes públicas son aquellas en las que la accesibilidad a los datos es universal, de forma que cualquier persona puede consultar el contenido de las transacciones. En esta categoría de redes no existen tampoco limitaciones en relación con la posibilidad de adquirir la condición de usuario, de forma que todo aquel cuyo equipo informático reúna unos determinados requisitos técnicos puede descargar la cadena de bloques y participar mediante la incorporación de transacciones a la misma. Como es evidente, este modelo de red *blockchain* permite el cumplimiento en grado máximo de los principios de distribución y descentralización, en la medida en que las redes públicas se basan tendencialmente en la igualdad de los nodos o servidores.

Por oposición a las anteriores, las redes privadas se caracterizan por la imposición de restricciones tanto al acceso a la información contenida en la cadena de bloques como a la posibilidad de inclusión de nuevas transacciones en la misma. Ello limita, claro está, la virtualidad de los principios de distribución y descentralización de manera significativa, toda vez que las redes privadas son administradas por una o varias autoridades centrales, a las que, como habrá de comprobarse seguidamente, se atribuye con carácter exclusivo la facultad para el otorgamiento de los correspondientes permisos de participación.

Por último, las redes híbridas, federadas o de consorcio poseen simultáneamente características propias de los dos tipos anteriores, puesto que, si bien en ellas el acceso a la información contenida en la cadena de bloques

40. Para una completa y didáctica explicación de esta cuestión, *cfr.*, por todos, Morales Barroso (2018: 50-51).

puede ser público, el control en relación con la validación de las transacciones se reserva a una categoría específica de usuarios.

El de la forma de acceso no es, en todo caso, el único criterio de clasificación de las redes *blockchain*. Presenta, en este sentido, idéntica relevancia la cuestión relativa al posible condicionamiento de la participación en la red consistente en la validación de las transacciones a la previa obtención del correspondiente permiso. Este aspecto comporta la distinción entre redes permissionadas y no permissionadas, categorización que es preciso diferenciar con claridad frente a la que opone las redes públicas a las redes privadas.

En este sentido, es claro que las redes privadas serán necesariamente permissionadas, pues carecería de sentido la imposición de límites para la incorporación de nuevas transacciones a la cadena de bloques si no se condicionara, al menos de la misma forma, la adquisición de la capacidad de validación. Sin embargo, las redes públicas no son forzosamente redes no permissionadas, pues es dable –y no solo conceptualmente, como demuestra la praxis– que la introducción de restricciones afecte tan solo a este último aspecto. De esta forma, la combinación de los dos criterios clasificatorios referidos permite diferenciar entre redes públicas, con o sin permisos, de una parte, redes privadas, de otra, y, en último lugar, redes híbridas, federadas o de consorcio.

Es evidente que los distintos tipos de redes *blockchain* ofrecen a los programadores un amplio abanico de posibilidades, en cuanto que permiten una adaptación de esta modalidad de tecnología de registro distribuido a necesidades muy variadas desde la perspectiva del grado de control que se desee reservar a favor de una hipotética autoridad central, pública o privada. Con idéntica claridad se impone la conclusión de que tan solo las redes públicas sin permisos se adecuan, en principio, al paradigma ideológico originario de la tecnología *blockchain*, puesto que tan solo mediante su empleo se garantiza la implantación *de los máximos niveles posibles* –debe retenerse esta matización, pues sobre ella se volverá seguidamente– de distribución, descentralización y desintermediación. En este sentido, la flexibilidad de la tecnología *blockchain*, la proliferación de casos de uso y el subsiguiente interés de las grandes compañías tecnológicas y de las autoridades públicas en liderar su desarrollo e implantación han conducido a una muy relevante transformación de aquella desde la perspectiva (no solo) filosófica, en la medida en que, de acuerdo con lo observado por algunos autores, a la etapa inicial o libertaria habrían sucedido las fases expansión y de consolidación

o madurez, habiéndose alcanzado un estadio en el que las redes privadas o permissionadas habrían desplazado a las redes públicas sin permisos⁴¹. Sin perjuicio de cuanto se dirá en el siguiente apartado, parece evidente que de lo anterior resulta la dilución o, en el mejor de los casos, el aplazamiento del proyecto de refundación de nuestras sociedades auspiciado por el movimiento *cyberpunk*.

Desde otra perspectiva, ha podido afirmarse que las redes *blockchain* de carácter privado presentan un impacto tecnológico limitado, en la medida en que se asimilarían al modelo, ya muy extendido, de la intranet⁴². Sin embargo, no por ello ha de infravalorarse la relevancia de esta categoría de redes, puesto que, si bien con respecto a las mismas parece obligado matizar el discurso relativo al carácter revolucionario de *blockchain* desde la perspectiva tecnológica, es igualmente cierto que, precisamente por su mayor manejabilidad en términos operativos, las redes privadas se hallan destinadas a producir las transformaciones más relevantes en la esfera económica⁴³.

2.4. Breve recapitulación: la controversia en torno a la tecnología *blockchain*

Como se ha apuntado a lo largo de la exposición precedente, dista de existir consenso en relación con el alcance, tanto efectivo como potencial, de la tecnología *blockchain*. En este sentido, frente a un relevante sector de opinión que, con expresiones en ocasiones notoriamente hiperbólicas⁴⁴, la presenta como un elemento clave en el futuro desarrollo de nuestras sociedades, se han alzado voces que alertan sobre la exageración de dicha visión, relativizan los avances que aquella propicia e incluso califican determinadas manifestaciones al respecto como una suerte de “discurso religioso, cripto-simbólico”⁴⁵, absolutamente ajeno a la realidad. En un punto intermedio se sitúan quienes,

41. Al respecto, *vid.* Dimitropoulos (2020: 1187-1188).

42. En este sentido, además de la referencia en la nota siguiente, *cf.* Herencia Antón (2021: 76).

43. En este sentido, *cf.* García Mexía (2018a: 29).

44. Destaca, entre las exposiciones más entusiastas en relación con la tecnología *blockchain*, la de Tapscott y Tapscott (2017: *passim*), algunas de cuyas valoraciones han sido cuestionadas en este mismo trabajo (*vid. supra*, apdo. 2.2.1). La hipérbole es característica, asimismo, de obras y escritos de tipo divulgativo, en los que se afirma, por ejemplo, que “el único límite que conoce la *blockchain* es la propia imaginación del ser humano” [Preukschat y Molero Manglano (2017: 15)].

45. En este sentido, especialmente, Herian (2020: 140 y ss.). Para una reflexión general sobre los equívocos a los que da lugar la “jerga *blockchain*”, con específica consideración de las dificultades asociadas a la misma desde la perspectiva regulatoria, *vid.* Walch (2017).

admitiendo la innovación que representa *blockchain*, adoptan una postura aparentemente más realista o prudente en relación con el fenómeno⁴⁶.

El examen detallado de las posiciones brevemente referidas y la toma de partido en el marco de esta polémica, compleja y rica en matices, exceden en mucho las pretensiones de la presente contribución. Nuestro más modesto objetivo será, por consiguiente, el de dar noticia de las principales líneas en torno a las cuales ha girado el debate, así como apuntar una serie de criterios para una más sosegada reflexión sobre la cuestión, que se encuentra, sin duda, llamada a continuar suscitando acaloradas discusiones durante largo tiempo. Algunos extremos, como la necesaria matización de la –pretendida por algunos– inmutabilidad de la cadena de bloques, han sido ya objeto de análisis específico, por lo que en este momento nos centraremos en aspectos diferentes de los ya tratados o en cuestiones conexas a los mismos, sobre las que resulta oportuno profundizar. Otros problemas, en fin, como el relativo a la posibilidad de empleo de la *blockchain* para fines delictivos, habrán de ser analizados en un momento posterior de la exposición, cuando se aborden los retos a los que se enfrenta la configuración del marco normativo aplicable a la misma⁴⁷.

De esta forma, un primer elemento a tomar en consideración es el referente a la efectiva facilitación por parte de esta tecnología de la tan ansiada desintermediación en la realización de un significativo número de categorías de transacciones, transformación que se presenta como correlato necesario de dos de los principios esenciales del funcionamiento de las redes *blockchain* –como ya sabemos, los de distribución y descentralización–. En el análisis de la cuestión se hará abstracción de la forzosa relativización de dicho aspecto sobre la base de la existencia de redes privadas o permissionadas, por tratarse de un extremo ya examinado en el apartado anterior del presente estudio y sobre el que no se considera necesario insistir.

Así, interesa destacar, en primer lugar, que, en contra de lo que algunas exposiciones sugieren, ni siquiera las redes públicas y sin permisos poseen un carácter absolutamente descentralizado. El ideal que se persigue mediante el

46. Cfr., en este sentido, la defensa del “criptorrealismo” de autores como García Mexía (2018a: 27), quien vaticina, en todo caso, un largo recorrido a *blockchain* y, en general, a las tecnologías de registro distribuido. En términos similares se refiere Dimitropoulos (2020: 1127) a lo común de la presentación de *blockchain* como un instrumento rodeado de un aura “mágica”, comprensión que rechaza como punto de partida en su investigación. Por todas, en fin, pueden consultarse igualmente las más ponderadas exposiciones de Finck (2019: *passim*) o Capiello (2021).

47. Apartado 3.1.

empleo de esta categoría de redes *blockchain*, tal y como con frecuencia se traslada a la opinión pública, es el defendido por el movimiento *cypherpunk*, a saber: la eliminación de toda intervención ajena a la de las partes de la correspondiente transacción, desarrollada ya por entidades del sector público, ya por sujetos u organizaciones de naturaleza privada. Sin embargo, como no ha dejado de subrayarse en algunos de los más relevantes análisis jurídicos de la tecnología *blockchain*, incluso esta modalidad de redes precisa de la intervención de sujetos encargados del mantenimiento del *software*⁴⁸, lo que implica la adopción de decisiones que afectan al funcionamiento de aquellas y, consiguientemente, a la actividad del conjunto de participantes y usuarios, por parte de una minoría.

Más aún, en segundo lugar, ha de señalarse que el correcto funcionamiento de algunas aplicaciones de las redes *blockchain* –como son los *smart contracts* o contratos inteligentes; en breve, programas informáticos que permiten la automatización de la ejecución de concretas operaciones, no necesariamente asociadas al cumplimiento de compromisos de naturaleza contractual, sobre los que se volverá en este y otros capítulos del presente volumen– exige la intervención de nuevas categorías de intermediarios, creadas *ad hoc* –por continuar con el ejemplo anterior, los denominados “oráculos”, que se ocupan de verificar el cumplimiento del hecho o factor externo que determina la ejecución automática de la operación u operaciones programadas en el *smart contract*–. Ello implica, como con buen tino se ha subrayado, la coexistencia de viejos y nuevos intermediarios⁴⁹, estado de cosas, como es obvio, manifiestamente alejado de la tierra prometida por los más entusiastas defensores de la tecnología *blockchain*⁵⁰.

En tercer lugar, la evolución de algunas de las principales redes, tendente al monopolio, representa un factor adicional de relativización de las ventajas comúnmente asociadas a la tecnología *blockchain*. Esta última cuestión afecta, de hecho, al propio núcleo de la retórica construida en torno a la misma, pues incide sobre la efectividad de los principios de distribución y descentralización, así como sobre otros aspectos esenciales, como son la sostenibilidad medioambiental e incluso la seguridad de las redes.

48. En este sentido, Finck (2019: 19 y 186 y ss.).

49. *Cfr.* nuevamente Finck (2019: 18-19); así como, entre otros, Dimitropoulos (2020: 1160). En la misma línea, ha podido señalarse expresivamente que la tecnología *blockchain* “no reduce el número de intermediarios, sino que los reubica”, en el sentido de que redefina su papel; *cfr.* Zaccaroni (2022: 255).

50. La proliferación de nuevas categorías de intermediarios en las redes *blockchain* ha conducido a algunos autores a “certificar” el fracaso de esta tecnología en este punto; en este sentido, por todos, Herian (2020: 113-114).

Con respecto a los efectos negativos que el mencionado fenómeno trae consigo desde la perspectiva de los principios de distribución y descentralización, una primera conclusión se impone con evidencia: la concentración del poder de decisión en manos de unos pocos servidores o nodos produce irremediamente una grave quiebra del principio de igualdad, elemento clave de las redes P2P. A la larga, una tal evolución podría incluso desincentivar la participación de quienes, pese a tener interés en ello, no pueden invertir los recursos necesarios para aspirar a obtener una retribución por su labor como validadores de las transacciones realizadas en la red. De esta forma, la tecnología *blockchain*, lejos de representar, como se ha pretendido, una oportunidad para la integración en los mercados de sujetos y colectivos tradicionalmente apartados de los mismos, se convertiría en un nuevo factor de exclusión. La garantía del ideal igualitario y, más en general, de los derechos de los usuarios, se erige, de esta forma, en reto fundamental de la regulación de las redes *blockchain*⁵¹.

Con todo, parece igualmente claro que la desigualdad de los participantes, que se manifiesta con una intensidad variable en función de la manera en que se configuren las redes *blockchain*, no es, al menos en principio, problemática en el contexto de su utilización por parte del sector público. Ciertamente, como se expondrá en este y otros capítulos de la presente obra, la amplitud de los objetivos y formas de la actividad administrativa trae consigo la posibilidad de implantación de casos de uso de características muy diversas. Con independencia de lo anterior, en relación con esta cuestión ha podido destacarse, amén de la ironía consustancial al hecho de que se interesen por las tecnologías de registro distribuido las que son autoridades centrales por antonomasia, la posibilidad de canalización de sus limitaciones y contradicciones internas hacia la consecución de fines de interés general⁵².

En relación con el segundo de los extremos apuntados –el impacto medioambiental de la tecnología *blockchain*–, ciertamente, como ya hemos tenido ocasión de destacar *supra*, el elemento decisivo viene representado, en último término, por la huella ecológica de los respectivos mecanismos de consenso, notoriamente dispares desde este punto de vista. Ello no obstante, no puede dejar de señalarse que la competición por hacerse con el control de la red implica, precisamente, el aumento exponencial del consumo energético

51. En este sentido, *cf.* las pertinentes reflexiones de Dimitropoulos (2020: 1176-1177, 1185 y 1188).

52. Al respecto, *cf.* nuevamente Herian (2020: 79). En idéntico sentido, con anterioridad, cabe citar el artículo de prensa “Governments may be big hackers of the blockchain”, publicado en *The Economist* el 1 de junio de 2017, disponible en: <https://www.economist.com/business/2017/06/01/governments-may-be-big-backers-of-the-blockchain>.

requerido para el desarrollo de la actividad de minado en redes como Bitcoin, en las que se emplea el denominado sistema de la prueba de trabajo. Por consiguiente, cabe concluir que, también desde esta perspectiva, el fenómeno puede llegar a adquirir tintes dramáticos.

Por último, la concentración del poder de decisión en manos de unos pocos nodos puede provocar un efecto muy negativo desde la perspectiva de la seguridad de la red. En este punto debe tenerse presente lo ya expuesto en relación con el consenso como base del funcionamiento de la *blockchain*: el que la validación de las transacciones requiera del acuerdo de los servidores o nodos constituye, junto al empleo de la criptografía asimétrica, la principal garantía de seguridad. Sin embargo, de asumir uno o varios servidores el control de hecho de la red, la probabilidad de éxito de operaciones contrarias al interés de la misma, cuando no pura y simplemente vulneradoras de la legalidad, puede llegar a incrementarse hasta límites insoportables. En este sentido, los especialistas alertan sobre el riesgo de que, en un escenario como el descrito, se produzca el conocido como ataque del 51 %, uno de los principales problemas de seguridad a los que puede llegar a enfrentarse la cadena de bloques. Este fenómeno tiene lugar cuando uno solo o varios nodos disponen de más de la mitad de la capacidad de cálculo de la red *blockchain*, lo que determina la eliminación del consenso como instrumento de gestión, en la medida en que aquel o aquellos podrá(n) imponer siempre al resto su criterio⁵³. Con respecto a Bitcoin, Nakamoto subrayó que cabría, efectivamente, dicha posibilidad, si bien defendió que en tales casos prevalecería, en buena lógica, el interés, compartido por *todos* los nodos, en garantizar la protección y continuidad del sistema⁵⁴. Sin embargo, parece que en este punto ha de convenirse con quienes señalan que esta visión no considera la posible existencia de incentivos ajenos a la red⁵⁵.

Íntimamente conectado con el anterior se encuentra un segundo aspecto, como es el relativo a la pretendida neutralidad de las redes *blockchain*. La cuestión entronca asimismo con el debate referente a la capacidad normativa del código, del que, como ya ha quedado dicho, se dará cuenta *infra*⁵⁶. Pese a ello, procede en este momento reflexionar brevemente sobre la corrección de las exposiciones que defienden que *blockchain* es una tecnología puramente

53. Sobre este reto para la seguridad de las redes *blockchain* y otros conexos, cabe remitirse, en la bibliografía española, a Márquez Solís (2017: 232) o a Morales Barroso (2018: 58-59).

54. Nakamoto (2008: 4).

55. Finck (2019: 21).

56. Apartado 3.2.

instrumental, inocua, ajena a toda ideología o interés diferente de la simplificación del sistema de relaciones entre los participantes en la red⁵⁷.

Si referido a la red o, más ampliamente, a las nuevas tecnologías, el concepto de *neutralidad* remite, en primer término, al profuso y conocido desarrollo jurisprudencial y normativo impulsado por las instituciones de la Unión Europea. Resultaría igualmente posible, en segundo lugar, su vinculación con la cuestión relativa a los sesgos de la inteligencia artificial y los sistemas algorítmicos, que comienza ya a estudiarse entre nosotros. Sin embargo, el debate en torno a la neutralidad de la tecnología *blockchain* afecta a aspectos netamente diferenciados de los anteriores, circunstancia determinante de la necesidad de dispensarle un tratamiento independiente.

En este sentido, puede resultar ciertamente paradójica la afirmación de la neutralidad de una tecnología cuyos fundamentos ideológicos han sido directamente vinculados con corrientes de pensamiento que cabe tildar de radicales, como se ha constatado en un momento anterior de la presente exposición⁵⁸. Es claro, en este sentido, que la pretensión de eliminación o, en el mejor de los casos, de sustitución del Estado por la autonomía individual en la gestión o supervisión de enteros sectores de actividad –aspecto esencial del movimiento *cypherpunk*– en modo alguno puede tacharse seriamente de neutra o inocua.

Con independencia de lo anterior, e incluso partiendo de que la *blockchain* no resulta apta para la consecución del objetivo criptoanarquista –lo que obliga a obviar la conexión ideológica más extrema de la tecnología, como se ha destacado *supra*–, algunos autores insisten vehementemente en su significación político-económica. En este sentido, las redes *blockchain* se pondrían, antes que nada, al servicio de la economía de mercado. El aspecto decisivo ya no sería el que, a través de su implantación, se tienda idealmente a la desintermediación, al menos parcial, de los intercambios económicos. Ni siquiera el que, como viene de subrayarse, el estado actual de la tecnología haya dado lugar a la aparición de nuevos modelos de intermediación, alejándose así de su objetivo inicial. Esencial al respecto sería, por el contrario, su utilidad en el impulso de la libre circulación de datos⁵⁹, fin, de hecho, perseguido con ahínco por la Comisión Europea –que ha afrontado la cuestión mediante la

57. Un muy reciente ejemplo de la referida comprensión puede encontrarse en Poncibò (2021: 141-142). En este sentido, la autora opone la neutralidad de la tecnología al carácter por definición ideológico del derecho.

58. Apartado 2.1.

59. En este sentido, Swan (2015: xi); para una crítica de la referida línea de desarrollo, *cf.*: Herian (2020: 105-106).

adopción de estrategias de signo diverso a lo largo del tiempo—, y para cuya consecución el desarrollo de la tecnología *blockchain* y, con ella, de la internet del valor, promete resultar decisivo⁶⁰.

No parece, sin embargo, que la constatación del carácter servicial de *blockchain* con respecto al sistema económico capitalista pueda sorprender. Como toda innovación tecnológica, *blockchain* precisa de financiación tanto para su desarrollo como para su efectiva implantación; en la medida en que aquella provendrá mayoritariamente de inversores pertenecientes al sector privado, resulta hasta cierto punto comprensible que su avance se oriente, en primer término, a la consecución de los objetivos de sus creadores y promotores⁶¹. Una conclusión diferente sería demostrativa ya de ingenuidad, ya de una actitud rayana en la hipocresía del personaje de Claude Rains en *Casablanca* (Michael Curtiz, 1943), cuya exclamación ante un indignado Humphrey Bogart, cuyo café ordena cerrar, se ha hecho justamente célebre —“¡Qué escándalo! He descubierto que aquí se juega”—.

En todo caso, cuestión diferente, si bien complementaria de la anterior, es lo discutible de la adscripción de la *blockchain* a las tesis del igualitarismo económico, basada en la transformación que resultaría de la efectiva desintermediación de amplios sectores de actividad. Como en tantas otras ocasiones, a este respecto los hechos hablan por sí solos: dejando a un lado lo lejano de la conversión en realidad de aquella promesa, resulta cuando menos indiciario de su carácter falaz el que muchos de los principales valedores de esta tecnología ocupen puestos de la máxima responsabilidad en las principales compañías del globo. Parece, en definitiva, que en este punto ha de darse la razón a los principales críticos de la retórica construida en torno a las tecnologías de registro distribuido⁶².

Ahora bien, si las redes *blockchain* poseen, efectivamente, un carácter servicial de los intereses de sus promotores y creadores, ello no prejuzga la bondad de su empleo por parte de las administraciones públicas. Más bien al contrario: una correcta selección de los casos de uso, acompañada de un adecuado diseño de la red, permitirá, precisamente, garantizar la satisfacción

60. Finck (2019: 118).

61. En este sentido, de nuevo, Finck (2019: 182 y ss.). Se produce así una llamativa paradoja, toda vez que la tecnología *blockchain*, vinculada inicialmente a movimientos antisistema, ha terminado, sin embargo, por verse respaldada por algunos de los principales actores económicos, que persiguen orientar la evolución de la misma en su beneficio; al respecto, *cfr.*: entre otros muchos, González-Meneses (2017: 28) y Dimitropoulos (2020: 1172).

62. En este sentido, por todos, Herian (2020: 136).

de aquel que ha de ser preservado por las mismas, que no es otro que el interés general. Sobre esta cuestión, en todo caso, habrá de volverse en un momento posterior de la exposición⁶³.

3. La regulación de la tecnología *blockchain*

Una vez expuestas las bases ideológicas y tecnológicas de *blockchain*, procede en este momento reflexionar brevemente sobre su regulación como tarea esencial –si bien no exclusiva, y probablemente ni siquiera principal– de los poderes públicos. En este sentido, como habrá de destacarse tanto en este como en otros capítulos de la presente obra, la (hasta la fecha desigual) intervención de los agentes públicos para favorecer el desarrollo y la implantación de la tecnología *blockchain* se ha basado no solamente en la adopción de concretas estrategias regulatorias, sino también en la incorporación de aquella en el ejercicio de determinadas potestades administrativas. No obstante su carácter complementario, ambas formas de afrontar el fenómeno poseen, como es notorio, una naturaleza diferenciada, razón por la que su tratamiento se abordará en fases sucesivas.

De esta forma, en las páginas que siguen se referirán sintéticamente, en primer término, las dificultades que presenta la configuración del marco jurídico aplicable a la tecnología *blockchain* (3.1). En segundo lugar, se analizarán críticamente las construcciones doctrinales que ven en el código informático una nueva fuente de producción normativa, hábil incluso para desplazar, en determinados contextos, al derecho institucional (3.2). El presente apartado se completará con una reflexión sobre las diferentes ópticas desde las que es posible abordar la regulación de esta modalidad de tecnología (3.3).

3.1. Los retos para el diseño de la disciplina jurídica aplicable a la tecnología *blockchain*

3.1.1. Mutabilidad de la tecnología *blockchain*

Al subrayar que la mutabilidad de *blockchain* dificulta la adopción de decisiones de tipo normativo en relación con la misma nos referimos no tanto a la existencia de un amplio abanico de posibilidades para la configuración de las redes, ca-

63. Apartado 4.

racterística designada en la exposición precedente como *flexibilidad*, cuanto a la falta de culminación del desarrollo de la propia tecnología. *Blockchain* es, en este sentido, un instrumento precisado de importantes avances, que deberán facilitar su implantación a gran escala: entre otros aspectos, la réplica de la totalidad de la información contenida en el libro mayor en los dispositivos del conjunto de servidores de la red, presupuesto del carácter distribuido de la misma, imposibilita en el momento actual el crecimiento que muchos auguran. Si bien algunos especialistas son optimistas al respecto, la superación de la limitación referida es aún una cuestión pendiente⁶⁴. Este es el motivo, en lo que aquí interesa, por el que no parece que ni el tratamiento jurídico ni la propia reflexión acerca de *blockchain* desde la perspectiva del derecho puedan aspirar a sentar principios o conclusiones de forma definitiva (¿alguna vez lo hacen?), puesto que los retos que aquella plantea, así como las posibilidades que ofrece, no pueden aún conocerse con total certidumbre (¿existe en algún ámbito?).

Con todo, la falta de madurez de la tecnología *blockchain* puede contemplarse, al mismo tiempo, como un aliado fundamental de las instancias dotadas de potestades normativas o, más en general, de regulación. Como con acierto se ha destacado, la intervención de los poderes públicos en relación con los fenómenos tecnológicos tan solo puede resultar eficaz en la medida en que se produzca en una fase lo suficientemente temprana como para garantizar que su desarrollo respetará los principios jurídicos esenciales del ordenamiento y, singularmente, los derechos de los ciudadanos⁶⁵. Dicho de otra forma, la mutabilidad de *blockchain* representa antes una oportunidad que un obstáculo para la configuración del marco normativo finalmente aplicable a la misma. En consecuencia –y sobre este extremo habrá de volverse *infra*⁶⁶–, la existencia de aspectos pendientes de revisión en el plano tecnológico no debe servir de fundamento a la adopción de un enfoque regulatorio de corte abstencionista.

3.1.2. La supranacionalidad del fenómeno

Un segundo desafío al que se enfrentan las autoridades públicas en la definición del marco normativo aplicable a las tecnologías de registro distribuido es el relativo a la posible implantación transnacional de las redes. En este sentido, la pretensión de disciplinar jurídicamente la actuación desarrollada en los entornos *blockchain* podría verse obstaculizada como consecuencia de

64. Sobre estas cuestiones, Finck (2019: 31-32).

65. Cfr. nuevamente Finck (2019: 33).

66. Apartado 3.3.2.

la forzosa circunscripción de la acción pública a los límites territoriales de los respectivos Estados. En consecuencia, en el caso de que las autoridades de un concreto país adoptaran una postura excesivamente rigurosa o restrictiva, los participantes de la red tan solo habrían de trasladarse a otro lugar del planeta si desearan eludir la aplicación del correspondiente sistema normativo⁶⁷.

La cuestión entronca directamente con una serie de dificultades de alcance más amplio que plantean las tecnologías de registro distribuido desde la perspectiva de la soberanía nacional⁶⁸ y se encuentra, además, íntimamente relacionada con diversos retos jurídicos que en su momento suscitó la aparición de internet⁶⁹. Como resulta evidente, el problema deriva de forma directa del carácter distribuido de las redes *blockchain* y se aproxima, además, en cuanto obstáculo para la efectividad del marco jurídico, a la garantía de pseudonimidad en los referidos entornos digitales y al posible desarrollo de usos de carácter delictivo⁷⁰. Un correcto tratamiento del mismo exige la consideración simultánea de tres extremos: de una parte, la diversidad de técnicas a disposición de los agentes públicos para la configuración del sistema normativo y regulatorio aplicable a la tecnología *blockchain*; de otra, la existencia de una pluralidad de tipos de operadores en la red, que representan otros tantos puntos de conexión de dicho marco; y, por último, el creciente interés de la traslación del debate y de la adopción de decisiones al respecto en el nivel supranacional.

En lo que hace al primer aspecto, debe subrayarse, sin perjuicio de lo que se expondrá en sucesivos epígrafes del presente estudio, que la respuesta normativa frente a la tecnología *blockchain* no puede en modo alguno plantearse desde la sola perspectiva de la conformidad a derecho de las correspondientes conductas. Abstracción hecha, como es lógico, de las particularidades que presenta en este sentido el problema de los usos delictivos, sobre el que se volverá seguidamente, las autoridades públicas pueden acudir a mecanismos de naturaleza diversa y alcance muy dispar para alcanzar los objetivos que, en cada momento, se consideren adecuados en relación con concretos casos de uso

67. A este respecto, por ceñirnos tan solo a las principales exposiciones en la materia, *cf.* De Filippi y Wright (2018: 182-183), Finck (2019: 58-60) y Dimitropoulos (2020: 1119, 1157 y ss.).

68. Nos referimos, en particular, a la erosión de la soberanía de los Estados que resulta no solo del surgimiento y consolidación de medios de pago alternativos a las monedas nacionales, sino también como consecuencia de la posible sustitución parcial de determinados actores institucionales en el desarrollo de concretas funciones de naturaleza pública. Sobre algunas de estas cuestiones habrá de volverse *infra*; para una reflexión general, que engloba el conjunto de aspectos referidos, hemos de remitirnos en este momento a De Caria (2021).

69. Sobre el particular, es obligada la remisión *in toto* a Muñoz Machado (2000).

70. Cuestión a la que se hará breve referencia seguidamente (apartado 3.1.3).

de las tecnologías de registro distribuido. Así, mandato y prohibición, en cuanto formas de actuación de implicaciones más inmediatas, habrán de reservarse para los supuestos en los que otros planteamientos, tales como el recurso a las medidas de fomento, se revelen insuficientes⁷¹. De esta forma, ha de concluirse que el problema de la potencial implantación transnacional de una determinada red *blockchain* se plantea, específicamente, en relación con aquellos casos de uso en los que no resulte posible acudir al resultado legítimamente perseguido por el Estado sin una intervención de sus agentes dotada de un grado máximo de intensidad, pues, de lo contrario, el reto vendrá realmente representado por la dificultad de alcanzar el necesario equilibrio entre las posiciones extremas de la hiperregulación y de la ausencia de disciplina jurídica. Como ha quedado dicho, en todo caso, sobre estas cuestiones habrá de volverse *infra*⁷².

En lo relativo al segundo aspecto, en la exposición precedente ha habido ya ocasión de hacer referencia a algunas de las diferentes modalidades de participantes en las redes *blockchain*. Ciertamente, el carácter distribuido de esta tecnología permite que los servidores o nodos, depositarios de una copia auténtica del libro mayor y encargados de la validación de las transacciones mediante la aplicación del correspondiente mecanismo de consenso, se trasladen de un punto a otro del globo sin perder por ello la posibilidad de continuar desarrollando dichas funciones. En todo caso, junto a ellos se encuentran otros muchos sujetos con diversos grados de intervención en la red y que la doctrina ha identificado como potenciales destinatarios de la regulación aplicable a la tecnología *blockchain*: desarrolladores de *software*, fabricantes de *hardware*, intermediarios y usuarios finales de las aplicaciones, entre otros, pueden incardinarse en el ámbito subjetivo de aplicación de las correspondientes normas o, en su caso, de las medidas de fomento adoptadas por las autoridades nacionales⁷³. En último término, el problema de la deslocalización es común

71. Sobre los diferentes grados de intensidad de la regulación aplicable a la tecnología *blockchain* y la necesidad de reservar los más elevados a las aplicaciones sensibles, *cf.*: García Mexía (2018b: 115).

72. Apartado 3.3.

73. En este sentido, entre otros, De Filippi y Wright (2018: 175 y ss.), García Mexía (2018b: 119-120), Sarzana di S. Ippolito y Nicotra (2018: 36 y ss.), o Finck (2019: 46 y ss.). Esta última autora (2019: 54) efectúa una interesante precisión en relación con la selección de los destinatarios de la normativa aplicable a la tecnología *blockchain*, al señalar que, mientras determinados operadores disponen de una capacidad efectiva de deslocalización a fin de evitar la aplicación de concretos marcos reguladores –piénsese, por ejemplo, en los servidores o nodos que se dedican profesionalmente a dicha labor–, otras categorías de sujetos, particularmente los usuarios finales de las aplicaciones, carecerán en la mayor parte de los casos de la referida capacidad o de incentivos suficientes para fijar su domicilio en función de la mayor o menor benignidad de las reglas que les resulten de aplicación, dato de extraordinaria relevancia en orden a la determinación de la estrategia de intervención a adoptar por parte de las autoridades públicas.

a numerosos sectores del derecho –ajenos, incluso, al tecnológico– y, aunque ciertamente represente un reto significativo, no ha comportado la forzosa abdicación de la actuación pública allá donde la misma ha resultado necesaria a fin de salvaguardar los principios fundamentales del ordenamiento.

En lo concerniente, en fin, al tercer aspecto, debe tenerse presente que tanto la reflexión en torno a la regulación de la tecnología *blockchain* como muchas de las principales iniciativas de carácter normativo se han desarrollado a nivel global, es decir, no han sido lideradas por un único Estado, sino por entidades de alcance territorial superior. Tal es el caso, particularmente relevante a nuestros efectos, de la Unión Europea: en 2018, la Comisión fundó el *European Blockchain Observatory & Forum*⁷⁴ y publicó, en enero de 2020, su propia estrategia *blockchain*⁷⁵; asimismo, participa, junto al conjunto de Estados miembros, Noruega y Liechtenstein, en la red EBSI (*European Blockchain Services Infrastructure*)⁷⁶; y, entre otras importantes iniciativas normativas⁷⁷, ha presentado el pasado 15 de

74. Sobre esta iniciativa de la Comisión Europea, *cf.* el sitio web: <https://www.eublockchainforum.eu/>.

75. La estrategia *blockchain* de la Comisión Europea persigue impulsar el liderazgo de la Unión en la implantación de las tecnologías de registro distribuido y garantizar que su desarrollo se acomoda a los principios y valores esenciales del ordenamiento jurídico comunitario. En este sentido, la propia Comisión identifica como elementos del denominado “*gold standard*” de *blockchain* la sostenibilidad medioambiental, la protección de los datos de carácter personal, la salvaguarda del marco normativo vigente en materia de identidad digital, la garantía de estándares elevados de ciberseguridad y la interoperabilidad de las redes. La Comisión se ha referido, igualmente, a las vías que habrán de transitarse para la consecución de los referidos objetivos (clarificación del marco normativo aplicable, aumento de las inversiones, cooperación, etc.). Para una visión en detalle al respecto, puede consultarse el sitio web: <https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy>.

76. De acuerdo con la definición aportada por la propia Comisión, EBSI es una red P2P de nodos interconectados encargados de la gestión de una infraestructura de servicios basada en la tecnología *blockchain*. El objetivo de la iniciativa es el desarrollo de aplicaciones por parte de las autoridades públicas participantes que puedan conectarse a la propia red, posibilidad que en un futuro podría igualmente extenderse a las organizaciones privadas. Los casos de uso articulados con carácter inicial permiten la automatización de los procesos de auditoría, la gestión por los particulares de sus propios certificados de estudios, la descentralización en la gestión de la identidad digital a través de las fronteras y el intercambio seguro de datos entre autoridades. Se prevé, asimismo, la implantación sucesiva de nuevas aplicaciones en relación con la financiación de las pequeñas y medianas empresas a través de *blockchain*, la prestación de servicios sociales de carácter transnacional y las peticiones de asilo. Sobre estas cuestiones, véase la información proporcionada por la Comisión en el sitio web: <https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure>.

77. Entre las que destacan particularmente la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos, COM(2020) 593 final, y la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre un régimen piloto de las infraestructuras del mercado basadas en la tecnología de registro descentralizado, COM(2020) 594 final, ambas de 24 de septiembre de 2020. Para un análisis conjunto de las mismas, *cf.* la esclarecedora exposición de Zaccaroni (2022: 257 y ss.).

enero de 2021 la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea (conocido como Reglamento eIDAS)⁷⁸. Por consiguiente, parece claro que, cuando menos en el contexto europeo, es posible advertir una apuesta decidida a favor de la cooperación supranacional como vía para la conformación de un entorno de reflexión, de un marco jurídico y de unas políticas públicas comunes con respecto a la tecnología *blockchain*, lo que coadyuva –sin garantizarla completamente⁷⁹– a la superación de las dificultades que, desde la perspectiva de la eficacia de las normas, resultan del carácter distribuido y (potencialmente) transnacional de las redes.

3.1.3. El desafío de los usos delictivos

Una tercera cuestión que ha de tenerse en cuenta desde la perspectiva de la regulación de la tecnología *blockchain* es su potencial “utilidad” para el desarrollo de conductas ilegales, habida cuenta, por una parte, de la posibilidad de participación pseudónima en las redes y, por otra, de la –pretendida por muchos– garantía de inmutabilidad de la cadena de bloques, que comportaría la irreversibilidad de las transacciones constitutivas de delito que se hubieran registrado en la misma. Dejando a un lado este segundo extremo, objeto de consideración crítica *supra*⁸⁰, interesa subrayar en este momento que el avance favorecido por las tecnologías de registro distribuido en términos de privacidad puede facilitar, al mismo tiempo, la comisión de delitos o, más en general, producir efectos muy negativos desde la perspectiva del cumplimiento normativo⁸¹.

El problema, apuntado ya por los líderes del movimiento *cypherpunk* –que no parecían, en todo caso, especialmente preocupados por ello, al menos si se consideran los términos empleados por Timothy C. May en su célebre *Manifiesto Criptoanarquista*–, se evidenció hace unos años a raíz de la utilización de bitcoins como medio de pago de artículos ilegales en la red TOR (acrónimo de *The Opinion Router*), así como para la realización de

78. Cuyo texto puede consultarse en el siguiente enlace: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0281>. En relación con su contenido e implicaciones en el ordenamiento jurídico español, hemos de remitirnos a la contribución de Berning Prieto en este mismo volumen y a la bibliografía allí citada.

79. En este sentido, entre otros, Finck (2019: 160-161) y Magnuson (2020: 107-108). *Cf.*: igualmente De Caria (2021: 41), para quien el reto planteado por la tecnología *blockchain* en términos de soberanía afecta no solo al nivel estatal de poder, sino también a organizaciones internacionales “que aspiran a adquirir soberanía, como la Unión Europea”.

80. Apartado 2.2.4.

81. Al respecto, entre otros, Finck (2019: 63-64).

actuaciones constitutivas de fraude fiscal o de blanqueo de capitales⁸². No parece, en este sentido, que hasta la fecha se hayan experimentado avances significativos desde esta perspectiva, a juzgar por las declaraciones del presidente de la Comisión Nacional del Mercado de Valores, que ha alertado recientemente sobre un aumento de las estafas piramidales ligadas a las criptodivisas⁸³.

Estas circunstancias, al menos en teoría, habrían motivado la reciente imposición por parte del Banco Popular de China de la prohibición de realización de pagos con bitcoins, decisión que ha provocado un efecto similar al del anuncio original de Elon Musk sobre la cotización del sector de las criptomonedas⁸⁴. La adopción de una política de signo tan restrictivo por el gigante asiático, tradicional valedor de la tecnología *blockchain*, se encuentra, ciertamente, lejos de representar el punto final de la misma⁸⁵, pero no puede obviarse la posibilidad de que llegue a convertirse en un obstáculo muy relevante para su desarrollo.

Desde una perspectiva general, la doctrina ha mostrado una cierta tendencia a relativizar el riesgo de que las redes *blockchain* se conviertan en un paraíso para los ciberdelincuentes. El tratamiento de la cuestión en la literatura especializada ha combinado consideraciones de política criminal con la reflexión sobre la propia naturaleza de los entornos *blockchain* y acerca de las limitaciones ínsitas a toda forma de intervención legal. La posibilidad de que determinados participantes en la red se sirvan de las características de las tecnologías de registro distribuido para la realización de actuaciones contrarias a derecho no justificaría, en definitiva, de acuerdo con la visión mayoritaria, medidas tan drásticas como la radical prohibición del empleo de la criptomoneda bitcoin como medio de pago por parte de la República Popular China.

82. *Vid.* el artículo publicado en *ABC* el 25 de septiembre de 2017, titulado “El bitcoin, ¿la moneda de los cibercriminales?”, disponible en: https://www.abc.es/tecnologia/redes/abci-bitcoin-moneda-cibercriminales-201706021218_noticia.html.

83. “La CNMV alerta de un incremento de estafas piramidales ligadas a criptodivisas”, artículo publicado en *ABC* el 29 de septiembre de 2021, disponible en: https://www.abc.es/economia/abci-cnmv-alerta-incremento-estafas-piramidales-ligadas-criptodivisas-202109291018_noticia.html.

84. Al respecto, *cf.* el artículo de prensa “El bitcoin pierde un 40% de su valor desde abril tras la prohibición de su uso en China como moneda”, en: <https://www.rtve.es/noticias/20210519/bitcoin-criptomoneda-pierde-valor-prohibicion-china/2091061.shtml>.

85. Así, tal y como cabía suponer, de acuerdo con las últimas noticias, Bitcoin parece haber recuperado el nivel de actividad previo al veto del Gobierno chino, impulsado por su expansión en Estados Unidos. *Cf.*: “Los criptomneros han recuperado los niveles récord de actividad previos al veto de China”, en *Business Insider*, 9 de diciembre de 2021, disponible en: <https://www.businessinsider.es/como-afectando-prohibicion-china-mineria-bitcoin-977915>.

En este sentido, se ha partido en ocasiones de la incapacidad de las autoridades públicas para evitar y, eventualmente, sancionar *toda* la actividad delictiva, característica común a todos los ámbitos, en modo alguno propia de aquellos en los que el empleo de las tecnologías de registro distribuido puede llegar a suponer una ventaja para el infractor⁸⁶. De esta forma, parece querer sugerirse que la delincuencia en las redes *blockchain* no presenta diferencias significativas con respecto a la que se produce en otros contextos, ya digitales, ya analógicos. En nuestra opinión, de aceptarse la anterior conclusión, es claro que de la misma tan solo se seguiría la improcedencia de la imposición de una prohibición general de actuación en los referidos entornos —en último término, la invalidez de los pagos con bitcoins nos situaría en la casilla de salida del apartado anterior, referido al carácter potencialmente transnacional de las redes y al perjuicio que de ello se deriva desde la perspectiva de la eficacia de los sistemas normativos nacionales—, en ningún caso la innecesariedad de la toma en consideración específica de las características de la tecnología *blockchain* para el diseño de estrategias de prevención y de detección de las actuaciones ilegales cuya realización pueda verse facilitada por aquella.

Mayor interés presentan, desde la perspectiva que ahora interesa, los estudios que consideran las especialidades de las tecnologías de registro distribuido y, en particular, las dinámicas de grupo que se observan en las redes *blockchain* como elementos clave en la lucha contra la criminalidad desarrollada en estos entornos digitales. Pese a las necesarias matizaciones, el carácter distribuido y descentralizado de las redes *blockchain* generaría un sentimiento de pertenencia a la comunidad que podría redundar —se argumenta— en una mayor eficacia de las normas de origen social, esto es, de las impuestas por los propios participantes⁸⁷. Sin perjuicio de cuanto se dirá *infra* sobre el carácter regulador del código informático y acerca del posible desplazamiento por el mismo del ordenamiento jurídico institucional⁸⁸, debe ahora reflexionarse, siquiera sea brevemente, sobre las posibilidades de reacción de la red ante las conductas ilegales producidas en su seno.

En relación con esta cuestión, hemos tenido ya ocasión de destacar cómo el discurso construido en torno a la capacidad de codecisión de los participantes en las redes *blockchain* es, ciertamente, cuestionable,

86. En este sentido, específicamente, De Filippi y Wright (2018: 192).

87. En este sentido, Magnuson (2020: 110), que, no obstante, matiza inmediatamente su discurso, analizando con detenimiento diversos factores que conducirían a la conclusión de que las normas sociales no resultan especialmente efectivas para luchar contra la criminalidad en el contexto de las redes *blockchain*.

88. Apartado 3.2.

consideradas la creciente monopolización de las mismas por parte de determinados operadores y, sobre todo, la limitación de la intervención de los nodos o servidores al desarrollo de una labor de validación predefinida algorítmicamente⁸⁹. A mayor abundamiento, debe tenerse presente que la realización de actividades delictivas en las redes *blockchain* es un hecho contrastado, y que la implantación global y las dimensiones de algunas de ellas no solo dificultan la cohesión del grupo y la adopción de estándares satisfactorios desde la perspectiva de la defensa de los intereses del conjunto de participantes –presupuestos de la efectividad de las normas de origen social–, sino que, además, otorgan un extraordinario potencial lesivo a los *hackers*⁹⁰. De ello resulta una significativa limitación de la capacidad reactiva de la red ante las infracciones eventualmente cometidas por parte de quienes la integran, en cuanto, en principio, reservada a los supuestos de irrogación de daños especialmente graves a la misma, en los que cabe acordar la reconstrucción de la cadena de bloques a través del mecanismo del *hard fork*.

Sin embargo, y no obstante su carácter de *ultima ratio*, entendemos que no debe infravalorarse la relevancia de este instrumento en la lucha contra la criminalidad en los entornos *blockchain*. La rectificación de la red Ethereum en el año 2016 fue acordada, como ya se ha expuesto, precisamente como reacción frente a la comisión de una infracción, la sustracción de criptomonedas, cuya gravedad resultaba no solo de la contravención de las normas rectoras de los comportamientos en la red, sino también de su carácter ilícito en aplicación del marco normativo institucional. La experiencia es demostrativa, en suma, de que los principios de funcionamiento de la tecnología *blockchain* posibilitan la corrección de determinadas conductas contrarias a derecho *por parte de los propios participantes*.

De lo señalado hasta el momento en relación con los límites de la eficacia de los ordenamientos institucionales –consecuencia del carácter distribuido y potencialmente transnacional de las redes *blockchain*– y la reducida, aunque en modo alguno irrelevante, capacidad reactiva de la red ante las conductas constitutivas de delito producidas en su seno, es posible extraer algunas conclusiones de interés. La primera de ellas es la referente a la recomendable aplicación de las construcciones sociológicas relativas a la lucha contra la criminalidad al específico contexto de las redes *blockchain*. Dada la complejidad de la materia, la limitación de la intervención a la perspectiva

89. *Vid. supra*, apartados 2.2.3 y 2.4.

90. *Cfr.* nuevamente Magnuson (2020: 111 y ss.).

legal en sentido estricto se considera insuficiente⁹¹. En este sentido, algunos autores se han esforzado en aplicar las teorías de prevención del crimen que gozan de una mayor aceptación a los entornos *blockchain*, subrayando las ventajas e inconvenientes de las mismas, así como los beneficios y riesgos de su implementación simultánea. De esta forma –se argumenta–, si bien los poderes públicos pueden adoptar puntos de partida diversos para la lucha contra la criminalidad en las redes *blockchain* –poniendo énfasis bien en la efectividad de los correspondientes regímenes sancionadores, bien en la percepción social sobre la bondad de las normas, bien, en fin, en la apariencia de cumplimiento general de las mismas–, debe tenerse en cuenta que su empleo concurrente no siempre resulta posible y en algunos casos puede llegar a revelarse contraproducente⁹².

La segunda conclusión relevante a los efectos de la presente exposición es la referente a la forzosa aceptación de los límites de las formas tradicionales de la acción pública para la lucha contra la criminalidad en las redes *blockchain*. Sin perjuicio de las soluciones apuntadas en el apartado anterior en relación con el problema del carácter transnacional de las tecnologías de registro distribuido, la descentralización que las mismas favorecen debilita notablemente la efectividad de las estrategias implementadas hasta nuestros días para la prevención y la detección de conductas delictivas en los referidos entornos digitales. La alternativa parece encontrarse en la reorientación de la acción pública hacia las propias redes, esto es, en la intervención institucional en la definición de sus normas rectoras, pues solo el liderazgo público en relación con el desarrollo e implantación de aquellas permitirá evitar las potenciales consecuencias indeseadas de la llamada revolución *blockchain*.

En definitiva, parece claro que la lucha contra la criminalidad en los entornos *blockchain* habrá de abordarse principalmente desde el ámbito tecnológico. En este sentido, como con acierto se ha destacado, los avances que hayan de conocer las tecnologías de registro distribuido deberán orientarse a la consecución de unos niveles de privacidad satisfactorios sin que ello perjudique la efectividad de los instrumentos empleados en el contexto del cumplimiento normativo⁹³. La reconducción de la evolución de la tecnología *blockchain* en el sentido indicado dependerá de la implicación de los agentes públicos en la supervisión de los correspondientes progresos y en la incentivación de su alineación con los principios esenciales de nuestro

91. En este sentido, por todos, Magnuson (2020: 107-108).

92. Cfr. de nuevo Magnuson (2020: 100-121).

93. Cfr. Finck (2019: 64).

sistema jurídico. De no adoptarse esta estrategia de forma temprana, podría terminar por resultar inevitable el recurso a severas medidas restrictivas, con los consiguientes efectos limitativos del avance tecnológico. El examen de los instrumentos que cabe emplear a tal fin habrá de desarrollarse *infra*⁹⁴.

3.1.4. El (difícil) encaje de *blockchain* en los sistemas normativos vigentes. Breve referencia a la protección de datos de carácter personal (remisión)

Un cuarto y último aspecto que ha de ser tomado en consideración en el análisis de los retos a los que se enfrentan las autoridades públicas a la hora de definir el marco normativo aplicable a la tecnología *blockchain* es el relativo a la dificultad de la reconducción de las aplicaciones desarrolladas sobre la base de la misma a los institutos del derecho vigente. La cuestión presenta una complejidad notable y es, además, transversal o común a varias disciplinas jurídicas, lo que justificaría sobradamente su tratamiento independiente. Por razones de espacio, la exposición sucesiva se limitará a dar cuenta de las principales áreas en las que se ha puesto de manifiesto el problema, y a aportar elementos de reflexión sobre la importancia del mismo desde la perspectiva de la selección del enfoque regulatorio a adoptar con respecto a las tecnologías de registro distribuido.

Un primer sector del ordenamiento en el que se ha evidenciado la dificultad de la subsunción de las aplicaciones y operaciones desarrolladas sobre la base de la tecnología *blockchain*, así como de los valores intercambiados en las redes, es –ello resulta evidente– el mercantil. En este sentido, particularmente discutida y discutible ha resultado la identificación de la naturaleza jurídica de las criptomonedas, puesto que las mismas casan mal con las diversas categorías conceptuales que proporcionan los sistemas normativos vigentes. Esta circunstancia, como con acierto se ha destacado, puede producir efectos muy negativos en los mercados, al resultar posible la concurrencia de subsectores normativos diversos –con las consiguientes dificultades para los operadores– incluso en la conclusión de transacciones de un valor económico limitado⁹⁵.

A este respecto, el Tribunal Supremo español, en una muy relevante Sentencia de la Sala 2.^a de 20 de junio de 2019 (recurso de casación núm. 998/2018), ha concluido que la criptomoneda bitcoin no puede recibir la

94. Apartado 3.3.

95. Al respecto, *cf.*: la completa exposición de Magnuson (2020: 155 y ss.).

consideración de dinero a los efectos de determinación de la responsabilidad civil derivada del delito:

“El *bitcoin* no es sino una unidad de cuenta de la red del mismo nombre. A partir de un libro de cuentas público y distribuido, donde se almacenan todas las transacciones de manera permanente en una base de datos denominada *Blockchain*, se crearon 21 millones de estas unidades, que se comercializan de manera divisible a través de una red informática verificada. De este modo, el *bitcoin* no es sino un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica denominada *bitcoin*, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta que de estas unidades se realiza a través de las plataformas de *trading Bitcoin*”.

De esta forma, de acuerdo con la visión del alto tribunal, la indemnización que correspondería abonar al declarado culpable del delito de estafa por la captación, mediante engaño, de clientes cuyas inversiones en bitcoins se había comprometido a gestionar, no consistiría en la devolución de las criptomonedas que se le entregaron a tal fin, sino del

“importe de la aportación dineraria realizada (daño), con un incremento como perjuicio que [se] concreta en la rentabilidad que hubiera ofrecido el precio de las unidades *bitcoin* entre el momento de la inversión y la fecha del vencimiento de sus respectivos contratos” (FJ 3).

Así, la no caracterización como dinero de la criptomoneda *bitcón* sirve al Tribunal Supremo para determinar los criterios aplicables a la cuantificación de la responsabilidad civil derivada del delito en el caso de autos. Ahora bien, la Sentencia no aporta precisión adicional alguna en relación con la calificación jurídica general de las criptomonedas, lo que se traduce no solo en la existencia de notables dosis de incertidumbre desde la perspectiva mercantil, sino también, en segundo lugar, en los ámbitos contable y tributario. Así lo ha destacado la doctrina especializada⁹⁶.

Un tercer sector del ordenamiento para el que *blockchain* representa un reto de envergadura, en cuanto tecnología disruptiva, como gusta de decirse, con respecto a los parámetros vigentes en la actualidad, es el acervo normativo

96. Por todos, Pedreira Menéndez y Álvarez Pérez (2018).

construido para la garantía del derecho fundamental a la protección de datos de carácter personal. Sin perjuicio de que sobre la cuestión se profundizará en otro lugar del presente volumen⁹⁷, interesa destacar en este momento dos aspectos esenciales en relación con la cuestión, a fin de dar breve cuenta del desafío que, en este contexto, representan las tecnologías de registro distribuido.

El primero de ellos es el relativo a la determinación de los destinatarios del conjunto de obligaciones dimanantes del 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, toda vez que, como con buen tino ha destacado la doctrina, el mismo fue concebido para su aplicación en contextos en los que el almacenamiento y el tratamiento de los datos se llevaban a cabo de manera centralizada⁹⁸. De esta forma, el carácter distribuido de *blockchain* –con todos los matices que se quieran– y la consiguiente corresponsabilidad de los servidores o nodos en la gestión y actualización de la cadena de bloques impiden identificar un operador único ante el que reclamar la observancia del referido bloque normativo. En consecuencia, de producirse la auspiciada expansión de la tecnología *blockchain*, podría llegar a resultar necesario un replanteamiento general del ámbito subjetivo de aplicación del Reglamento.

El segundo de ellos es el concerniente a la garantía de los derechos de rectificación y supresión. La tecnología *blockchain* no imposibilita en absoluto, como hemos tenido ocasión de comprobar, la rectificación de la cadena de bloques; sin embargo, no deja de ser cierto que la referida operación puede, en ocasiones, llegar a resultar muy gravosa y, además, que su exigibilidad en las redes de implantación simultánea en Estados miembros de la Unión y terceros países se enfrenta a las tantas veces referidas dificultades de la aplicación supraterritorial de las normas. La segunda cuestión ha sido ya analizada *supra*⁹⁹, por lo que en este momento bastará con aludir a la alternativa proporcionada por la tecnología *blockchain* en relación con el primer aspecto, consistente en la adhesión a la cadena de un bloque rectificativo de la información con respecto a la que se ejercita la pretensión conectada con los derechos mencionados, de acuerdo con su configuración normativa y jurisprudencial.

Es claro que una contribución de estas características no puede aspirar a la propuesta de soluciones a los problemas referidos, merecedores de un análisis

97. Cfr. la contribución de los profesores Boix Palop y Pereiro Cárceles.

98. En este sentido, por todos, Finck (2019: 88 y ss.).

99. Apartado 3.1.2.

autónomo. Lo que interesa destacar, a modo de cierre del presente apartado, es que el difícil encaje de *blockchain* en las categorías jurídicas conocidas hasta la fecha debe ser tomado en consideración a la hora de seleccionar el enfoque a adoptar para su regulación. De esta forma, como conclusión en este punto, forzosamente preliminar –en cuanto que ha de entenderse sin perjuicio de cuanto se dirá *infra*¹⁰⁰–, consideramos que las aproximaciones más conservadoras al fenómeno deben, cuando menos, tener en cuenta los riesgos y consecuencias negativas inherentes a la aplicación de los vigentes sistemas normativos a la tecnología *blockchain*, decisión equiparable, particularmente en algunos casos, a su mantenimiento en un problemático limbo jurídico.

3.2. La (pretendida) capacidad normativa del código (*code as law*)

Examinadas ya las dificultades más relevantes a las que se enfrentan las autoridades públicas en la definición del marco normativo aplicable a la tecnología *blockchain*, y con carácter previo a la reflexión crítica acerca de los principales enfoques regulatorios que cabe adoptar a tal fin, procede abordar, como se ha anunciado *supra*, la cuestión relativa a la pretendida capacidad normativa del código, al que se incorporan las reglas de funcionamiento de la cadena de bloques. En extrema síntesis, los posicionamientos doctrinales que habrán de ser objeto de consideración específica en las páginas que siguen parten de desarrollos previos en relación con los efectos del avance tecnológico sobre la producción normativa, para concluir, de una parte, que el creciente grado de automatización de la praxis jurídica conducirá a un replanteamiento de las formas de creación del derecho, pasando de un sistema de disposiciones escritas a otro esencialmente algorítmico, y, de otra, que la expansión de las tecnologías de registro distribuido traerá consigo el desplazamiento por parte del código informático del ordenamiento jurídico institucional. Con carácter preliminar, ha de destacarse que, aun tratándose de un debate con reminiscencias comunes al suscitado recientemente entre nosotros en relación con la naturaleza jurídica de los algoritmos empleados por las administraciones públicas¹⁰¹, el relativo al *code as law* posee unos contornos netamente diferenciados y hunde sus raíces en planteamientos doctrinales desarrollados hace ya más de dos décadas.

100. Apartado 3.3.

101. Nos referimos, claro está, al debate planteado entre quienes consideran que los algoritmos empleados por las administraciones públicas son auténticas disposiciones de rango reglamentario y quienes niegan tal caracterización; por todos, respectivamente, Boix Palop (2020) y Huergo Lora (2020).

En este sentido, el punto de partida de las teorías que defienden que el código de funcionamiento de *blockchain* terminará por sustituir a las normas jurídicas institucionales por las que hoy nos regimos es el célebre estudio de J. R. Reidenberg, publicado en 1998. De acuerdo con la tesis del autor, a finales del pasado siglo, los operadores en la sociedad de la información se enfrentaban a grandes dificultades por razón de la falta de certidumbre en lo relativo al marco jurídico aplicable a sus relaciones, punto de partida común al de los comerciantes medievales, cuya interacción daría lugar al surgimiento y posterior consolidación de la *lex mercatoria*¹⁰². Las soluciones técnicas implementadas en la red permitirían la imposición de determinadas reglas de comportamiento, opción de la que podrían servirse las autoridades públicas para la efectiva realización de sus políticas¹⁰³. Este nuevo *corpus*, denominado *lex informatica*, presentaría importantes ventajas frente a las tradicionales formas de producción normativa como consecuencia de su potencial aplicación transnacional –en cuanto que alcanzaría al conjunto de la red–, de su flexibilidad –esto es, de su capacidad de adaptación a las concretas circunstancias que puedan darse ya en la red, ya en determinadas áreas geográficas por razón de la aprobación de las correspondientes normas nacionales–, y de las mayores garantías que proporcionaría desde la perspectiva del cumplimiento normativo –toda vez que la *lex informatica* facilitaría la ejecución autónoma y preventiva de sus propias reglas, en lugar de fiarlo todo al control *ex post* de las conductas de los participantes en la red–¹⁰⁴. No obstante lo anterior, la modificación de la *lex informatica* presentaría, como principal dificultad, su condicionamiento a la forzosa aceptación de las correspondientes reformas por parte del conjunto de participantes en la red¹⁰⁵. Su relación con el derecho institucional se plantearía, en fin, simultáneamente en términos de competencia y de colaboración, pues, si bien podría revelarse apta para llegar a sustituir a los ordenamientos jurídicos tradicionales allá donde poseyera una mayor capacidad para resolver los problemas en cada caso planteados, la *lex informatica* podría igualmente servirse de aquel tanto para fomentar su expansión como para consolidarse con carácter definitivo¹⁰⁶.

En las tesis de Reidenberg profundizaría poco tiempo después L. Lessig. En opinión de este autor, la posibilidad de regulación del ciberespacio dependería de las características técnicas del mismo, esto es, de su “arquitectura”; en este

102. Reidenberg (1998: 553-554).

103. Reidenberg (1998: 568).

104. Reidenberg (1998: 577 y ss.).

105. Reidenberg (1998: 582-583).

106. Reidenberg (1998: 583 y ss.).

sentido, la evolución de la red tendería a su configuración como un espacio altamente regulable¹⁰⁷. La disciplina aplicable al ciberespacio resultaría de la conjunción de la ley (institucional), las normas (de origen social), las restricciones e incentivos del mercado y el código informático¹⁰⁸. Se daría así una relación de competencia entre el primero y el último de los factores de regulación referidos, cuya evolución transcurriría por senderos en principio independientes y terminaría por comportar el desplazamiento de la ley por el código –*code as law*–, transformación de una extraordinaria significación tanto desde la perspectiva de la legitimidad del marco regulador de la red como desde el punto de vista de la soberanía estatal, habida cuenta de que los redactores del código serían, en primer término, las grandes corporaciones transnacionales¹⁰⁹. Los Estados, por último, habrían de reaccionar a fin de poder garantizar la vigencia de los principios jurídicos fundamentales en el ciberespacio, para lo cual resultaría esencial una toma de conciencia colectiva al respecto¹¹⁰.

En opinión de un relevante sector doctrinal, las teorías de Reidenberg y Lessig encontrarían un nuevo impulso en la implantación y desarrollo de las aplicaciones algorítmicas y de las tecnologías de registro distribuido. De particular interés al respecto son, en la literatura extranjera, las contribuciones de autores como De Filippi y Wright, Hildebrandt, Reyes o Casey y Niblett, así como, entre nosotros, la de especialistas como García Mexía. Punto de partida común a todas ellas es que la incidencia de las nuevas tecnologías trascendería, en el ámbito jurídico, la mera facilitación de nuevos formatos o soportes, en cuanto que aquellas supondrían la transformación de la producción normativa desde el paradigma tradicional –basado en el lenguaje humano, en la difusión a través de la imprenta y en la interpretación del significado último de las normas– hacia un nuevo modelo en el que las potestades públicas se ejercerían a partir del tratamiento de la información y de los datos¹¹¹. Los algoritmos y las tecnologías predictivas facilitarían un grado tal de automatización en la elaboración de las normas que comportaría la sustitución de las reglas y principios jurídicos que hoy conocemos por instrucciones específicas –según la traducción literal, “micro-directivas”–, emitidas para la regulación de cada concreta situación a partir de los criterios y objetivos seleccionados por los agentes públicos e incorporados a las correspondientes aplicaciones informáticas¹¹². En este

107. Lessig (2001: 57 y ss.; 89 y ss.).

108. Lessig (2001: 166 y ss.).

109. Lessig (2001: 376 y ss.).

110. Lessig (2001: 400, 423-424).

111. Por todos, Hildebrandt (2016: *passim*).

112. Al respecto, es obligada la remisión *in toto* a Casey y Niblett (2017).

marco, el empleo de las tecnologías de registro distribuido daría lugar a un nuevo modelo de producción normativa, el designado como “criptoderecho”¹¹³ o *lex cryptography*¹¹⁴, novísima manifestación del *code as law* de Lessig integrada por un conjunto de disposiciones dictadas y ejecutadas mediante *smart contracts*.

La automatización de la producción normativa impulsada por esta relevante innovación traería consigo transformaciones dotadas de una extraordinaria significación. Por un lado, este nuevo *corpus* se caracterizaría por una disminución radical de la ambigüedad de las normas, en la medida en que permitiría la determinación *ex ante* de las reglas específicamente aplicables a cada situación. Ello comportaría, a su vez, el desplazamiento práctico de la labor de fiscalización judicial, por definición desarrollada *ex post*, por sistemas de *compliance* de naturaleza preventiva y eficacia superior¹¹⁵, y la consiguiente transformación de la labor del jurista, que habría de superar la tradicional visión con respecto a su propia profesión, considerada habitualmente como inmune al impacto de las nuevas tecnologías¹¹⁶.

Idénticos avances se producirían, por otro lado, desde la perspectiva de la efectividad de la regulación. Las autoridades públicas dispondrían, de acuerdo con la visión del fenómeno sostenida en la literatura objeto de examen, de instrumentos más eficaces para el diseño e implementación de sus políticas. Los más recientes desarrollos tecnológicos les permitirían afrontar con mayor inmediatez los retos y problemas a los que se enfrentan en su labor diaria; su intervención se vería limitada a la sola fijación de objetivos o principios generales, cuya traducción en reglas de aplicación concreta sería efectuada por los *smart contracts*, así como a través del empleo de algoritmos.

113. Reyes (2017: *passim*) y García Mexía (2018b: *passim*).

114. De Filippi y Wright (2015: 48 y ss.).

115. En este sentido, por todos, De Filippi y Wright (2015: 50-51, 2018: 195 y ss.), Reyes (2017: 407-408), y Casey y Niblett (2017: 1433 y ss.). En el último de los trabajos citados (2017: 1436) se identifica como principal límite de la retracción de la intervención judicial el control de constitucionalidad de las leyes.

116. Sobre el cambio de mentalidad del jurista, *cfr.* particularmente Hildebrandt (2016: 2). La transformación de las profesiones jurídicas derivaría no solo de la progresiva retracción de la intervención judicial como mecanismo fundamental de garantía de una correcta aplicación de las normas, sino también –e incluso principalmente– del consiguiente replanteamiento de la labor del abogado, en cuanto que el asesoramiento ya en el sector público, ya en el sector privado, ganaría relevancia en detrimento de su tradicional intervención ante la autoridad judicial. En este sentido, *cfr.* particularmente Casey y Niblett (2017: 1440-1441), quienes subrayan, asimismo, la necesidad de que el jurista desarrolle un trabajo de naturaleza interdisciplinar para el adecuado desempeño de su función en un mundo de instrucciones emitidas a través de sistemas algorítmicos.

El criptoderecho forzaría, en definitiva, a un replanteamiento global de los procedimientos normativos¹¹⁷.

Las transformaciones referidas encontrarían reflejo, en fin, en la propia cultura jurídica. A este respecto, presenta un especial interés la completa exposición de C. L. Reyes. De acuerdo con la autora, la automatización de los procedimientos de garantía del cumplimiento normativo no solo traería consigo, entre otros aspectos, una confusión de *law in the books* y *law in action*¹¹⁸, sino que también representaría un factor (adicional) de aproximación de las tradiciones continental y de *common law*, dado que en este último contexto dejaría de resultar necesario, cada vez en más ámbitos, convencer a la autoridad judicial de que al caso litigioso resulta o no aplicable la solución dada a un concreto precedente¹¹⁹.

Pese a lo sugerente de los posicionamientos doctrinales de referencia, reseñados aquí en apretada síntesis, debe, en todo caso, llamarse la atención sobre la existencia de diversos factores que nos conducen a dudar acerca de la probabilidad de que las mutaciones que aquellos auguran en el ámbito de la producción normativa lleguen efectivamente a producirse, así como de los riesgos asociados a las mismas¹²⁰.

En primer lugar, ha de considerarse el hecho de que el alcance de la automatización en la producción normativa se presenta en los propios estudios reseñados como muy limitado, no solo por razón del aún muy reducido número de *smart contracts* que operan, en la actualidad, a gran escala¹²¹, sino también porque se admite expresamente que la referida automatización resulta tan solo plausible en relación con aquellos ámbitos en los que quepa la formulación apriorística de reglas absolutamente precisas e incondicionadas. En este sentido, las principales exposiciones en la materia subrayan que la juridificación del código plantea importantes inconvenientes, derivados de la falta de flexibilidad del lenguaje informático. De esta forma, las ventajas que, desde la perspectiva de la mayor certidumbre de las normas jurídicas, presenta la *lex cryptography*, se verían contrarrestadas por la imposibilidad

117. Cfr. Casey y Niblett (2017: 1437-1438), y Reyes (2017: 430-432). Esta última autora defiende, igualmente, que la consolidación de las estructuras criptojurídicas dará lugar al desplazamiento de la producción normativa hacia los técnicos (2017: 436).

118. Reyes (2017: 435-436).

119. Reyes (2017: 429).

120. Sobre estas cuestiones habrá de volverse brevemente *infra*, con referencia a los límites de la automatización de la actividad administrativa mediante el empleo de *smart contracts* (apartado 4).

121. En este sentido, particularmente, Magnuson (2020: 168-169).

de adaptación del código a realidades o circunstancias no previstas inicialmente mediante su (re)interpretación por parte de la autoridad judicial, lo que podría frustrar la efectiva consecución de los objetivos perseguidos por los poderes públicos¹²². Así, algunos autores apuntan a la posibilidad de que el código, si diseñado defectuosamente o de manera incompleta, dé lugar a consecuencias indeseadas¹²³, llegando incluso a suponer un obstáculo al desarrollo de actividades en principio conformes a la legalidad¹²⁴. A la vista del estado actual de la técnica, la alternativa consistiría en la reserva de un ámbito de actuación a los oráculos de los *smart contracts*, lo que, si bien resolvería el problema de la rigidez, comportaría al mismo tiempo una relativización de la propia innovación, al hacer que el sistema hubiera de depender, en todo caso, de la intervención humana en mayor o menor grado¹²⁵. En conclusión, en tanto no se produzca una transformación de los sistemas informáticos que permita la redefinición de los patrones normativos incorporados al código a partir de la constatación de situaciones no contempladas en el momento de su elaboración, difícilmente encontrará la tecnología *blockchain* un área de influencia relevante en el contexto de la producción normativa. El Estado –y, con él, otros poderosos intermediarios– sobrevivirá a las tecnologías de registro distribuido¹²⁶.

En segundo lugar, han de tenerse en cuenta las negativas consecuencias que la automatización de la producción normativa y de las técnicas de *compliance* presentaría desde la perspectiva de la autonomía del individuo. La promesa de la tecnología *blockchain* consiste en la eliminación práctica de la alternativa del incumplimiento en todos los órdenes¹²⁷. El ideal de la observancia sin excepciones de las normas resulta, ciertamente, atractivo: es obvio que, si en la actualidad las autoridades públicas no aspiran a su consecución, ello es debido, abstracción hecha del fenómeno de la corrupción, antes a la adopción de una postura pragmática en relación con los límites de su capacidad de actuación que a consideraciones de otro tipo. Sin embargo, ha de advertirse sobre el hecho de que un avance no contenido de la *lex cryptographia* comportaría peligrosas restricciones de la libertad individual –en la medida

122. En este sentido, desde una perspectiva general, *cf.*: Reyes (2017: 437-438), De Filippi y Wright (2018: 199-201), y Finck (2019: 81-83). Esta última autora alerta, en relación con los obstáculos al control judicial que derivarían de la implantación de la *lex cryptographia*, sobre los riesgos para el principio de separación de poderes que resultarían de una tal transformación.

123. Al respecto, especialmente, Casey y Niblett (2017: 1438 y ss.), y Reyes (2017: 439-441).

124. De Filippi y Wright (2018: 201).

125. En este sentido, específicamente, García Mexía (2018b: 125).

126. De Filippi y Wright (2015: 51); *cf.* asimismo, entre otros, Lassège (2021: 70-71).

127. Al respecto, *cf.* particularmente Reyes (2017: 433).

en que el incumplimiento normativo ha de presentarse, particularmente en ciertos sectores del derecho, como una opción para el particular, que habrá de poder escoger entre la observancia de las reglas y el padecimiento de las consecuencias jurídicas asociadas a la opción contraria¹²⁸, que podrían incluso consistir –se señala–, una vez alcanzados los desarrollos necesarios en el contexto de la internet de las cosas, en la aplicación automatizada de medidas de compulsión sobre las personas¹²⁹. Con todo, en la literatura de referencia se ha precisado que la autoría del código es siempre humana, razón por la que resultaría posible –y particularmente relevante– la participación de juristas y otros expertos en la definición de la extensión y límites del criptoderecho y en la configuración de mecanismos de protección del ciudadano, ante eventuales aplicaciones de las normas integrantes de aquel que resulten contrarias a los principios jurídicos esenciales¹³⁰. De lo contrario, su consolidación podría dar lugar, tal y como ha ocurrido en otros momentos históricos, a la aparición de movimientos de resistencia y a la conformación de un marco jurídico independiente, alternativo a las tecnologías de registro distribuido¹³¹.

En tercer lugar, debe subrayarse la ausencia de validez –*rectius*: de constatación efectiva– de las conclusiones alcanzadas en los estudios que sirven de base a las tesis de última generación sobre el desplazamiento de la normativa institucional por el código como fuente principal de regulación en las sociedades de la era *blockchain*. En este sentido, Cappiello ha señalado en una muy reciente contribución cómo la aparición de internet y la anunciada emancipación de la *lex informatica* con respecto a los sistemas jurídicos tradicionales no se han podido verificar. De acuerdo con la exposición de la autora, el referido advenimiento supuso, ciertamente, un muy relevante paso en la evolución de la compleja relación entre el derecho y las nuevas tecnologías; sin embargo, ni internet ni los sistemas de código abierto han podido sustraerse a la disciplina jurídica institucional, dado que nunca han alcanzado el estatus de ordenamientos autónomos que el sector doctrinal referido ha pretendido atribuirles. Ello se debería, en su opinión, a que los referidos sistemas carecerían de una aceptación universal, en cuanto diseñados para alcanzar los objetivos de sus propios programadores, así como de una auténtica legitimación político-jurídica. Estas características serían comunes,

128. En este sentido, *cfr.*, entre otros, Kohl (2021: 27).

129. Casey y Niblett (2017: 1443-1444).

130. *Cfr.* nuevamente Casey y Niblett (2017: 1443-1445), quienes se refieren en este contexto a la posible “robotización” del individuo, así como De Filippi y Wright (2018: 204).

131. En este sentido, Reyes (2017: 441 y ss.), que se refiere, asimismo, a la posibilidad –considerada más remota– de que el fenómeno impulse la implantación de modelos de gobernanza de carácter endógeno.

en fin, a las redes *blockchain*, la efectividad de cuyas reglas dependería, en último término, de la posibilidad de reclamar su cumplimiento a través de las vías proporcionadas por los sistemas normativos institucionales¹³².

En conclusión, a la vista del estado actual de la cuestión y de las perspectivas de avance en un futuro más o menos inmediato, no parece que el código informático que disciplina el funcionamiento de las redes *blockchain* pueda llegar no ya a sustituir, sino tan siquiera a equipararse en importancia a la normativa institucional de origen ya estatal, ya supranacional. De esta forma, las autoridades públicas continúan disponiendo de instrumentos eficaces para mantener las tecnologías de registro distribuido “en el redil” de los valores y principios esenciales de los respectivos ordenamientos jurídicos. La cuestión decisiva, en suma, será la de determinar cómo habrán de utilizarse aquellos a fin de garantizar la necesaria “interoperabilidad” entre el código informático y el sistema normativo institucional¹³³. Al estudio de los referidos mecanismos y enfoques regulatorios se dedican las páginas que siguen.

3.3. Un repaso de los principales enfoques regulatorios aplicables a la tecnología *blockchain*

Llegados a este punto, procede ya abordar el estudio de las principales estrategias de que disponen las autoridades públicas, tanto nacionales como supranacionales, para la regulación de la tecnología *blockchain*, así como de los casos de uso desarrollados en aplicación de la misma. En este sentido, en la exposición sucesiva se ensayará una aproximación preliminar a la cuestión, a fin de perfilar criterios de intervención útiles para el ejercicio de las potestades normativas —y, más en general, de naturaleza pública— en el ámbito objeto de análisis. El referido aspecto, como viene destacando la doctrina especializada desde hace (relativamente) largo tiempo, está llamado a desempeñar un

132. Capiello (2021: 34-36); en el mismo sentido, ya Finck (2019: 85).

133. En este sentido, *cfr.* la expresiva reflexión conclusiva de Finck (2019: 87). Desde una perspectiva complementaria, ha podido defenderse la necesaria cooperación entre el código informático y el sistema institucional como vía alternativa tanto al criptoanarquismo como al “ciberpaternalismo”, entendiéndose por tal el sistema en el que los ordenamientos jurídicos tradicionales prevalecen en términos absolutos sobre la regulación “social” de las redes *blockchain*; en este sentido, *cfr.* Poncibò (2021: 152). En un sentido parcialmente similar, en fin, se tiende a subrayar los aspectos en relación con los que se produce una influencia recíproca entre ambos sistemas, en la medida en que, a la vez que el código asume una forma próxima a la normativa, el ordenamiento se traduce progresivamente en código; en este sentido, *cfr.* Dimitropoulos (2020: 1142).

papel decisivo en el impulso y la consolidación de los servicios financieros basados en la tecnología *blockchain*¹³⁴.

En todo caso, parece conveniente advertir sobre el carácter tan solo relativo de las conclusiones que puedan llegar a alcanzarse, habida cuenta de que cada sector de la realidad posee especialidades que lo hacen merecedor de un tratamiento diferenciado, con independencia de que constituya un elemento común a todos ellos la posibilidad de su transformación a partir del empleo de las tecnologías de registro distribuido. De esta forma, como habrá de comprobarse seguidamente, ninguno de los enfoques regulatorios aplicables a la tecnología *blockchain* es preferible, en principio, con respecto a los demás: la adopción por parte de las autoridades públicas de prácticamente cualquiera de ellos es comprensible en función tanto del concreto ámbito de actuación de que se trate como, sobre todo, del conocimiento disponible en el momento en que se aborde la configuración del correspondiente marco normativo o el diseño de las políticas e iniciativas de que se trate.

3.3.1. Prohibicionismo y abstencionismo

Cuanto viene de decirse ha de ser matizado, en todo caso, cuando se consideran específicamente las alternativas prohibicionista y abstencionista como estrategias regulatorias aplicables a la tecnología *blockchain*. La primera de ellas, como ha tenido ocasión de destacarse *supra*¹³⁵, ha sido adoptada, por ejemplo, por las autoridades chinas en relación con la aceptación de la criptomoneda bitc oin como medio de pago; considerado lo expuesto hasta el momento, no parece que, en l neas generales, la misma plantee excesivas dificultades desde la perspectiva de la comprensi n de su funcionamiento e implicaciones¹³⁶.

Con todo, debe llamarse la atenci n sobre un aspecto al que no se ha hecho referencia hasta el momento, como es el relativo a la desprotecci n a la que pueden conducir determinadas pol ticas prohibicionistas en el marco de la regulaci n de la tecnolog a *blockchain*. En este sentido, la posibilidad de

134. En este sentido, *cfr.* Swan (2015: 89).

135. Apartado 3.1.3.

136. En concreto, en relaci n con la limitada eficacia de los marcos normativos cuya aplicaci n puede eludirse mediante el traslado a jurisdicciones m s permisivas; *cfr.* el apartado 3.1.2. En este sentido, una s ntesis de las principales desventajas de la adopci n de un enfoque limitativo o conservador frente a las tecnolog as de registro distribuido, particularmente desde la perspectiva de la ineffectividad del marco normativo, puede verse en Magnusson (2020: 187).

la huida hacia jurisdicciones más permisivas en relación con la adquisición y el intercambio de criptomonedas no solo es problemática desde el punto de vista de la efectividad del sistema normativo institucional, sino también en relación con las exigencias de acceso a dicha actividad: mientras que, en el contexto de una regulación que admite dicha forma de uso de la tecnología *blockchain*, cabe adoptar cautelas específicas a favor, concretamente, de los pequeños inversores –exigencia de supervisión profesional para la realización de determinadas operaciones–, la opción de la prohibición total supone una renuncia a toda posibilidad de configuración de un sistema mínimo de garantías a favor de aquellos¹³⁷. En este sentido, la falta de efectividad de la prohibición se manifiesta no solo en términos de inobservancia de la misma, sino también de alejamiento con respecto a su fin último.

Desde otra perspectiva, debe tenerse presente que la opción prohibicionista puede articularse con carácter limitado no solo por razón de su objeto –es decir, en relación con una aplicación específica de la tecnología *blockchain*, como en el caso chino–, sino también desde la perspectiva temporal. En este último supuesto, se trataría, pura y simplemente, de diferir la admisibilidad jurídica de un concreto caso de uso hasta el momento en que se alcance un determinado horizonte temporal o en que se produzca un específico desarrollo normativo, habilitante de la correspondiente utilización de la tecnología *blockchain*. Como es sabido, esta ha sido la opción seguida por el Gobierno español, que introdujo la disposición adicional sexta de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común, mediante el Real Decreto-ley 14/2019, de 31 de octubre, imponiendo la prohibición de autorizar sistemas de identificación y firma basados en tecnologías de registro distribuido, en las relaciones entre los particulares y las entidades integrantes del sector público, “en tanto que no sean objeto de regulación específica por el Estado en el marco del derecho de la Unión Europea”. Sobre esta controvertida previsión, no obstante, habrá de volverse brevemente *infra*¹³⁸.

La segunda de las alternativas referidas consiste básicamente en la adopción de una actitud pasiva ante el fenómeno; dicho con otras palabras, supone ignorar, conscientemente o no, los retos que la tecnología *blockchain* plantea a los reguladores, manteniendo inalterados con carácter indefinido

137. El referido extremo es subrayado en un reciente artículo publicado en *Financial Times*, el 3 de noviembre de 2021, titulado “UK crypto derivatives ban fails to protect retail investors” y disponible en: <https://www.ft.com/content/6e79e3e0-c7c9-4577-998c-5c79d24cf1d2>.

138. Apartado 4.

los marcos normativos aplicables, en su caso, a los sectores de actividad concernidos. De la sola descripción de esta opción resultan con evidencia, en nuestra opinión, las desventajas asociadas a la misma: más allá de las dificultades prácticas que plantea la extensión por vía analógica de la normativa vigente a las actividades desarrolladas en las redes *blockchain*, la renuncia al análisis de las alternativas en el momento en que la tecnología se encuentra en su fase inicial o embrionaria –como ha quedado dicho, momento fundamental para reflexionar sobre las políticas públicas que cabría implementar con respecto a la misma– supone una auténtica abdicación con respecto al deber de garantizar que su implantación y consolidación futuras no se producirán en detrimento de los derechos de los ciudadanos. No es de extrañar, en definitiva, que el enfoque abstencionista haya sido considerado como una aproximación a evitar “en todo caso”¹³⁹.

3.3.2. *Wait and see*

Netamente diferenciado del abstencionismo se presenta el enfoque comúnmente denominado *wait and see*. El mismo consiste en la recopilación y el análisis por parte de las autoridades públicas de la información relativa a los efectos y, en su caso, las dificultades específicamente planteadas por la aplicación del marco jurídico vigente a los diferentes casos de uso de la tecnología *blockchain*; es decir, supone la no promoción temporal de iniciativas de tipo normativo en la materia mientras, simultáneamente, se realizan consultas de carácter más o menos informal con los principales operadores y, en su caso, se estudian los avances experimentados en otras jurisdicciones. El objetivo último de esta aproximación es la toma consciente de decisiones para la regulación del fenómeno, que pueden consistir ya en la aprobación de un *corpus* normativo *ad hoc*, ya en continuar con la aplicación, efectuadas las oportunas adaptaciones, de la disciplina jurídica en vigor¹⁴⁰. Se trata, en suma, de llevar a cabo la evaluación necesaria para la identificación y posterior gestión, a través de la adopción del marco normativo correspondiente, del denominado “riesgo permitido”, esto es, de aquel que la sociedad está dispuesta a asumir a partir del impulso o de la consolidación de un concreto avance tecnológico¹⁴¹.

139. En este sentido, Finck (2019: 154).

140. Esta es la descripción de la estrategia regulatoria del *wait and see* proporcionada por Finck (2019: 154). En un sentido similar, *cfr.*: Magnuson (2020: 178).

141. Sobre la noción de “riesgo permitido” y el papel que, al respecto, corresponde al derecho regulatorio, véase, en nuestra doctrina, Esteve Pardo (2021: 42-43).

Es claro que el enfoque del *wait and see* representa una actitud adecuada desde la perspectiva de la configuración de la regulación aplicable a una tecnología novedosa, cuyos principios de funcionamiento e implicaciones resultan desconocidos para las autoridades. En dicho contexto, los operadores continúan, durante un cierto tiempo, participando en los mercados sin sujeción a un régimen jurídico específico –esto es, diferente del aplicable, con carácter general, al sector de actividad de que se trate–, lo que con frecuencia se traduce en un cierto grado de tolerancia en relación con los efectos menos graves de su actuación, en el caso de que de la misma resulte un incumplimiento legal de carácter puntual. Sin embargo, si se considera esta última circunstancia junto con las dificultades, ya aludidas, que desde diversas perspectivas plantea la aplicación de los institutos jurídicos que hoy conocemos a la tecnología *blockchain*¹⁴², no cabe sino concluir, de acuerdo con la doctrina especializada, que el *wait and see* no puede en modo alguno ser considerado como una estrategia duradera, sino, más bien, como la fase inicial de un proceso complejo, que habrá de proseguir con la adopción de un enfoque regulatorio más concreto¹⁴³, pues, de lo contrario, se correría el riesgo de que el vacío normativo provocado por la parcial inacción pública fuera colmado mediante una intervención privada apenas sujeta a límites¹⁴⁴.

Con todo, el paso de la aproximación de *wait and see* hacia la definitiva adopción de la regulación específicamente aplicable a *blockchain* y sus casos de uso no ha de producirse necesariamente de forma abrupta. Es posible, por el contrario, combinar la tarea de análisis de las dinámicas y procesos desarrollados en dichos ámbitos con el establecimiento temporal de estándares o normas de *soft law*¹⁴⁵ a cuyo incumplimiento no se asocie la aplicación de un régimen sancionador determinado. Cabe, igualmente, el desarrollo puntual de estrategias más incisivas en los supuestos de detección de conductas cuyo ajuste a la legalidad pueda resultar dudoso por razón de la especialidad que, en este punto, representa el empleo de tecnologías de registro distribuido, como sería la remisión de cartas admonitorias, modalidad de actuación administrativa informal consistente en la formulación de un requerimiento al operador correspondiente, solicitándole ya el cese en la realización de una acción susceptible de ser sancionada de conformidad con la normativa vigente, ya la adopción de las medidas positivas necesarias para la corrección

142. Apartado 3.1.4.

143. De nuevo, Finck (2019: 155).

144. En este sentido, en el contexto de una reflexión muy crítica acerca la estrategia regulatoria del *wait and see*, *cf.*: Herian (2020: 42-43).

145. En relación con esta posibilidad y las alternativas que se exponen seguidamente, *cf.*: nuevamente Finck (2019: 157).

de aquella –interpretación que, en último término, el operador afectado podrá discutir¹⁴⁶–.

Sea como fuere, también esta etapa se caracteriza, como viene de señalarse, por su transitoriedad, en la medida en que resultará necesario adoptar, más tarde o más temprano, un enfoque regulatorio que permita la definición de un marco normativo dotado, cuando menos, de una cierta vocación de eficacia jurídica. Al estudio de dos de las principales modalidades de estrategias a las que, a tal fin, pueden acudir las autoridades –la autorregulación regulada, de una parte, y los conocidos como *sandboxes* regulatorios, de otra–, se dedican los siguientes apartados.

3.3.3. La autorregulación regulada

El interés de la estrategia del *wait and see* para el diseño de la disciplina jurídica aplicable a la tecnología *blockchain* es sintomático del enorme desafío que esta tarea representa para las autoridades públicas. La recta comprensión de sus implicaciones en un momento en el que los avances se suceden a un ritmo frenético, dando lugar, además, a importantes controversias, de las que se ha dado breve noticia *supra*¹⁴⁷, se presenta como un cometido difícilmente alcanzable para los poderes públicos. Desde otra perspectiva, como también ha habido ocasión de exponer¹⁴⁸, tanto el carácter transnacional de las redes *blockchain* como la constante búsqueda por parte de determinados actores de espacios en los que operar sin sujeción a control alguno suponen importantes obstáculos para la reconducción de esta tecnología a un marco normativo netamente institucional. En un contexto como el descrito, no parece, en suma, un desatino dudar de la capacidad real de las administraciones para afrontar este reto por sí solas.

Se abre paso, así, la alternativa de dotar a las normas sociales, entendiendo por tales las que los operadores en el ecosistema *blockchain* se dan a sí mismos, de un cierto grado de relevancia institucional, con simultánea determinación de los estándares mínimos y de los procedimientos que aquellos habrán de observar a fin de obtener el referido reconocimiento. El objetivo de alcanzar

146. Un excelente análisis de la figura y de sus principales implicaciones jurídicas puede encontrarse en García Luengo (2018; en relación con el aspecto específicamente referido en el texto, esto es, la posibilidad de contestación del contenido de las cartas admonitorias, *cf.*: pp. 121 y ss.).

147. Apartado 2.4.

148. Apartado 3.1.2.

este último podría incentivarse de múltiples maneras, tanto mediante el empleo de las técnicas habituales de la actividad de fomento como a través de una relajación o disminución *ad hoc* de la intensidad de los instrumentos propios de la policía administrativa. De esta forma, si acorde con el marco definido por parte de los correspondientes actores públicos, las referidas normas sociales se erigirían en instrumento fundamental para la garantía del interés general que a estos últimos corresponde en primer término promover, pues su intervención, aun de forma tan solo mediata, podría alcanzar allá donde los medios tradicionales de la actividad administrativa se revelan hoy insuficientes. La sujeción a mecanismos de control o supervisión de carácter público de una normación de origen privado en expansión permitiría, en definitiva, a los poderes públicos adaptarse a nuevas realidades sin abdicar de sus potestades de regulación: muy al contrario, la opción referida evidenciaría con claridad una creciente ambición de intervención, justificada por razón de la necesaria garantía de que el desarrollo científico y tecnológico no perjudique los derechos de los ciudadanos.

Como es sabido, estas son, expuestas en extrema síntesis, las bases sobre las que se asienta la denominada “autorregulación regulada”, noción que engloba un amplio y heterogéneo conjunto de técnicas de intervención administrativa y que ha sido objeto de tempranos y profusos análisis entre nosotros, a los que resulta obligado remitirse *in toto*¹⁴⁹. No procede, claro está, ahondar en este momento en las certeras reflexiones desarrolladas por quienes más ampliamente han estudiado la cuestión; en lo que aquí interesa, bastará con constatar lo oportuno de la regulación pública de la autorregulación –manifestación destacada de un proceso de conmixtión de derecho público y derecho privado que alcanza a una muy significativa proporción de sectores del ordenamiento¹⁵⁰– para la conformación del marco normativo aplicable no solo a las TIC y, singularmente, a internet, como hace tiempo subrayó la mejor doctrina¹⁵¹, sino también y muy especialmente, hoy, a las tecnologías de registro distribuido.

En este sentido, es claro que convergen en las redes *blockchain* las principales variables que han motivado el surgimiento y desarrollo de la autorregulación regulada: erosión de la soberanía estatal, aumento de la complejidad social y sustitución del sector público por el privado como referente en la especialización

149. Nos referimos, claro está, a los excelentes estudios de Esteve Pardo (2002) y Darnaculleta i Gardella (2005), que, pese al tiempo transcurrido desde su aparición y a los desarrollos que el fenómeno ha conocido, constituyen aún ineludibles referencias en la materia.

150. Al respecto, *cfr.* muy especialmente Velasco Caballero (2014: *passim*).

151. Sobre el particular, entre nosotros, ya tempranamente, Muñoz Machado (2000).

científico-técnica son factores unánimemente destacados por los estudiosos del fenómeno que se identifican con facilidad, igualmente, al observar las transformaciones propiciadas por *blockchain*. Y, sin duda, el avance de esta tecnología y las incógnitas que a partir del mismo se plantean aconsejan la adopción de una actitud proactiva por parte de las autoridades públicas desde la perspectiva de la regulación, a fin de evitar que las redes *blockchain* se rijan por normas definidas por una minoría de operadores poderosos, que no tomen en consideración suficientemente el interés general. En definitiva, la opción por la regulación pública de la autorregulación de los participantes en las redes *blockchain* no solo favorecerá una mayor involucración ciudadana en el ejercicio del poder público: garantizará, asimismo, la salvaguarda del interés general; facilitará una adecuada flexibilidad, evitando de esta forma la petrificación de las soluciones normativas y que el ordenamiento se sitúe permanentemente por detrás de la técnica; permitirá, en fin, una intervención temprana, impidiendo así la consolidación de situaciones contrarias a los objetivos de las políticas públicas¹⁵². La conformación del marco público de la autorregulación privada exigirá, en todo caso, la adopción de cautelas específicas, a fin de que no se desconozcan los parámetros jurídico-constitucionales en los que aquella deberá desenvolverse¹⁵³.

En definitiva, la autorregulación regulada proporciona a los poderes públicos, en el ámbito que nos ocupa, herramientas de actuación de notable interés¹⁵⁴ que, no obstante, han de ser empleadas con mesura. De esta forma, tal y como se destacó entre nosotros al analizar la regulación de internet¹⁵⁵, la solución (y sus límites) ya están inventados: en el nivel de los principios, nada nuevo hay, pues, bajo el sol.

3.3.4. Los denominados *sandboxes* regulatorios

Hemos de apresurarnos a matizar la anterior conclusión al considerar específicamente las posibilidades que ofrecen los conocidos como “espacios controlados de pruebas” o *sandboxes* regulatorios. Estos pueden ser calificados, ciertamente, como una auténtica institución jurídica de nuevo cuño, reciente objeto,

152. Cfr. al respecto la sólida exposición de Finck (2019: 172 y ss.).

153. En este sentido, nuevamente en el contexto de una más amplia reflexión muy crítica con la técnica regulatoria que nos ocupa, Herian (2020: 55 y ss.).

154. No es de extrañar que, como destaca el profesor Aguado i Cudolà en este mismo volumen, la Agencia Española de Normalización haya acudido a esta técnica para la definición de un marco de referencia en materia de gestión autónoma de la identidad digital (Norma UNE 71307-1:2020).

155. De nuevo, Muñoz Machado (2000).

además, de atención por parte del legislador estatal, que, como es notorio, ha adoptado hace poco más de un año la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero. Conviene notar que la apuesta institucional por la figura en España no se ha agotado con la aprobación de la Ley citada, pues la Carta de derechos digitales de 14 de julio de 2021 se refiere específicamente a la implantación de “las condiciones que permitan la creación de espacios de pruebas controladas para desarrollar nuevos modelos de negocio, aplicaciones, procesos o productos basados en la tecnología (*sandbox*)” en el marco de las proclamaciones referidas a la empresa en el entorno digital (párrafo XX, apartado 6).

Pese a la extraordinaria relevancia de la Ley 7/2020, de 13 de noviembre, para el impulso del avance tecnológico, la innovación y la atracción de inversiones en sectores económicos estratégicos, las referencias a sus contenidos¹⁵⁶ en la exposición sucesiva habrán de ser, por razones de espacio, tan solo superficiales, pues, en el marco de la presente reflexión, interesa sobre todo destacar la idoneidad de los *sandboxes* regulatorios como instrumentos para la identificación de criterios de normación de la tecnología *blockchain*. Con todo, por razón de su carácter novedoso, parece necesario efectuar una brevísima delimitación conceptual de la institución, así como hacer sucinta referencia a las principales implicaciones jurídicas de su aparición y próxima consolidación, que, tanto por la decisión de las instituciones para su puesta en marcha como por las especialidades que presentan dentro del más amplio contexto de los que han dado en denominarse “experimentos jurídicos”¹⁵⁷, no cabe sino considerar como segura.

En los estudios del fenómeno son frecuentes las referencias al origen del término “*sandbox*”, locución inglesa con la que se designan las cajas de arena que se utilizan como espacios en los que pueden jugar los niños en condiciones seguras. Los *sandboxes* regulatorios responden, ciertamente, a esta idea, en la medida en que, a través de los mismos, las autoridades reguladoras competentes en los respectivos sectores admiten el desarrollo controlado de actividades sujetas a autorización en condiciones más favorables que las resultantes de la aplicación del régimen ordinario por un tiempo limitado. Con ello se persigue, en primer término, favorecer avances tecnológicos que, de otra forma, se verían obstaculizados por la imposición de requisitos de acceso al ejercicio

156. Para una exposición de las múltiples aristas de la norma con referencia al entonces Anteproyecto de Ley, hemos de remitirnos al clarificador estudio de Huergo Lora (2018).

157. Sobre el particular, en nuestra doctrina, *cfr*: la exhaustiva y sugerente exposición de Doménech Pascual (2019).

de las correspondientes actividades que se consideran excesivamente severos, en cuanto que a la incertidumbre característica del propio método científico-técnico se uniría la forzosa realización por parte de los operadores de un esfuerzo adicional, consistente en soportar las cargas administrativas previstas con carácter general. Al mismo tiempo, los espacios *controlados* de pruebas se caracterizan, precisamente, por la configuración, con carácter previo a su puesta en marcha, de un régimen específico de fiscalización por parte de las autoridades administrativas, a fin de que la modulación o inaplicación parcial del régimen legal ordinario no traiga consigo riesgos juzgados inasumibles para los bienes jurídicos a cuya protección se dirige precisamente aquel. La sola descripción de la figura permite intuir la controversia doctrinal planteada en torno a la misma, toda vez que, frente a quienes subrayan de forma acrítica sus virtudes, principalmente referidas a la facilitación de la innovación y el desarrollo tecnológicos¹⁵⁸, no han dejado de alzarse voces que cuestionan la metodología empleada en el más amplio contexto de la experimentación jurídica, tanto desde el punto de vista de la calidad de los resultados como desde la perspectiva de la que se considera precaria situación en que pueden quedar los bienes y derechos precisados de protección específica¹⁵⁹, o que alertan sobre su difícil engarce con los principios de legalidad, transparencia, igualdad y seguridad jurídica, entre otros¹⁶⁰.

Con independencia de lo anterior, el referido es, expuesto en apretada síntesis, el paradigma al que responde el esquema incorporado por la Ley 7/2020, de 13 de noviembre¹⁶¹. La norma articula un procedimiento específico para la autorización de la realización de actividades en el marco del espacio controlado de pruebas, al que pueden acceder, previa solicitud, los promotores de proyectos “que aporten una innovación de base tecnológica aplicable en el sistema financiero y que se encuentren suficientemente avanzados para probarse” y que presenten, además, “potencial utilidad o valor añadido sobre los usos ya existentes” en, al menos, uno de los

158. En este sentido, especialmente, Delgado Larena-Avellaneda (2021: 172 y ss.).

159. *Vid.*, en especial, Ranchordás (2021: 21 y ss.).

160. A este respecto, *cfr.* Finck (2019: 158-160).

161. Con todo, ha de señalarse que ha resultado controvertida la interpretación del ámbito objetivo de aplicación de la norma, en la medida en que se han alzado voces que defienden que el mismo alcanza potencialmente a cualesquiera actividades, con independencia de su eventual sujeción o no al requisito de la previa obtención de una autorización administrativa para su realización; en este sentido, particularmente, Zunzunegui (2020: 7). No obstante, como con acierto ha señalado Huergo Lora (2018: 51-52), pese a la ambigüedad del texto legal en este punto, es claro que la articulación de un mecanismo autorizador en la Ley 7/2020, de 13 de noviembre, caracterizado por su laxitud, persigue justamente facilitar el acceso excepcional a la realización de actividades que, de otra forma, se encontrarían sometidas a requisitos más severos.

ámbitos enumerados en el artículo 5.2. La evaluación de los proyectos, que competará a la autoridad supervisora correspondiente en función del sector de que se trate, de resultar positiva, no implicará la posibilidad de inicio de la actividad, pues el mismo se encuentra condicionado a la previa suscripción de un protocolo entre aquella y el promotor (artículos 7 y 8). La realización de las pruebas se someterá al control de los monitores designados por las respectivas autoridades competentes, que podrán acordar incluso su interrupción en los supuestos de incumplimiento de las disposiciones legales o de las previstas en el protocolo (artículos 15 y 16). En el caso de que el examen que habrá de llevarse a cabo al finalizar las pruebas arroje un resultado favorable, se prevé la denominada “pasarela de acceso a la actividad”, consistente en la posibilidad de que la autoridad competente acuerde la tramitación de la solicitud de autorización para la realización de la actividad en régimen ordinario de conformidad con lo previsto en el artículo 33 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (artículos 17 y 18).

A los efectos de la presente exposición, interesa destacar especialmente la previsión incorporada por la disposición final primera de la Ley, de conformidad con la cual “[e]l desarrollo y resultado de las pruebas se tendrá en cuenta a los efectos de simplificar la legislación existente, eliminar barreras y duplicidades innecesarias, establecer procedimientos más ágiles y minimizar las cargas administrativas a las que se encuentran sometidas las entidades financieras, todo ello al objeto de seguir impulsando un marco regulatorio eficiente para las actividades económicas”. La norma, ciertamente, evidencia la íntima conexión del régimen excepcional que articula la Ley 7/2020, de 13 de noviembre, con la aportación de elementos de reflexión al legislador estatal en orden a la sucesiva revisión del marco normativo aplicable a los sectores de actividad en los que se produzcan avances relevantes¹⁶², entre los que, con toda probabilidad, se contarán más pronto que tarde aquellos en los que se dé un uso prioritario o, cuando menos, creciente a la tecnología *blockchain*. En este punto, la disposición final citada posee unas implicaciones aparentemente limitadas si comparadas con las características de los *sandboxes* regulatorios desde la perspectiva aquí considerada, en la medida en que se refiere tan solo a la posibilidad de que las pruebas realizadas bajo el paraguas de esta fórmula aconsejen una relajación o flexibilización de los estándares legales vigentes, sin mencionar la posible incorporación o sustitución parcial de los parámetros aplicables por otros cuya conveniencia se haya puesto de manifiesto durante

162. En este sentido, específicamente, Delgado Larena-Avellaneda (2021: 181).

el período de vigencia de las normas definidas en el protocolo. Es claro, en este sentido, que las tecnologías de registro distribuido presentan un notable interés para los sectores de actividad a los que se extiende la aplicación de la Ley 7/2020, de 13 de noviembre, y que su avance puede traducirse en el diseño de nuevas aplicaciones cuyos riesgos asociados, convenientemente mitigados por medio de la introducción de mecanismos específicos de control, se juzgue oportuno asumir. En este contexto, la experiencia resultante de la realización de la actividad en el marco del espacio controlado de pruebas permitiría abogar por una intensificación de la fiscalización pública, no por la simplificación de los procedimientos, único escenario que contempla la norma. De esta forma, la disposición final primera de la Ley 7/2020, de 13 de noviembre, que acierta, desde una perspectiva general, en la caracterización de los *sandboxes* regulatorios como instrumentos a disposición del legislador, adopta una visión reduccionista y marcadamente influenciada por un horizonte desregulador cuyas virtudes, en nuestra opinión, en ocasiones se sobrevaloran.

4. Blockchain y administraciones públicas: aproximación general

4.1. Consideraciones introductorias

Descritos ya sucintamente los principales enfoques que pueden adoptar las autoridades dotadas de potestades normativas y de regulación para hacer frente a los retos que plantea *blockchain*, procede en este momento reflexionar, de forma igualmente sintética, acerca de las transformaciones que puede experimentar la actuación de las administraciones públicas a partir de su empleo.

A este respecto, debe comenzar por destacarse la preponderancia prácticamente absoluta del sector privado sobre el público en la utilización de *blockchain*. En este sentido, cabría considerar que la flexibilidad de las tecnologías de registro distribuido, entendida ahora en términos de versatilidad o de posibilidad de traslación a contextos diferentes de aquel en el que las mismas tienen su origen, se encuentra aún lejos de ser explotada en toda su potencialidad por parte de las administraciones públicas, que se situarían en el vagón de cola en dicho contexto. No es de extrañar, de esta forma, que las principales exposiciones generales en la materia se refieran casi exclusivamente a las transformaciones que esta modalidad de tecnología traerá consigo en los ámbitos empresarial y financiero, y que limiten, en consecuencia, el análisis del impacto de aquella sobre los poderes públicos al estudio de los desafíos

que la misma representa, precisamente, para el ejercicio de las potestades normativas y de regulación¹⁶³. Solo en fechas muy recientes ha comenzado la doctrina jurídica a prestar una atención específica al empleo de la tecnología *blockchain* por parte de las administraciones públicas y a las perspectivas de futuro del fenómeno, punto de vista que, como resulta evidente, se adopta en la presente obra colectiva con carácter preferente.

El referido predominio del sector privado sobre el público es debido no solo al origen de *blockchain*, sino también al creciente protagonismo de las entidades de derecho privado en el fomento del avance tecnológico y, sobre todo, a la filosofía subyacente al fenómeno: en cuanto que la distribución y la descentralización facilitarían, con los matices que ya nos son conocidos, la eliminación o sustitución de quienes actúan como intermediarios en la realización de numerosas categorías de actividades o transacciones, el empleo por parte de las administraciones públicas de la tecnología *blockchain* hallaría en su carácter servicial de los intereses generales un notable obstáculo, en la medida en que comportaría una tendencial asimilación de su posición jurídica a la de los particulares¹⁶⁴.

La circunstancia recién referida ha conducido a un relevante sector de la doctrina especializada a la apuesta por una mayor corresponsabilidad ciudadana en el ejercicio del poder público¹⁶⁵. En este sentido, la implantación de la tecnología *blockchain* en el sector público se conectaría directamente con la atribución del ejercicio de potestades administrativas a sujetos de derecho privado, ya ampliamente estudiada entre nosotros. La principal cuestión jurídica que se plantearía a partir de la comprensión aludida sería la relativa al alcance de los límites jurídico-constitucionales oponibles a dicho factor de transformación de la actividad administrativa¹⁶⁶, en la medida en que *blockchain* trascendería ampliamente las manifestaciones tradicionales del fenómeno, conduciendo incluso, de acuerdo con algunas visiones extremas, a cuestionar la necesidad misma del Estado y de los Gobiernos,

163. Cfr., por todos, Finck (2019).

164. En este sentido, cfr. particularmente Atzori (2015: *passim*), así como, entre otros, Sarzana di S. Ippolito y Nicotra (2018: 143-144), o Carullo (2021: 45).

165. Destaca, en este sentido, la exposición de Tapscott y Tapscott (2017: 297 y ss.), en la que se vincula dicha transformación con una mayor eficacia de la actuación de las instituciones públicas, lo que, en consecuencia, posibilitaría la consecución simultánea de dos objetivos aparentemente contrapuestos: “más Estado” y “menos Estado”. Por su parte, Swan (2015: 31, 54) se ha referido a esta transformación como el resultado de un avance natural en términos de eficiencia, subrayando, asimismo, el reto que representa la traslación de cotas de responsabilidad tradicionalmente atribuidas a los poderes públicos hacia los ciudadanos. En el presente volumen, cfr., particularmente, la exposición del profesor Aguado i Cudolà.

166. Extremo que certeramente subrayan Pollicino y De Gregorio (2021: 3).

que podrían llegar a ser sustituidos por las conocidas como organizaciones descentralizadas autónomas (*DAOs*, por sus siglas en inglés)¹⁶⁷.

En un sentido diametralmente opuesto al defendido por este último sector doctrinal se manifiestan quienes abogan por el empleo exclusivo de redes privadas o público-permisionadas por parte de las administraciones públicas. De acuerdo con estos autores, la utilización de la tecnología *blockchain* no comportaría una transformación radical de la forma de ejercicio de las potestades administrativas, si bien podría impulsar, en algunos casos, mejoras notables desde la perspectiva de la efectiva observancia de algunos de los principios que disciplinan aquellas. Con algunos matices relevantes, tal es la posición que sostienen varios de los autores que colaboran en el presente volumen¹⁶⁸.

No obstante, como ya es posible deducir a partir de lo expuesto hasta el momento, conviene advertir que las ventajas que algunos observan en el uso de la tecnología *blockchain* por parte de las administraciones públicas han sido objeto de viva contestación. En este sentido, como se tendrá ocasión de comprobar en algunos de los sucesivos capítulos, particularmente en determinados sectores de la actuación de los poderes públicos, las tecnologías de registro distribuido no parecen aportar, a la vista de su actual grado de desarrollo, valor añadido alguno. Así las cosas, no resulta ocioso recordar que la implantación de *blockchain* en el sector público no puede ser vista como un fin en sí mismo¹⁶⁹. Con ello no quiere decirse en modo alguno que las tecnologías de registro distribuido no puedan, como se verá seguidamente, facilitar importantes avances para las administraciones públicas¹⁷⁰, ni tampoco que estas –y en concreto, a los efectos que aquí interesan, el nivel de gobierno local– deban obviar su potencial transformador: su intervención, con seguridad, no solo impulsará el avance de la tecnología *blockchain*, sino que también contribuirá a reconducirla hacia la consecución de fines de interés general y fomentará el desarrollo de aplicaciones verdaderamente útiles en el ámbito jurídico-público.

167. En este sentido, destaca el radical posicionamiento de De Filippi y Wright (2015: 39). Como se ha destacado *supra* (nota al pie núm. 9), estos argumentos han sido sólidamente contestados por Atzori (2015).

168. En este sentido, *cfr.* particularmente las contribuciones de Berning Prieto, Presno Linera y García Majado.

169. Como tampoco parece que deba serlo, por referencia a los servicios públicos, la descentralización propiciada por la implantación de la tecnología *blockchain* en dicho ámbito; en este sentido, *cfr.* especialmente Atzori (2015: 21).

170. En este sentido, pese a la adopción de una postura crítica o, en el mejor de los casos, realista en relación con el empleo de la tecnología *blockchain* por parte de las administraciones públicas, *cfr.* Hermstrüwer (2021: 104).

4.2. Breves reflexiones sobre las principales ventajas y los desafíos del empleo de las tecnologías de registro distribuido por parte de las administraciones públicas

La perspectiva de la implantación de las tecnologías de registro distribuido en el sector público ha venido acompañada de una entusiasta acogida doctrinal, que ha visto en *blockchain*, además de ventajas comunes a su empleo en otros contextos¹⁷¹, la oportunidad definitiva de resolver muchas de las principales disfuncionalidades de aquel; de mejorar la forma en que se relacionan las administraciones públicas entre sí y con los ciudadanos; de hacer realidad, en fin, ambiciosas proclamaciones legales que por falta de medios, inercia o ausencia de una auténtica involucración de los principales actores institucionales son habitualmente inobservadas¹⁷². Con todo, no puede dejar de subrayarse que *blockchain* plantea retos específicos en el contexto de la actividad administrativa que han de ser cuidadosamente tomados en consideración, a fin de que las ventajas derivadas de su empleo en dicho ámbito compensen las dificultades adicionales que, en determinados casos, pueden presentarse¹⁷³.

Sobre los extremos referidos habrá de reflexionarse en profundidad en los sucesivos capítulos de la presente obra, en los que se abordará el estudio de la utilización de *blockchain* por parte de los Gobiernos locales en ámbitos diversos. De esta forma, las consideraciones que se exponen a continuación se presentan como una síntesis de los principales elementos de la disrupción que supondría la generalización del uso de las tecnologías de registro distribuido por parte de las administraciones públicas, con sucinta

171. Nos referimos, en concreto, al mayor nivel de seguridad que proporciona la tecnología de la cadena de bloques con respecto a otros sistemas de almacenamiento de información, cuestión a la que ya nos hemos referido *supra* y sobre la que no se considera necesario profundizar en este momento.

172. Piénsese, particularmente, en el derecho de los ciudadanos a no aportar los documentos que ya se encuentren en poder de la Administración actuante o que hayan sido elaborados por cualquier otra Administración [artículos 28.1 y 53.1.d) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común], la garantía de cuya efectividad a través del empleo de la tecnología *blockchain* ha sido auspiciada, entre nosotros, por Pereiro Cárceles (2019a: 144-145). Otro tanto cabe decir con respecto a las mejoras que *blockchain* ofrecería desde la perspectiva de la interoperabilidad de las administraciones públicas, avance que, en todo caso, se considera que exigiría un consenso en relación con el protocolo informático a utilizar, de acuerdo con las exposiciones de autores como Muñoz Carmona (2018: 13) o Macchia (2021: 120). Sobre los efectos benéficos de la utilización de la tecnología *blockchain* por parte del sector público, en general, *cf.*, por último, la breve exposición de Fernández Hergueta (2017).

173. A dicha dualidad se ha referido, entre nosotros, Tejedor Bielsa (2020: 120-121). En la doctrina extranjera, destacan las reflexiones de Hermstrüwer (2021), sobre las que habrá de volverse seguidamente.

consideración, asimismo, de los desafíos que la referida transformación podría traer consigo.

Un primer aspecto de interés es el relativo a los avances que facilita la tecnología *blockchain* desde la perspectiva de la transparencia, la lucha contra el fraude y la confianza ciudadana. El funcionamiento de la cadena de bloques permite, como ha habido ocasión de explicar *supra*, el acceso a la información contenida en la red a los usuarios de la misma –o al público general, en función del tipo de red por el que se opte–, lo que, claro está, favorece el cumplimiento del principio de transparencia y los efectos benéficos asociados al mismo, entre los que destaca especialmente la mejora en la trazabilidad de los procedimientos de concurrencia competitiva, como se subraya en diversas contribuciones del presente volumen¹⁷⁴. Además, como ha puesto de manifiesto la doctrina especializada¹⁷⁵, algunos de estos elementos –singularmente, la mejora en la lucha contra el fraude– se verían asimismo potenciados a través del favorecimiento de la automatización de los procedimientos mediante el uso de la tecnología *blockchain*, extremo sobre el que se volverá seguidamente.

Ciertamente, en un contexto como el actual parece difícil incurrir en exageraciones al ponderar la relevancia de la cuestión. No es de extrañar, así, que este sea unánimemente considerado uno de los puntos fuertes del empleo de la tecnología *blockchain* por parte de las administraciones públicas¹⁷⁶. Con todo, no puede dejar de subrayarse que la mayor transparencia que ofrecen las redes *blockchain* ha dado lugar al planteamiento de dudas en relación con la posible disminución de garantías desde la perspectiva del derecho a la protección de datos de carácter personal, cuestión a la que se dedica específicamente uno de los capítulos de la presente obra colectiva¹⁷⁷.

Un segundo aspecto relevante es el referente al cambio de paradigma que la criptografía asimétrica, elemento esencial del funcionamiento de la tecnología *blockchain*, facilita en relación con la autodeterminación informativa de los ciudadanos. La que ha dado en denominarse identidad “autosoberana” –traducción literal de la expresión anglosajona “*self-sovereign identity*”– o “gestionada autónomamente” –denominación que se considera preferible,

174. Véanse, en particular, las contribuciones de los profesores Hernando Rydings y Bueno Armijo.

175. Pereiro Cárceles (2019a: 151).

176. En este sentido, entre otros, Macchia (2021: 125); así como, en nuestra doctrina, Pereiro Cárceles (2019a: 144) y Tejedor Bielsa (2020: 120).

177. *Cfr.* la contribución de los profesores Boix Palop y Pereiro Cárceles.

en cuanto más correcta desde el punto de vista técnico-jurídico— comporta la posibilidad de que los ciudadanos seleccionen la información o los datos que desean compartir con terceros —a los efectos que aquí interesan, con las administraciones públicas— en cada caso concreto, pudiendo limitarse a exhibir aquellos que sean estrictamente necesarios para el desarrollo de o para el acceso a la actividad de que se trate. Dicha posibilidad, en contraposición a lo que viene de señalarse, constituye un extraordinario avance desde la perspectiva del derecho a la protección de datos de carácter personal; para algún autor, de hecho, se trata del “principal atractivo de la tecnología *blockchain*”¹⁷⁸. Con todo, esta importante mejora encuentra un obstáculo muy relevante en la ya referida disposición adicional sexta de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común, incorporada, como es sabido, por el Real Decreto-ley 14/2019, de 31 de octubre. Sobre estas cuestiones, en todo caso, se volverá asimismo en sucesivos capítulos de la presente obra colectiva, a los que en este momento hemos de remitirnos¹⁷⁹.

Un tercer aspecto, dotado de una extraordinaria significación en el más amplio contexto de la digitalización del funcionamiento del sector público, es el relativo al favorecimiento de la automatización de los procedimientos. La combinación de la tecnología *blockchain* con la internet de las cosas, por medio del empleo de *smart contracts*, permitiría la realización automatizada de una multiplicidad de actuaciones administrativas, lo que se traduciría en una tramitación más eficaz de los procedimientos —particularmente, los de concurrencia competitiva—¹⁸⁰, en una significativa mejora de la gestión documental, en una reducción de los períodos de ejecución de concretas prestaciones contractuales o, en fin, en importantes avances en el ámbito de la prestación de los servicios públicos —posibilidad, esta última, que presenta un interés cualificado en el ámbito local—¹⁸¹. En todo caso, como se expone en el capítulo de la profesora Hernando Rydings, dicha posibilidad se presenta en la actualidad, en contextos como el de la valoración de las ofertas contractuales, como muy limitada, toda vez que el mecanismo de los *smart contracts* —que, como se sabe, permite la realización automatizada de una determinada actuación una vez se verifica el hecho externo que se configura en el correspondiente programa como condición de la misma— resulta, por su

178. Muñoz Carmona (2018: 44).

179. *Cfr.* particularmente las contribuciones de Berning Prieto y Aguado i Cudolà.

180. A este respecto, en nuestra doctrina, es obligada la remisión *in toto* al excelente estudio de Pereiro Cárceles (2019b). *Cfr.* asimismo las reflexiones sobre el particular de Bueno Armijo en este mismo volumen.

181. En relación con esta última esfera de actividad, *cfr.* la contribución de la profesora Garrido Juncal en el presente volumen.

propia naturaleza, auténticamente útil tan solo en los supuestos de utilización de criterios de valoración y selección íntegramente cuantificables¹⁸², pues en otro caso se requeriría de la intervención de oráculos, lo que privaría de interés a su implantación en el referido contexto. Y dicha posibilidad, además, no se halla exenta de riesgos, en la medida en que la configuración incorrecta de los algoritmos empleados en la valoración de las ofertas y en la adjudicación de los contratos plantearía, lógicamente, dificultades adicionales a las derivadas de la incursión en error en la realización de las referidas operaciones por parte del órgano de contratación.

La cuestión no es baladí, y entronca directamente con las limitaciones de los *smart contracts* que, desde una perspectiva general, ha observado la doctrina, y a las que ya se ha hecho breve referencia *supra*¹⁸³. En este sentido, las ventajas que, en términos de seguridad jurídica y de eficiencia, presenta la automatización que favorecen los referidos programas informáticos, se ven muy significativamente relativizadas por la realidad de la aplicación de las normas, que exigen de los operadores jurídicos el desarrollo de una importante y en ocasiones compleja labor de ponderación y de interpretación, por su propia naturaleza no automatizable (o, al menos, no íntegramente). Como es sabido, la imposible predeterminación exhaustiva de todas las actuaciones que habrán de desarrollar las administraciones con vistas a la satisfacción del interés público requiere del reconocimiento a favor de las mismas de, en algunos casos, amplios márgenes de apreciación o de la atribución a su favor de potestades de naturaleza discrecional, cuya eliminación total podría dar lugar a graves problemas. El ansiado horizonte de una seguridad jurídica cuasi total conduce, así, a un contexto de rigidez extrema, y ello por dos motivos fundamentales: en primer lugar, como consecuencia de la prácticamente imposible incorporación al funcionamiento de la red del conjunto de variables que las normas habitualmente no prevén con carácter expreso, pero que el operador jurídico efectivamente toma en consideración; y en segundo lugar, por razón de la difícil introducción de cambios en la cadena de bloques, en la medida en que, como ya ha habido ocasión de exponer, pese a lo incorrecto de la afirmación de su carácter absolutamente inmutable, la modificación de sus contenidos se encuentra sujeta a exigencias técnicas muy severas, lo que plantea problemas, específicamente, en los supuestos en que hayan sido objeto de ejecución automatizada actuaciones que, en una fase posterior de control, se demuestren inválidas¹⁸⁴.

182. En idéntico sentido, *cfr.*, en nuestra doctrina, Tejedor Bielsa (2020: 124).

183. Apartado 3.2.

184. Sobre estas cuestiones, *cfr.*, por todos, Hermstrüwer (2021: 112 y ss.).

Por consiguiente, a los obstáculos de naturaleza jurídica –en esencia, los conexos al derecho a la protección de datos personales, con las matizaciones referidas, así como, en el derecho español, los resultantes de la disposición adicional sexta de la LPAC– se suman las limitaciones de carácter técnico. Las que presentan los *smart contracts* no son, de hecho, las únicas que han de considerarse al hacer balance sobre el interés del desarrollo de aplicaciones basadas en *blockchain* para su utilización por parte de las administraciones públicas. Desde una perspectiva más amplia, debe tenerse en cuenta, en primer término, que las tecnologías de registro distribuido se encuentran –en particular, en lo relativo a su empleo mediante redes de naturaleza no permissionada– aún en una fase embrionaria o incipiente. A mayor abundamiento, en segundo lugar, algunas redes *blockchain* –en concreto, aquellas que se basan en la prueba de trabajo como mecanismo de consenso– han mostrado signos de un cierto “agotamiento”, motivado por el constante y exponencial aumento de la capacidad computacional que exige su adecuado funcionamiento. A lo anterior se añade, en fin, la variable económica: el desarrollo de casos de uso de *blockchain* en el sector público exigirá, en ocasiones, la realización de importantes inversiones dinerarias¹⁸⁵, lo que aconseja, desde este punto de vista, una ponderación adecuada de los beneficios que para su funcionamiento posibilita el estado actual de la técnica.

Los factores referidos justifican, en nuestra opinión, la incorporación tardía o, al menos, paulatina de las administraciones públicas al universo *blockchain*. Una implantación generalizada y excesivamente rápida de esta tecnología en el sector público –considerado, además, el en algunos casos penoso viacrucis que ha resultado ser el proceso de digitalización de las administraciones públicas– podría dar lugar a dificultades añadidas, cuando no a decisiones erróneas en términos estratégicos, lógicamente indeseables. Se antoja más prudente, en suma, la articulación inicial de casos de uso de la tecnología *blockchain* con un impacto económico o con un alcance territorial limitado. En este contexto, como con acierto ponen de manifiesto varios de los coautores del presente volumen, el mundo local constituye, precisamente, un entorno excelente para el desarrollo experimental de dichas aplicaciones. Antes de dar paso a las contribuciones sucesivas, en las que se volverá sobre esta cuestión, y a modo de cierre del presente estudio preliminar, habrán de considerarse algunos casos de uso específicos de la tecnología *blockchain* por parte del sector público desde la perspectiva referida.

185. A este respecto, con referencia a la insuficiencia de las inversiones en el contexto italiano, *cfr.* Macchia (2021: 119).

4.3. Casos de uso de la tecnología *blockchain* en el sector público (selección)

Como viene de señalarse, en la exposición sucesiva se reflexionará muy sintéticamente sobre diversos casos de uso de *blockchain* por parte del sector público. A tal fin, se han elegido aplicaciones de las tecnologías de registro distribuido diferentes de aquellas a cuyo estudio se dedican específicamente los restantes capítulos del presente volumen, a los que, a dichos efectos, hemos en este momento de remitirnos. Además del referido criterio, la selección parte de la toma en consideración de dos aspectos complementarios: por un lado, el grado de madurez e implantación de las correspondientes aplicaciones; por otro, su efectiva utilidad para la mejora del funcionamiento del sector público y para la satisfacción de las necesidades y demandas de los ciudadanos. Sobre la base de lo anterior, se ha optado por considerar el empleo de *blockchain* en tres ámbitos concretos: los registros públicos, la gestión de certificados y diplomas, y el sector sanitario.

En lo que hace al primero de los ámbitos referidos, ya la propia conceptualización de las redes *blockchain* –como libro mayor distribuido– da una idea aproximada acerca de la promesa de disrupción vinculada a esta modalidad tecnológica. La utilización de *blockchain* en el ámbito registral presentaría, así, importantes efectos positivos, tales como el mayor grado de seguridad e integridad de la información, la simplificación de la gestión burocrática –consecuencia, entre otros factores, del favorecimiento de la interoperabilidad– o la facilitación del acceso público a la información incorporada al registro; aspectos que, como resulta evidente, redundarían en significativas mejoras desde la perspectiva de la seguridad del tráfico, objetivo a cuya consecución se orienta, en primer término, el propio sistema registral¹⁸⁶. Asimismo, de acuerdo con lo afirmado en una de las obras que han conocido mayor difusión en relación con la cuestión que nos ocupa, la combinación en este ámbito de las tecnologías de registro distribuido con la *IoT* presentaría un notable interés desde la perspectiva del cumplimiento normativo, al posibilitar el ejercicio automatizado de determinadas potestades administrativas mediante el empleo de los datos incorporados a la cadena de bloques¹⁸⁷. A la luz de las anteriores consideraciones, no parece que pueda extrañar que la utilización de la tecnología *blockchain* en el ámbito registral se erija en uno de los más

186. Extremos subrayados entre nosotros por Ibáñez Jiménez (2018: 404), Muñoz Carmona (2018: 51 y ss.) y Pereiro Cárceles (2019a: 148).

187. A título ejemplificativo, la aplicación de la tecnología *blockchain* en este ámbito permitiría, según se ha afirmado, bloquear la circulación de los vehículos que no hubieran superado la preceptiva inspección técnica; en este sentido, *cfr.*: Tapscott y Tapscott (2017: 233-234).

relevantes (y extendidos) casos de uso de la misma por parte del sector público, como ponen de manifiesto los más recientes análisis generales en la materia¹⁸⁸.

De acuerdo con algunas exposiciones, el impacto de la tecnología *blockchain* en la gestión de los registros públicos no se limitaría, en todo caso, a los extremos señalados. En este sentido, la transformación se extendería a la propia figura del registrador, en cuanto que su intervención, se argumenta, podría terminar por resultar prescindible¹⁸⁹. En consecuencia, el que se antojaba utópico ideal de la desintermediación alcanzaría al ámbito registral, lo que, a su vez, incidiría directamente sobre enteros sectores de la actividad económica.

Como es obvio, lo anterior supondría admitir la hipótesis del desarrollo de la función registral por parte de la comunidad *blockchain*. La descentralización y la desintermediación en este ámbito traerían consigo la posibilidad de creación y consolidación de registros paralelos a los institucionales, lo que provocaría efectos muy negativos sobre la protección de los derechos patrimoniales y de los intereses de los ciudadanos, finalidad última del sistema. Ante el referido riesgo, es claro que la implantación de las tecnologías de registro distribuido en el ámbito registral deberá partir de la configuración permisionada de las redes¹⁹⁰. En un escenario como el descrito, no parece poder plantearse seriamente la posibilidad de la eliminación de la figura del registrador, auspiciada por los posicionamientos doctrinales aquí criticados. Lo anterior, claro está, ha de ser entendido sin perjuicio de la necesidad, llegado el caso, de reconsiderar en profundidad la formación que haya de exigirse al personal encargado de los registros.

En definitiva, si bien cabe afirmar, a la vista del actual estado de la cuestión, que la implantación de la tecnología *blockchain* en el ámbito registral podría facilitar mejoras muy significativas, se impone con idéntica evidencia la conclusión relativa al forzoso rechazo de una transformación radical de dicha función, consistente en la traslación de su ejercicio a una red de carácter no permisionado. La garantía de los derechos de los ciudadanos exige la atribución a la autoridad de potestades de control efectivo sobre el contenido del registro, salvaguarda que hoy no parece posible articular a través de una red pública sin permisos. En suma, la tecnología *blockchain*, tal y como hoy la

188. *Cfr.*, en concreto, Hermstrüwer (2021: 109), donde puede consultarse un amplio listado de países en los que se ha recurrido a la tecnología *blockchain* para la gestión de los registros de la propiedad inmobiliaria.

189. Por todos, en este sentido, *cfr.* Muñoz Carmona (2018: 56).

190. En este sentido, especialmente, Ibáñez Jiménez (2018: 405-406).

conocemos, no motivará la reedición del movimiento ludita entre los titulares de los registros¹⁹¹.

En lo relativo al segundo caso de uso objeto de análisis, debe subrayarse, en primer término, el interés que el mismo presenta para la garantía de la interoperabilidad del contenido de los certificados y diplomas, avance cuya significación resulta manifiesta, máxime en el contexto del Espacio Europeo de Educación Superior. No puede extrañar, así, que esta sea una de las aplicaciones impulsadas por la red EBSI (*European Blockchain Services Infrastructure*), en la que participan, como se ha destacado *supra*¹⁹², la Comisión Europea, los Estados miembros de la Unión, Noruega y Liechtenstein.

La referida no es, sin embargo, la única ventaja que presenta el empleo de *blockchain* en el ámbito ahora considerado. La gestión de certificados y diplomas mediante las tecnologías de registro distribuido reforzaría el control ciudadano con respecto al acceso por parte de terceros a la información contenida en el expediente académico; garantizaría, de nuevo, mayores niveles de integridad; posibilitaría, asimismo, la emisión y validación de los certificados a través de procedimientos automatizados; y, en fin, en conexión con este último aspecto, permitiría una reducción significativa de los costes asociados a dichas operaciones¹⁹³. A nadie puede asombrar, así, que esta aplicación haya conocido ya importantes desarrollos, entre los que la doctrina especializada ha podido destacar una iniciativa impulsada por la Universidad Carlos III de Madrid¹⁹⁴.

En nuestra opinión, la implantación de la tecnología *blockchain* en el ámbito ahora considerado cumple los estándares exigibles a las estrategias de digitalización del sector público. Se trata, en primer lugar, de un caso de uso que presenta innegables ventajas tanto desde la perspectiva del funcionamiento del sector público como desde el punto de vista de la satisfacción de las necesidades de los ciudadanos. Asimismo, en segundo lugar, el liderazgo en la materia ha sido asumido por la Unión Europea, lo que favorece la articulación de sistemas plenamente interoperables entre los respectivos Estados y redundando en beneficio, precisamente por dicha razón, del cumplimiento de uno de los principales

191. Sobre estas y otras cuestiones conexas, *cfr.* asimismo las lúcidas reflexiones del profesor Bueno Armijo en el presente volumen.

192. Apartado 3.1.2.

193. En este sentido, *cfr.* Pereiro Cárceles (2019a: 149), así como, con referencia a la iniciativa de la red EBSI, la intervención de Jesús Ruiz en el *webinar* “*Blockchain y Administraciones Públicas*”, organizado por la Diputación de Alicante y la Fundación Democracia y Gobierno Local el pasado 1 de febrero de 2021, disponible en: <https://www.youtube.com/watch?v=xY2DhOxKyK8>.

194. *Cfr.*, de nuevo, Pereiro Cárceles (2019a: 149).

objetivos que se persiguen con la introducción de la tecnología *blockchain* en el ámbito de referencia. La decisión parece, en tercer lugar, eficiente, al exigir la realización de inversiones económicas (relativamente, es decir, por comparación con las requeridas en otros sectores) no muy elevadas y favorecer, al mismo tiempo, disminuciones significativas en los costes de gestión de la actividad afectada. Se presenta, en definitiva, como una iniciativa de impacto (tan solo inicialmente) limitado, que puede –además de impulsar, en general, el desarrollo de la tecnología *blockchain*– desplegar efectos muy beneficiosos en relación con el avance y la consolidación de las libertades comunitarias.

Por último, en lo referente a la aplicación de las tecnologías de registro distribuido en el sector sanitario, interesa destacar especialmente, dadas las características del caso español, la posibilidad de superación de los problemas, por todos conocidos, derivados de la falta de interoperabilidad de los programas informáticos utilizados por las comunidades autónomas. Como ha destacado la doctrina especializada, el empleo en este contexto de la tecnología *blockchain* permitiría la creación de perfiles que el ciudadano podría gestionar de manera autónoma, toda vez que se le atribuiría la decisión última sobre la exhibición de sus propios datos de salud¹⁹⁵ en atención a las circunstancias concurrentes en cada caso. De ello resultaría un importante avance ya no solo desde la perspectiva del derecho a la autodeterminación informativa –extremo que ya ha quedado apuntado *supra*, al dar breve noticia de la propuesta de reforma del Reglamento eIDAS–, sino también en términos de eficacia, puesto que se daría una solución satisfactoria al problema recién referido¹⁹⁶.

Sin embargo, el potencial disruptivo de la tecnología *blockchain* en el sector sanitario no se agotaría en la vertiente que viene de considerarse. Muy al contrario: las aplicaciones e hipotéticos casos de uso abarcarían múltiples ámbitos y posibilitarían mejoras en el cuidado de los pacientes –en aspectos tales como el fomento de hábitos de vida saludables a través de aplicaciones móviles, el seguimiento automatizado del tratamiento prescrito por el personal sanitario, el diagnóstico y tratamiento a distancia, o la utilización de datos masivos para la adopción de decisiones en materia de salud pública–, la investigación médica –experimental, clínica y epidemiológica– o la gestión de la Administración sanitaria –a título meramente ejemplificativo, en relación con la gestión

195. Categoría de datos personales que, como se señala en un importante estudio sobre el empleo de la tecnología *blockchain* en el sector sanitario, engloba no solo los incorporados al historial clínico, sino también otros, tales como los datos genéticos, demográficos, administrativos o relativos a los hábitos de salud; *cf.*: Motsi-Omojiade y Kharlamov (2021: 174-175).

196. A este respecto, *cf.*, en nuestra doctrina, Muñoz Carmona (2018: 57 y ss.) y Pereiro Cárceles (2019a: 148-149).

documental del consentimiento manifestado para la dispensa de un tratamiento o para la hospitalización de un paciente—. En los análisis más recientes del fenómeno se ha podido subrayar la existencia de importantes diferencias tanto en lo relativo a la efectiva puesta en marcha de las correspondientes aplicaciones —algunas ya consolidadas, otras todavía *in fieri*— como desde la perspectiva geográfica, dado el claro predominio de Estados Unidos en el sector, que se considera impulsado por la laxitud del acervo normativo aplicable en aquel país en materia de protección de datos de carácter personal¹⁹⁷. Como es obvio, no resulta posible, en una contribución de estas características, profundizar en el estudio de esta compleja problemática, por lo que la exposición ha de detenerse en la certificación de la existencia de la misma.

Confiamos en que la panorámica ofrecida en las páginas precedentes haya facilitado la comprensión del extraordinario reto que representa la implantación de *blockchain* en el sector público. Los avances que, en el ámbito referido, posibilita este instrumento, no permiten en modo alguno relativizar la necesidad de reflexión previa con respecto a las deficiencias de la organización y la actividad administrativas que se persiga corregir y los obstáculos, tanto tecnológicos como jurídicos, a los que habrá de hacerse frente. Con seguridad, el lector encontrará en las contribuciones que integran el presente volumen muy valiosas reflexiones al respecto. Es hora, por consiguiente, de dar paso a las mismas.

5. Bibliografía

Atzori, M. (2015). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713.

Boix Palop, A. (2020). Los algoritmos son reglamentos: La necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones. *Revista de Derecho Público: Teoría y Método*, 1, 223-270.

Cappiello, B. (2021). Blockchain-Based Organizations and the Governance of On-Chain and Off-Chain Rules: Towards Autonomous (Legal) Orders? En B. Cappiello y G. Carullo (eds.). *Blockchain, Law and Governance* (pp. 13-42). Cham: Springer.

197. Sobre estas cuestiones, *cfr.* la completa exposición de Motsi-Omoijiade y Kharlamov (2021: *passim*).

- Carrascosa Cobos, C., Kuchkovsky Jiménez, C. y Preukschat, Á. (2017). Hacktivismo, cypherpunks y el nacimiento de la blockchain. En Á. Preukschat (coord.). *Blockchain: la revolución industrial de internet* (pp. 189-194). Barcelona: Gestión 2000.
- Carullo, G. (2021). The Role of Blockchain in the Public Sector: An Overview. En B. Cappiello y G. Carullo (eds.). *Blockchain, Law and Governance* (pp. 43-57). Cham: Springer.
- Casey, A. J. y Niblett, A. (2017). The Death of Rules and Standards. *Indiana Law Journal*, 92, 1401-1447.
- Darnaculleta i Gardella, M^a M. (2005). *Autorregulación y derecho público: la autorregulación regulada*. Madrid: Marcial Pons.
- De Caria, R. (2021). Blockchain and sovereignty. En O. Pollicino y G. De Gregorio (eds.). *Blockchain and Public Law. Global Challenges in the Era of Decentralisation* (pp. 41-59). Cheltenham/Northampton: Edward Elgar Publishing.
- De Filippi, P. y Wright, A. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Disponible en: <https://ssrn.com/abstract=2580664>.
- (2018). *Blockchain and the Law. The Rule of Code*. Cambridge/London: Harvard University Press.
- Delgado Larena-Avellaneda, J. E. (2021). El “sandbox” español. En M. Barrio Andrés (dir.). *Criptoactivos. Retos y desafíos normativos*. Las Rozas: Wolters Kluwer.
- Dimitropoulos, G. (2020). The Law of Blockchain. *Washington Law Review*, 95-3, 1117-1192.
- Doménech Pascual, G. (2019). Experimentos en la teoría y la práctica del derecho. *XIII Seminario de Teoría y Método (STEM)*.
- Esteve Pardo, J. (2002). *Autorregulación. Génesis y efectos*. Cizur Menor: Aranzadi.
- (2021). *Principios de derecho regulatorio. Servicios económicos de interés general y regulación de riesgos*. Madrid: Marcial Pons.
- Fernández Hergueta, R. (2017). El sector público y el uso de la blockchain. En Á. Preukschat (coord.). *Blockchain: la revolución industrial de internet* (pp. 94-98). Barcelona: Gestión 2000.
- Finck, M. (2019). *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press.

- García Luengo, J. (2018). Las cartas admonitorias como alternativa al ejercicio de la potestad sancionadora. En A. Huergo Lora (dir.). *Problemas actuales del derecho administrativo sancionador* (pp. 101-128). Madrid: Iustel.
- García Mexía, P. (2018a). Introducción general. En P. García Mexía (dir.). *Criptoderecho. La regulación de Blockchain* (pp. 23-35). Las Rozas: Wolters Kluwer.
- (2018b). Del ciberderecho al criptoderecho. La criptorregulación. En P. García Mexía (dir.). *Criptoderecho. La regulación de Blockchain* (pp. 75-140). Las Rozas: Wolters Kluwer.
- González-Meneses, M. (2017). *Entender Blockchain. Una Introducción a la Tecnología de Registro Distribuido*. Cizur Menor: Aranzadi.
- Greenspan, G. (2017). *The Blockchain Immutability Myth*. Disponible en: <https://www.coindesk.com/markets/2017/05/09/the-blockchain-immutability-myth/>.
- Herencia Antón, J. (2021). Fundamentos tecnológicos de los criptoactivos. En M. Barrio Andrés (dir.). *Criptoactivos. Retos y desafíos normativos* (pp. 63-77). Las Rozas: Wolters Kluwer.
- Herian, R. (2020). *Regulating Blockchain. Critical Perspectives in Law and Technology*. New York: Routledge.
- Hermstrüwer, Y. (2021). Blockchain and public administration. En O. Pollicino y G. De Gregorio (eds.). *Blockchain and Public Law. Global Challenges in the Era of Decentralisation* (pp. 105-122). Cheltenham/Northampton: Edward Elgar Publishing.
- Hildebrandt, M. (2016). Law as Information in the Era of Data-Driven Agency. *The Modern Law Review*, 79-1, 1-30.
- Huergo Lora, A. (2018). Un “espacio controlado de pruebas” (*regulatory sandbox*) para las empresas financieras tecnológicamente innovadoras. *El Cronista del Estado Social y Democrático de Derecho*, 76, 48-59.
- (2020). Una aproximación a los algoritmos desde el derecho administrativo. En A. Huergo Lora (dir.) y G. M. Díaz González (coord.). *La regulación de los algoritmos* (pp. 23-87). Pamplona: Aranzadi.
- Ibáñez Jiménez, J. W. (2018). *Derecho de Blockchain y de la tecnología de registros distribuidos*. Cizur Menor: Aranzadi.
- Kohl, U. (2021). Blockchain utopia and its governance shortfalls. En O. Pollicino y G. De Gregorio (eds.). *Blockchain and Public Law. Global Challenges in the Era of Decentralisation* (pp. 13-40). Cheltenham/Northampton: Edward Elgar Publishing.

- Lassège, J. (2021). Some Historical and Philosophical Remarks on the Rule of Law in the Time of Automation. En B. Cappiello y G. Carullo (eds.). *Blockchain, Law and Governance* (pp. 59-72). Cham: Springer.
- Lessig, L. (2001). *El Código y otras leyes del ciberespacio*. Madrid: Taurusesdigital (traducción de E. Alberola).
- Low, K. F. K. y Mik, E. (2020). Pause the Blockchain Legal Revolution. *International and Comparative Law Quarterly*, 69, 135-175.
- Macchia, M. (2021). Blockchain e pubblica amministrazione. *Federalismi.it*, 2, 117-129.
- Magnuson, M. (2020). *Blockchain Democracy. Technology, Law and the Rule of the Crowd*. Cambridge: Cambridge University Press.
- Márquez Solís, S. (2017). Seguridad y *blockchain*. En Á. Preukschat (coord.). *Blockchain: la revolución industrial de internet* (pp. 227-233). Barcelona: Gestión 2000.
- Morales Barroso, J. (2018). ¿Qué es Blockchain? En P. García Mexía (dir.). *Criptoderecho. La regulación de Blockchain* (pp. 39-74). Las Rozas: Wolters Kluwer.
- Motsi-Omoijiade, I. y Kharlamov, A. (2021). Blockchain for healthcare applications and use cases. En O. Pollicino y G. De Gregorio (eds.). *Blockchain and Public Law. Global Challenges in the Era of Decentralisation* (pp. 157-190). Cheltenham/Northampton: Edward Elgar Publishing.
- Muñoz Carmona, A. (2018). *Implicaciones jurídicas del uso de blockchain en la Administración pública* [Trabajo Fin de Máster]. Universidad de Murcia.
- Muñoz Machado, S. (2000). *La regulación de la red. Poder y Derecho en Internet*. Madrid: Taurus.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Disponible en: <https://bitcoin.org/bitcoin.pdf>.
- Núñez Miller, J. (2017). Criptografía asimétrica y consenso aplicado a la *blockchain*. En Á. Preukschat (coord.). *Blockchain: la revolución industrial de internet* (pp. 203-219). Barcelona: Gestión 2000.
- Pastor Sempere, C. (2018). Internet del valor. En R. Vilarroig Moya y C. Pastor Sempere (dirs.). *Blockchain: Aspectos Tecnológicos, Empresariales y Legales* (pp. 79-124). Cizur Menor: Aranzadi.

- Pedreira Menéndez, J. y Álvarez Pérez, M.^a B. (2018). Consideraciones sobre la tributación y la calificación contable de las operaciones con moneda digital (Bitcoins) en las empresas. *Quincena fiscal*, 3, 17-50.
- Pereiro Cárceles, M. (2019a). Usos de la tecnología *blockchain* en la Administración pública. En B. Puentes Cociña y A. Quintiá Pastrana (dirs.). *El derecho ante la transformación digital. Oportunidades, riesgos y garantías* (pp. 141-154). Barcelona: Atelier.
- (2019b). La utilización de *blockchain* en los procedimientos de concurrencia competitiva. *Revista General de Derecho Administrativo*, 50.
- Pollicino, O. y De Gregorio, G. (2021). Blockchain and Public Law: An introduction. En O. Pollicino y G. De Gregorio (eds.). *Blockchain and Public Law. Global Challenges in the Era of Decentralisation* (pp. 1-11). Cheltenham/Northampton: Edward Elgar Publishing.
- Ponce de León, P. J. (2018). *Blockchain*, un nuevo patrón tecnológico. En R. Vilarroig Moya y C. Pastor Sempere (dirs.). *Blockchain: Aspectos Tecnológicos, Empresariales y Legales* (pp. 35-77). Cizur Menor: Aranzadi.
- Poncibò, C. (2021). Blockchain and Comparative Law. En B. Cappiello y G. Carullo (eds.). *Blockchain, Law and Governance* (pp. 137-156). Cham: Springer.
- Preukschat, Á. y Molero Manglano, Í. (2017). Introducción. ¡Bienvenido a la generación *blockchain*! En Á. Preukschat (coord.). *Blockchain: la revolución industrial de internet* (pp. 15-20). Barcelona: Gestión 2000.
- Ranchordás, S. (2021). *Experimental Regulations and Regulatory Sandboxes: Law without Order?* Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3934075.
- Reed, J. (2016). *Blockchain. The essential guide to understanding the blockchain revolution*.
- Reidenberg, J. R. (1998). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, 76-3, 553-593.
- Reyes, C. L. (2017). Conceptualizing Cryptolaw. *Nebraska Law Review*, 96-2, 384-445.
- Sarzana di S. Ippolito, F. y Nicotra, M. (2018). *Diritto della blockchain, intelligenza artificiale e IoT*. Milán: Wolters Kluwer.
- Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly.
- Tapscott, D. y Tapscott, A. (2017). *La revolución blockchain*. Barcelona: Ediciones Deusto (traducción de J. M. Salmerón).

- Tejedor Bielsa, J. (2020). Transformación digital, “blockchain” e inteligencia artificial en la Administración pública. *Revista Española de Derecho Administrativo*, 209, 111-138.
- Velasco Caballero, F. (2014). *Derecho público más derecho privado*. Madrid: Marcial Pons.
- Walch, A. (2017). *Blockchain's treacherous vocabulary: One More Challenge for Regulators*. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3019328.
- Zaccaroni, G. (2022). *Le Roi est Mort, Vive le Roi! La blockchain e il diritto dell'Unione europea*. *Annali AISDUE*, 249-274.
- Zunzunegui, F. (2020). Aproximación al espacio controlado de pruebas (*Regulatory Sandbox*). Comentario a la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero. *Regulación financiera: Revista de Derecho del Mercado Financiero*, Working Paper 6/2020.

Ciudades inteligentes y tecnología de cadena de bloques: hacia un ejercicio compartido de funciones públicas¹

Vicenç Aguado i Cudolà
Catedrático de Derecho Administrativo.
Universidad de Barcelona

SUMARIO. 1. **Introducción: La aportación de la tecnología de cadena de bloques a la ciudad inteligente.** 2. **El concepto de ciudad inteligente.** 2.1. La ciudad inteligente: un concepto holístico. 2.2. La relevancia jurídica del concepto de ciudad inteligente. 2.3. La ciudad inteligente desde la perspectiva del derecho a la ciudad. 2.4. Los servicios de interés general en la ciudad inteligente: panorámica general. 2.4.1. Principios generales. 2.4.2. Derechos de los usuarios. 3. **La aplicación de la tecnología de cadena de bloques a la ciudad inteligente.** 3.1. La tecnología de cadena de bloques: tipología. 3.2. La regulación de la tecnología de cadena de bloques en el ámbito de las administraciones públicas. 3.3. Ventajas y riesgos de la tecnología de cadena de bloques en la ciudad inteligente: ¿una mayor eficiencia, sostenibilidad y seguridad en las transacciones? 3.3.1. Transparencia. 3.3.2. Comunicación sin intermediación. 3.3.3. Integridad y no manipulación de los datos. 3.3.4. Inclusión de las personas. 3.4. La aplicación de la tecnología de cadena de bloques a los diferentes tipos de servicios en la ciudad inteligente. 3.4.1. Energía y medio ambiente. 3.4.2. Movilidad. 3.4.3. Seguridad y emergencias. 3.4.4. Servicios de atención a las personas: educación, sanidad y servicios sociales. 3.5. La participación de la ciudadanía en la gobernanza de las ciudades inteligentes mediante tecnología de cadena de bloques. 4. **Conclusiones: La aportación de**

1. Esta publicación es parte del proyecto de I+D+i: PID2020-114735GB-I00, financiado por MCIN/ AEI/10.13039/501100011033/.

la tecnología de cadena de bloques al desarrollo de la ciudad inteligente y sus retos jurídicos. 5. Bibliografía.

1. Introducción: La aportación de la tecnología de cadena de bloques a la ciudad inteligente

El objetivo general de este trabajo es examinar los aspectos jurídicos que presenta la tecnología *blockchain* o de cadena de bloques en el ámbito de las *smarts cities* o ciudades inteligentes. Esta perspectiva se focaliza en el ámbito de las relaciones entre administraciones y ciudadanos, reguladas por el derecho administrativo. La tesis que se defiende en este trabajo es que la tecnología puede ser un importante elemento de transformación en el ámbito de las relaciones entre Estado y sociedad², afectando al ejercicio de determinadas funciones públicas. Tales funciones, consideradas como propias del ejercicio de autoridad como la fe pública, el registro, la constatación de determinados hechos y su adecuación a la legalidad, pueden llegar a realizarse de forma compartida, al distribuirse entre los usuarios de una determinada red, asegurando aspectos como su trazabilidad, inmutabilidad y transparencia.

Este proceso de cambios lo situamos en el contexto de las ciudades inteligentes (*smarts cities*). Los proyectos de ciudades inteligentes buscan esencialmente la aplicación de las tecnologías para prestar unos servicios de interés general más eficientes. Para ello, las administraciones públicas, como responsables de estos servicios, están incorporando progresivamente diversos tipos de tecnologías de la información y la comunicación. Entre las más relevantes destacaremos el internet de las cosas, los grandes volúmenes de datos (*big data*), los datos abiertos (*open data*), la nube (*cloud computing*), las redes 5G, así como la tecnología de la inteligencia artificial (IA), a la que nos referiremos brevemente para contextualizarlas en el ámbito de las ciudades inteligentes y la tecnología de cadena de bloques (*blockchain*). Por tanto, una de las características es la integración de diversas tecnologías de carácter avanzado con la finalidad de gestionar de forma más eficiente las infraestructuras y los servicios de que dispone la ciudad, poniendo en el centro del sistema a la ciudadanía no solo como un mero usuario o receptor pasivo, sino como un agente que participa activamente en este proceso. A continuación realizaremos una breve exposición, sin perjuicio de remitirnos

2. Sobre la evolución de las relaciones entre Estado y sociedad como elemento de cambio en el derecho administrativo, *vid.* Esteve Pardo (2013).

a un examen más completo sobre estas tecnologías (Agencia Española de Protección de Datos, 2020).

En un lugar relevante se sitúa internet de las cosas (*internet of the things*; *IoT* en su acrónimo inglés), que permite a las administraciones recoger una gran variedad y cantidad de datos a través de sensores repartidos por toda la ciudad, instalados en semáforos, señales, contenedores de basura, farolas para el alumbrado, edificios, aparcamientos, etc. Sensores que pueden recolectar a través de imágenes, sonidos o cifras, datos relativos a movimiento, a la emisión de gases, líquidos, la intensidad de la luz, etc. En base a la obtención masiva de datos se puede, entre otras cosas, realizar una mejor gestión del transporte y de la movilidad, una más eficiente recogida de los residuos o una planificación más adecuada del patrullaje de los servicios de seguridad.

De forma complementaria también podemos destacar la tecnología vestible o portable (*wearable*), que consiste en que las personas llevan encima de su ropa o complemento (reloj, brazaletes, gafas, anillos, collares, pendientes, muñequeras, auriculares, cinturones, calcetines, zapatillas, etc.) un dispositivo que recoge todo tipo de datos como pueden ser, entre otros, el ritmo cardiaco, el estado de salud, las rutas que se realizan, los hábitos alimenticios, la higiene del sueño... Aquí, a diferencia de internet de las cosas, donde los sensores están diseminados en diversos puntos estratégicos de la ciudad, es el propio ciudadano quien los lleva encima durante su interacción con la ciudad.

Los grandes volúmenes de datos (*big data*) son todos aquellos que se obtienen de forma masiva y que son difíciles de obtener y gestionar debido a sus propias características, como su cantidad, su variabilidad y el carácter exponencial de su crecimiento. En base a estos grandes volúmenes de datos debidamente tratados (minería de datos) pueden elaborarse perfiles de usuarios que permiten adoptar decisiones sobre ellos o bien predecir o anticipar sus conductas³. Dichos datos pueden estar en abierto (*open data*), de forma que son puestos a disposición de cualquier persona. Estos datos son almacenados

3. Así, el 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 (Reglamento General de Protección de Datos). En esta norma europea se define la elaboración de perfiles [art. 4.4] como “toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamientos, ubicación o movimientos de dicha persona física”.

en una nube (*cloud computing*), de forma que se permite el acceso a los usuarios, de forma rápida, económica y sencilla, desde cualquier punto en el que se disponga de conexión. La importancia de toda esta información puede ser un elemento relevante para que los gobiernos y las administraciones públicas puedan diseñar adecuadamente sus políticas públicas teniendo en cuenta las necesidades de la población, al mismo tiempo que permite realizar de forma más precisa las mejoras normativas necesarias para llevarlas a cabo.

Por su parte, las redes 5G o de quinta generación de telefonía móvil presentan como principal aspecto el permitir un mayor ancho de banda y una mayor velocidad en la descarga de datos, de forma que permiten una conexión prácticamente en tiempo real. Entre las ventajas que pueden comportar estas redes se encuentra el control remoto de los dispositivos, lo que evita riesgos; así, entre los ejemplos relevantes, encontramos el de la conducción autónoma de vehículos, la telemedicina, la cirugía remota, el control del sistema de alumbrado o de suministro de agua y energía, así como de recogida de residuos, entre otros.

Las tecnologías de inteligencia artificial se refieren a la capacidad de las máquinas de analizar e interpretar datos para aprender de los mismos y emplearlos para fines concretos de forma flexible y en constante evolución. Especial relevancia tiene la aplicación de la inteligencia artificial a los algoritmos, en cuanto conjuntos ordenados y finitos de operaciones que permiten hallar una solución a un problema. La novedad en este ámbito la constituyen los algoritmos predictivos, que permiten anticipar escenarios y situaciones y adoptar decisiones en base a los mismos (Huergo Lora, 2020). La aplicación de la inteligencia artificial permite ir evolucionando y aprendiendo del propio algoritmo con la idea de ir mejorando la búsqueda de soluciones.

El inconveniente que pueden presentar estas tecnologías es su funcionamiento de forma centralizada, produciéndose riesgos de que su control quede en manos de uno o varios intermediarios, o de que se produzca su manipulación, su apropiación, o incluso su desaparición. En este punto, cobran especial relevancia las tecnologías de registro distribuido, entre las que se encuentran las de cadena de bloques (*blockchain*). En el ordenamiento jurídico encontramos definiciones legales de estas tecnologías. Así, la Ley aragonesa 1/2021, de 11 de febrero, de simplificación administrativa, considera que “tendrá la consideración de sistema electrónico de registro distribuido el que permita el almacenamiento de la información, o su representación digital mediante huella electrónica, de manera permanente, simultánea y sucesiva en una base de datos distribuida, de manera que quede garantizada la inmutabilidad

de dicha información y se permita la auditoría de su integridad²⁴. Entre los elementos clave de esta definición encontramos que el almacenamiento de la información es distribuido “de forma permanente, simultánea y sucesiva”, así como la característica esencial de la “inmutabilidad” de la información y la posibilidad de control de su integridad. Este carácter inmutable constituye, como veremos, una de las grandes ventajas que ofrece esta tecnología, de forma que, por una parte, permite sustituir los medios tradicionales de acreditación de determinados hechos y, por otra, implica en este proceso a los usuarios de la red.

La tecnología de cadena de bloques ha venido teniendo un gran desarrollo a partir de las denominadas criptomonedas, siendo la más conocida el bitcóin. Ahora bien, esta tecnología viene refiriéndose a cualquier tipo de transacción sin necesidad de un intermediario, por lo que su potencialidad es inmensa y tiene una proyección amplísima. Se lleva a cabo a través de nodos descentralizados que están encriptados uniéndose mediante un código de unión (*hash*). Se trata, en definitiva, de un inmenso libro de cuentas o anotaciones donde se van registrando los diversos bloques, donde se insertan las transacciones u operaciones, que se distribuyen por toda la red, donde los usuarios lo aprueban y a partir de entonces se añade a una cadena que lo realiza de forma intangible. Existe un tiempo determinado para escribir en un bloque, de forma que, una vez ha finalizado, se cierra, y resulta necesario crear otro bloque que se añade al anterior de forma entrelazada, formando una cadena. En el caso de que se quisiera modificar el bloque, alterando la información, la cadena se fragmentaría.

De esta forma se garantiza su inmodificabilidad, ya que para hacerlo se requeriría una tecnología de unas dimensiones igualmente inmensas. Este gigantesco libro de registros queda al alcance de todos, de forma que dicha operación puede ser verificada de forma descentralizada por los usuarios del sistema en lugar de por una autoridad única centralizada. A ello debe añadirse la denominada tokenización (*tokenization*), que es el proceso que permite proteger los datos sensibles a través de añadir una capa de protección mediante un algoritmo como simple dato o indicador de referencia que permite unir con el dato sensible para su identificación sin exponerlo. Los datos sensibles se

4. La regulación del *blockchain* en esta Ley se basa en la “enmienda ciudadana” presentada por M. Á. Bernal Blay que fue asumida por dos grupos parlamentarios en las Cortes de Aragón. *Vid.* “Aragón regula la primera Identidad Digital Blockchain mundial”, disponible en: <https://www.clubdeinnovacion.es/aragon-identidad-digital-blockchain/>. *Vid.* también el Boletín Oficial de las Cortes de Aragón, X Legislatura, Procedimientos Legislativos, Proyecto de Ley núm. 107, 5 de febrero de 2021, p. 7022, disponible en: [https://www.cortesaragon.es/bases/boca2.nsf/\(BOCAID\)/B408FA6EC16B540AC12586730039D212?OpenDocument](https://www.cortesaragon.es/bases/boca2.nsf/(BOCAID)/B408FA6EC16B540AC12586730039D212?OpenDocument).

convierten así en formato encriptado y aleatorio denominado *tokens*. Así, entre los beneficios que se han destacado de la tecnología de cadena de bloques, se encuentran la transparencia, la inmutabilidad, la descentralización, el anonimato y la privatización.

Como veremos, la aplicación de la tecnología *blockchain* puede permitir, por ejemplo, una mayor seguridad de estos datos. Así, esta tecnología permite almacenar y gestionar los datos de forma descentralizada, de forma que queda en manos de quien genera la información y no en intermediarios. Debe pensarse que una gestión centralizada de estos datos puede resultar más vulnerable, quedando expuestos los datos⁵, así como a delitos como robos o extorsiones⁶. A través de *blockchain* podría también asignarse una identidad digital a cada uno de los ciudadanos, que facilitara su relación con la ciudadanía y ser un mecanismo relevante para su participación. Se ha destacado además la importancia que esta tecnología puede tener para la gestión de la información pública, de forma que se realice de forma segura y transparente⁷.

Las ventajas que puede ofrecer la tecnología de cadena de bloques han llevado a considerar la aplicación de esta tecnología al ámbito de las administraciones públicas y, en general, al sector público, así como específicamente a las ciudades inteligentes. Las características de esta tecnología plantean la sustitución de algunas de las funciones que en la actualidad vienen realizando las administraciones públicas, como puede ser de registro (por ejemplo, de entidades y asociaciones, de vehículos, etc.), de verificación de hechos (pago de impuestos o tasas) y de comprobar el cumplimiento de los requisitos y exigencias establecidos por la normativa jurídica (cumplimiento de la normativa de seguridad; Torregrossa, 2018). Este proceso de sustitución puede generar resistencias en el momento de su aplicación por parte de las organizaciones públicas, basadas en un funcionamiento de tipo burocrático.

Se produce lo que podríamos denominar un ejercicio compartido de funciones públicas. Es decir, los ciudadanos dejan de situarse en una posición

5. Este tipo de problemas se ha suscitado, por ejemplo, con el acceso a la web de la tarjeta de movilidad de la Autoridad del Transporte Metropolitano de Barcelona, donde hubo que cerrar este acceso al quedar expuestos los datos de los usuarios, según la noticia que puede consultarse en la siguiente dirección electrónica: www.lavanguardia.com/local/barcelona/20211007/7773666/cierran-nueva-web-t-mobilitat-grave-agujero-seguridad.amp.html.

6. *Vid.* “Blockchain para mejorar la seguridad de los datos en las ciudades inteligentes”, consultable en la siguiente dirección electrónica: <https://www.eysmunicipales.es/actualidad/blockchain-para-mejorar-la-seguridad-de-los-datos-en-las-ciudades-inteligentes>.

7. Iglesias (2020).

meramente pasiva para convertirse en coadministradores (Arena, 2017: 426). La tecnología de registro compartido permite una participación conjunta de la ciudadanía en la realización de ciertas funciones públicas de registro, prueba, comprobación y verificación de hechos que hasta ahora se consideraban propias y exclusivas de las administraciones públicas. No se trataría tanto de una privatización de estas funciones públicas que pasan de la Administración pública a un particular, sino de una gestión entre todos aquellos que interactúan en la red. Estaríamos, por tanto, ante una compartición de las funciones públicas en el ámbito de la gestión cívica de un bien común que sería la ciudad inteligente.

La metodología a utilizar en este trabajo será partir de la definición de lo que constituye una ciudad inteligente, si se trata de un concepto que puede tener relevancia jurídica, de las principales ventajas y riesgos que comporta⁸. Una vez realizado, se procederá a examinar las ventajas y los riesgos que puede comportar la tecnología de cadena de bloques (*blockchain*) a la ciudad inteligente, así como el marco jurídico que puede dar respuesta a los mismos. En este sentido, cobra especial importancia la creación de un estatuto digital, como conjunto de derechos y deberes, para atribuir a la ciudadanía el papel relevante que está llamada a ocupar en la ciudad inteligente. Ante un marco jurídico que, como veremos, tiene todavía una cierta imprecisión y está en proceso de construcción, cobran asimismo una gran relevancia los principios generales. A continuación, se examinarán la tipología y las características de la tecnología de la cadena de bloques. Ante los diversos sistemas de registro distribuido, las administraciones deberán tomar la decisión de si son adecuados o no para las necesidades que estas tienen, así como cuál de ellos resulta más apropiado. Tal decisión, ampliamente discrecional, deberá basarse en un juicio de proporcionalidad. Seguidamente, veremos cómo incide la tecnología *blockchain* en diversos servicios, como la energía y el medio ambiente, la movilidad, la seguridad y las emergencias, así como la atención a las personas (educación, salud y servicios sociales). Veremos, en definitiva, las posibilidades de participación de la ciudadanía y su implicación en la realización de estas funciones públicas a través de la utilización de esta tecnología.

8. Tal y como se ha destacado, las nuevas tecnologías “no dejan de ser herramientas que deben usarse conociendo muy bien sus potencialidades y limitaciones, y cuya aplicación debe darse siempre acompañada y supeditada a programas de reforma integral” (Serale *et al.*, 2018: 6). También se ha destacado cómo “la mayor parte de la literatura actual se centra en su dimensión tecnológica, o en exaltar y magnificar sus hipotéticos beneficios, sin tratar realmente de valorarlas de forma sistemática o analizar con rigor su implementación o limitaciones” (Vega Maza, 2019: 111).

2. El concepto de ciudad inteligente

2.1. La ciudad inteligente: un concepto holístico

La noción de ciudad como estructura política ha tenido una gran importancia histórica en el pasado. Así, cabe pensar en las *polis* de la Grecia clásica, la relevancia de la idea que se tuvo de *civitas* como comunidad organizada políticamente frente a la noción de *urbs* como mero espacio físico urbano, las ciudades estado medievales como las italianas o las de la Liga Hanseática. Sin embargo, esta noción fue decayendo con el proceso de construcción, durante la época moderna y contemporánea, del Estado basado en la idea de soberanía nacional y en la necesidad de crear unas estructuras de poder centralizadas, para superar la fragmentación de poder existente durante el Antiguo Régimen. La tecnología ha tenido un importante papel en la conformación de las ciudades, primero a través de las revoluciones industriales que propiciaron a partir del siglo XIX el éxodo de las zonas rurales a las grandes conurbaciones actuales y, posteriormente, a través de la revolución digital que ha permitido su aplicación a la nueva realidad urbana. En la actualidad, por tanto, la idea de ciudad vuelve a recuperarse como un espacio fundamental, como centro de decisiones políticas públicas para la prestación de servicios esenciales a la ciudadanía.

En este proceso de evolución debe aludirse a dos fenómenos fundamentales. Por una parte, el hecho de que una gran parte de la población mundial se concentra en determinadas áreas urbanas. Así, se ha calculado que en la actualidad representa la mitad de la población mundial, cifra que es previsible que llegue a incrementarse hasta cerca del setenta por ciento. Ello ha comportado el surgimiento de modelos de ciudad alternativos al clásico del municipio. De esta forma, han aparecido la ciudad por refundición simplificada, que se une con otros niveles superiores (provincia, comunidad autónoma, región, etc.); la ciudad por agregación, en la que se mantiene la estructura propia en el marco de una realidad más compleja como una conurbación urbana (áreas metropolitanas); así como la ciudad de régimen especial (con una regulación legal *ad hoc* debido a la situación de asimetría con otras realidades municipales) (Font i Llovet, 2021: 20).

Por otro lado, debe destacarse que, hacia finales del siglo XX, el fenómeno del desarrollo de las tecnologías de la información y la comunicación propicia una socialización del conocimiento, que tiene también su impacto en las

ciudades. Se trata de una revolución digital que supone un punto de inflexión como lo supuso en su momento la revolución industrial.

En estas coordenadas de una revolución digital en constante evolución surge el concepto de ciudad inteligente, que parte de la utilización en el ámbito urbano de las nuevas tecnologías de la información y comunicación para conseguir objetivos que giran en torno a las ideas de sostenibilidad, eficiencia y participación.

La expresión de ciudad inteligente es una traducción del término anglosajón de *smart city*. Como se ha destacado, el calificativo de “inteligente” no se refiere a una característica de la ciudad en sí misma considerada, sino al hecho de utilizar las tecnologías de la información y la comunicación para afrontar los retos que se plantean en la actualidad (Font i Llovet, 2021: 20-21).

Se trata, como se ha afirmado, de un concepto holístico, en cuanto no se refiere solamente a la incorporación de nuevas tecnologías, sino que pone en el centro del sistema al ciudadano en cuanto sujeto activo que interactúa con los diversos actores políticos, sociales y económicos. Esta idea de implicación, de participación ciudadana, deviene uno de los elementos consustanciales para que una ciudad pueda ser considerada como inteligente (Font i Llovet, 2021: 20-21).

Ahora bien, este concepto denota una cierta ambigüedad e imprecisión. En este sentido, algunas definiciones han puesto el acento en cuestiones como las tecnologías utilizadas; otras se han centrado en el tema de los datos; se ha puesto, en fin, énfasis en las diversas finalidades. Con base en una sistematización de estos criterios diversos se ha definido el concepto de ciudad inteligente como “aquel municipio que utiliza la tecnología de manera intensiva, innovadora y colaborativa para recopilar y analizar los datos de la ciudad con el fin prestar servicios centrados en las personas inclusivos, eficientes, resilientes y sostenibles” (Cerrillo i Martínez, 2020). La ciudad inteligente presenta, en este sentido, diversas facetas que, en su conjunto, ponen de relieve la necesidad de poner la tecnología al servicio de las personas, situándola como un actor que interactúa con los poderes públicos, con la sociedad y el mercado.

Bajo el concepto de ciudad inteligente se han estructurado una serie de ejes o puntos principales: *smart governance*, *smart economy*, *smart mobility*,

*smart environment, smart people y smart living*⁹. La concurrencia de alguno de estos puntos permite, a juicio de la Unión Europea, considerar que nos encontramos ante una ciudad inteligente (Velasco Rico, 2019). La envergadura tecnológica que se requiere para llevar a cabo dichos objetivos comporta que habitualmente se utilicen fórmulas de colaboración público-privada. Ello puede llevar, tal y como se ha puesto de relieve, a una transformación del modelo de gobernanza en la que adquiere una mayor relevancia el peso de las grandes empresas tecnológicas, que están mejor preparadas y tienen grandes recursos a su disposición para utilizar a su favor todas estas ventajas tecnológicas. Sin negar la relevancia de la iniciativa empresarial como motor de desarrollo económico y tecnológico, el marco jurídico debe establecer las normas que permitan una protección jurídica de la ciudadanía y de los intereses generales.

2.2. La relevancia jurídica del concepto de ciudad inteligente

Como hemos visto, sobre el concepto de ciudad inteligente no existe todavía un consenso generalizado, por lo que se trata de un concepto emergente, que viene siendo analizado desde ámbitos científicos muy diversos, como “la Arquitectura, la Ingeniería, las Ciencias Políticas y el Derecho o las Ciencias Empresariales” (Cabezuelo-Lorenzo *et al.*, 2016). Entre los elementos comunes a las diversas definiciones, encontramos “la aplicación de las TIC para mejorar la calidad de vida de sus habitantes y asegurar un desarrollo económico, social y ambiental sostenible”. Como hemos apuntado anteriormente, el rasgo tecnológico no deviene por sí solo el elemento definidor de la ciudad inteligente, sino que el mismo está al servicio del bienestar y de la calidad de vida de la ciudadanía, así como de lograr un desarrollo sostenible, cuya referencia indiscutible vendrá dada por los Objetivos de Desarrollo Sostenible de la Agenda 2030, propiciados por las Naciones Unidas.

Pese a los elementos imprecisos del concepto y su carácter no jurídico, el mismo presenta una cierta utilidad. Así, se ha destacado que permite ampliar los límites del estudio del derecho administrativo, como también acercar esta disciplina al universo de las políticas públicas (Velasco Rico, 2019). También permite examinar la relación entre tecnología y derecho, así como las ventajas y los riesgos de los avances tecnológicos (Aguado i Cudolà, 2018).

9. Se hace referencia a estas características para definir una *smart city* en el Informe de la Dirección General para políticas internas del Parlamento Europeo, de enero de 2014, “Mapping Smart Cities in the EU”.

Las ciudades inteligentes han propiciado una serie de situaciones que adquieren relevancia desde un punto de vista jurídico: mayor intromisión en el ámbito de la privacidad y protección de datos, crecimiento de la brecha digital entre las empresas (entre grandes y pequeñas y medianas) y entre los ciudadanos (entre los adaptados tecnológicamente y los que no lo están), un incremento de la colaboración público-privada (las administraciones deben acudir a las empresas que están preparadas tecnológicamente), prestaciones más seguras, eficientes y económicas, mayor canalización de información y datos, facilidad de participación (Aguado i Cudolà, 2018).

Pese a las innegables repercusiones jurídicas que plantea la configuración de la ciudad inteligente, todavía carecemos de un marco jurídico adecuado para regular esta realidad. La regulación de la compleja realidad de las ciudades inteligentes se contiene, en estos momentos, esencialmente en “normas técnicas de carácter voluntario” (Velasco Rico, 2019). Todo ello pone de relieve la importancia de identificar principios y reglas que permitan dar respuestas a los retos que plantea la ciudad inteligente. Partiendo de esta premisa se considera fundamental realizar una aproximación a la ciudad inteligente desde varias perspectivas fundamentales: la primera, relativa al derecho a la ciudad, en cuanto “derecho de derechos”, que sitúa en el centro del sistema al ciudadano como usuario de los servicios y bienes que la tecnología pone a su disposición de una forma más eficiente, al mismo tiempo que lo hace partícipe de las políticas públicas que han de definir la ciudad inteligente; la segunda sería la identificación de unos principios jurídicos que den cohesión al ordenamiento jurídico ante una realidad que está en constante proceso de evolución y desarrollo propiciado por los avances tecnológicos; y la tercera, referente a un estatuto digital, en cuanto conjunto de derechos y deberes, que garantizan un uso adecuado de la tecnología en el entorno de la ciudad inteligente.

2.3. La ciudad inteligente desde la perspectiva del derecho a la ciudad

El derecho a la ciudad se ha teorizado, especialmente desde el ámbito de la sociología, como un derecho que reivindica el espacio urbano frente a su privatización y mercantilización¹⁰. Desde un punto de vista jurídico, los autores se han referido al mismo como un derecho emergente, especialmente a partir de la Carta Europea de Salvaguarda de los Derechos Humanos en la Ciudad. Se trata, como se ha señalado gráficamente, de un “derecho de derechos”.

10. Lefebvre (2017).

Así, de acuerdo con J.-B. Auby, el derecho a la ciudad haría referencia a los asuntos y mecanismos jurídicos en torno a cuatro problemas: los espacios públicos; las infraestructuras y los servicios públicos; la regulación del uso de los suelos, y el gobierno urbano¹¹.

Entre los derechos que prevé esta Carta se reconoce el de “acceder libremente a los servicios municipales de interés general”, afirmándose para ello que “las ciudades signatarias se oponen a la comercialización de los servicios personales de ayuda social y velan para que existan servicios fundamentales de calidad a precios aceptables en otros sectores de los servicios públicos”. Por su parte, en la misma Carta, entre los derechos relativos a la Administración democrática local, se alude específicamente a la eficacia de los servicios públicos (art. XXIII), estableciéndose que “las autoridades locales aseguran la eficacia de los servicios públicos y su adaptación a las necesidades de los usuarios y velan para evitar cualquier situación de discriminación o de abuso”. Asimismo, encontramos el mandato de que “las administraciones locales se dotarán de instrumentos de evaluación de su acción municipal y tendrán en cuenta los resultados de dicha evaluación”. Pese a que este derecho no tiene un reconocimiento jurídico explícito, resulta un referente relevante en las regulaciones que atañen a las entidades locales.

En el ámbito de las infraestructuras y los servicios públicos, como señala J.-B. Auby, se producen en el ámbito urbano o de la ciudad una serie de características singulares como una densidad particular, una interconexión, ciertos servicios públicos están presentes de forma más abundante, algunos son exclusivos de las ciudades, la libertad de comercio e industria propicia unos servicios públicos de carácter económico.

Desde la tesis que defendemos en este trabajo, el concepto de ciudad inteligente debe enfocarse desde la perspectiva del derecho a la ciudad, de forma que ponga en el centro del sistema el bienestar de la ciudadanía y el acceso a los bienes comunes que se encuentran en la ciudad de forma más eficiente y sostenible, mediante el uso de las tecnologías de la información y la comunicación. Como se ha destacado, la tecnología en sí misma no deviene la finalidad de la ciudad inteligente, como tampoco la gestión, en la que habitualmente se acude a fórmulas de externalización. Si bien es importante avanzar en la innovación y fomentar el desarrollo tecnológico a través de iniciativas empresariales, no puede perderse de vista que ello debe orientarse

11. Auby (2018).

a asegurar este derecho a la ciudad. En esta línea, las propias características de la tecnología de cadena de bloques, tal y como veremos, pueden contribuir a una mayor transparencia, seguridad y trazabilidad mediante un proceso de descentralización. Ello no obsta a que también tenga sus riesgos, que deberán ser objeto de regulación para evitar usos indeseados de los avances tecnológicos.

2.4. Los servicios de interés general en la ciudad inteligente: panorámica general

2.4.1. Principios generales

Los servicios públicos han venido ocupando un papel central en la construcción del derecho administrativo desde que los autores franceses de principios del siglo XX establecieron los mimbres doctrinales, en base a la jurisprudencia del Consejo de Estado francés, extendiéndose a los países basados en el sistema de régimen administrativo con sus propias adaptaciones y peculiaridades. Para dar coherencia al sistema, ante la diversidad de regímenes jurídicos de los servicios públicos, se identificaron unos principios comunes, denominados leyes de Rolland. Estos principios serían el de igualdad, el de continuidad o regularidad, así como el de adaptación constante o mutabilidad del progreso técnico. A ello se añade la superposición de la noción de servicios de interés general, acuñada por la Unión Europea, con el objetivo de establecer una noción funcional que permitiera la aplicación del derecho europeo a sistemas con diversos regímenes jurídicos. Se trata, en definitiva, de una noción que permite establecer obligaciones de servicio público, así como derechos exclusivos a determinadas actividades que se consideran esenciales para la ciudadanía y que como tales deben garantizar las administraciones públicas, estableciendo excepciones y limitaciones a las reglas de la competencia.

La construcción jurídica de los servicios públicos realizada durante el siglo XX debe adaptarse a una nueva realidad. En este contexto, como hemos visto, la ciudad adquiere una relevancia fundamental en cuanto que estructura política que ha de gestionar áreas con una gran concentración de población, lo que exige unos servicios públicos eficientes. Por otra parte, el desarrollo exponencial de las nuevas tecnologías comporta un cambio en el funcionamiento de estos servicios que requiere una adaptación de los principios y las reglas tradicionales.

El principio de igualdad en el acceso a los servicios públicos adquiere una relevancia fundamental, en cuanto la irrupción de las nuevas tecnologías puede provocar un aumento de las desigualdades sociales¹². En este entorno digital resultará fundamental la caracterización del acceso a la tecnología como un derecho fundamental, en cuanto esta supondrá la puerta de entrada a los servicios públicos. Así, algunos autores vienen considerando internet como un bien común, y que el acceso al mismo debería ser reconocido como un derecho fundamental (m4Social, 2021).

También debe hacerse especial mención a la aparición de nuevos tipos de discriminación, como puede ser la denominada discriminación algorítmica, producida por los sesgos algorítmicos (*algorithmic bias*). La aplicación de operaciones algorítmicas a la toma de decisiones sobre los servicios públicos presenta unas nuevas características. Esta novedad no afecta tanto a los motivos o las circunstancias que dan lugar a la discriminación, cuanto a que la misma puede producirse a través de unos entornos más opacos y menos transparentes, basados en decisiones automatizadas y con empleo de las técnicas de la inteligencia artificial. Por ello, resulta fundamental acceder al código fuente, si bien garantizando la seguridad del sistema¹³. A efectos de aplicar las garantías del procedimiento de elaboración de las normas, algunos autores han defendido que los algoritmos son reglamentos (Boix Palop, 2020a), al argumentar que están realizando una función equivalente a las normas jurídicas. Otros autores (Huerco Lora, 2020) sostienen, en cambio, que las funciones de los algoritmos varían en función de su ámbito de actuación, por lo que no puede hablarse propiamente de una única naturaleza. A mi entender, el algoritmo es, sin lugar a dudas, un instrumento que posibilita la adopción de decisiones de forma automatizada que pueden adquirir relevancia jurídica. En ocasiones, pueden llegar a tener valor normativo; por ejemplo, cuando establecen los criterios o condiciones con base en los que debe otorgarse el bono social; pero en otros casos constituirán meras decisiones de aplicación del ordenamiento jurídico, como cuando se toma la decisión de otorgar o denegar en concreto este beneficio social.

Por lo que se refiere al principio de continuidad o regularidad, el mismo comporta que el servicio se preste ya sea de forma seguida o bien con una

12. *Vid.* “Cómo los algoritmos perpetúan la desigualdad en España. Inteligencia artificial versus derechos humanos”. Disponible en: <https://www.lavanguardia.com/tecnologia/20211026/7814332/como-algoritmos-perpetuan-desigualdad-espana.html>.

13. De especial interés es el litigio mantenido por la Fundación CIVIO contra la Administración General del Estado con relación al acceso al código fuente del algoritmo del bono social. La documentación esencial de este proceso puede consultarse en la siguiente dirección electrónica: <https://civio.es/acceso-a-bono-social/>.

frecuencia regular. El uso de la tecnología puede ser un factor para garantizar esta prestación continuada, así como para realizar un seguimiento o una trazabilidad de cómo ha venido prestándose dicho servicio. No solo resultará importante que el servicio se preste de esta forma continuada, sino también la verificación de que se esté prestando a lo largo del tiempo con un determinado nivel de calidad, dentro de unos márgenes aceptables, de forma que no se produzca una devaluación o degradación del mismo.

También se plantea la aplicación del principio de mutabilidad o adaptación al progreso técnico, regla que se encuentra incorporada en la regulación de las concesiones (art. 159.4 de la Ley 9/2017, de contratos del sector público, según el cual: “El concesionario deberá mantener las obras de conformidad con lo que, en cada momento y según el progreso de la ciencia, disponga la normativa técnica, medioambiental, de accesibilidad y eliminación de barreras y de seguridad de los usuarios que resulte de aplicación”). También con una función distinta debe aludirse a cómo el desarrollo tecnológico puede llegar a ser una causa de exención de responsabilidad de la Administración por el funcionamiento de los servicios públicos.

2.4.2. Derechos de los usuarios

El hecho de que la noción de ciudad inteligente ponga en el centro del sistema a los ciudadanos pone de relieve la importancia de un estatuto digital, en cuanto conjunto de derechos y deberes. De una parte, este estatuto digital debe tender a hacer efectiva la participación en la ciudad inteligente, de forma que permita hacer partícipe al ciudadano en la utilización de la tecnología, a fin de que pueda interrelacionarse de forma más eficiente con la Administración, así como hacerle partícipe en la toma de decisiones e incluso, como hemos visto, en el ejercicio de determinadas funciones públicas. Por otra parte, este estatuto digital debe erigirse en un mecanismo de protección efectiva de la ciudadanía frente a los riesgos que puede generar la tecnología en la ciudad inteligente, evitando su utilización sesgada, discriminatoria, o en general que atente contra los derechos que tiene reconocidos.

Por lo que se refiere a los principales derechos que tiene la ciudadanía en sus relaciones con la administración pública electrónica, debemos acudir a la Ley 39/2015, de 1 de octubre, de procedimiento administrativo. Entre el elenco de derechos que allí se relacionan, se hace mención específica del derecho de las personas a comunicarse con las administraciones públicas a través de

un punto de acceso general electrónico de la Administración, así como del derecho a ser asistidas en el uso de medios electrónicos en sus relaciones con las administraciones públicas [art. 13.a) y b)]. Además, también se regulan específicamente el derecho y la obligación de relacionarse electrónicamente con las administraciones públicas (art. 14). Así, se establece como regla general que las personas puedan relacionarse de forma electrónica con carácter voluntario, estableciendo la obligación para determinados sujetos y habilitando al reglamento para extenderla a “ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios”.

A este respecto, se plantea la cuestión relativa a en qué medida este derecho podría alcanzar a la utilización de una determinada tecnología en su relación con las administraciones públicas. El derecho habla -sin especificar- de “medios electrónicos en sus relaciones con las administraciones públicas”. Para hacer efectivo este derecho, uno de los principios que establece la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, es el de interoperabilidad (arts. 3.2, 38, 45, 156, 157 y 158, y disposición adicional novena). Como veremos posteriormente, la legislación de procedimiento administrativo común ha establecido trabas a la implantación de las tecnologías de registro distribuido en las relaciones de la Administración con la ciudadanía, a la espera de una regulación europea. En todo caso, la implantación de esta tecnología deberá partir de una ponderación de los derechos e intereses implicados y considerar los riesgos que puedan llegar a producirse.

Desde la perspectiva de la protección de datos encontramos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Entre los derechos propios de este ámbito encontramos el derecho de acceso (art. 13), el derecho de rectificación (art. 14), el derecho de supresión (art. 15), el derecho a la limitación del tratamiento (art. 16), el derecho a la portabilidad (art. 17) y el derecho de oposición (art. 18). Hay que añadir el Título X de esta Ley, titulado “Garantía de los derechos digitales”. En el entorno de internet se incluyen también el derecho a la neutralidad de la red y acceso universal, los derechos a la seguridad y educación digital, el derecho al olvido, a la portabilidad y al tratamiento digital, la desconexión digital, así como la protección de menores. Asimismo, también deben tenerse presentes la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación.

Ahora bien, la aplicación de todos estos derechos plantea especificidades e incluso situaciones paradójicas según el entorno tecnológico de que se trate. Así, en el caso de la tecnología de cadena de bloques sus propias características intrínsecas de inmutabilidad, descentralización y transmisibilidad suponen importantes retos desde la perspectiva de los derechos de acceso, rectificación, oposición, así como del de olvido, cuestiones que tratan, en esta misma obra, los profesores Andrés Boix y Manuel Pereiro.

Para dar soluciones a estos retos, algunos autores han planteado la sustitución de la cancelación de datos por una imposibilidad de uso, a través de mecanismos de encriptación que se ejecutan con carácter automático por medio de *smart contracts* (Sebastián Cermeño, 2016).

Entre las iniciativas en el proceso de reconocimiento de este estatuto, debe aludirse a la Carta de Derechos Digitales elaborada por el Grupo asesor de Expertas y Expertos constituido por la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital del Gobierno de España. Dicha Carta “no tiene carácter normativo, sino que su objetivo es reconocer los novísimos retos de aplicación e interpretación que la adaptación de los derechos al entorno digital plantea, así como sugerir principios y políticas referidas a ellos en el citado contexto”.

Ahora bien, el debate científico no puede partir exclusivamente de la perspectiva de la protección de datos (Huergo Lora, 2020). Por tanto, el estatuto digital del ciudadano, si bien incorpora estos derechos, debe también configurarse desde otros ámbitos, de forma que permita hacer efectiva la participación del ciudadano en los servicios de la ciudad digital, así como su posición de usuario de los mismos cuando interactúa con las administraciones públicas a través de medios digitales.

3. La aplicación de la tecnología de cadena de bloques a la ciudad inteligente

3.1. La tecnología de cadena de bloques: tipología

La tecnología de cadena de bloques (*blockchain*) es una de las tecnologías de registro distribuido (*distributed ledger technology* o, en su acrónimo en inglés, *DLT*), también denominadas de registro compartido. El desarrollo ini-

cial de esta tecnología ha ido vinculado fundamentalmente a las transacciones con criptomoneda, especialmente a partir de la crisis y colapso del año 2008, que generó una gran desconfianza en el sistema financiero (Alonso Suárez, 2021: 108), por lo que se ideó un mecanismo alternativo que prescindía de los intermediarios. Ahora bien, como veremos en los apartados siguientes, esta tecnología no se limita a este ámbito, sino que tiene también una gran potencialidad en el ámbito del sector público.

En el avance de *blockchain* han tenido una especial relevancia los *smart contracts*. Se trata de aplicaciones que no se limitan al registro de transacciones, sino que permiten ejecutarse cuando se dan determinadas condiciones previstas de antemano en la cadena de bloques. Pese a su denominación no se trata propiamente de un contrato, sino de un programa autoejecutable que forma parte del mismo. La ventaja de estas aplicaciones es que el consentimiento de las partes se ha producido anteriormente, limitándose a hacer efectivas las disposiciones previstas en el contrato cuando se verifica automáticamente que han concurrido unas determinadas condiciones. En el ámbito de las administraciones públicas los *smarts contracts* podrían posibilitar las decisiones automatizadas, que encontrarían cobertura en el artículo 41 de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público (Quintana Cortés, 2020: 160-162).

Existen diversos tipos de cadenas de bloques. Esta tipología dependerá de cómo se haya configurado su arquitectura, dando permisos a los usuarios para unirse, leer o añadir bloques. La división fundamental entre cadenas de bloques está, por una parte, en si son públicas o privadas; así como, por otra parte, si son permissionadas o no. Si la cadena se configura de forma pública ello quiere decir que cualquier persona con la capacidad tecnológica necesaria puede unirse y leer los bloques. Si además de pública es no permissionada cualquier persona puede agregar bloques, mientras que si es permissionada solo pueden agregar bloques los participantes autorizados. En cambio, si la arquitectura es privada únicamente los usuarios autorizados pueden unirse y leer. Si la red es privada no permissionada los usuarios autorizados también pueden agregar bloques, mientras que si es permissionada solamente el operador puede hacerlo.

Como se ha advertido, las administraciones públicas preferirán las redes privadas para ejercer un control respecto a las validaciones y los registros (Quintana Cortés, 2020: 159). Debe tenerse en cuenta, como se ha advertido, que los “sistemas regulatorios están diseñados para mantenerlos cerrados y centralizados” (Alonso Suárez, 2021: 110).

Para la implantación de esta tecnología, la Administración deberá evaluar “si la solución adoptada es la más adecuada o, por el contrario introduce riesgos que no permitan ser gestionados” (Agencia Española de Protección de Datos, 2020: 48). Tanto para establecer la tecnología de bloques como para escoger una tipología concreta de red, las administraciones dispondrán de un margen de apreciación, en el que deberán tener en cuenta el estatuto digital de la ciudadanía, así como justificar que su decisión cumple el test de proporcionalidad, ponderando las ventajas y los riesgos desde la perspectiva de la satisfacción del interés general y de la garantía de los derechos.

3.2. La regulación de la tecnología de cadena de bloques en el ámbito de las administraciones públicas

La implantación de esta tecnología requiere una regulación adecuada, que posibilite su implantación con las debidas garantías. Como veremos, su marco jurídico está en una situación embrionaria. Por ello, se ha destacado que “su desarrollo y posterior consolidación se ven obstaculizados por la mala publicidad y las trabas regulatorias” (Alonso Suárez, 2021: 110).

En el ámbito de la Unión Europea encontramos el Reglamento (UE) n.º 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 el que se deroga la Directiva 1999/93/CE (conocido como Reglamento eIDAS). Este Reglamento parte de la necesidad de establecer niveles de seguridad para asegurar un buen funcionamiento del mercado interior. Para ello, regula tres aspectos fundamentales: a) establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro; b) establece normas para los servicios de confianza, en particular para las transacciones electrónicas, y c) establece un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

Debe destacarse cómo este Reglamento europeo distingue entre “sistema de identificación electrónica”, que es un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica

a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica, y la “autenticación”, que constituye un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico. Esta distinción, según ha apuntado acertadamente Bernal Blay¹⁴, es relevante por cuanto, como veremos a continuación, permite dar un margen de regulación a las comunidades autónomas que sea respetuoso con la legislación establecida por el Estado español.

El Reglamento eIDAS, que es de aplicación directa en los Estados miembros, está en proceso de revisión por una iniciativa de la Comisión Europea para una identidad digital europea de forma que los ciudadanos puedan a través de sus carteras digitales acceder a diversos tipos de servicios sin necesidad de facilitar en todo momentos sus datos. Se trata, por tanto, de instrumentar un mecanismo de identificación que podría ser expedido por entidades públicas y privadas y que permita actuar por toda Europa otorgando un mayor control a la ciudadanía sobre sus propios datos personales.

En 2018 los Estados miembros de la UE y Noruega crearon la Asociación Europea de Blockchain (*European Blockchain Services Infrastructures* o *EBSI* en su acrónimo en inglés). Esta asociación trabaja en cuatro grandes proyectos o estrategias como son: la identidad digital autosoberana, el registro de las titulaciones universitarias, documentos de auditoría digitales y el intercambio o uso compartido de datos fiables.

En el ámbito concreto del Estado español la regulación del *blockchain* ha encontrado resistencias debido a una posición quizás excesivamente cautelosa, que se basa en el aplazamiento de la toma de decisiones hasta que exista un marco jurídico europeo. Esta posición se ha justificado en la Estrategia sobre Seguridad Nacional 2017, que mencionaba entre los riesgos actuales las ciberamenazas y el espionaje. En concreto, se advierte que la hiperconectividad ha comportado la exposición a determinadas actuaciones delictivas como el robo de datos e información, el *hackeo* de dispositivos móviles y sistemas industriales, o los ciberataques contra infraestructuras críticas. Entre las actuaciones prioritarias que se preveían para hacerles frente se encuentra la ciberseguridad.

14. *Vid.* la referencia que hemos mencionado anteriormente en la siguiente dirección electrónica: [https://www.cortesaragon.es/bases/boca2.nsf/\(BOCAID\)/B408FA6EC16B540AC12586730039D212?OpenDocument](https://www.cortesaragon.es/bases/boca2.nsf/(BOCAID)/B408FA6EC16B540AC12586730039D212?OpenDocument).

En este contexto, el Gobierno aprobó el Real Decreto-ley 14/2019, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Entre las medidas más polémicas que prevé esta norma con rango de ley encontramos fundamentalmente tres: a) el DNI electrónico como medio exclusivo y excluyente para acreditar la identidad digital de la ciudadanía; b) las restricciones de bases de datos y la prohibición de almacenar digitalmente en nubes de servidores alojados en terceros Estados respecto a la Unión Europea; y c) la prohibición transitoria de utilización de las tecnologías de registro compartido. Dichas medidas se han considerado inconstitucionales¹⁵, entre otras razones, por cuanto suponen una limitación injustificada de la potestad de autoorganización de las comunidades autónomas en base a una extralimitación de los títulos competenciales del Estado sobre bases del régimen jurídico de las administraciones públicas y el procedimiento común (art. 149.1.18 CE), así como sobre seguridad pública (art. 149.1.29 CE).

En el ámbito concreto de las tecnologías de registro distribuido, entre las que se encuentra la de cadena de bloques, se prevé la modificación de la LPAC para regular la aplicación de las tecnologías de registro distribuido en las relaciones de la Administración y la ciudadanía. Esta regulación se justifica en el Preámbulo de dicho Real Decreto-ley de la siguiente forma:

“Las restricciones impuestas a los sistemas de identificaciones y firmas basados en tecnologías de registro distribuido en ningún caso suponen una prohibición general. Simplemente, se restringe puntualmente y de forma meramente provisional su uso como sistema de identificación y firma de los interesados cuando estos últimos se interrelacionan con la Administración y mientras no haya más datos o un marco regulatorio *ad hoc* de carácter estatal o europeo que haga frente a las debilidades que implica su uso para los datos y la seguridad pública. La falta de un marco regulatorio *ad hoc* sobre estas nuevas tecnologías justifica que, con carácter urgente y en ejercicio de su competencia para dictar legislación básica, el Estado intervenga sobre la materia con carácter provisional hasta que se avance en el seno de la Unión Europea en el tratamiento de este tipo de tecnologías”.

15. En este sentido pueden mencionarse los recursos de inconstitucionalidad promovidos por el Gobierno de la Generalitat de Cataluña (718-2020) y por el Gobierno vasco (1220-2021), así como Cotino Hueso (2020) y Boix Palop (2020b).

En la parte dispositiva de esta norma se introduce una “Disposición adicional sexta. Sistemas de identificación y firma previstos en los artículos 9.2 c) y 10.2 c)”, con la siguiente redacción:

“1. No obstante lo dispuesto en los artículos 9.2 c) y 10.2 c) de la presente Ley, en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del derecho de la Unión Europea.

2. En todo caso, cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal a que hace referencia el apartado anterior deberá contemplar asimismo que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública”.

Se trata, como podemos ver, de una regulación transitoria que prohíbe los sistemas de identificación y de firma basados en las tecnologías de registro distribuido. Dicha prohibición se levantará cuando se realice una regulación por parte del Estado en el marco de una normativa de la Unión Europea. Se prevé, asimismo, el papel de la Administración General del Estado como “autoridad intermedia”. Ahora bien, este carácter transitorio afecta a dos elementos fundamentales de la cadena de bloques, como son la identificación de la ciudadanía y la firma digital. Asimismo, la imposición de la intermediación preceptiva de la Administración General del Estado diluye una de las ventajas que presentan estas tecnologías: la eliminación de la figura del intermediario y su sustitución por la distribución característica de la cadena de bloques.

Pese a este marco normativo, encontramos diversas normas autonómicas que han procedido a regular el uso de la tecnología de registro distribuido, si bien utilizando cláusulas de salvaguarda para evitar su incompatibilidad con la LPAC, sometiéndola a su régimen de prohibición transitorio. En este sentido, podemos hacer referencia en Cataluña al Decreto 76/2020, de 4 de agosto, de administración digital (art. 55.3), según el cual: “La identificación de las personas físicas se puede realizar mediante los sistemas establecidos en las oficinas de asistencia en materia de registro y otros sistemas basados en un registro distribuido de identidades”. Si bien se precisa en la disposición

adicional decimosexta que: “La identificación de las personas físicas se puede realizar mediante sistemas basados en un registro distribuido de identidades, de acuerdo con la disposición adicional sexta de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas”.

En el caso de Aragón debe destacarse la mencionada Ley 1/2021, de 11 de febrero, de simplificación administrativa. Así, en la Ley aragonesa se distingue entre los sistemas de identificación y firma en la sede electrónica y sedes asociadas (plataforma de identificación y firma de los usuarios Cl@ve, plataforma de identificación y firma electrónica utilizada por la Administración General del Estado, o un sistema equivalente), y la utilización de los registros distribuidos. Según esta Ley, “podrán utilizarse sistemas electrónicos de registro distribuido para asegurar la aportación, acreditación e integridad de los datos y documentos en cualquier expediente, procedimiento o registro, sin perjuicio de lo establecido en el artículo anterior respecto de identificación y firma”. Asimismo, se prevé que “podrán también utilizarse sistemas electrónicos de registro distribuido, con plena validez legal, para la realización de tramitación administrativa automatizada conforme a la normativa básica estatal y, en particular, en cualesquiera procedimientos de contratación pública”. Dicha distinción puede abrir posibilidades, si bien de momento limitadas, a la legislación autonómica.

La Agencia Española de Normalización (UNE, acrónimo de Una Norma Española), a través del Comité Técnico de Normalización 71/SC 307, ha elaborado la “Norma UNE 71307-1:2020. Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre Blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de referencia”, de 11 de enero de 2021¹⁶. Esta norma técnica establece, por vez primera, un marco de referencia para que los usuarios puedan crear, sin intermediarios ni autoridades centralizadas, una identidad digital autogestionada. Dichas reglas surgidas de la autorregulación tienen carácter voluntario y no vinculante jurídicamente (Tarrés Vives, 2003), pero pueden constituir un elemento fundamental de referencia para la implementación de esta tecnología en el ámbito de las administraciones públicas.

16. Puede adquirirse el texto completo o consultarse un extracto de esta norma en abierto en la siguiente dirección electrónica: <https://tienda.aenor.com/norma-une-71307-1-2020-n0064986>.

3.3. Ventajas y riesgos de la tecnología de cadena de bloques en la ciudad inteligente: ¿una mayor eficiencia, sostenibilidad y seguridad en las transacciones?

3.3.1. Transparencia

Entre las ventajas que se han dado de la tecnología de cadena de bloques debemos aludir a la transparencia. El hecho de que en las redes públicas pueda unirse y leer los bloques cualquier usuario con capacidad tecnológica posibilita acceder a la información que se ha escrito en los bloques encadenados. En las redes privadas este acceso, y por tanto esta transparencia, se limitará a las personas autorizadas a acceder a la red. En el caso de que las administraciones públicas opten por redes de carácter privado para la implantación de la tecnología *blockchain*, deberán establecer un marco adecuado con criterios objetivos para que los usuarios puedan acceder a las mismas en condiciones de igualdad.

El marco legal de la transparencia viene configurado por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. En esta Ley se prevé de una parte la publicidad activa, en base a la cual los sujetos obligados deben poner a disposición de la persona una serie de informaciones sin esperar a una petición; y de otra, se regula el acceso a la información por parte de la ciudadanía. En la Ley se detalla el tipo de documentos e información que debe proporcionarse, como contratos, convenios, subvenciones, presupuestos, cuentas anuales, retribuciones percibidas por altos cargos y responsables de entidades públicas, autorizaciones de compatibilidad de empleados públicos, declaraciones anuales de bienes y actividades de los representantes locales, así como información estadística.

Por mucho que esté abierta al público, esta información no incluye la relativa a los procesos de toma de decisiones o a su posterior cumplimiento (así, por ejemplo, en relación con el cumplimiento del contrato, de la ejecución de la subvención, etc.). En este sentido, se ha destacado que no es lo mismo la transparencia de la información que la transparencia de los procesos de gobierno (Jolíás, 2017: 2).

También debe aludirse a la Ley 37/2007, de 16 de noviembre, sobre reutilización de información del sector público. Esta Ley define la reutilización

como “el uso de documentos que obran en poder de las administraciones y organismos del sector público, por personas físicas o jurídicas, con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública”.

La ventaja que puede aportar la cadena de bloques es la trazabilidad o el seguimiento de los procesos, de forma que no se contemple únicamente el acceso a la información de documentos, sino que se pueda igualmente enlazarlos en el marco de un proceso.

3.3.2. Comunicación sin intermediación

Una de las grandes ventajas de la tecnología de cadenas de bloques, especialmente en las cadenas públicas no permissionadas, es que la comunicación se realiza sin intermediarios. En el ámbito de los mercados un papel relevante lo han venido ocupando las entidades bancarias, que han sido sometidas a un fuerte control administrativo, para garantizar la estabilidad del sistema financiero y la confianza de los inversores. La irrupción de las tecnologías de registro distribuido puede agitar las tranquilas aguas en que se han venido moviendo las entidades bancarias. Así, esta tecnología puede evitar determinados riesgos que ahora se producen con el robo de las tarjetas bancarias o con fraudes en que se suplanta al tercero intermediario de confianza (*fishing*).

Por su parte, en el sector público, las administraciones públicas han venido a situarse en la posición de intermediario, que se ha venido justificando en su posición al servicio de los intereses generales y de sujeción a la legalidad. Como hemos visto anteriormente, la legislación ha atribuido por razones de seguridad pública la condición de “autoridad intermedia” a la Administración General del Estado en cualquier sistema de identificación basado en tecnología de registro distribuido.

Las características propias de esta tecnología que tiene carácter distribuido comportan una dificultad de identificación de responsabilidades en el caso de que se produzca un tratamiento de datos de carácter personal (Agencia Española de Protección de Datos, 2020: 45). Se deberá, por tanto, valorar y justificar adecuadamente si esta dificultad comporta un incumplimiento de la normativa de protección de datos o bien si existen medios de determinación de esta figura que posibilitan esta implantación.

3.3.3. Integridad y no manipulación de los datos

El hecho de que *blockchain* se base en una gestión descentralizada comporta que el libro de registros en que consiste se encuentre a disposición de los usuarios de la red y no de una autoridad centralizada. La distribución de los datos entre estos comporta que no puedan ser objeto de manipulación. En efecto, los datos gestionados a través de una autoridad centralizada en el caso de un ciberataque podrían llegar a ser manipulados, borrados o robados. En cambio, si dichos datos obran encriptados en los usuarios de la red estos pueden acreditar dicha transacción. No es una única entidad quien puede acreditarlo, sino todos los usuarios de esa red.

La característica de la integridad que puede proporcionar la tecnología de cadena de bloques puede resultar de gran relevancia para la realización de funciones de acreditación del cumplimiento de determinados requisitos establecidos por la normativa.

3.3.4. Inclusión de las personas

El funcionamiento descentralizado de la cadena de bloques puede facilitar una mayor inclusión de las personas tanto desde una perspectiva de cohesión territorial como desde una perspectiva de cohesión social. En el primer aspecto, hemos señalado cómo uno de los fenómenos que han potenciado el fenómeno de la ciudad es el de las grandes concentraciones o aglomeraciones urbanas. Este fenómeno ha producido una distribución desigual en el territorio de forma que otras zonas quedan prácticamente despobladas o con una muy baja densidad de población, en lo que se conoce como la España vaciada. El hecho de establecer una gestión descentralizada de las redes permite sustituir determinadas actuaciones de las administraciones públicas, con lo que no resultará necesario desplazarse hacia las grandes áreas urbanas para poder ser usuarios de determinados servicios. En cualquier caso, la efectividad de ello dependerá de asegurar una adecuada conectividad, así como sensores y dispositivos que están desplegados por todo el territorio, garantizando su trazabilidad y seguimiento a través de la tecnología de cadena de bloques. Desde un punto de vista de cohesión social, cobra relevancia la aplicación de los principios de igualdad, así como de garantizar que la diversidad de perfiles no sea objeto de discriminación.

3.4. La aplicación de la tecnología de cadena de bloques a los diferentes tipos de servicios en la ciudad inteligente

3.4.1. Energía y medio ambiente

En el ámbito de la ciudad inteligente encontramos servicios municipales de tipo básico como el alumbrado público, el suministro de agua o el saneamiento, que son de competencia local. Entre los diversos proyectos de *smart cities* encontramos cómo se han centrado en la prestación más eficiente de muchos de estos servicios que enumera la LRBRL. Así, por ejemplo, podemos destacar el alumbrado público¹⁷ a través de diversos dispositivos que favorecen el ahorro energético, o bien la recogida de residuos, que permite detectar cuándo un contenedor de basuras está lleno.

La tecnología *blockchain* puede acreditar el origen de la energía a través de su trazabilidad¹⁸. Así, por ejemplo, cuando necesitamos verificar

17. Entre las ventajas que las TIC pueden comportar para la gestión del alumbrado público se ha destacado que permiten “la reducción de costes de mantenimiento, posibilitando la verificación en tiempo real de consumos, anomalías y alertas, y reduciendo los tiempos de detección y corrección de averías (...) Así, una adecuada telegestión del alumbrado público en tiempo real, permite identificar fallos en encendidos y apagados, además de evitar encendidos y apagados imprevistos o no deseados, asegurándonos en cada instante de que hay un compromiso entre la calidad en el servicio y el coste del mismo” (Doncel y Ezcurra, 2015).

18. En la Resolución del Parlamento Europeo, de 3 de octubre de 2018, sobre las tecnologías de registros distribuidos y las cadenas de bloques: fomentar la confianza con la desintermediación (2017/2772(RSP)), se tratan específicamente la energía y las aplicaciones respetuosas del medio ambiente. En este sentido, se señalan los siguientes puntos:

“4. Destaca que la TRD puede transformar y democratizar los mercados de energía al permitir a los hogares producir energía respetuosa del medio ambiente e intercambiarla unos con otros; destaca que estas tecnologías ofrecen escalabilidad y flexibilidad a operadores de centrales, proveedores y consumidores;

5. Subraya que la TRD puede apoyar la producción y consumo de energía verde y podría mejorar la eficiencia de los intercambios de energía; señala que la TRD puede transformar el funcionamiento de la red y permitir a las comunidades y personas ofrecer servicios de red así como integrar recursos renovables de forma más eficiente; hace hincapié asimismo en que la TRD puede crear alternativas a los programas de inversión en energías renovables patrocinados por el Estado;

6. Señala que la TRD puede facilitar las infraestructuras de transmisión y distribución de energía y crear un nuevo ecosistema de transacciones en torno a los vehículos eléctricos; destaca que la TRD mejora la presentación de informes en materia de energía y permite un seguimiento preciso de los certificados de energía renovable o de carbono;

7. Destaca que la TRD puede apoyar la electrificación de comunidades rurales pobres mediante pagos alternativos y mecanismos de donación;

8. Subraya la necesidad de fomentar soluciones técnicas que consuman la menor energía posible y que sean, en general, tan respetuosas del medio ambiente como sea posible; destaca que varios mecanismos de consenso, como ‘prueba de trabajo’, ‘prueba de participación’, ‘prueba de autoridad’, ‘prueba de tiempo transcurrido’, entre otros,

que dicha energía es de origen renovable¹⁹. En el ámbito específico del medio ambiente se han desarrollado sistemas de control del aire, exigidos por la legislación medioambiental, a través de la tecnología de registro distribuido. Así, a través de la introducción de esta tecnología en este proceso de control, se puede “probar la confiabilidad de los datos, monitorear las fechas de los certificados de calibración del equipo y el reporte de datos”²⁰.

La tecnología de cadena de bloques puede aplicarse a la recogida de residuos²¹. De esta forma, esta tecnología permite, por ejemplo, conocer todo el proceso por el que pasa un envase de plástico, a través de su identificación con un código QR. El objetivo deviene la reducción de los residuos de envases de plástico y su recuperación para ser reutilizados.

3.4.2. Movilidad

La movilidad se ha convertido en uno de los retos importantes en el ámbito de la ciudad inteligente, en la cual la utilización de tecnologías de registro distribuido puede comportar aportaciones de interés²². Se plantea la necesidad de gestionar los desplazamientos masivos de personas que se trasladan diariamente desde su domicilio al lugar de trabajo, bien a acompañar a los hijos

tienen necesidades diferentes de consumo de energía; pide a la Comisión que añada una dimensión de eficiencia energética en todas sus actividades relacionadas con la TRD y que explore mediante iniciativas de investigación el impacto energético y la eficiencia energética de los distintos mecanismos de consenso;

9. Pide una evaluación de los modelos de gobernanza dentro de los distintos mecanismos de consenso en desarrollo, teniendo en cuenta las necesidades potenciales de sistemas, actores y organizaciones intermediarios para validar y verificar la autenticidad de los intercambios y evitar a tiempo comportamientos fraudulentos;

10. Destaca que la TRD puede ofrecer nuevas oportunidades a la economía circular por incentivar el reciclaje y permitir sistemas de confianza y reputación en tiempo real”.

19. *Vid.* el post: “Blockchain aplicado a la energía renovable. ¿Cómo puede el ‘blockchain’ acreditar el origen de la energía verde?”, disponible en: <https://www.iberdrola.com/innovacion/blockchain-energia>.

20. Blockchain Archives - HOPU - Ciudades inteligentes: dispositivos IoT de calidad del aire, monitoreo medio ambiental, ruido e inteligencia de diseño urbano.

21. *Vid.* el post: “Tecnología *blockchain* aplicada al reciclaje”, disponible en: <https://www.retema.es/articulo/tecnologia-blockchain-aplicada-al-reciclaje-rhw7j>.

22. En la Resolución del Parlamento Europeo, de 3 de octubre de 2018, sobre las tecnologías de registros distribuidos y las cadenas de bloques: fomentar la confianza con la desintermediación (2017/2772(RSP)), se pusieron de relieve las posibilidades de esta tecnología en el ámbito del transporte. Así, se destaca “el potencial de la TRD en los ámbitos de movilidad y logística, incluida la matriculación y administración de vehículos, la verificación de distancias entre ellos, los seguros inteligentes y la recarga de vehículos eléctricos”.

a los centros escolares o por motivos diversos. Los objetivos de esta gestión del tráfico son diversos, pero de gran relevancia. Así, entre otros, podemos citar el evitar congestiones y atascos, limitar las emisiones de gases contaminantes, reducir la siniestralidad, así como reducir las distancias mejorando los tiempos en los desplazamientos. A ello se añade el hecho de combinar el transporte colectivo con el transporte particular, así como de realizar una gestión adecuada de los aparcamientos.

3.4.3. Seguridad y emergencias

El desarrollo tecnológico tiene una doble perspectiva desde la seguridad pública. Por un lado, bien se generan nuevos riesgos y formas de delincuencia o bien los delitos tradicionales se desarrollan en entornos hasta ahora insospechados. Así, en el ámbito del *blockchain* el desarrollo de las criptomonedas ha comportado delitos de tipo económico como estafas y fraudes de tipo piramidal²³. Por otro lado, la aplicación de las tecnologías de la información y la comunicación puede incrementar la eficiencia de las fuerzas y cuerpos de seguridad, a través de nuevos instrumentos de control de la población como el reconocimiento facial en imágenes captadas por cámaras de videovigilancia (Pérez Guerrero, 2020), la predicción a través de algoritmos de conductas que potencialmente pueden comportar un riesgo para la seguridad (Díaz González, 2020b), la identificación de denuncias falsas, los mensajes que constituyan amenazas o coacciones, etc.

Aunque pueda parecer ciencia ficción o propio de sistemas totalitarios, pueden encontrarse diversos ejemplos no solo en los países más avanzados, sino también en nuestra realidad más cotidiana. Así, puede mencionarse, entre muchos otros, la aplicación de algoritmos para detectar amenazas en redes sociales (Departamento de Policía de Boston, EE. UU.), para la identificación del lenguaje del odio en Twitter (Universidad Autónoma de Madrid y Ministerio del Interior del Gobierno de España), para hacer reconocimiento facial por la Policía (Departamento de Policía de la Ciudad de Nueva York, Departamento de Policía de Orlando, Policía del Estado de Michigan, EE. UU.), predecir el riesgo de reincidencia criminal (E-riscanvi, Departamento de Justicia, Generalitat de Cataluña), predecir el comportamiento humano (*Palantir Policing Algorithm* desarrollado por la Policía y los servicios de

23. Vid. “El nuevo auge de las criptomonedas copia el viejo fraude piramidal”. Disponible en: <https://elpais.com/economia/2021-07-24/el-nuevo-auge-de-las-criptoestafas.html>.

inteligencia en Dinamarca), así como identificar las quejas fraudulentas a la Policía (Veripol, Policía Nacional española)²⁴.

Este tipo de avances tensionan aún más las costuras del binomio libertad y seguridad, poniendo en un brete el difícil equilibrio existente entre ambas. Tal situación puede comprometer el Estado de derecho, sustituyéndolo por un Estado de carácter policial, por lo que habrá de insistirse en la implementación de esta tecnología en el escrupuloso cumplimiento de los derechos y libertades fundamentales a la hora de valorar su introducción por parte de las administraciones públicas.

Por lo que se refiere a la prestación de servicios de seguridad, la tecnología de cadena de bloques tendría utilidad para el seguimiento y la trazabilidad de los equipajes abandonados en las zonas de transporte, como puertos y aeropuertos. Este es el caso de la iniciativa planteada en el Newark's Liberty International Airport²⁵.

En el ámbito de las actuaciones de las fuerzas y cuerpos de seguridad se ha planteado el tema de las denuncias contra los abusos policiales que en EE. UU. han llevado a una gran reacción de protestas por discriminación racial, a consecuencia de los sucesos acontecidos como reacción al asesinato por asfixia de G. Floyd a manos de agentes de la autoridad²⁶. Así, algunas entidades han propuesto que queden registrados de forma distribuida los informes sobre este tipo de conductas. En esta línea una Orden ejecutiva aprobada por el expresidente de EE. UU. D. Trump, sobre reformas policiales, incluye la creación de una base de datos de malas praxis de la Policía²⁷. La potencialidad de esta técnica como instrumento de denuncia debe examinarse con especial cautela, debido a

24. Tales ejemplos pueden encontrarse en la noticia de prensa aparecida en *La Vanguardia* el 26 de octubre de 2021: “Cómo los algoritmos perpetúan la desigualdad en España. Inteligencia artificial versus derechos humanos”. Disponible en: <https://www.lavanguardia.com/tecnologia/20211026/7814332/como-algoritmos-perpetuan-desigualdad-espana.html>.

25. “Are Smart Street Lights the Future of Security Tech? New technology makes it possible to turn ordinary streetlamps into data-gathering networks. But is it too much of a good thing?”. Disponible en: <https://www.govtech.com/em/disaster/smart-street-lights-security-tech.html>.

26. *Vid.* el post: “Mala conducta policial quedará registrada en *blockchain*”. Disponible en: <https://www.bitcoin.com.mx/mala-conducta-policial-quedara-registrada-en-blockchain/>; así como: “Base de datos *blockchain* de brutalidad policial deja a malos policías al descubierto. El Protocolo PAN de Police Accountability Now es una base de datos anónima y resistente a la censura de denuncias por mala conducta policial, construida sobre Ethereum y IPFS”. Disponible en: <https://decrypt.co/es/32644/base-de-datos-blockchain-brutalidad-policial-deja-malos-policias-sin-escondite>.

27. <https://www.vox.com/2020/6/16/21292816/trump-police-reform-executive-order-explained>.

los problemas que puede plantear en las garantías de los agentes implicados, así como la complejidad en la eliminación o desaparición de estos informes en el caso de que no se correspondan con la realidad o cuando se haya extinguido la responsabilidad sobre los mismos.

La seguridad privada también deviene un ámbito en el que la tecnología de cadena de bloques puede realizar aportaciones de interés. De esta forma, se ha planteado la utilización de *blockchain* para asegurar la integridad y la trazabilidad de las fechas de las grabaciones de las cámaras de videovigilancia²⁸. Tales grabaciones pueden llegar a ser consideradas documentos públicos, por lo que resulta necesario acreditar no solamente el hecho en sí producido, sino el momento en el que se produjo.

Para finalizar este apartado, cabe hacer referencia también a algunas iniciativas que proponen un modelo de ciudad inteligente en el que las empresas, a través de las nuevas tecnologías, asumirían el ejercicio de funciones propias de las administraciones, como la seguridad, las decisiones judiciales, la recaudación y gestión de los tributos, el sistema educativo, etc.²⁹. Dicha propuesta extrema de privatización de funciones públicas choca frontalmente con el papel que tienen reservados constitucionalmente los poderes públicos, si bien nos permite ver la fuerza de este tipo de tecnologías y la necesidad de fijar límites y garantías en su implementación.

3.4.4. Servicios de atención a las personas: educación, sanidad y servicios sociales

Los servicios de atención a las personas cobran una gran relevancia en el ámbito de la ciudad inteligente destinada a conseguir el bienestar de la ciudadanía de forma eficiente a través de las nuevas tecnologías. La relevancia de las TIC en los servicios públicos personales se manifiesta en múltiples aspectos. En el ámbito de los servicios sociales encontramos, por ejemplo, la teleasistencia y la geolocalización, que permiten promover la autonomía personal de los usuarios³⁰. La aplicación de las tecnologías puede repercutir en la reducción de los

28. Aguilera Sillero (2021).

29. *Vid.* el post: “Así es la ciudad completamente privada que planea uno de los grandes empresarios del *bitcoin*”, disponible en: <https://www.eleconomista.es/internacional/noticias/11091271/03/21/Asi-es-la-ciudad-completamente-privada-que-planea-uno-de-los-grandes-empresarios-del-bitcoin.html>; así como: “Vision in Northern Nevada”, disponible en: <https://www.blockchains.com/real-life-sandbox/>.

30. Santás (2013).

plazos de atención y listas de espera. Entre las ventajas que se han señalado³¹ encontramos las siguientes: “1.- Facilita el acceso a los servicios sociales y al trabajador social, reforzando el papel de profesional de referencia; 2.- Democratiza conocimientos e información sobre recursos, procedimientos y oportunidades; 3.- Capacita a los/las usuarios/as para una mayor inclusión y participación social, ya que aumenta sus habilidades sociales y su capital relacional; 4.- Favorece una mejor planificación profesional, reducir listas de espera y disponer de más tiempo para la intervención social intensiva”.

Por lo que se refiere a la educación, una de las principales aportaciones que plantearía *blockchain* sería con relación a las titulaciones académicas a través de verificaciones y acreditaciones mediante cadenas de bloques. En cualquier caso, la educación supone tanto el objeto de aplicación de esta tecnología como un medio de facilitar el conocimiento sobre la misma, así como la constitución de plataformas de innovación especializadas que permitan la investigación y desarrollo en este ámbito³².

Respecto al ámbito sanitario se ha destacado la virtualidad de *blockchain* respecto al control y a la transparencia sobre los datos sanitarios, así como tendría relevancia para el tema de la trazabilidad de los medicamentos y de las vacunas. Una de las cuestiones que ha puesto de relieve la emergencia sanitaria de la COVID-19 ha sido que las vacunas puedan llegar a los destinatarios con las adecuadas condiciones de temperatura y de conservación, siguiendo todo el proceso de distribución desde que salen del laboratorio hasta que llegan a su destino, reduciendo el riesgo que pueden producir vacunas fraudulentas o que no cuentan con los debidos controles y autorizaciones de las autoridades sanitarias³³.

31. Santás (2013).

32. En el ámbito de la educación, la Resolución del Parlamento Europeo de 2018 alude a los siguientes aspectos:

“17. Destaca el potencial de la TRD para la verificación de cualificaciones académicas, la certificación educativa encriptada (por ejemplo, certificados en bloques) y los mecanismos de transferencia de créditos;

18. Destaca que la falta de conocimiento sobre el potencial de la TRD disuade a los ciudadanos europeos de utilizar soluciones innovadoras para sus negocios;

19. Destaca la necesidad de establecer entidades sin ánimo de lucro, por ejemplo, centros de investigación, que constituirían plataformas de innovación que se especializarían en tecnología TRD con el fin de desempeñar funciones educativas sobre la tecnología en los Estados miembros”.

33. “Cómo puede ayudar la tecnología en la vacunación. Telefónica Empresas ofrece a las comunidades autónomas una solución integral, que permite agilizar la administración segura de las vacunas”; disponible en: <https://www.economista.es/salud-innovacion/noticias/11170264/04/21/Como-puede-ayudar-la-tecnologia-en-la-vacunacion-.html>.

En el ámbito de los servicios sociales, la tecnología de cadena de bloques se puede utilizar para el ámbito propio de la atención primaria y los servicios básicos, que son de clara competencia municipal. Así, por ejemplo, las medidas relativas a la lucha contra la pobreza energética a través de mecanismos como el bono social³⁴. De esta forma, los entes locales pueden recibir información en tiempo real de los cortes por impago. Esta información recibida de forma encriptada puede ser de gran ayuda para la tramitación de las prestaciones económicas de urgencia social. De esta forma, encontramos convenios entre entidades municipales y empresas suministradoras de energía eléctrica³⁵.

La cooperación al desarrollo y la ayuda humanitaria pueden ser también ámbito importante para la utilización de la tecnología de cadena de bloques. Así, para enviar remesas de dinero se puede seguir la trazabilidad entre emisor y receptor, a través de criptomonedas, garantizando la confidencialidad y evitando represalias³⁶.

“Covid 19 la vacuna con trazabilidad *Blockchain*”; disponible en: <https://www.signeblock.com/covid-19-la-vacuna-con-trazabilidad-blockchain/>.

34. “*Blockchain* agiliza la implantación de servicios sociales. Un proyecto desarrollado por Ayesa e Izertis para Endesa contempla el primer sistema *blockchain* de Europa para agilizar la tramitación del bono social a personas en riesgo de exclusión”; disponible en: <https://www.computing.es/analytics/casos-exito/1116552046201/blockchain-agiliza-implantacion-de-servicios-sociales.1.html>. Según se señala:

“De esta forma, los consistorios podrán tener la información en tiempo real, recibiendo al instante los datos de las personas que han recibido avisos de corte por impago del suministro eléctrico. Mientras que los servicios sociales cruzarán al instante esta información con su propia base de datos y constatarán rápidamente con la compañía eléctrica si se trata de un cliente que cumple con los criterios para beneficiarse del Bono Social (regulado por una ley estatal).

Blockchain permite tener toda la información en una base de datos distribuida entre todos los implicados, de forma segura y encriptada, manteniendo las operaciones realizadas inmutables, de forma transparente y trazable, respetando además la normativa sobre protección de datos y derecho al olvido. Además, este proyecto permitirá en el futuro crear una red distribuida a la que se podrán unir otros ayuntamientos y comunidades autónomas”.

35. El Ayuntamiento de Málaga y Endesa firman un acuerdo para evitar el corte de luz a personas sin recursos. (2019). *Málaga Hoy*, 11-11-2019; disponible en: https://www.malahoy.es/malaga/ayuntamiento-malaga-endesa-corte-luz_0_1408959415.html.

36. Vid. “*Blockchain*: una revolución para el sector social. Conoce cómo el *Blockchain* afecta al sector social”, de Concepción Galdón, disponible en: <https://www.fundacionmapfre.org/premios-ayudas/premios/premios-fundacion-mapfre-innovacion-social/tendencias/blockchain-revolucion-sector-social/>. Según se señala en este blog: “En mayo de este año, 2017, **Naciones Unidas** envió fondos a más de **10 000 personas en Siria** a través de la plataforma de criptomonedas Ethereum. El envío de ayuda usando criptomonedas permite **garantizar que el dinero llega** a aquellos a quienes está destinado (la trazabilidad es una de las grandes fortalezas de *Blockchain*) pero de una manera en que nadie más que los interesados pueden saber quién envía el dinero y quién lo recibe (la seguridad de la encriptación es la otra fortaleza que hace que este protocolo sea superior a los que conocíamos). En un entorno en el que ser identificado como receptor de ayuda de ONU es una sentencia

3.5. La participación de la ciudadanía en la gobernanza de las ciudades inteligentes mediante tecnología de cadena de bloques

Como hemos visto anteriormente, el concepto de ciudad inteligente pone en el centro del sistema al ciudadano (*smart citizen*), circunstancia que comporta la superación de una visión meramente pasiva de las personas, sino considerarlas como actores relevantes en la gobernanza de las ciudades inteligentes. En este sentido, se trata de una participación ciudadana que no solamente se basa en la toma de decisión, sino que está basada en la gestión (Tornos Mas, 2017). Como hemos visto, estamos asistiendo a un proceso de transformación en las relaciones entre Estado y sociedad en donde a través de las tecnologías la ciudadanía puede implicarse en el ejercicio de determinadas funciones públicas tradicionales, dando asimismo unas mayores ventajas de inmutabilidad, transparencia y participación. Ello no obsta a que las administraciones deban valorar en términos de oportunidad y proporcionalidad las ventajas y los riesgos asociados a dicho proceso. En algunos casos, no solamente estaremos ante meros riesgos, sino que pueden producirse incluso incumplimientos de la normativa (Agencia Española de Protección de Datos, 2020).

De acuerdo con lo establecido en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, los municipios constituyen los “cauces inmediatos de participación ciudadana en los asuntos públicos” (art. 1.1). Esta Ley menciona entre las competencias propias de los entes locales: “la promoción en su término municipal de la participación de los ciudadanos en el uso eficiente y sostenible de las tecnologías de la información y las comunicaciones” [art. 25.2.ñ]. Competencia que se corresponde con el derecho que la misma legislación reconoce a los vecinos “de participar en la gestión municipal de acuerdo con lo previsto en las leyes” [art. 18.1.b)]. Encontrándose la regulación en los artículos 69 a 72 de la Ley, en los que se prevén aspectos como la información sobre la actividad de las corporaciones locales (art. 69), las sesiones del pleno (art. 70), procedimiento y órganos de participación, así como iniciativa popular para actuaciones y normas (art. 70bis), las consultas populares (art. 71), o el desarrollo de las asociaciones para la defensa de los intereses de los vecinos (art. 72). Ahora bien, cabría dar una mayor cobertura normativa a las nuevas formas de participación basadas no tanto en la toma de decisión cuanto en la gestión e implicación ciudadana.

de muerte, *Blockchain* ha permitido mantener a flote **iniciativas locales de ayuda a quienes siguen atrapados por la guerra**. Es un caso de aplicación de *Blockchain* en el sector social”.

Por tanto, vemos cómo el ordenamiento jurídico alude al papel de los municipios en el fomento de la participación en el uso eficiente y sostenible de las TIC. El papel de esta tecnología puede ser relevante para realizar procesos participativos, por ejemplo, sobre los presupuestos municipales, a través de votaciones donde se asegura la emisión del voto mediante su registro digital en un libro distribuido del cual pueden guardar copia todas las personas implicadas. De esta forma, el proceso participativo resulta transparente, generando la confianza entre la ciudadanía de que se ha realizado con todas las garantías posibles. También puede ser relevante para el seguimiento de las diversas formas de participación.

Si bien la participación de la ciudadanía en el ámbito municipal tiene un marco jurídico para vehicularla a través de los mecanismos tradicionales, requeriría de una mayor concreción legal que diera cobertura a las tecnologías de registro distribuido, estableciéndose las garantías adecuadas para poder implementarla. En este punto, la entidad local, en uso de sus potestades de autoorganización, podría determinar en qué condiciones se incorpora esta tecnología de registro distribuido, así como en qué tipo de funciones públicas participa la ciudadanía a través de la misma. Sobre estas cuestiones, en todo caso, hemos de remitirnos al tratamiento que de las mismas se hace en el capítulo de esta misma obra de los profesores Patricia García Majado y Miguel Ángel Presno Linera.

4. Conclusiones: La aportación de la tecnología de cadena de bloques al desarrollo de la ciudad inteligente y sus retos jurídicos

A través del concepto de ciudad inteligente, se han articulado una serie de proyectos que tienen en común el desarrollo de las tecnologías de la información y la comunicación para una mayor eficiencia de los servicios, con el objetivo de mejorar la calidad y el bienestar de la ciudadanía. Dichos proyectos, que requieren una gran inversión de recursos humanos, materiales y financieros, han sido impulsados por empresas con una cierta capacidad tecnológica y han encontrado en las administraciones públicas un importante cliente. Para llevar a cabo dichos proyectos se han venido utilizando diversos tipos de tecnologías, como el internet de las cosas, los grandes volúmenes de datos (*big data*), los datos abiertos (*open data*), la nube (*cloud computing*), las redes 5G, las tecnologías de registro distribuido, entre las que se encuentran las de cadenas de bloques (*blockchain*), así como la inteligencia artificial (IA).

En concreto, la tecnología de cadena de bloques puede suponer una aportación relevante para mejorar la eficiencia de los servicios de interés general en el contexto de la ciudad inteligente, aportando determinadas ventajas a través de mayor transparencia, inmutabilidad y descentralización. Se trata de una tecnología que se encuentra en proceso de desarrollo y que todavía no tiene un marco jurídico que permita su plena implementación en el ámbito de las administraciones públicas. En cualquier caso, el conjunto de derechos, principios y reglas existentes permiten que las administraciones públicas puedan comenzar a evaluar su implementación valorando diversos aspectos ya sea de oportunidad o de coste económico, ya sea de garantizar tanto derechos como el correcto ejercicio de funciones públicas. Las ventajas existentes hacen augurar su establecimiento gradual en el ámbito de las relaciones entre administraciones públicas y ciudadanía, a medida que vaya cambiando en algunos aspectos el ejercicio de determinadas funciones públicas.

Hasta la fecha, la cadena de bloques ha tenido una cierta mala prensa por cuanto se ha asociado fundamentalmente a las criptomonedas. También se percibe una cierta resistencia por parte de las administraciones públicas, que ven cómo pueden ser sustituidas por *blockchain* en la realización de ciertas funciones. Ello ha llevado incluso a que el marco jurídico haya establecido ciertas prohibiciones y limitaciones, cuando menos de forma transitoria y a la espera de que exista un mayor consenso regulatorio a nivel europeo.

En todo caso, la aplicación de estas tecnologías debería pasar, desde la interpretación que se defiende en este trabajo, por una concepción de la ciudad inteligente realizada desde el derecho a la ciudad. En torno a este derecho cabría articular un estatuto digital integrado por un conjunto de derechos y deberes, por la aplicación de unos principios generales adaptados a este nuevo entorno y por el establecimiento de reglas que permitan hacerlos efectivos.

Debe también ponerse de relieve el avance que la implementación de esta nueva tecnología puede suponer para el ejercicio compartido de funciones públicas o que hasta ahora se consideraban como tales, eliminando la figura de intermediarios. Ello no supone que tal tipo de actividades no sean objeto de una adecuada regulación que permita a las administraciones públicas tomar las decisiones más adecuadas en la forma de su implementación, valorando los derechos e intereses tanto generales como de la ciudadanía.

5. Bibliografía

Agencia Española de Protección de Datos (2020). *Tecnologías y Protección de Datos en las AA. PP.* Disponible en: <https://www.aepd.es/sites/default/files/2020-11/guia-tecnologias-admin-digital.pdf>.

Aguado i Cudolà, V. (2018). Los servicios de interés general en la ciudad inteligente: ¿una prestación más eficiente a costa de mayores desigualdades sociales? En V. Aguado i Cudolà, V. Parisio y Ò. Casanovas i Ibàñez (dirs.). *El derecho a la ciudad: el reto de las smart cities*. Barcelona: Atelier.

Aguado i Cudolà, V., Parisio, V. y Casanovas i Ibàñez, Ò. (dirs.). (2018). *El derecho a la ciudad: el reto de las smart cities*. Barcelona: Atelier.

Aguilera Sillero, J. M.^a (2021). *Los retos de la videovigilancia como servicio*. Disponible en: https://www.seguritecnia.es/tecnologias-y-servicios/videovigilancia-y-cctv/los-retos-de-la-videovigilancia-como-servicio_20210113.html.

Alamillo Domingo, I. (2019a). Las tecnologías de registro distribuido (*blockchain*) y la transformación del procedimiento administrativo. *El Consultor de los Ayuntamientos*, 1, 57-65. Disponible en: <https://www.gtt.es/boletinjuridico/las-tecnologias-de-registro-distribuido-blockchain-y-la-transformacion-del-procedimiento-administrativo/>.

– (2019b). El RDL 14/2019: una extraordinariamente urgente e innecesaria reforma del régimen de identificación y firma electrónica en la LPAC. *El Consultor de los Ayuntamientos*, 12, 112-123.

Alejandro Romero, C. (2017). Aspectos jurídicos de la *Smart City: Smart regulation*, desarrollo sostenible e innovación en la gestión del territorio. En *Documento para su presentación en el VIII Congreso Internacional en Gobierno, Administración y Políticas Públicas GIGAPP. (Madrid, España) del 25 al 28 de septiembre de 2017*. Disponible en: http://www.gigapp.org/administrator/components/com_jresearch/files/publications/abs_355_1504529343PonenciaCarmenAlejandro.pdf.

Alonso Suárez, L. (2021). La aplicación de la tecnología *blockchain* en las ciudades inteligentes: hacia una gestión urbana descentralizada e inteligente. *European Review of Digital Administration & Law*, 2 (1), 107-126.

Andreani, S., Bianconi, F. y Filippucci, M. (2015). *Smart cities e contratti di paesaggio: l'intelligenza del territorio oltre i sistemi urbani*. *Istituzioni del federalismo: rivista di studi giuridici e politici*, 4, 895-925.

- Antoniazzi, S. (2019). *Smart City: diritto, competenze e obiettivi (realizzabili?) di innovazione. federalism.it. Rivista di Diritto Pubblico Italiano, Comparato, Europeo.*
- Arena, G. (2017). Un nuevo derecho para la administración compartida. *Revista de Administración Pública*, 203, 423-441.
- Arteaga Moralejo, J. (2019). *Blockchain en procesos de participación ciudadana: innovando desde la práctica en el Ayuntamiento de Alcobendas.* En C. Güemes, J. Resina y C. Cruz-Rubio (eds.). *Participación ciudadana: experiencias inspiradoras en España.* Madrid: GIGAPP. Centro de Estudios Políticos y Constitucionales.
- Association for Computing Machinery US Public Policy Council (USACM). (2017). *Statement on Algorithmic Transparency and Accountability.* Disponible en: https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf.
- Auby, J.-B. (2018). La ciudad, ¿nueva frontera del derecho administrativo? *TransJus Working Papers Publications*, 3. Disponible en: <http://diposit.ub.edu/dspace/handle/2445/123327>.
- Auby, J.-B. y De Gregorio, V. (2015). Le smart cities in Francia. *Istituzioni del federalismo: rivista di studi giuridici e politici*, 4, 975-993.
- Barrio Andrés, M. (2016). La smart city: versión 2.0 del municipio. *Documentación Administrativa, Nueva Época*, 3.
- Benítez-Eyzaguirre, L. (2020). *Blockchain para la transparencia, gestión pública y colaboración.* *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, 18 (1), 23-32. Disponible en: <https://revistas.ucm.es/index.php/TEKN/article/view/71514>.
- Biswas, K. y Muthukkumarasamy, V. (2016). *Securing Smart Cities Using Blockchain Technology.* Disponible en: <https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198>.
- Boix Palop, A. (2020a). Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones. *Teoría y método. Revista de Derecho Público*, 1. Disponible en: <http://www.revistasmarcialpons.es/revistaderechopublico/article/view/33>.
- (2020b). El Reial decret llei 14/2019, el constrenyiment de les comunitats autònomes en matèria d'utilització d'eines digitals i electròniques i l'increment del control administratiu de l'opinió i de la informació en xarxes. *Revista catalana de dret públic*, 61, 14-29. Disponible en: <https://doi.org/10.2436/rcdp.i61.2020.3526>.

- Cabezuelo-Lorenzo, F., Bonete-Vizcaíno, F. y Sánchez-Martínez, M.^a (2016). Análisis de la información y documentación científica española sobre el fenómeno de las *smart cities*, el hábitat de los nativos digitales. *Cuadernos de Documentación Multimedia*, 27 (1).
- Caporale, M. (2015). L'attuazione delle *smart cities*. Competenze e coordinamento tra livelli di governo. *Istituzioni del federalismo: rivista di studi giuridici e politici*, 4, 949-973.
- Carloni, E. y Vaquero Piñeiro, M. (2015). Le città intelligenti e l'Europa. Tendenze di fondo e nuove strategie di sviluppo urbano. *Istituzioni del federalismo: rivista di studi giuridici e politici*, 4, 865-894.
- Cerrillo i Martínez, A. (2020). Los servicios de la ciudad inteligente. En C. Barrero Rodríguez y J. M. Socías Camacho (coords.). *La ciudad del siglo XXI: Transformaciones y retos*. Actas del XV Congreso de la Asociación Española de Profesores de Derecho Administrativo (AEPDA). Madrid: INAP.
- Cotino Hueso, L. (2018). La obligación de relacionarse electrónicamente con la Administración y sus escasas garantías. *IDP. Revista de Internet, Derecho y Política*, 26. Disponible en: <https://www.raco.cat/index.php/IDP/article/download/339092/430032>.
- (2020). La (in)constitucionalidad de la “intervención”, “mordaza” o “apagón” de las telecomunicaciones e internet por el Gobierno en virtud del Real Decreto-ley 14/2019. *Revista General de Derecho Administrativo*, 54. Disponible en: <https://www.cotino.es/articulos-capitulos/>.
- Delgado Jiménez, A. (2015). Del derecho a la ciudad al reto de la ciudad sostenible e inteligente: la ciudad sostenible al servicio del derecho a la ciudad y la ciudad inteligente al servicio de la ciudad sostenible. *Revista de Derecho Urbanístico y Medio Ambiente*, 300.
- Díaz, O. (2014). *Smart cities* i administracions locals: algunes reflexions jurídiques. En AA. VV. *Smart city. Cap al municipi intel·ligent*. Barcelona: Diputació de Barcelona. Disponible en: <https://www1.diba.cat/uliep/pdf/54269.pdf>.
- Díaz González, G. M. (2020a). Las *human rights cities*: ¿defensa de los derechos humanos u obstaculización de las relaciones internacionales del Estado? En C. Barrero Rodríguez y J. M. Socías Camacho (coords.). *La ciudad del siglo XXI: Transformaciones y retos*. Actas del XV Congreso de la Asociación Española de Profesores de Derecho Administrativo (AEPDA). Madrid: INAP.
- (2020b). Algoritmos y actuación policial: la policía predictiva. En A. Huergo Lora (dir.) y G. M. Díaz González (coord.). *La regulación de los algoritmos* (pp. 181-234). Thomson Reuters Aranzadi.

- Doncel, E. y Ezcurra, I. (2015). *Tendencias tecnológicas en la gestión del alumbrado público en las Smart Cities*. Disponible en: <https://wellnesstg.com/tendencias-tecnologicas-en-la-gestion-del-alumbrado-publico-en-las-smart-cities/>.
- Esteve Pardo, J. (2013). *La nueva relación entre Estado y sociedad: aproximación al trasfondo de la crisis*. Madrid: Marcial Pons.
- Eubanks, V. (2018). *Automating Inequality. How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- Federal Trade Commission (2016). *Big Data. A Tool for Inclusion or Exclusion? Understanding the issues*. Disponible en: <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>.
- Fernández Salmerón, M. (2015). Soluciones innovadoras y gestión avanzada en entornos urbanos. Problemas jurídicos derivados de la contratación pública en el desarrollo de "ciudades inteligentes". En *Istituzioni del federalismo: rivista di studi giuridici e politici*, 4, 995-1024.
- Font i Llovet, T. (2021). La ciudad inteligente como actor global. *European Review of Digital Administration & Law*, 2 (1), 19-32.
- Gigliani, F. (2015). La "domanda" di amministrazione delle reti intelligenti. *Istituzioni del federalismo: rivista di studi giuridici e politici*, 4, 1049-1069.
- Gil, E. (2016). *Big data, privacidad y protección de datos*. Madrid: Agencia Española de Protección de Datos.
- Greenfield, A. (2014). The truth about smart cities: 'In the end, they will destroy democracy'. *The Guardian*. Disponible en: <https://www.theguardian.com/cities/2014/dec/17/truth-smart-city-destroy-democracy-urban-thinkers-buzzphrase>.
- Guglielmi, G. J. (2016). *Open Data y servicio público*. Los datos públicos abiertos son un servicio público. *Revista General de Derecho Administrativo*, 41.
- Huergo Lora, A. (2020). Una aproximación a los algoritmos desde el derecho administrativo. En A. Huergo Lora (dir.) y G. M. Díaz González (coord.). *La regulación de los algoritmos* (pp. 23-87). Thomson Reuters Aranzadi.
- Iglesias, F. (2020). Todas las aplicaciones *Blockchain* para *Smart Cities*. *Observatorio Blockchain*, 5-6-2020. Disponible en: <https://observatorioblockchain.com/blockchain/todas-las-aplicaciones-blockchain-para-smart-cities/>.

- Jolíás, L. (2017). *Blockchain, transparencia y el futuro del Gobierno Abierto*. Disponible en: <https://acog17.dryfta.com/component/dryfta/abstract/public/31/blockchain-transparencia-y-el-futuro-del-gobierno-abierto>.
- Lefebvre, H. (2017). *El derecho a la ciudad* (introducción de M. Delgado, traducción de la primera edición de 1967). Madrid: Capitán Swing.
- m4Social (2021). *Internet, dret fonamental: Propostes per a reduir la bretxa digital i social. Estudi per analitzar el marc legal existent i possibles iniciatives entorn de la reclamació de l'accés a Internet com a dret fonamental*. Disponible en: https://es.slideshare.net/m_4Social/internet-dret-fonamental-propostes-per-a-reduir-la-bretxa-digital-i-social-250277264?from_action=save.
- O'Neil, C. (2016). *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy*. New York Times.
- Pérez Guerrero, F. (2020). Seguridad y ciudad inteligente: Las videocámaras con inteligencia artificial en la vía pública. En C. Barrero Rodríguez y J. M. Socías Camacho (coords.). *La ciudad del siglo XXI: Transformaciones y retos*. Actas del XV Congreso de la Asociación Española de Profesores de Derecho Administrativo (AEPDA). Madrid: INAP.
- Piñar Mañas, J. L. (dir.). (2017). *Smart Cities. Derecho y técnica para una ciudad más habitable*. Madrid: Reus.
- Quadra-Salcedo, T. de la y Piñar Mañas, J. L. (dirs.). (2018). *Sociedad digital y derecho*. Madrid: BOE. Ministerio de Industria, Comercio y Turismo. Red.es.
- Quintana Cortés, J. L. (2020). La tecnología *blockchain* y su pretendida aplicación a la contratación pública como mecanismo para lograr mayor integridad. *Revista Española de Control Externo*, 64, 152-173.
- Santás, J. I. (2013). Una experiencia. Uso de las Tecnologías de la Información y la Comunicación (TIC) para la intervención social en servicios sociales. *XII Congreso Estatal de Trabajo Social*. Disponible en: <http://www.navarra.es/NR/rdonlyres/0835B9AF-FC55-4364-94C9-BDDD8ACE3D1F/297020/JoselgnacioSantas.pdf>.
- Santiago Iglesias, D. (2016). La implementación de proyectos *smart city* en núcleos urbanos de tamaño medio: análisis de experiencias en Castilla y León. *Revista Jurídica de Castilla y León*, 39.
- Sartori, L. (2015). Alla ricerca della *smart citizenship*. *Istituzioni del federalismo: rivista di studi giuridici e politici*, 4, 927-948.

- Sebastián Cermeño, J. (2016). Blockchain in financial services: Regulatory landscape and future challenges for its commercial application. *BBVA Research Working Paper 16/20*. Disponible en: https://www.bbvaesearch.com/wp-content/uploads/2016/12/WP_16-20.pdf.
- Serale, F., Redl, C. y Muenta-Kunigami, A. (2018). *Blockchain en la Administración pública. ¿Mucho ruido y pocos bloques?* Washington: Banco Interamericano de Desarrollo.
- Tarrés Vives, M. (2003). *Normas técnicas y ordenamiento jurídico*. Valencia: Tirant lo Blanch.
- Tornos Mas, J. (2017). *Bienes comunes y administración compartida*. Disponible en: http://idpbarcelona.net/docs/recerca/bens/admon_compartida.pdf.
- Torregrossa, M. (2018). *Blockchain para servidores públicos: todo lo que necesitas saber*. Su guía rápida sobre las oportunidades y los riesgos. *Apolitical* [blog], 26-6-2018. Disponible en: <https://apolitical.co/solution-articles/es/blockchain-para-servidores-publicos-todo-lo-que-necesitas-saber>.
- Valero Torrijos, J. (2015). Ciudades inteligentes y datos abiertos: implicaciones jurídicas para la protección de los datos de carácter personal. *Istituzioni del federalismo: rivista di studi giuridici e politici*, 4, 1025-1047.
- Valero Torrijos, J. y Robles Albero, J. R. (2015). *Open smart cities: ¿De quién son los datos?* En AA. VV. *Regulating Smart Cities. Actas del 11.º Congreso Internacional Internet, Derecho y Política (Barcelona, 2-3 de julio de 2015)*. Barcelona: Universitat Oberta de Catalunya. Disponible en: http://edcp.uoc.edu/proceedings_idp2015.pdf.
- Van-Halen Rodríguez, J. (2015). Ciudades sostenibles: un reto inaplazable. *Revista de Derecho Urbanístico y Medio ambiente*, 300, 17-38.
- Vega Maza, M. (2019). El auge de *blockchain* y sus posibilidades reales de aplicación en los registros de las administraciones públicas. *IDP. Revista de Internet, Derecho y Política*, 28. Disponible en: <https://www.raco.cat/index.php/IDP/article/download/373501/467089>.
- Velasco Rico, C. I. (2019). La ciudad inteligente: entre la transparencia y el control. *Revista General de Derecho Administrativo*, 50. Disponible en: <http://laadministracionaldia.inap.es/noticia.asp?id=1509545>.
- Villarejo Galende, H. (2015). *Smart cities: una apuesta de la Unión Europea para mejorar los servicios públicos urbanos*. *Revista de Estudios Europeos*, 66, 25-51.

Tecnología *blockchain* y entidades locales: nuevas formas de funcionamiento interno y de interacción con el ciudadano

Antonio David Berning Prieto

Profesor ayudante doctor de Derecho Administrativo.

Universidad Pablo de Olavide

SUMARIO. 1. Introducción: la tecnología de registro distribuido al servicio de las administraciones públicas. 2. Breve referencia a la propuesta de regulación de *blockchain* en el futuro Reglamento eIDAS-2. 3. La problemática en el sector público de la descentralización de nodos: ¿*blockchain* privada, pública o mixta para la Administración local? 4. El procedimiento administrativo como paradigma de aplicación de la tecnología *blockchain* en actuaciones y trámites susceptibles de automatización (*smart procedure*). 5. El uso de *blockchain* como registro electrónico en general, y de apoderamientos en particular. 6. La contabilidad o llevanza de libros contables en entidades locales como posible aplicación de *blockchain*. 7. Identidad digital basada en *blockchain*. Especial referencia a la identidad autosoberana regulada en el Proyecto europeo “ReIDAS-2” para el establecimiento de una identidad digital europea o eID y su aplicación a las entidades locales. 8. *Blockchain* como posible forma de garantizar la fiabilidad del voto electrónico y la participación ciudadana en el ámbito local (remisión). 9. Breve referencia al posible uso de *blockchain* en los convenios interadministrativos (*smart public agreements*). 10. Conclusiones. 11. Bibliografía.

1. Introducción: la tecnología de registro distribuido al servicio de las administraciones públicas

La irrupción de las nuevas tecnologías en las administraciones públicas comenzó hace ya años, con la aún entonces en vigor Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, aunque de forma aún primigenia, la cual fue objeto de modificaciones durante su vigencia para incluir determinadas adaptaciones relacionadas con la introducción de las nuevas tecnologías (por ejemplo, la Ley 24/2001, de 27 de diciembre, que modificó los artículos 38 y 59 para regular las notificaciones y registros electrónicos). Esta norma fue complementada posteriormente por la Ley 59/2003, de Firma Electrónica, que regulaba en su artículo 4 el uso de esta tecnología por las administraciones públicas; también, indirectamente, por la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico, así como por las disposiciones reglamentarias que cada Administración pública aprobaba para regular sus particularidades propias en materia de administración electrónica.

El verdadero punto de inflexión se produjo con la aprobación de la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, la cual fue una norma realmente innovadora que permitió un desarrollo paulatino (aunque desigual) de la administración electrónica española, como ya entonces advirtieron Gamero y Martínez¹, para quienes dicha norma supuso la llegada de la era de la información a la actividad y al procedimiento administrativos. Durante su vigencia se publicaron dos importantes normas que pretendían unificar ese inicialmente desigual desarrollo de la administración electrónica²: los reales decretos 3/2010 y 4/2010, por los que se regulan el Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, respectivamente.

La entrada en vigor de las leyes 39 y 40/2015, de 1 de octubre, de Procedimiento Administrativo Común y Régimen Jurídico del Sector Público, respectivamente, impusieron la implantación de la administración electrónica

1. Gamero y Martínez (2010: 80).

2. No en vano el prof. Gamero hablaba de “islas de administración electrónica”, en referencia a ese desigual desarrollo de soluciones técnicas que provocaban un funcionamiento excepcional en la gestión interna, pero que a la hora de interoperar con el resto de las administraciones públicas encontraban obstáculos que lo impedían o dificultaban, en Gamero Casado (2009: 293).

en el funcionamiento de las administraciones públicas, por lo que ha pasado de ser potestativa a ser preceptiva.

La Unión Europea es una clara precursora de las nuevas tecnologías, no solo para el uso privado en el mercado único europeo, sino también para su uso en las administraciones públicas, ya que, por ejemplo, el Reglamento (UE) 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, al regular los sistemas de firma electrónica, indirectamente está condicionando los que deben admitirse por las administraciones en sus relaciones con los ciudadanos.

Más recientemente, la Unión Europea ha puesto énfasis, en diversos instrumentos normativos, en la necesidad de incrementar la confianza y el uso de medios de identificación electrónica en el mercado interior, como en el artículo 5 del Reglamento (UE) 2017/1128 del Parlamento Europeo y del Consejo, de 14 de junio, relativo a la portabilidad transfronteriza de los servicios de contenidos en línea en el mercado interior, o la Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo, de 20 de junio, para permitir la utilización de herramientas y procesos digitales en el derecho de sociedades. Y el pasado 3 de junio fue presentada la Propuesta de modificación del Reglamento (UE) 910/2014 (ReIDAS), para establecer un marco jurídico de la identidad digital europea, lo que demuestra la relevancia de esta cuestión en el plano europeo, y que sin duda alterará la forma en que las administraciones públicas admiten sistemas de identificación electrónica de los ciudadanos en la prestación de servicios públicos o en los procedimientos administrativos que tramitan.

Las nuevas tecnologías, por tanto, han irrumpido ampliamente en el sector público, de forma que ya no son solo la gestión documental y procedimental electrónica, la necesidad de generar expedientes y archivos electrónicos, y la utilización de certificados electrónicos de firma o sello electrónico, e incluso de autenticación de sitio web para la sede electrónica, sino que van más allá y comienzan a incluirse tecnologías basadas en inteligencia artificial, con el auge de las *smart cities*³ y,

3. Las *smart cities* han sido objeto de un profuso estudio por parte de la doctrina española y europea; pueden consultarse algunos trabajos al respecto en el monográfico de la revista *European Review of Digital Administration and Law*, ed. Aracne Editrice, cuyo primer volumen correspondiente al periodo junio–diciembre de 2020 se ha dedicado a: *The use of artificial intelligence by public administration*.

últimamente, también *blockchain*⁴, en el funcionamiento electrónico del sector público⁵.

Estas tecnologías tienen, sin duda, múltiples beneficios, que solo se encuentran supeditados, para su aprovechamiento por parte de las administraciones públicas, a una regulación suficientemente garantista como para hacer uso de las mismas con la certeza y flexibilidad (la rigidez en la regulación puede dar lugar a la imposibilidad de aplicar determinadas soluciones) que tales tecnologías requieren, tanto para la propia Administración como para los ciudadanos.

Las tecnologías de registro distribuido⁶, entre ellas la de cadena de bloques o *blockchain*, pueden describirse, siguiendo a Alamillo⁷, como aquellas basadas en criptografía de clave pública que permiten la creación de un registro inalterable gestionado de forma descentralizada, de forma que gracias a un *software* y un libro de registro distribuido se pueden registrar transacciones que cualquier persona puede visualizar, donde los nodos independientes van verificando sucesivamente los distintos bloques que han de incorporarse al libro mayor de forma encadenada y segura (gracias a la aplicación de algoritmos⁸ matemáticos y la consiguiente obtención de *hashes* que se incorporan a la cadena a efectos de trazabilidad). De esta forma se puede asegurar que una transacción es válida y única, gracias al consenso de todos los nodos, en el que se sustenta la seguridad del sistema en lugar de confiarla a un tercero. La seguridad, por tanto, se encuentra en la concepción misma del sistema. Debido a su funcionamiento también se denomina libro mayor electrónico.

Esta novedosa tecnología aplicada a las administraciones públicas, con las adaptaciones necesarias, como se verá, puede suponer múltiples beneficios

4. Nótese que el Gobierno de Aragón fue pionero a nivel europeo en la adjudicación de contratos para la prestación de servicios de registro distribuido (*blockchain*) para la recepción y valoración de ofertas en determinados procedimientos de adjudicación; en la actualidad se encuentra en fase de evaluación el Expte. HAP_SGT_5/2021, del Departamento de Hacienda y Administración Pública de la Comunidad Autónoma de Aragón, con el objeto de adjudicar el contrato del desarrollo y evolución del sistema de licitación electrónica con tecnología de Registro distribuido (*blockchain*) de la Comunidad Autónoma de Aragón (disponible a través de la Plataforma de Contratos del Sector Público).

5. Puede consultarse también un mapa de iniciativas a nivel mundial basadas en *blockchain* en la web: <https://www.eublockchainforum.eu/initiative-map> (última consulta efectuada el 30/09/2021).

6. Más comúnmente conocidas como DLT, de sus siglas en inglés: *distributed ledger technologies*.

7. Alamillo Domingo (2020: 248 y ss.).

8. Para un exhaustivo estudio sobre la implicación de los algoritmos puede consultarse Huergo y Díaz (2020).

para el funcionamiento de la administración electrónica, ya que goza de determinadas características que garantizan unos niveles de seguridad y confianza superiores que autores como Tapscott⁹ denominan los siete principios esenciales:

- Integridad en la red: la confianza es intrínseca al sistema y no depende de cada miembro, sino que es cifrada y distribuida, esto es, las cadenas de bloques (encadenados) son seguras gracias a la infraestructura de clave pública unida a la aplicación de la función *hash*, y cualquier usuario en la red puede visualizar lo que en la misma sucede.
- Poder distribuido: el sistema distribuye el poder de forma igualitaria sin que ningún usuario ostente mayor poder que otro, de forma que son los propios usuarios los que tienen el control sobre sus datos y ninguno puede vulnerar el sistema, ya que el resto lo visualizaría inmediatamente.
- El valor como incentivo: el origen de *blockchain* radica en la moneda virtual bitc in, en cuyo sistema su creador¹⁰ estableci  medidas de consenso y retribuci n econ mica como valores que pretendi n persuadir a los usuarios a actuar correctamente, ya que gracias a la capacidad de procesamiento empleada y puesta al servicio del sistema se obtiene una retribuci n, por lo que los propios mineros tienen el inter s en mantener la confianza y seguridad de la cadena de bloques, ya que de ello depende el valor de sus retribuciones.
- Seguridad: el sistema tiene medidas de seguridad suficientes que garantizan la autenticidad de las transacciones, as  como la confidencialidad de sus integrantes, gracias a la criptograf a como fundamento del sistema, ya que se emplean como regla general sistemas asim tricos de clave p blica y privada (PKI o *Public Key Infrastructure*).
- Privacidad: *blockchain* permite que los usuarios puedan controlar sus datos personales, de forma que deciden qu  tipo de informaci n y en qu  medida la comparten con los dem s, ya que la identidad no es la base del sistema, sino la certeza de lo que en  l se registra, lo cual queda perfectamente garantizado independientemente de aquella.
- Garant a de preservaci n de derechos: los sistemas *blockchain* permiten efectuar transacciones y garantizar que no se efect an dos

9. Tapscott y Tapscott (2017: 57 y ss.).

10. Nakamoto (2008). Accesible en la direcci n web: <https://nakamotoinstitute.org/bitcoin> ( ltima consulta efectuada el 30/09/2021).

veces, por lo que los derechos de las personas que hacen uso de los mismos se encuentran garantizados por el propio funcionamiento intrínseco del sistema.

- Inclusión: al ser un sistema descentralizado, con *blockchain* se permite eliminar obstáculos que impiden o dificultan la participación en la red, como sucede con personas que no tienen posibilidad de abrir una cuenta corriente bancaria, o países en vías de desarrollo que no disponen de registros de la propiedad; podrían hacer uso de este sistema para acreditar el derecho de propiedad de aquellas personas que, de otra forma, no podrían hacerlo.

El autor aboga por la observancia de estos principios básicos en el establecimiento de toda red *blockchain*, de forma que no solo se erija en una tecnología, sino también en una forma de crear una nueva generación de empresas e instituciones públicas innovadoras de alto rendimiento, consiguiendo que cualquier persona pueda beneficiarse de sus ventajas, y ofreciendo soluciones a problemas que, de otra forma, serían de difícil superación.

Esta visión generalista de *blockchain* nos proporciona sin duda un amplio horizonte, cuya línea comprende supuestos mucho más allá del establecimiento de un nuevo sistema de registro o identificación, sin perjuicio de que el presente trabajo se centre en aquellos aspectos relativos a las administraciones públicas, a la gestión pública o al procedimiento administrativo.

2. Breve referencia a la propuesta de regulación de *blockchain* en el futuro Reglamento eIDAS-2

Aunque la propuesta de regulación a que se refiere este apartado será objeto de tratamiento en profundidad en otro capítulo de la presente obra en relación con los medios de pago, se torna necesario un breve apunte al respecto para proporcionar al lector una visión completa de lo que supondría a corto o medio plazo su aprobación y cómo afectaría a lo que en el presente capítulo se trata.

Recientemente se ha publicado la Propuesta¹¹ del Parlamento Europeo y del Consejo para crear un marco de trabajo a fin de regular la identidad digital en Europa, que podría dar como resultado un Reglamento eIDAS-2, por ser su objetivo principal modificar el Reglamento 910/2014 o ReIDAS actualmente

11. COM(2021) 281 final, de 3 de junio.

en vigor para adecuarlo a la realidad digital y mejorar su regulación y eficacia, ampliar su aplicación al sector privado y promover unas identidades digitales de confianza para todos los ciudadanos europeos. Entre otros aspectos como la identidad digital autosoberana, cuya mención se hará en el apartado correspondiente¹², contiene por primera vez una regulación del libro mayor electrónico que sin duda daría cabida a sistemas como *blockchain*.

En este sentido, se establece en la Propuesta que los libros mayores distribuidos proporcionan pruebas inmutables de la trazabilidad de las operaciones o datos que se registran en los mismos, con base en servicios de confianza ya existentes que se integran en ellos, como el sellado electrónico de tiempo y la secuenciación con el creador de los datos de origen, por lo que su funcionamiento en este sentido es similar al de la firma electrónica. Por tanto, se apuesta por los libros mayores electrónicos cualificados para evitar la fragmentación del mercado interior y conseguir un marco paneuropeo único que garantice la integridad de los datos. Además, se reconoce que este sistema proporciona un beneficio adicional a los tradicionales servicios de confianza, que se concreta en una gobernanza descentralizada, óptima para relaciones entre múltiples partes.

Gracias a esta Propuesta se trabajará en una regulación común para todos los Estados miembros que permita el reconocimiento transfronterizo de servicios de confianza basados en este tipo de tecnología, lo cual supone un gran avance en cuanto a su implantación no solo por el sector privado, donde se ha calculado que se encuentra el mayor porcentaje de casos de uso (más del 75 %), sino también por el sector público, donde el porcentaje se reduce al 10 % en la actualidad.

En este sentido, en la Sección 11 de la Propuesta se propone la regulación del artículo 45 *nonies* en relación con los efectos jurídicos de los libros mayores electrónicos, estableciéndose que no se denegarán efectos jurídicos ni se inadmitirán judicialmente libros mayores por el mero hecho de encontrarse en soporte electrónico, aun en el caso de no cumplir los requisitos de los libros mayores cualificados.

No obstante, se precisa que, en el caso de los libros mayores cualificados, gozarán de la presunción de unicidad y autenticidad de los datos que contienen, de la exactitud de su fecha y hora y del orden cronológico secuencial interno,

12. *Vid.* apartado 7 del presente capítulo.

debiéndose para ello cumplir los requisitos establecidos en el artículo 45 *decies* de la Propuesta, esto es:

- estar creados por uno o más prestadores cualificados de servicios de confianza;
- garantizar la unicidad, autenticidad y correcta secuenciación de las entradas de datos grabadas;
- garantizar el orden cronológico secuencial correcto de los datos que contienen y la exactitud de la fecha y la hora de la entrada de datos;
- grabación de los datos de modo que sea posible detectar de forma inmediata cualquier modificación posterior de estos.

Como indica Alamillo¹³, aunque haya voces que aboguen por la desregulación de los libros mayores electrónicos, en mi opinión, por el origen de esta tecnología (principalmente me refiero a Bitcoin), que propugnaba el establecimiento de una moneda sin injerencias por parte del poder público, ninguna duda cabe de que el derecho debe regular este tipo de cuestiones para proporcionar seguridad jurídica a los usuarios, que, en definitiva, pueden ser ciudadanos, administraciones públicas o empresas, ya que esta tecnología tiene mucho que ofrecer al funcionamiento *ad intra* y *ad extra* del sector público.

3. La problemática en el sector público de la descentralización de nodos: ¿*blockchain* privada, pública o mixta para la Administración local?

Las soluciones basadas en *blockchain* son diversas, y en primer lugar, para su establecimiento, es necesario adoptar una primera decisión acerca de la utilización de sistemas públicos o privados, en función de si cualquier usuario de la red puede constituirse en nodo o si solo los “invitados” o que cumplen determinadas características pueden serlo.

En el primer caso, las *blockchain* públicas, son accesibles por cualquier usuario en red, de forma que puede acceder y verificar la información contenida en la red; este modelo es el seguido por la mayoría de las criptomonedas y *Ethereum*.

En el segundo caso, las *blockchain* privadas o permissionadas, son restringidas, esto es, no abiertas al público en general, y, por tanto, no todo

13. Alamillo Domingo (2021).

usuario en red puede acceder a las mismas, sino que debe hacerse mediante habilitación específica.

Por último, existen *blockchain* híbridas o mixtas, que combinan cadenas de bloques públicas y privadas, de forma que los nodos participantes son privados o permisionados, pero las cadenas de bloques (transacciones y operaciones realizadas en su seno) son visibles para cualquier usuario.

En el seno de las administraciones públicas, resulta imprescindible tener en cuenta que la información que se almacena es confidencial; específicamente, en la Administración local se encuentran el padrón municipal de habitantes y determinados datos personales en él contenidos, el registro contable, etc. En consecuencia, la elección del sistema *blockchain* a implantar debe tener en cuenta esta circunstancia, por lo que el sistema privado o permisionado contaría con los beneficios asociados a esta tecnología, al mismo tiempo que permitiría un efectivo control sin injerencias en las operaciones que en el seno de la misma se generen.

Teniendo en cuenta las diferencias existentes entre estos sistemas, como se ha examinado con anterioridad en esta obra, parece que las administraciones públicas podrían optar por un sistema *blockchain* basado en nodos permisionados (en determinados casos también híbridos), ya que entre sus características principales¹⁴ se encuentra que el acceso se realiza a través de claves generadas por la red (en lugar de ser generadas por los usuarios); el consenso de los participantes puede ser dinámico, según las necesidades de la Administración pública, para lo cual, por ejemplo, se podría hacer uso de la prueba de autoridad; para cualquier cambio en la red debe existir consenso entre los miembros de la red (si, por ejemplo, un total de doscientas administraciones públicas tiene que aceptar una modificación, es difícil que un posible fraude sea puesto en conocimiento del resto y menos probable que el resto lo acepte sin más), lo cual proporciona agilidad al mismo; y, especialmente, su velocidad, ya que las transacciones por segundo (tps) son muy superiores a las de las redes públicas.

Es por ello por lo que el propio Ibañez Jiménez¹⁵ expone que cuando las administraciones públicas dispongan de nodos interconectados y se haya proporcionado acceso a los funcionarios según sus competencias, minimizarán los costes de traslado de información tanto interna como interorgánica.

14. Para un excelente resumen comparativo de las características de las distintas *blockchains* (públicas y privadas) puede consultarse Ponce de León (2018: 73).

15. Ibañez Jiménez (2018: 176).

Por tanto, está reconociendo implícitamente la necesidad de que el sistema *blockchain* que se implante sea de naturaleza permitida, lo cual está en línea con lo aquí defendido.

Dos son las soluciones posibles en cuanto al establecimiento de nodos: como se ha comentado anteriormente, de manera que cada Administración pública actúe como nodo interconectado al resto, o bien haciendo que múltiples funcionarios de la propia Administración tengan competencia para actuar como nodos de la red. Esta última opción sería la que proporcionaría más rapidez a las transacciones, pero ofrecería menos garantías, en tanto en cuanto, como se ha apuntado anteriormente, la mayor seguridad que ofrece el sistema es la descentralización, y si con un sistema permitido se reduce, con uno de este tipo y además vinculado en su totalidad a miembros de una sola Administración pública se podría desvirtuar absolutamente el sistema, por lo que abogaría por la primera opción, que en este caso resultaría más adecuada.

4. El procedimiento administrativo como paradigma de aplicación de la tecnología *blockchain* en actuaciones y trámites susceptibles de automatización (*smart procedure*)

Uno de los ámbitos más interesantes para la aplicación de *blockchain* es el procedimiento administrativo, ya que existen multitud de trámites susceptibles de automatización, y, al igual que los *smart contracts* basados en esta tecnología son capaces de activar cláusulas determinadas de manera automática cuando se cumplen determinadas condiciones, también se pueden automatizar determinados trámites o actuaciones durante la sustanciación del procedimiento.

Me refiero a la petición de informes, a la formación del propio expediente administrativo o a la apertura de los trámites de audiencia e información pública y, en definitiva, todo trámite susceptible de automatización cumplida una determinada condición que, en este caso, se encontrará sujeta a los trámites procedimentales concretos del procedimiento administrativo que corresponda, según establezca cada gestor procedimental de la Administración pública de que se trate para cada procedimiento.

Y es que el artículo 41 LRJSP aboga por la automatización al regular la actividad administrativa automatizada, definiéndola como cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración pública en el marco de un procedimiento administrativo y en la

que no haya intervenido de forma directa un empleado público. En relación con el ejercicio de la actividad administrativa automatizada debe tenerse en cuenta en el ámbito local que el artículo 13.3 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos (RAE, en adelante), dispone que habrá de estarse a lo dispuesto en la disposición adicional octava del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración local con habilitación de carácter nacional, en cuya virtud, y a los efectos del ejercicio en soporte electrónico de las funciones reservadas a los funcionarios regulados en dicha norma, los puestos a ellos reservados tendrán la consideración de órganos, sin perjuicio de lo dispuesto en el Título X de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

En este sentido, existen grandes posibilidades de relación entre la actividad administrativa automatizada y la tecnología *blockchain*, en tanto en cuanto muchos trámites sujetos a automatismos en la sustanciación del procedimiento administrativo pueden ser gestionados a través de redes de registro distribuido.

Se ha hecho referencia anteriormente a los *smart contracts*, que suponen la existencia en una red *blockchain* (cadena de bloques) de un programa o contrato que se ejecuta automáticamente cuando se cumplen determinadas condiciones, de forma que todas las partes de dicho contrato tienen conocimiento inmediato del cumplimiento de la condición que corresponda sin la necesidad de que intervenga un tercero y valide la operación. Hay diversas plataformas basadas en DLT (tecnologías de registro distribuido de las que, como se ha visto anteriormente, *blockchain* es una tipología concreta) que han desarrollado *smart contracts* en profundidad, tales como *Ethereum* o *Hyperledger*, entre otras, con resultados plenamente satisfactorios.

Aplicando al procedimiento administrativo esta conceptualización, podría utilizarse en diversas fases y trámites de este, ya que normalmente el impulso de oficio del procedimiento administrativo *ex* artículo 71 LPAC se manifiesta en el paso de una fase a otra tras la incorporación, por ejemplo, de un informe preceptivo al procedimiento. Una vez que el informe requerido entra en la red *blockchain*, se incorporaría al procedimiento administrativo y, al cumplirse la condición (la recepción del informe), daría lugar al paso a la siguiente fase sin la intervención humana correspondiente, tal y como se lleva a cabo en diversas administraciones públicas en la actualidad mediante gestores de procedimiento administrativo, pero de forma mucho más rápida

y segura, en tanto en cuanto no existiría riesgo de pérdida de información, ya que existirían réplicas de la información en cada nodo.

Esta automatización inteligente e integrada sería replicable en todas aquellas actuaciones de impulso del procedimiento administrativo, dando lugar a un verdadero procedimiento con trámites autoejecutables o *smart procedure* que podría incrementar la eficiencia en la actuación administrativa, reduciendo así la intervención humana en aquellas tareas meramente mecánicas y reservando la intervención humana cualificada para aquellos trámites o actuaciones que verdaderamente lo requieren, lo cual es un problema que se da en muchas administraciones públicas.

5. El uso de *blockchain* como registro electrónico en general, y de apoderamientos en particular

La función registral, siguiendo a Meilán¹⁶, es una función del Estado manifestada en la existencia de registros que se refieren a variados aspectos y sectores de la vida humana que, según su tipología, operan en el ámbito del tráfico jurídico-privado o en el “ámbito o giro” de las administraciones públicas, en relación con su actuación y especialmente en su relación con los ciudadanos. En este sentido, existen múltiples registros referidos a personas, como el registro de empresas clasificadas en materia de contratación pública y el padrón municipal de habitantes; o a bienes, como el registro de aguas, de vehículos, el catálogo de montes, o los inventarios en materia de patrimonio histórico, por lo que ninguna duda cabe de su relevancia y utilidad públicas.

Y, por supuesto, los tradicionales registros públicos de los que, conforme al artículo 16.1 LPAC, toda Administración pública tiene el deber de disponer para efectuar el correspondiente asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, organismo público o entidad vinculada o dependiente de estos, que deberán ser electrónicos preceptivamente (sin perjuicio de la creación de una Oficina de Asistencia en Materia de Registros para que las personas no obligadas a relacionarse electrónicamente con la Administración puedan seguir realizando sus trámites físicamente, pero que en la práctica supondrá la necesaria incorporación de lo allí presentado en el sistema electrónico de gestión documental interna),

16. Meilán Gil (2010: 527).

pudiéndose también anotar en los mismos las salidas de los documentos oficiales dirigidos a otros órganos o particulares.

Una de las principales funcionalidades que puede proporcionar la tecnología *blockchain* en el ámbito de las administraciones públicas es la de servir de base tecnológica para las funciones de registro, de forma que ya no solo se emplease como registro electrónico general al que se refiere el párrafo anterior, sino que, por ejemplo, pudiese probarse frente a terceros la efectiva inscripción registral de un vehículo por haberse transmitido su titularidad o la efectiva inscripción de un ciudadano en el padrón municipal de habitantes. Esto, en un estadio avanzado de su implantación, siguiendo el ejemplo de Preukschat¹⁷ con otro tipo de bienes, permitiría que el fabricante inscribiese el activo (el vehículo) en la red *blockchain* y, una vez enviado al concesionario, inscribir la transmisión, y hacerlo nuevamente cuando un particular lo adquiriera, pudiendo incluso este último arrendar los vehículos si se dedicase a ello a través de un *smart contract* cuyo objeto sea la cesión del derecho de uso durante un tiempo determinado, dejando prueba de toda la cadena de adquisiciones y cesiones del vehículo. La misma operativa, pero en este caso incluso más sencilla, sería la inscripción de un ciudadano en el registro del padrón municipal de habitantes, de forma que, una vez inscrito, si modificase posteriormente su domicilio, pudiese inscribirse en su nueva ubicación y quedase además prueba de la cadena de inscripciones anterior, lo cual permitiría adicionalmente detectar actuaciones fraudulentas en este tipo de inscripciones, habituales en la práctica para la obtención de ayudas y subvenciones que exigen el empadronamiento en un municipio determinado para adquirir la condición de beneficiario, por cualquier Administración interesada en ello. Como puede vaticinarse, esto proporciona grandes utilidades a esta tecnología aplicable a diferentes ámbitos, especialmente en nuestra especialidad, ya que la seguridad jurídica que ofrecen los registros públicos es indudable y, gracias a esta tecnología, se puede incrementar la fiabilidad del sistema.

Sin embargo, se encuentra con una problemática importante, en tanto en cuanto *blockchain* no almacena el documento de la transacción de que se trate, sino que esta tecnología lo que almacena es el *hash* resultante de aplicar el algoritmo correspondiente al documento de transmisión, de forma que posteriormente se puede comprobar que el mismo no ha sido modificado (comparando el código *hash* registrado y el obtenido nuevamente del documento en cuestión).

17. Preukschat (2017: 125-126).

Y es que además, como señala Boldó Roda¹⁸, se podría incluir tanto un acto administrativo válido como uno que adolezca de nulidad absoluta¹⁹, puesto que el sistema no verificará los requisitos del acto administrativo en cuestión, sino que simplemente acreditará que dicho documento quedó registrado en un instante determinado en la red; esto es, que la transacción existió en ese momento, pero nada acredita en relación con la adecuación a derecho de su contenido concreto, o de la competencia del órgano que dicta el acto, por ejemplo, cuestiones que escapan a esta tecnología.

No obstante, lo mismo ocurre con un registro electrónico ordinario, ya que, conforme al apartado 1 del artículo 16 LPAC, en el mismo se practica asiento de todo documento presentado o recibido, anotándose igualmente la salida de documentos oficiales dirigidos a otros órganos o a particulares, respetando en todo caso el orden temporal de recepción o salida (apartado 2), emitiéndose automáticamente un recibo consistente en copia autenticada del documento que incluya hora y fecha de presentación, así como recibo acreditativo de otros que lo acompañen con garantía de integridad y no repudio (apartado 3).

Igualmente, debe recordarse en este punto que la red *blockchain* no debe almacenar todos los documentos y datos como si de un dispositivo de almacenamiento masivo se tratase, y este es un aspecto muy relevante para la comprensión de esta tecnología, sino que como prueba de la existencia de datos y documentos se hace uso de la huella digital o electrónica de los mismos. Un ejemplo de este aspecto se encuentra en la posibilidad regulada en la disposición adicional decimosexta LCSP de enviar una huella electrónica de la oferta para posteriormente enviar la oferta completa, definiéndose aquella como un conjunto de datos cuyo proceso de generación garantiza que se relacionan de manera inequívoca con el contenido de la oferta propiamente dicha, y que permiten detectar *a posteriori* posibles alteraciones del contenido de esta, garantizando así su integridad.

Para suplir dicha carencia, tal y como aboga Tur Fáundez²⁰, habría de recurrirse a otros protocolos de consenso que permitiesen cierto almacenamiento en la cadena de bloques, al menos de forma que pueda probarse la existencia real del documento, lo cual cumplirían, por ejemplo,

18. Boldó Roda (2018: 130).

19. Para un estudio exhaustivo de los supuestos de invalidez que pueden darse en Derecho Administrativo puede consultarse mi obra en Berning Prieto (2019).

20. Tur Fáundez (2018: 47).

los protocolos *Proof of Existence* u otros similares como *Stampery* u *OpenTimeStamps*, que permitirían:

- garantizar la inmutabilidad del documento, ya que una vez anclado el código *hash* del documento -resultante de aplicar un algoritmo matemático al mismo- a la cadena de bloques, no puede modificarse sin que se pueda advertir la manipulación por cualquier usuario del sistema que lo compruebe;
- garantizar el momento exacto en que ha sido incorporado a la cadena de bloques, gracias al sellado de tiempo o *time stamping*;
- garantizar su propia existencia, gracias a las múltiples réplicas que en los distintos nodos se almacenarían.

No obstante, como se apuntaba anteriormente, no será posible almacenar todos los documentos íntegramente, ya que los costes de transacción serían desorbitados, pero sí su código *hash*, como se apuntaba, que es único para el documento del que se obtiene, y cuya manipulación es imposible sin ser detectada.

Pues bien, un sistema *blockchain* puede cumplir perfectamente todas las condiciones necesarias para servir de registro público, por lo que su implantación para esta funcionalidad sería una alternativa que permitiría, además, ser más resistente a ataques de terceros o a pérdida de información por fallos del sistema, puesto que, si la misma información recogida en un determinado bloque se encuentra replicada en diversos nodos, difícilmente la pérdida de uno de ellos por cualquier motivo daría lugar a la pérdida de información, pues la cadena recuperaría el bloque de cualquier nodo y continuaría formando la secuencia o el encadenamiento de nodos. Ello obligaría a almacenar también los documentos, evidentemente, en lugar distinto a la red distribuida, por lo que funcionarían paralelamente el registro en la red *blockchain* y el almacenamiento íntegro de los documentos registrados, de forma que en cualquier momento se pueda verificar una determinada presentación o inscripción registral mediante la comparación del *hash* del documento original almacenado y el que conste en los nodos de la red.

Otro tipo de registros públicos, como el Registro de la Propiedad o el Mercantil, se toparían con un inconveniente adicional, y es que es un tercero independiente (el registrador) quien dota de control jurídico y garantías a lo inscrito y que, además, ha sido previamente verificado y autorizado por un notario (sistema de doble garantía), el cual comprueba previamente a su inscripción que la operación resulta ajustada a derecho; en estos casos no se trata de que *blockchain* sustituya al registrador, pero sería posible que

este, una vez efectuados los controles procedentes, efectuase la inscripción correspondiente en la red *blockchain*, aunque algún autor²¹ no se muestra muy halagüeño con esta posibilidad.

Autores como Ibáñez Jiménez²² apuntan las posibilidades que en materia registral tiene la tecnología *blockchain*, si bien serían “*blockchains* registrales internas”; y es que no debe olvidarse que uno de los principales caracteres que tiene esta tecnología y que la hacen tan polivalente es precisamente su capacidad de implantación en prácticamente cualquier entorno, con las debidas adaptaciones según las funcionalidades a utilizar. Y, en este sentido, el autor cita varias aplicaciones en materia registral, a saber:

- posibilidad de comunicación de datos entre registros centrales y periféricos;
- intercambio de datos con terceras partes, incluidos órganos jurisdiccionales o notarios;
- práctica de asientos registrales de presentación automática;
- uso y control de identidades digitales de personas físicas o jurídicas;
- prueba y verificación imparciales de hechos o documentos;
- incorporación de nuevos servicios registrales, como bases de datos, servicios estadísticos, de situación de bienes registrados o de identificación de bienes muebles.

Estas nuevas funcionalidades proporcionan grandes posibilidades a esta tecnología, ya que permiten incrementar exponencialmente los supuestos de uso de la misma, a la vez que incrementan la seguridad jurídica de la información que accede a la red, adquiriendo así un potencial prácticamente ilimitado.

En este sentido, a la vista de los beneficios que podría reportar, ninguna duda cabe de que podría utilizarse la tecnología *blockchain* también para el registro electrónico de apoderamientos regulado en el artículo 6 LPAC. Este aspecto entra en íntima conexión con la utilización de *blockchain* para la identidad autosoberana (que se examinará en el siguiente apartado del presente capítulo), ya que ambos podrían complementarse en la práctica de forma muy beneficiosa. Por tanto, la implantación de un registro electrónico de apoderamientos con base en tecnología *blockchain* no plantearía problema alguno, como se ha expuesto anteriormente para los registros electrónicos en general.

21. Perete Ramírez (2018: 197).

22. Ibáñez Jiménez (2018: 177).

Pero, es más, es bien sabido que el artículo 5 LPAC regula la representación en el procedimiento administrativo y, en su virtud, la misma puede acreditarse por cualquier medio válido en derecho que deje constancia fidedigna de su existencia y, por tanto, no existe ningún obstáculo para que no solo el registro electrónico de apoderamientos se base en dicha tecnología, sino que el propio acto de apoderamiento se efectúe en favor de un tercero haciendo uso también de la misma.

Así, dado que mediante *blockchain* se pueden acreditar y verificar atributos de una persona, podría acreditarse de forma fehaciente que un tercero posee el atributo de representar a otra, representación que además ha sido otorgada a través de una red *blockchain*. Como puede apreciarse, las posibilidades de esta tecnología son prácticamente infinitas, ya que no solo permite el establecimiento de un registro electrónico de apoderamientos en la red, sino también la acreditación de la identidad del representante y la verificación de su condición (atributo) como tal que ha sido conferida por cualquier persona (representado).

6. La contabilidad o llevanza de libros contables en entidades locales como posible aplicación de *blockchain*

En el ámbito local la llevanza de libros contables es una de las principales finalidades para las que podría implementarse la tecnología *blockchain*, dado que se proporcionaría un grado de seguridad muy elevado a las cuentas municipales.

La regulación de esta cuestión en el ámbito local parte del Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales, que dispone un título VI para regular el “presupuesto y gasto público”, y en su seno un capítulo III, “de la contabilidad”, estableciéndose en el artículo 203.1 lo siguiente:

“Corresponderá al Ministerio de Hacienda a propuesta de la Intervención General de la Administración del Estado:

a) Aprobar las normas contables de carácter general a las que tendrá que ajustarse la organización de la contabilidad de los entes locales y sus organismos autónomos.

b) Aprobar el Plan General de Cuentas para las entidades locales, conforme al Plan General de Contabilidad Pública.

- c) Establecer los libros que, como regla general y con carácter obligatorio, deban llevarse.
- d) Determinar la estructura y justificación de las cuentas, estados y demás documentos relativos a la contabilidad pública”.

A dicha exigencia normativa responde la Orden HAP/1781/2013, de 20 de septiembre, por la que se aprueba la Instrucción del modelo normal de contabilidad local, la cual, con relación al “soporte de los registros contables”, dispone que “las bases de datos del sistema informático donde residan los registros contables constituirán soporte suficiente para la llevanza de la contabilidad de la entidad contable, sin que sea obligatoria la obtención y conservación de libros de contabilidad en papel o por medios electrónicos, informáticos o telemáticos”.

Esta previsión normativa, como ya ha apuntado algún autor como Alamillo²³, permitiría la utilización de *blockchain* como sistema contable de registro distribuido, de forma que los asientos vayan accediendo a la cadena de bloques y replicándose en los distintos nodos, garantizando así su inalterabilidad y confiriendo una elevada seguridad al sistema, ya que se evitaría así que cualquier amenaza externa (virus, troyanos...) pudiese comprometer la certeza y veracidad de la llevanza contable de la entidad local.

Evidentemente *blockchain* no entraría a valorar el contenido de los asientos contables, al igual que ocurre en el soporte papel, sino que garantiza que un determinado asiento se ha llevado a cabo en un momento determinado.

Por tanto, dado que la normativa contempla de forma suficientemente amplia la posibilidad de utilizar un soporte electrónico para la llevanza de los libros de contabilidad, sería incluso aconsejable su implantación a corto o medio plazo, ya que se podría llevar la contabilidad a través de bases de datos seguras basadas en *blockchain* y ello proporcionaría una elevada fiabilidad al sistema, de forma que un tercero no podría acceder a alterar la contabilidad pública y, de darse el caso, existirían réplicas de la información fácilmente recuperables.

A mayor abundamiento, el uso de esta tecnología para la llevanza contable proporcionaría al sistema un elevado grado de transparencia, al conferir la certeza de veracidad de lo que en el registro distribuido consta,

23. Alamillo Domingo (2020: 250).

impulsando así los principios establecidos por la legislación vigente en materia de transparencia y fomentando así la participación ciudadana en asuntos públicos, como se verá en otro capítulo de la presente obra, e incrementando la confianza de los ciudadanos en relación con la llevanza de las cuentas públicas municipales.

7. Identidad digital basada en *blockchain*. Especial referencia a la identidad autosoberana regulada en el Proyecto europeo “ReIDAS-2” para el establecimiento de una identidad digital europea o eID y su aplicación a las entidades locales

La identificación de los ciudadanos ha sido una competencia tradicionalmente centralizada, siendo el propio Estado garante de gestionar la identidad de los ciudadanos a efectos de conseguir un efectivo control de la seguridad pública. Sin embargo, es una realidad que, como apunta Pérez Bes²⁴, esta estructura de control centralizado llega a quebrar en el mundo digital, llegando el usuario a controlar sus identidades e incluso pudiendo tener más de una identidad para usar diversos servicios ofrecidos *online*, lo cual, como se puede advertir, no está exento de riesgos.

La introducción de *blockchain* en escena puede llegar a reducir tales riesgos hasta el punto de eliminarlos casi por completo, ya que permitiría un control del individuo sobre su identidad, pero confiando en la red para garantizar su veracidad, de manera que incluso la propia Administración (central, autonómica o local) podría disponer de una red *blockchain* para hacer uso de la cadena de bloques ante la que previamente el usuario ha acreditado su identidad, para aceptarla si se comprueba un nivel aceptable de confianza del garante de dicha identidad.

Y es que la utilización de *blockchain* para proveer de identidad digital a los ciudadanos es una de las novedades más interesantes que puede proporcionar esta tecnología, pues, hasta ahora, la prestación de servicios de identificación o firma electrónica se encuentra confiada a terceros, que siempre deben intervenir para la acreditación de la identidad de cualquier persona, física o jurídica. La identidad autogestionada es, siguiendo la definición de Alamillo²⁵, aquella creada y gestionada por cada individuo, sin la intervención de terceros, y que goza de determinadas características, a saber:

24. Pérez Bes (2018: 158).

25. Alamillo Domingo (2020: 252-253).

- identidad del individuo sin intervención de terceros,
- control por parte del individuo de su identidad digital,
- acceso del individuo a todos sus datos,
- transparencia de los sistemas y algoritmos,
- persistencia y portabilidad de las identidades digitales,
- interoperabilidad,
- economía de datos,
- protección de los derechos de la persona.

Siguiendo al citado autor, gracias a esta tecnología el usuario puede obtener testimonios de datos de identidad que son producidos por entidades verificadoras, y que pueden ser presentados a cualquier entidad (cualquier Administración pública, por ejemplo, como las entidades locales) sin necesidad de intervención externa, ya que la identidad y el resto de atributos de la persona han sido enlazados en la red de nodos de forma que se pueden comprobar por parte de la citada entidad directamente de la red *blockchain* donde se encuentran almacenados en algún bloque, sin necesidad de intervención de tercero alguno.

El mayor impedimento normativo a la utilización de esta tecnología se encuentra en el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Previamente a su entrada en vigor, los artículos 9 y 10 de la LPAC eran lo suficientemente amplios y neutrales tecnológicamente como para que *blockchain* hubiese tenido cabida a la hora de identificarse y firmar electrónicamente ante la Administración. Sin embargo, la citada norma vino a modificar dichos preceptos y, en este sentido, establece la obligatoriedad, en caso de pretender adoptar la Administración “cualquier otro sistema, que las administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad”, de solicitar autorización previa de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, regulación que se reproduce en el artículo 15.3.a) RAE.

Dicha autorización debe expedirse en el plazo de tres meses, pudiendo ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior, siendo el sentido del silencio administrativo desestimatorio.

Dicha limitación de “los sistemas que sean distintos a aquellos del certificado y sello electrónico” se fundamenta, siguiendo el preámbulo de la norma, en “verificar si el sistema validado tecnológicamente por parte de la Administración u organismo público de que se trate puede o no producir afecciones o riesgos a la seguridad pública”.

Pero, es más, concretamente para el uso de *blockchain* se introdujo una disposición adicional sexta en la LPAC que prohíbe temporalmente, mediante el establecimiento de la imposibilidad de obtener autorización para ello, el uso de sistemas de registro distribuido a los efectos de identificación y firma de los ciudadanos ante las administraciones públicas, en tanto en cuanto no sean objeto de desarrollo normativo estatal sobre la base del derecho de la Unión Europea que se apruebe. Además, prevé que, en cualquier caso, en cualquier sistema de identificación basado en tecnología de registro distribuido, la Administración General del Estado actuará como autoridad intermedia y ejercerá las funciones que corresponda para garantizar la seguridad pública. Como puede apreciarse, en la actualidad existe una clara prohibición del uso de esta tecnología a los efectos de identificación y firma en el seno de un procedimiento administrativo.

Ello no impide que se utilice en la actualidad esta tecnología en el seno de las administraciones públicas para diversas finalidades distintas, como ha sido tratado en epígrafes anteriores, sino que la prohibición se encuentra limitada a las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de la LPAC; por tanto, el personal al servicio de la Administración sí podría teóricamente identificarse y firmar haciendo uso de sistemas de registro distribuido, al no haberse previsto la misma prohibición para dicho colectivo en la LRJSP, sino únicamente referida a los interesados en el procedimiento administrativo.

Por tanto, los procedimientos o servicios basados en tecnologías de registro distribuido no podrán hacer uso, a su vez, de sistemas de identificación o firma basados en las mismas, pero sí podrán emplear, como aprecia Alamillo²⁶, certificados cualificados, DNI-e o cualquier sistema admitido como Cl@ve, por lo que su uso en el establecimiento de nuevas fórmulas de gestión administrativa es posible.

De hecho, los recientes y prolíferos trabajos de la *European Blockchain Partnership* (EBP), creada en 2018 por la Comisión Europea (con comienzo

26. Alamillo Domingo (2020: 273).

de actuaciones en 2019 con la *Telecommunications Work Facility* del programa *Connecting Europe Facility* -CEF-), han dado como resultado el establecimiento en 2020 de la *European Blockchain Services Infrastructure* (EBSI), que pretende establecer una red de nodos en todos los Estados miembros participantes, y que en España está representada por la Secretaría General de Administración Digital²⁷, dando comienzo en 2021 el *Digital Europe Programme*, en virtud del cual ya están comenzando a introducirse casos de uso reales para incrementar los servicios públicos digitales²⁸ europeos.

En este sentido, la Propuesta ReIDAS-2 citada anteriormente apuesta por la identidad digital autosoberana o SSI²⁹ con un alto nivel de confianza a nivel europeo.

Como apunta Alamillo³⁰, la Propuesta incluye el establecimiento de la obligación de los Estados miembros de emitir a las personas físicas y jurídicas una Cartera de Identidad Digital Europea (*European Digital Identity Wallet*), de forma que permita al usuario almacenar datos de identidad, credenciales y atributos vinculados a su identidad, proporcionarlos a las partes en que confían cuando lo soliciten, pudiendo utilizarlos para la autenticación en línea o fuera de línea, y crear sellos y firmas electrónicas cualificadas, pudiendo la misma ser emitida directamente por el Estado, por mandato de este o por entidades públicas o privadas reconocidas por el mismo, lo cual, a juicio del autor, “permitiría desarrollar un mercado con operadores privados que ejercen potestades administrativas en régimen de competencia [...] y constituiría una fórmula de política industrial muy conveniente”. Gracias a este sistema el ciudadano tendría pleno control de su identidad y atributos (gracias, por su parte, a la regulación de un nuevo servicio de confianza de certificación electrónica de atributos de identidad cuyo certificado expedido tendría la misma validez que en soporte papel y que permitiría probar un dato en lugar de aportarlo), de sus datos, en definitiva, y podría compartírselos con terceros en función de sus necesidades, de forma voluntaria. Además, según establece el artículo 12.b de la Propuesta, las entidades del sector público que establezcan

27. Los representantes de cada Estado pueden consultarse en la dirección web: <https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/List+of+EBP+representatives> (última consulta efectuada el 30 de septiembre de 2021).

28. Los servicios públicos digitales son medidos a nivel europeo gracias a un indicador específico que mide el grado de interacción entre empresas o ciudadanos y administraciones públicas, haciendo uso de las ventajas que ofrece la tecnología; sobre el particular, puede verse Berning Prieto (2017: 21).

29. Por sus siglas en inglés: *Self-Sovereign Identity*.

30. Alamillo Domingo (2021).

la obligación de identificarse electrónicamente deberán admitir la Cartera de Identidad Digital Europea como medio de identificación electrónica, por lo que de aprobarse la misma sería un claro avance en gestión de la identidad digital autogestionada o autosoberana.

8. *Blockchain* como posible forma de garantizar la fiabilidad del voto electrónico y la participación ciudadana en el ámbito local (remisión)

Estrechamente relacionada con la identidad digital autosoberana examinada en el apartado anterior se encuentra la posibilidad de emitir válidamente un voto electrónico haciendo uso de la tecnología *blockchain*, así como promover la participación ciudadana en la Administración local.

Hay diversas iniciativas en nuestro país que están intentando poner en práctica esta tecnología al servicio del voto electrónico o la participación ciudadana, de forma, por ejemplo, que una votación contenga el listado público de los votantes que han participado y que, una vez registrado un votante, pueda insertar un voto privado y anónimo con la opción deseada, de manera que no exista relación entre los votantes, y siendo por tanto los votos emitidos anónimos; o para la elaboración de presupuestos participativos con presentación por parte de los ciudadanos de propuestas en una plataforma pública; iniciativas basadas en *blockchain* que resultan sin duda interesantes para su extensión a nuevas áreas de aplicación de esta tecnología aún sin explorar.

No obstante, dado que el tratamiento de esta cuestión es objeto de estudio exhaustivo en otro capítulo de la presente obra, debemos remitirnos al mismo para el estudio de la misma.

9. Breve referencia al posible uso de *blockchain* en los convenios interadministrativos (*smart public agreements*)

La unilateralidad que rige en Derecho Administrativo, como apunta Toscano Gil³¹, es superada únicamente en dos supuestos: los contratos y los convenios administrativos, que se caracterizan por la bilateralidad y la voluntariedad. Los contratos administrativos se regulan por la normativa específica vigente en esta materia, actualmente la Ley 9/2017, de Contratos del Sector Público,

31. Toscano Gil (2017).

mientras que los convenios administrativos se rigen fundamentalmente por la LRJSP, concretamente en sus artículos 47 a 53 (a excepción de los convenios celebrados como forma de terminación de un procedimiento administrativo, que se regulan en el artículo 86 LPAC).

Como ya se ha comentado anteriormente, ya se han puesto en marcha determinados proyectos en materia de contratación pública basados en *blockchain*, con especial aplicación en *smart contracts* o contratos inteligentes, que de esta forma se pueden autogestionar (sin necesidad de intervención de terceros de confianza) a partir de determinadas condiciones que, una vez cumplidas, hacen que se ponga en marcha el mecanismo contractual previamente configurado.

Sin embargo, resta por explorar la posibilidad de la aplicación de *blockchain* a los convenios administrativos, ya que podría suponer una ventaja a la hora de su ejecución, del mismo modo que se lleva a cabo en determinados contratos públicos.

Los convenios administrativos se caracterizan por ser un acuerdo de voluntades de carácter vinculante entre las partes, de las que al menos una de ellas es una Administración pública, precisando Bustillo Bolado³² que con una finalidad distinta a la mera satisfacción de sus necesidades clientelares con bienes y servicios ofrecidos por profesionales y empresarios.

Pues bien, gracias a la tecnología *blockchain* podría incrementarse la eficiencia en la gestión de estos convenios, ya que del mismo modo que los contratos pueden autoejecutarse, los convenios también, en función de determinadas cláusulas cuyo cumplimiento pueda verificarse automáticamente. De este modo, teniendo en cuenta que la tradicional finalidad de los convenios interadministrativos es coordinar las actuaciones de la pluralidad de actores públicos que suelen concurrir, cada uno con sus respectivas competencias, sobre un mismo territorio, cuando uno de dichos actores o sujetos parte del convenio cumple una determinada condición contemplada previamente en el mismo, dicho cumplimiento operaría como detonador para que una consecuencia jurídica también prevista en aquel entre en juego y se desplieguen sus efectos, de forma automática e inteligente.

La puesta en marcha de esta tecnología en la ejecución de los convenios interadministrativos, por tanto, podría dar lugar a múltiples funcionalidades,

32. Bustillo Bolado (2017: 1059).

ya que a muchas de las situaciones derivadas de su ejecución les serían de aplicación, y los beneficios que están detectándose en la proliferación de los *smart contracts* basados en una DLT como *blockchain* en el ámbito jurídico-público se verificarían de este modo también.

10. Conclusiones

Blockchain es una tecnología innovadora que sin duda puede proporcionar grandes beneficios al sector público y a la innovación, ya que sus posibilidades son prácticamente inabarcables y se irá extendiendo en un futuro a ámbitos inexplorados en la actualidad.

Sin embargo, no todos los aspectos relativos a *blockchain* son positivos, ya que existen algunas cuestiones que deben ser objeto de examen y mejora, como la incidencia de *blockchain* en el medio ambiente. El elevado consumo energético para la resolución de algoritmos por parte de los nodos integrantes en el sistema supone un elevado coste medioambiental que debe medirse bien para asegurar que existe un equilibrio entre los pros y los contras de esta tecnología. Quizás más que cuestionar esta tecnología sería más inteligente propiciar la inversión en fuentes de energía renovable, para que la energía a consumir sea generada utilizando fuentes con escaso impacto en el medio ambiente. No obstante, en la situación actual, en la que aún las fuentes de energía disponibles no son renovables en un alto porcentaje³³, debe examinarse esta cuestión con cautela.

Existen también dificultades relativas a la capacidad (y dificultad) de implantación en las administraciones públicas de los nodos que reproduzcan cientos de transacciones diarias, y la consiguiente capacidad de almacenamiento requerido a tal fin para replicar la información, que requerirá una alta inversión inicial para su puesta en marcha.

Sin embargo, los beneficios que a medio y largo plazo puede reportar *blockchain* merecen detenerse a examinar todas estas cuestiones y darles una solución para garantizar su viabilidad de la forma más equilibrada posible,

33. Puede consultarse el porcentaje de generación eléctrica en España según la fuente energética empleada en la web oficial de Red Eléctrica de España: <https://www.ree.es/es/datos/generacion/estructura-generacion> (última consulta efectuada el 15 de octubre de 2021), en la que se aprecia que la generación de electricidad gracias a fuentes renovables no llega al 40 %.

puesto que la innovación en el sector público es imprescindible en aras de un incremento de su eficiencia y eficacia, a la vez que elevaría la confianza del ciudadano en su actuación.

A mayor abundamiento, de acuerdo con el derecho reconocido por el artículo 53.1.h) LPAC a los interesados en el procedimiento administrativo a cumplir las obligaciones de pago a través de los medios electrónicos previstos en el artículo 98.2 de la citada Ley, ninguna duda cabe de que sería interesante, una vez se regule convenientemente en un futuro próximo³⁴, que las administraciones públicas pudiesen admitir medios de pago basados en tecnologías de registro distribuido, lo cual permitiría, entre otros, el pago de tasas o precios públicos de forma sencilla sea cual sea el medio de pago de que disponga el ciudadano, incluyendo el euro digital o bitc in, entre otros.

Todo ello, con el fin de estar dotadas de los medios conforme al estado actual de la ciencia y la t cnica y, as , conseguir la mayor eficacia en su actuaci n, exigencia derivada del propio art culo 103.1 de la Constituci n Espa ola.

11. Bibliograf a

Alamillo Domingo, I. (2020). R gimen jur dico de la administraci n digital: aspectos tecnol gicos, plataformas y servicios de intermediaci n. En I. Mart n Delgado (dir.). *El procedimiento administrativo y el r gimen jur dico de la Administraci n p blica desde la perspectiva de la innovaci n tecnol gica*. Madrid: Iustel.

– (2021). La propuesta de Reglamento eIDAS 2: la identidad digital autosoberana y la regulaci n de *Blockchain*. *Diario La Ley*, 22/06/2021.

Berning Prieto, A. D. (2017). La administraci n electr nica y los servicios p blicos digitales al albor de los progresos de la Uni n Europea y el “Horizonte Europa 2020”. Su relaci n con las leyes 39/2015, de Procedimiento Administrativo Com n de las Administraciones P blicas y 40/2015, de R gimen Jur dico del Sector P blico. En I. Mart n Delgado (dir.). *La reforma de la administraci n electr nica: Una oportunidad para la innovaci n desde el Derecho*. Madrid: Instituto Nacional de Administraci n P blica.

34. En la actualidad la Uni n Europea est  trabajando en la regulaci n de activos digitales, incluidos los basados en tecnolog as de registro distribuido, como se puede examinar en la direcci n web: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain> ( ltima consulta efectuada el 30/09/2021).

- (2019). *Validez e invalidez de los actos administrativos en soporte electrónico*. Cizur Menor (Navarra): Thomson-Reuters-Aranzadi.

- Boldó Roda, C. (2018). *Blockchain* como registro. La experiencia *namecoin* y los nombres de dominio. En R. Vilarroig Moya y C. Pastor Sempere (dirs.). *Blockchain: aspectos tecnológicos, empresariales y legales*. Cizur Menor (Navarra): Thomson-Reuters-Aranzadi.

- Bustillo Bolado, R. O. (2017). Los convenios. En E. Gamero Casado (dir.). *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público* (tomo I). Valencia: Tirant lo Blanch.

- Gamero Casado, E. (2009). Interoperabilidad y administración electrónica: conéctense, por favor. *Revista de Administración Pública*, 179.

- Gamero Casado, E. y Fernández Ramos, S. (2020). *Manual básico de Derecho Administrativo*. Madrid: Tecnos.

- Gamero Casado, E. y Martínez Gutiérrez, R. (2010). El Derecho Administrativo ante la Era de la Información. En E. Gamero Casado y J. Valero Torrijos (dirs.). *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*. Cizur Menor (Navarra): Thomson-Reuters-Aranzadi.

- Huergo Lora, A. (dir.) y Díaz González, G. M. (coord.). (2020). *La regulación de los algoritmos*. Cizur Menor (Navarra): Thomson-Reuters-Aranzadi.

- Ibáñez Jiménez, J. W. (2018). *Blockchain: primeras cuestiones en el ordenamiento español*. Madrid: Dykinson.

- Meilán Gil, J. L. (2010). Administración pública y función registral. *Anuario da Facultade de Dereito da Universidade da Coruña*, 14.

- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

- Perete Ramírez, C. (2018). *Blockchain*, privacidad y protección de datos de carácter personal. En P. García Mexía (dir.). *Criptoderecho. La regulación de Blockchain*. Madrid: Wolters Kluwer.

- Pérez Bes, F. (2018). Identidad y *blockchain*. En P. García Mexía (dir.). *Criptoderecho. La regulación de Blockchain*. Madrid: Wolters Kluwer.

- Ponce de León, P. J. (2018). *Blockchain, un nuevo patrón tecnológico*. En R. Vilarroig Moya y C. Pastor Sempere (dirs.). *Blockchain: aspectos tecnológicos, empresariales y legales*. Cizur Menor (Navarra): Thomson-Reuters-Aranzadi.
- Preukschat, A. (2017). *La revolución industrial de internet*. Barcelona: Gestión 2000.
- Tapscott, D. y Tapscott, A. (2017). *La revolución blockchain*. Barcelona: Deusto.
- Toscano Gil, F. (2017). La nueva regulación de los convenios administrativos en la Ley 40/2015 de régimen jurídico del sector público. *Revista General de Derecho Administrativo*, 45.
- Tur Fáundez, C. (2018). *Smart contracts: análisis jurídico*. Madrid: Reus.

Transparencia y protección de datos personales en el uso de la tecnología *blockchain*: especial consideración de su impacto en el ámbito local

Andrés Boix Palop

Profesor titular de Derecho Administrativo.

Universitat de València

Manuel Pereiro Cárceles

Investigador doctor en Derecho Administrativo.

Universitat de València

SUMARIO. 1. El impulso a la transparencia de la actividad administrativa mediante el uso de medios electrónicos. 2. Transparencia y *blockchain*. 2.1. El uso de la tecnología *blockchain* como mecanismo de control de la legalidad. 2.2. El uso de la tecnología *blockchain* como mecanismo de control de la eficacia. 2.3. El uso de la tecnología *blockchain* como presupuesto de la participación en la vida pública. 3. Posibilidades de mejora de la transparencia administrativa a través del uso de la tecnología *blockchain*. 4. Intersección (y compatibilidad) entre transparencia y protección de datos personales en el empleo de la tecnología *blockchain*. 5. Colisiones entre la utilización de la tecnología *blockchain* y la regulación en materia de protección de datos personales. 5.1. El problema de la identificación de la responsabilidad por el tratamiento de la información. 5.1.1. Redes privadas y permisionadas. 5.1.2. Redes públicas no permisionadas. 5.2. La exigencia de consentimiento expreso. 5.3. Compatibilidad con el derecho de acceso a los datos personales. 5.4. Compatibilidad con el derecho de portabilidad. 5.5. Compatibilidad con el derecho de rectificación. 5.6. Compatibilidad con el derecho de supresión. 5.7. Anonimización de datos personales. 5.8. La prohibición de adopción de decisiones individuales automatizadas en el uso de *smart contracts*. 6. Bibliografía.

1. El impulso a la transparencia de la actividad administrativa mediante el uso de medios electrónicos

Desde hace unos años, una de las principales exigencias que la sociedad contemporánea demanda al sector público es el cumplimiento de medidas de transparencia que coadyuven en la consecución de una mejor organización y funcionamiento administrativos. Para ello la transparencia cumple con una doble función. Por una parte, la de control, en su doble dimensión de legalidad y eficacia, lo que es de vital importancia para detectar actuaciones ilícitas, así como para mejorar la calidad de la actividad administrativa -entendida esta en un sentido amplio-. Por otra, supone un presupuesto necesario para la participación de los ciudadanos -como personas físicas o a través de personas jurídicas- en la vida pública, lo que, además de constituir un elemento que contribuye a la legitimidad de la actuación de los poderes públicos, sirve para estimular la dinamización económica en el sector privado.

Conforme se ha ido siendo consciente de la importancia que tiene este principio en la forma de entender la Administración contemporánea y la gestión de intereses públicos, se ha ido produciendo en España un extraordinario avance legislativo a través del que se ha conseguido regular un logrado régimen de obligaciones en materia de publicidad informativa cuyo cumplimiento se apoya en una gestión documental telemática y en el uso de medios electrónicos. Este impulso a la transparencia electrónica está protagonizado por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTBG), así como por una larga retahíla de normas autonómicas y municipales que desarrollan sus previsiones a la vez que incorporan sus propias peculiaridades, aunque en el ámbito sectorial ya existían algunas leyes de excepcional importancia en la materia, tales como la Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente, y la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. A su vez, dicha tendencia también ha ido quedando reflejada en las más relevantes normas generales de relación con la ciudadanía que integran el derecho administrativo, tal y como son las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común (LPAC), y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), a través de las que se ha normalizado el empleo de medios electrónicos en las intercomunicaciones informativas que se produzcan en el marco de las relaciones jurídicas administrativas. También puede observarse en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, cuya regulación,

fuertemente impulsada por la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, tiene como uno de sus principales objetivos combatir la corrupción a través de un sistema de contratación pública más innovador, eficiente, transparente e íntegro, en el que se incremente la publicidad de los procedimientos contractuales¹. Como se desarrolla en este trabajo, la incidencia de esta transformación afecta además particularmente a unas administraciones que prestan de forma directa servicios a los ciudadanos como son los entes locales, para los que tanto la transformación que supone la transición a la administración electrónica como el empleo de herramientas tecnológicas como las aquí analizadas suponen un reto de particular relieve².

Esta inusitada expansión de la transparencia a través de su incorporación en las leyes administrativas no habría sido posible si no hubiese existido un avance en las tecnologías de la información y la comunicación que la hiciese realmente posible. Pero, además, ello ha requerido una vehemente voluntad política y una elevada inversión de recursos económicos que, sin embargo, y en la práctica, no siempre han sido suficientes para asegurar un despliegue de los medios y la tecnología necesarios para realizar esta transición al ritmo deseable (o siquiera al impuesto por las normas que establecían calendarios de implantación que se han ido incumpliendo de forma casi generalizada, lo que ha llevado incluso a las sucesivas prórrogas que hemos conocido respecto del calendario de implantación de la LPAC, que en algunas de sus partes llegó a conceder un lustro de período de adaptación a las administraciones públicas para poner a punto los medios electrónicos necesarios para su completa implantación).

Ha sido precisamente este, el de la mejora en la gestión de la información administrativa, uno de los aspectos esenciales en este avance. Así, se han ido adoptando las técnicas informáticas necesarias tanto para incrementar su agilidad y aprovechar sus potenciales beneficios como para promover la difusión y puesta en conocimiento de la información a la ciudadanía, ya sea con carácter general, ya por razones de interés público, o en el marco de procedimientos administrativos. Para ello ha sido necesario someter a nuestras administraciones públicas a una profunda transformación en su funcionamiento, introduciendo los medios electrónicos como vía a través de la cual realizar esa gestión avanzada de la información que desemboca, como una de sus principales consecuencias, en una mayor transparencia de la gestión pública.

-
1. Martín Delgado (2020: 48 y 49) y Valero Torrijos (2015: 40).
 2. Boix Palop (2019).

De conformidad con lo anterior, se manifiesta como un elemento de extraordinaria importancia que las administraciones públicas -y los entes públicos y privados que pululan en torno a las mismas- escojan las soluciones técnicas que mejor se adapten a los principios jurídicos por los que deben regirse: eficacia, jerarquía, descentralización, desconcentración, coordinación y, por supuesto, transparencia. Con ese fin las entidades públicas han ido incorporando en su funcionamiento sistemas de información tales como bases de datos o almacenamientos en la nube que sirven para cumplir adecuadamente con la mayor parte de las funciones que tienen atribuidas, pero que adolecen de algunos problemas derivados del carácter centralizado por el que se singularizan. Algunos de estos problemas son un menor grado de estabilidad y seguridad, siendo más proclives a los fallos generalizados en el sistema y a que los ataques maliciosos dirigidos contra este funcionen, y una escalabilidad limitada por la que el servidor posee restricciones en su capacidad para gestionar datos, lo que no es una cuestión baladí dado el incremento exponencial de los mismos que se necesita para el ejercicio de los modelos más avanzados de gobernanza.

Tratando de dar solución a estos problemas surgen las tecnologías de registro distribuido (*blockchain*, cadena de bloques) como nuevas alternativas posibles para gestionar los almacenamientos de información y los procesos de intercomunicación informativa. Si bien su introducción en el sector privado está teniendo un impacto notable, especialmente por la disrupción que ha supuesto el mercado de las criptomonedas, en el sector público su entrada parece estar siendo más lenta, limitándose, con la excepción de casos puntuales como el del Gobierno de Estonia, a la puesta en marcha de *sandboxes* o proyectos de alcance muy concreto. Una suerte de experiencias piloto que merecen una opinión positiva en tanto que permiten descartar fallos e identificar aquellos usos en los que *blockchain* muestra su eficacia, pero que para su desarrollo deberán venir acompañadas de una política regulatoria de progresiva implantación de la tecnología en determinados ámbitos de la gestión pública³.

Hasta el momento, su uso en la actividad administrativa se ha producido en torno a tres ejes: la comprobación de la identidad electrónica; registros de información en numerosos sectores; y la automatización de procesos a través de *smart contracts* o contratos inteligentes⁴. Con todo, algunos de los elementos que conforman el diseño de las tecnologías de *blockchain*, así como algunas posibilidades de trazabilidad, seguridad y delimitación de contenidos visibles y

3. Pereiro Cárceles (2019b: 153).

4. En relación con el de uso de *smart contracts* en la actividad administrativa automatizada, Pereiro Cárceles (2019a).

de los que no (pero que aun así se conservan para su posible control y auditoría sin que puedan ser alterados), parece claro que se pueden ajustar muy bien a algunos de los retos que deben afrontar las administraciones públicas en la gestión de sus procedimientos y servicios. Y es que las características intrínsecas propias de esta tecnología coinciden plenamente con los principios previstos en el artículo 3 LRJSP -entre los que se encuentra el de transparencia- en que se fundamenta la actividad administrativa, lo que puede hacer recomendable su uso en aquellos supuestos en que las redes centralizadas podrían tener dificultades para garantizar algunos de estos principios de forma eficiente. Muy especialmente cuando pueda ser deseable que no exista un tercero, o incluso la propia Administración, en una posición intermedia de registro, control y verificación de identidades o cualquier otro dato. En estos casos podría delegarse esta función en una tecnología robusta y fiable que aportará a todas las partes las debidas garantías sobre los elementos del proceso, en términos de identidad, transparencia y trazabilidad de las aportaciones o actuaciones realizadas por cada parte si no existieran impedimentos de rango legal que obligasen a que la Administración esté presente como intermediaria⁵.

Por último, ha de ser señalado que dentro de lo poco legislado en materia de *blockchain* en España la norma más importante en vigor en estos momentos, si bien de origen gubernativo (el reciente Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones), ha sido más bien un freno que un incentivo al desarrollo de la tecnología. Como es sabido ha introducido su prohibición de uso, si bien temporal hasta que exista regulación en la materia de ámbito europeo, a efectos de identificación en las relaciones entre administraciones públicas y ciudadanos (regulación con un origen y una explicación muy concretos que puede aplazar interesantes desarrollos de identificación ante terceros sin necesidad de una intervención en cada caso de la Administración como intermediario de verificación tecnológica de la identidad digital del ciudadano en cuestión)⁶.

2. Transparencia y *blockchain*

Uno de los rasgos más característicos de *blockchain* es la transparencia que garantiza. En la medida en que la información que se introduzca en la red queda registrada de forma que es visible para los individuos que acceden a la misma,

5. Hernández San Juan (2019: 26).

6. Alamillo Domingo (2019b), Merchán Murillo (2019) y Boix Palop (2021: 23-24).

puede afirmarse que la cadena de bloques es una tecnología que fomenta la transparencia. Además, dicha característica se ve reforzada por otras dos propiedades esenciales de las redes *blockchain*: la inmutabilidad y la permanencia. Conforme a estos rasgos intrínsecos de la tecnología, las transacciones que se realizan empleando esta tecnología son inalterables, de forma que no resulta posible manipular ningún dato que se introduzca en la misma, que quedará para siempre almacenado e individualizado a través de su *hash* particular en los nodos de todos los participantes de la red. Además, el registro de las transacciones se acompañará de un sellado de tiempo que permitirá conocer en qué momento concreto se aportó esa información, lo que garantiza un elevado potencial a efectos de auditar la integridad de la información aportada, así como de verificar el cumplimiento de los plazos. En definitiva, sus posibilidades de uso y su carácter transparente actuarían como factores clave para facilitar un acceso de los ciudadanos a cuanta información de su interés sea introducida en las mismas, lo que potenciaría la realización de las funciones de control y participación que antes hemos establecido que la transparencia en su vertiente pública tiene atribuidas. El *blockchain* constituye una tecnología disruptiva cuyo espíritu concuerda a la perfección con el movimiento favorable al derecho a saber que a través de los avances normativos en la materia se ha ido consagrando a través de mecanismos concretos en la gestión pública.

Estas características y posibilidades pueden ser aprovechadas en numerosos contextos, siendo el más reseñable de los que nos ocupan el de las obligaciones de información previstas en la normativa de transparencia pública. Sin embargo, las posibilidades de incrementar la transparencia mediante su uso no se agotan aquí, sino que alcanzan también otros aspectos tales como el acceso a la información de los procedimientos administrativos, la identificación de los órganos intervinientes en los mismos o la gestión de los servicios públicos.

2.1. El uso de la tecnología *blockchain* como mecanismo de control de la legalidad

Una de las principales funciones asociadas a la transparencia a la que el uso de la tecnología *blockchain* da respuesta es al control de legalidad de las actuaciones de los miembros o nodos que forman parte de la red. Esto quiere decir que mediante su empleo será más sencillo detectar algunos incumplimientos que quedarían expuestos al tratarse de una red distribuida que no se puede manipular por un sujeto concreto y en la que quedan registradas todas las transacciones desde el momento en que se realicen. La información que

se introduzca en la red, por aportación directa del ciudadano o de la Administración o ente público, o que se obtenga de oráculos⁷, no podrá ser en ningún caso modificada ni falseada, debido a la inmutabilidad por la que se rige esta tecnología. Esta imposibilidad de cambiar los registros de información en la red, así como la auditabilidad que propicia el acceso universal a estos, actúan como un incentivo destacado en la evitación del fraude y, en consonancia, como una herramienta útil en la lucha contra la corrupción. Cualquier incompatibilidad -por ejemplo, las prohibiciones para contratar o recibir dinero del sector público- o incumplimiento de un requisito -la solvencia del empresario, la tenencia de una titulación específica...- que se produzca en el marco de un procedimiento puede ser detectado automáticamente mediante el uso de tratamientos automatizados si la red tiene acceso a la información disponible sobre esos asuntos. De igual manera, los incumplimientos en las aportaciones documentales, así como el quebrantamiento de los plazos o la omisión de trámites, podrían quedar patentes a través del uso de *smart contracts* en la gestión de procedimientos administrativos.

Por su parte, en uno de los casos paradigmáticos de aplicación como es la identidad digital, la tecnología *blockchain* también actúa como elemento de extraordinario valor para prevenir cualquier manipulación que se quisiera acometer respecto a la identidad digital de una persona. A través de estos sistemas el conocimiento de datos relativos a los ciudadanos solo se producirá cuando estos otorguen el acceso, de tal manera que son sus propios titulares quienes mantienen un absoluto control de qué información están facilitando a otros sujetos -y, en particular, a las entidades públicas-. Todo este proceso es transparente, de tal manera que el ciudadano conocerá en todo momento qué información es la que ha facilitado a cada sujeto, pudiendo incluso limitar que aquella pueda volver a ser consultada por haber sido transferida a terceros a los que no les ha facilitado el acceso, lo que detiene o dificulta enormemente la transferencia de datos personales a terceros o su uso incumpliendo la finalidad con la que se facilitaron aquellos. La robustez en términos de seguridad de la que hace gala la tecnología impediría siempre y en todo caso un otorgamiento del acceso a datos personales por parte de persona distinta a aquella que cuenta con la clave necesaria para realizar tal operación.

De igual manera, el empleo del *blockchain* también puede ser de enorme interés en relación con el control de los presupuestos públicos. En este supuesto,

7. Conforme señala Vivas Augier (2017: 123), oráculos son agentes que proveen a la red *blockchain* de información externa a la que los *smart contracts* pueden acceder por sí solos y actúan en representación suya para ejercer acciones fuera de su alcance.

la tecnología puede ayudar a una mejor fiscalización del cumplimiento de los gastos comprometidos en los mismos, pues permite registrar en tiempo real cualquier desembolso económico que sea llevado a cabo respecto a las partidas pertinentes, por lo que su auditabilidad por parte de los ciudadanos queda mejor garantizada.

Desde esta perspectiva no hay duda de que el empleo de la tecnología basada en *blockchain* para estas cuestiones puede constituir un acicate en el cumplimiento efectivo de la rendición de cuentas que los ciudadanos exigen a la gestión pública. Una rendición de cuentas que se ve reforzada por la inmutabilidad y la seguridad que caracterizan las redes *blockchain* y que no alcanza únicamente a las relaciones jurídicas estrictamente administrativas que se establecen entre el ciudadano y las entidades públicas, sino también a las relaciones administrativas y, en lo que es de especial interés para los Gobiernos locales, a la gestión de servicios públicos, ya corresponda esta a las propias entidades públicas o se haya externalizado por medio de la concesión de su gestión indirecta a sujetos privados.

2.2. El uso de la tecnología *blockchain* como mecanismo de control de la eficacia

Otra de las funciones asociadas a la transparencia que pueden resultar mejor garantizadas por el uso de la tecnología basada en sistemas de *blockchain* es la identificación y detección de los posibles fallos que pudiera haber en el sistema, no ya necesariamente de vulneraciones normativas, porque al tratarse de una tecnología que permite el seguimiento o la trazabilidad de cualquier proceso, el funcionamiento de los servicios o las funciones públicas también puede ser automáticamente analizado y auditado, dando lugar a la detección de problemas de eficacia o calidad que pudieran existir en su desarrollo. Por ejemplo, en el marco de la gestión administrativa, el ciudadano podría conocer las dilaciones de los procedimientos o, en el campo de la transparencia administrativa, advertir de fallos que pudieran existir en la publicación de información, por no encontrarse esta lo suficientemente detallada o incumplir los principios de calidad que exige el artículo 5 LTBG.

Sin embargo, donde es de especial relevancia esta función es en el ámbito local, en que se produce la ejecución de la mayor parte de los servicios públicos, y más aún si se tiene en cuenta que la digitalización en su prestación comienza

a ser una realidad a través de las denominadas *smart cities*⁸. El funcionamiento de estas ciudades inteligentes depende de una interacción constante de ingentes cantidades de información que podrían no ser asumibles a través de redes centralizadas. En este sentido, una red compleja e interconectada a la par que descentralizada como es *blockchain* en conjunción con el uso de internet de las cosas (*Internet of Things*) podría asegurar una más eficiente prestación de la amalgama de servicios a los que hay que hacer frente en estos entornos digitalizados. Estos servicios o funciones irían desde un mejor desarrollo de los servicios públicos propiamente dichos -transporte público, abastecimiento de agua...- a una más adecuada y sostenible gestión de las infraestructuras a partir de las conductas y preferencias de uso de los ciudadanos -comportamiento en los espacios públicos, datos socioeconómicos...-. *Blockchain* permite establecer comunicaciones informativas entre distintos nodos -que pueden corresponder a sensores colocados en distintos puntos de la ciudad- que cumplen con estándares muy elevados de seguridad y transparencia, lo que admitiría un mayor conocimiento público de su funcionamiento y un mejor control en la utilización de los datos que el individuo aporte para recibir la prestación de un servicio o una función concretos. A su vez, un uso avanzado de la información a través de técnicas de *big data* o inteligencia artificial podría operar en beneficio de una mayor satisfacción de los ciudadanos que habitan o visitan el municipio, para lo cual se requerirá que su reutilización cumpla con los requisitos legalmente exigidos. En cualquier caso, la transparencia de la red, junto a la veracidad y la inmutabilidad que la caracterizan, actúan como un presupuesto necesario e inquebrantable para que terceros, bien sean los propios ciudadanos o las administraciones públicas, hagan un uso avanzado de la información a efectos de detectar sus fallos o carencias, así como de mejorar los servicios ofrecidos.

2.3. El uso de la tecnología *blockchain* como presupuesto de la participación en la vida pública

Como última de las funciones de la transparencia pública sobre las que puede incidir *blockchain* es preciso mencionar el papel trascendental que aquella cumple para el ejercicio de la participación de los sujetos privados en general y de los ciudadanos en la vida pública. No cabe olvidar que cuando en el ordenamiento jurídico administrativo se alude a la participación esta puede referirse a la participación política o a la de tipo administrativo, e incluso puede hablarse de participación en el sector privado, introduciendo mecanismos de

8. Velasco Rico (2019).

pluralidad e intervención de los ciudadanos o de individuos que tengan algún interés cualificado en órganos de decisión de entidades u organizaciones de naturaleza privada.

Dejando de lado esta última posibilidad, en el ámbito local la participación administrativa es la que recibe una especial consideración, en tanto que la dimensión política de las actuaciones de los Gobiernos locales es más reducida que en otros niveles competenciales. En el municipio es la gestión de las actividades cotidianas la que recibe mayor atención, por lo que las posibilidades de intervención de los ciudadanos se circunscriben mayoritariamente a esta esfera de actuación. En este sentido, son numerosos los supuestos de participación administrativa en los que los ciudadanos pueden intervenir a efectos de manifestar su parecer en distintas circunstancias: jurados ciudadanos, consultas ciudadanas, audiencias públicas... También son destacados los avances en relación con el destino de una parte de los recursos públicos a través de los denominados presupuestos participativos, cada vez de uso más generalizado.

En los casos anteriores la tecnología *blockchain* podría actuar como red que sirviera de fundamento base para el intercambio de opiniones en la que las aportaciones que se realizasen quedarían registradas de forma inmutable y permanente, y a través de los sistemas adecuados los ciudadanos podrían controlar si sus intervenciones o reivindicaciones están siendo o no atendidas.

Y es que no hay que olvidar que la participación únicamente podrá ser efectiva si los ciudadanos -o las entidades privadas que van a colaborar con la Administración- disponen de cuanta información disponible exista en relación con la cuestión en la que pretenden intervenir. Solo de esta forma será posible evaluar la situación y realizar aportaciones sensatas o tomar decisiones racionales fundadas. De igual manera, el proceso participativo constará de una serie de intercambios de información, algunos a través de aportaciones documentales y otros mediante la expresión de meras opiniones o pareceres que deberán ser conocidos por el resto de implicados en la cuestión a efectos de que puedan ser replicados, admitidos o denegados los argumentos. El uso para todo ello de sistemas basados en *blockchain*, como tecnología transparente que es, puede permitir que todos estos procesos de intercomunicación con administraciones y sujetos privados implicados sean auditados fácilmente, en cuanto que habrá un registro público de aquellos y se tratará de cuestiones que mayormente inciden en el interés general de los vecinos. A su vez favorece el debate público y sirve para garantizar que la toma de la decisión final se ha realizado cumpliendo con las exigencias

necesarias para confirmar que la participación se ha ejercido por parte de un ciudadano debidamente informado.

3. Posibilidades de mejora de la transparencia administrativa a través del uso de la tecnología *blockchain*

Las tecnologías de registro distribuido como las que se basan en *blockchain* tienen un enorme potencial para actuar como tecnología a través de la que gestionar los trámites de información y dar conocimiento de la actividad de interés público al individuo, bien sea como interesado o en su mera condición de ciudadano legitimado para conocer cuantos aspectos no sean restringidos por la ley relativos a la gestión pública, con la ventaja de conformar entornos donde la tecnología aporta total confianza en la trazabilidad y transparencia de todo lo que se defina en el proceso en cuestión como transparente, sin necesidad de que haya de darse una actuación de la Administración que haga transparentes estos elementos o datos, y que pueda además decidir no hacerlo con parte de ellos, automatizando el proceso y la garantía, que pasa a depender de su correcta definición tecnológica. Por defecto, además, las redes *blockchain* son transparentes, es decir, están configuradas para que sus transacciones sean accesibles por cualquier individuo, lo que supone una primera muestra de la enorme virtualidad que el uso de esta tecnología tiene para dar cumplimiento a las obligaciones de información pública previstas en la normativa.

En particular, de gran interés es la exploración de las posibilidades que la utilización de la tecnología *blockchain* ofrece a la gestión de la publicidad activa. En cuanto que la puesta a disposición de esta información en estos casos es semiautomática, es decir, sin necesidad de evaluación previa al estar los contenidos previa y claramente delimitados en la norma -no obstante, no hay que olvidar que los límites al acceso también les resultan aplicables-, su inclusión en la red y su publicación podrían realizarse a través de sistemas automatizados que localicen la información, la validen con el uso de la tecnología *blockchain* y la difundan. Además, la información quedaría registrada garantizando su integridad dado el poder que tiene *blockchain* para comprobar la veracidad -que no verdad- de la información aportada y para que esta quede adecuadamente registrada. A través de *smart contracts* esta información podría recogerse de bases de datos, registros o incluso webs, en cuanto que consiste en una tarea automatizada. Por su parte, el órgano responsable de transparencia -en muchas ocasiones, el secretario del ayuntamiento o un órgano al que específicamente se

le ha atribuido la función- no deberá encargarse de ir subiendo la información, sino simplemente de realizar una labor de control o supervisión, comprobando que el proceso se realiza sin incidencias, y detectando si la información originaria puede detentar vicios o debiera verse limitada por incurrir algún interés contrapuesto a la transparencia. El órgano responsable únicamente tendría que encargarse de añadir el documento o dato original a la red para que automáticamente este ya se añada en un nuevo bloque de la cadena publicándose en todos aquellos sitios para los que el sistema esté preparado, eliminando duplicidades e introduciendo mayor celeridad en la gestión de la información que hay que difundir de forma activa. Obviamente este órgano actuará como responsable ante cualquier eventual reclamación que un ciudadano pudiera oponer en relación con la información o falta de ella que se contemple en los portales de transparencia, lo cual es verdaderamente importante que quede terminantemente claro, puesto que la descentralización por la que se rigen estas redes plantea serias dificultades para identificar a un responsable al que el ciudadano se dirija en caso de cualquier fallo o reclamación que se le plantee oponer.

Siguiendo esta línea, cuanto mayor alcance tenga la red no solo en cuanto a la información de la que disponer, sino también respecto a las distintas fuentes informativas de las que nutrirse y a través de las cuales debe publicar la información, mayor grado de integración tendrá el sistema y menores esfuerzos adicionales tendrán que acometer los responsables de transparencia para cumplir con las obligaciones que tienen atribuidas. Para ello es de vital importancia la interoperabilidad y que las redes locales que se construyan puedan a su vez intercambiar información con otras propias de otros niveles competenciales o de otras administraciones o entidades públicas con las que se relacionan. En este sentido son de vital relevancia iniciativas tales como la incorporación de las entidades públicas a redes de mayor extensión, como son el *European Blockchain Services Infrastructure*, o cualquiera de las llevadas a cabo por miembros integrantes de Alastria, así como la normalización de los estándares de los protocolos *blockchain*, a cuyo respecto se han producido unos primeros avances en España a través de la reciente Norma UNE 71307-1 aprobada por la Agencia Española de Normalización. Sorteado este problema -así como otros no menores relacionados con los costes medioambientales y económicos que puede necesitar el desarrollo de una aplicación conforme a esta tecnología-, solo cabe aducir que su uso requerirá el empleo de menor cantidad de recursos humanos y materiales para cumplir con el plantel de obligaciones de publicidad activa que exigen las leyes, ordenanzas y reglamentos de transparencia administrativa.

Pero, además, si algo garantiza *blockchain* no es solo un funcionamiento más ágil y eficaz en beneficio de las entidades públicas, sino también una obtención de información de interés público de mayor calidad por parte de los ciudadanos. Conforme a esta idea, *blockchain* constituye la tecnología idónea para cumplir con los principios que la LTBG contempla en su artículo 5. Así, una interconexión de la información a través de una red de este tipo aseguraría una permanente actualización de los contenidos, de forma que cualquier variación en un dato -piénsese, por ejemplo, en uno de tipo organizativo, institucional o económico- podría verse reflejada inmediatamente en el correspondiente portal de transparencia si la aplicación informática estuviese debidamente configurada para ello. De este modo, el principio de periodicidad, según el cual la información debe ser actualizada de forma frecuente, queda satisfecho. También quedaría garantizada la veracidad de la información -que no la verdad, que por medios electrónicos no siempre puede comprobarse- en el sentido de certificar su autenticidad, fiabilidad e integridad, así como el cumplimiento de la cadena de custodia del proceso que se ha llevado a cabo para su publicación. Todo ello, además, redundaría en beneficio del potencial reutilizador de la información, que, al ser de mayor calidad, provoca que su uso con estos fines obtenga mejores resultados, lo que no es baladí teniendo en cuenta los beneficios económicos y sociales que pueden acabar produciéndose a partir de esta actividad.

Igualmente, el sistema debe articularse de modo que facilite la búsqueda y localización de cualquier información que desee conocer el usuario y que forme parte de la red, para lo que será precisa una simplificación de las condiciones de acceso y de utilización de estas redes a cuyo funcionamiento no está acostumbrada la ciudadanía. Y es que, como señala Cerrillo i Martínez, en muchas ocasiones la eficacia de los derechos no se ve comprometida por su configuración jurídica, sino por otras razones como la falta de información y conocimiento de los usuarios o de recursos humanos y técnicos apropiados para su desempeño⁹. Solo si se consigue que la información se presente de modo que los ciudadanos accedan a ella con facilidad se estará consiguiendo una transparencia verdaderamente efectiva y que no se queda en el mero plano normativo. Con este fin es importante destacar la importancia de que la red sea diseñada desde el principio teniendo en cuenta esta circunstancia, aplicando una suerte de principio “*blockchain* por diseño”¹⁰ conforme al cual los técnicos informáticos en colaboración con los juristas especializados desarrollen la aplicación siendo conscientes de que su finalidad es la publicidad de información,

9. Cerrillo i Martínez (2016: 176).

10. Bernal Blay (2018).

pero haciéndola conciliar con la protección de datos personales u otros intereses con los que la transparencia pudiera colisionar¹¹. Tampoco cabe duda de que el uso de la tecnología *blockchain* para la realización de las obligaciones de publicidad activa también cumple con unos elevados estándares de celeridad e inmediatez que mejoran la difusión sin solicitud previa de información pública como consecuencia de, además de su elevada capacidad computacional para manejar cantidades ingentes de datos, la automatización que el uso de *smart contracts* admite para el tratamiento de la información en la red.

En cuanto al procedimiento de derecho de acceso, cuenta con el problema de que su desarrollo resulta más difícilmente automatizable al deberse realizar en la mayoría de los casos una correspondiente valoración de la solicitud y la aplicación de unos test de interés público y de ponderación que precisan, al menos en principio, de intervención humana. Como es obvio, el *blockchain* no va a aportar una solución a la aplicación de los límites previstos en los artículos 14 y 15 LTBG, en cuanto que no poseen una aplicación automática¹² -como sí ocurre con las causas de inadmisión contempladas en el artículo 18.1 LTBG y con los datos especialmente protegidos¹³-. En este sentido, aunque se automatizase parcialmente este procedimiento, obviando las aportaciones que respecto a la toma de decisiones podría hacer la inteligencia artificial¹⁴, se requeriría la intervención de un órgano responsable con seres humanos que lo integren para el cumplimiento del trámite consistente en ponderar los intereses en conflicto con la facilitación de la información, lo que precisa de un análisis racional de fondo que no tiene carácter mecánico. No obstante, una automatización parcial mediante el uso de *smart contracts* sí podría tener utilidad para aportar trazabilidad al procedimiento, tal y como se ha demostrado posible mediante el desarrollo de algunas experiencias en materia de contratación pública¹⁵ o de gestión de averías¹⁶. De esta forma, el ciudadano podría conocer aspectos del procedimiento

11. Jiménez Serranía (2020-2021: 192).

12. Entre otras, Resolución del Consejo de Transparencia y Buen Gobierno (CTBG) 327/2016, de 17 de octubre, y resoluciones de la *Comissió de Garantia del Dret d'Accés a la Informació Pública* (GAIP) 719/2019, de 15 de noviembre, y 137/2021, de 28 de enero.

13. Federación Española de Municipios y Provincias (2017: 206).

14. Gamero Casado (2021).

15. Sobre la aplicación de la tecnología *blockchain* en los procedimientos de contratación pública, consúltese, por todos, Pereiro Cárceles (2019a). En este sentido, como se explica en la referida obra, la iniciativa más importante llevada a cabo al respecto es la abanderada por el Gobierno de Aragón para el registro y la evaluación de las licitaciones en los procedimientos abiertos simplificados de contratación pública. Una explicación pormenorizada del procedimiento puede encontrarse en Tejedor Bielsa (2020).

16. A través de una *smart grid* -red inteligente de usuarios interconectados que trata de asegurar un sistema energético sostenible y eficiente con altos niveles de seguridad y calidad en el suministro- *blockchain* es capaz de ofrecer soluciones analíticas para gestionar las inte-

tales como si se está tramitando su solicitud, el tiempo que está tardando o en qué fase se encuentra.

Del mismo modo la trazabilidad del procedimiento podría igualmente suscitar interés en el caso de las solicitudes de acceso a información que se encuentre en poder de terceros públicos o privados -en este caso se regirán por el artículo 4 LTBG-. Para ello será necesario que al menos la entidad pública, que es la que solicita la información para darle acceso, forme parte de la red *blockchain*. En el caso de tratarse de distintos órganos públicos correspondientes a la misma Administración, o incluso pertenecientes al sector público del mismo ámbito territorial, lo lógico sería que todos ellos gestionasen su información a través de esa misma red actuando como nodos. En cualquier caso, no cabe duda de que las aportaciones documentales serían más rápidas y eficaces, lo que redundaría en una mayor agilidad para dar respuesta a las solicitudes de acceso, debiendo respetar obviamente los trámites y plazos exigidos por la ley para que aquellos sujetos susceptibles de que la información les afecte puedan presentar las correspondientes alegaciones, en caso de no estar conformes con su puesta en conocimiento.

Otro aspecto en el que el uso de la tecnología *blockchain* podría tener sentido es el de la acreditación de la identidad, no siendo necesario para ello aportar ningún dato personal, sino bastando con cerciorar que se trata de un ciudadano tal y como exige el artículo 17.2.a) LTBG -en consonancia con lo previsto en el artículo 66.1 LPAC-. Sí podrían aportarse datos adicionales en el caso de que el solicitante quisiera que se tuviese en cuenta alguna condición cualificada para valorar la conveniencia del acceso a la información -por ejemplo, ser investigador-. Para ello se aportará simplemente la información que certifique la existencia de esa condición especial, sin necesidad de aportar más datos, lo cual coadyuva en una protección de los datos personales más amplia de a la que acostumbramos con la utilización de los medios actuales. A nuestro parecer existe un marco jurídico administrativo proclive para el empleo de la identidad digital sustentada en la tecnología *blockchain* en estos supuestos¹⁷, en cuanto que esta, como sistema de identificación de los interesados en el procedimiento, podría encontrar encaje en alguna de las modalidades previstas en el artículo 9.2 LPAC, en especial en la de su apartado c), relativa a “sistemas de clave concertada y cualquier otro sistema que las administraciones públicas consideren válido”, dado el funcionamiento de

rupciones en el servicio, trazando la detección de la avería y su resolución, de forma que el ciudadano sea conocedor de todo el proceso.

17. Alamillo Domingo (2019a, 60 y ss.).

criptografía asimétrica por el que se rige. Además, el empleo de esta tecnología como sistema de identificación es acorde con la adaptación del Reglamento europeo que regula la materia¹⁸ en consonancia con las previsiones 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, en cuyo artículo 4.2.1 del Anexo se establecen unos estándares de seguridad que con el uso de *blockchain* están plenamente garantizados. Sin embargo, ello requeriría la derogación de la disposición adicional sexta LPAC, introducida a través del artículo 3.3 del Real Decreto-ley 14/2019, de 31 de octubre, a la que ya nos hemos referido antes, que por el momento prohíbe expresamente el empleo de sistemas de identificación basados en registro distribuido en los procedimientos administrativos¹⁹.

La utilización de *blockchain* a efectos de hacer posible el ejercicio del derecho de acceso puede suscitar enorme interés en relación con la información que manejan los prestatarios de servicios públicos de las *smart cities*, en la medida en que se manejan cantidades ingentes de información cuya gestión a través de redes centralizadas podría ser complicada. Sin embargo, el respaldo legal que en la LTBG, a través de su artículo 4, se otorga para la realización de este derecho, posee algunas limitaciones. En primer lugar, debido al significado estricto de servicio público al que alude el precepto²⁰, que podría dejar fuera algunos servicios de carácter impropio que se presten en el municipio -por ejemplo, el transporte colaborativo-. En este sentido, algunas leyes autonómicas de transparencia han tratado de dar solución a esta cuestión extendiendo su aplicación a servicios sociales -Andalucía, Región de Murcia, Comunidad Valenciana...-, e incluso, en el caso de Cataluña, a los servicios de interés general o universal. En segundo lugar, porque el derecho de acceso que contiene tal precepto es indirecto: se realiza siempre a través del órgano público responsable con el que el prestador privado se encuentre vinculado, de tal manera que no podría haber un acceso automático directo de datos relativos a los prestadores por parte de los ciudadanos, lo que a mi parecer sería más eficaz de cara a aprovechar la inmediatez

18. Reglamento (UE) n.º 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 el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

19. Alonso Suárez (2021: 114).

20. En relación con la LTBG, Barrero Rodríguez (2014: 95). En el mismo sentido, en relación con la Ley de transparencia de la Comunidad Valenciana, Pereiro Cárceles y Doménech Pascual (2019: 34).

de la que adolece *blockchain* en sus transmisiones de información. Y es que hay que tener en cuenta que los costes adicionales, tanto en términos económicos como de tiempo, que supondría el otorgamiento directo del acceso, serían ínfimos para una entidad que ya utiliza *blockchain* como tecnología a través de la que gestionar la información relacionada con la prestación del servicio. En cualquier caso, a ello no obsta el que existiera un mecanismo de impugnación ante el órgano público responsable del control o supervisión del servicio ante eventuales reclamaciones que los ciudadanos hagan respecto a las denegaciones en el acceso resueltas por los prestatarios privados. No obstante, como ya se ha apuntado antes, este procedimiento de ejercicio mediato del derecho de acceso podría ser parcialmente automatizable a través de *smart contracts*, aunque debiendo tener en cuenta en todo caso la necesidad de establecer un periodo de alegaciones para que el ente privado del que se solicita la información pueda alegar motivos -como podría ser la protección de los secretos empresariales- que justifiquen la denegación del acceso.

4. Intersección (y compatibilidad) entre transparencia y protección de datos personales en el empleo de la tecnología *blockchain*

Si por algo se caracteriza la tecnología *blockchain* es por tener una extraordinaria capacidad de conciliar la transparencia de sus transacciones con un elevado nivel de protección de la privacidad de los datos. ¿Pero cómo pueden concordar estas dos propiedades? ¿No es contradictorio incrementar la transparencia con, a su vez, garantizar la privacidad de la información? La realidad es que los sistemas basados en el empleo de tecnología de *blockchain* son por defecto transparentes y seguros, pero a su vez, haciendo uso de sus técnicas criptográficas que combinan el uso de una clave privada que únicamente conoce el usuario y una clave pública cognoscible por cualquier usuario y que actúa como una suerte de identificador del individuo, resulta posible articular un régimen de privacidad a la carta que puede ser de gran interés para recibir servicios públicos o entablar relaciones jurídicas con administraciones públicas en entornos digitalizados.

Una respuesta a cómo se pueden conciliar ambos intereses puede encontrarse a partir del funcionamiento de muchas de las redes *blockchain* que ya han sido puestas en marcha en algunos campos, y que permiten ejemplificar esta capacidad de garantizar a la vez una mayor transparencia pero preservando datos de carácter personal. Tomando como ejemplo el

diseño ideado por Zyskind, Nathan y Pentland²¹, en estas redes la información se trocea y se distribuye entre los distintos nodos de la red, como forma de asegurar su desconcentración y también una mayor seguridad ante su eventual modificación. Posteriormente, puede hacerse uso de la tecnología *blockchain* para incrustar los datos y rastrear todas las unidades de información, de forma que, una vez localizada esta, puede compartirse con terceros -y estos a su vez con otros- sin necesidad de descifrar la información, por lo que esta no será conocida más allá de por quien posea la clave precisa para ello, actuando como una suerte de caja negra. La información es rastreable y localizable por defecto, pero existen mecanismos técnicos que permiten mantener oculta aquella información de carácter sensible cuyo acceso solo se podrá otorgar mediante el uso de la clave privada. Hasta aquí, la cuestión tecnológica estricta. A partir de este punto, con una correcta articulación jurídica respecto de quién ha de decidir, mediante el uso de esa clave privada, y en qué casos, cuándo, cómo y por quién se ha de poder acceder a esa concreta información más sensible y donde aparecen los datos de carácter personal, se puede entender con facilidad el porqué de las posibilidades que brinda la tecnología para lograr por defecto una correcta articulación de transparencia y protección de datos de carácter personal.

Esta capacidad de autodeterminación informativa posee un enorme potencial para desarrollar sistemas de identificación electrónica sustentados en la tecnología *blockchain*. De hecho, disponemos ya de algunos casos de aplicación en nuestro país, como es el proyecto IdentiCAT de identidad digital descentralizada presentado por el Gobierno de Cataluña²². Por una parte, el particular -sea una persona física o jurídica- podría disponer de una especie de perfil con todos sus datos personales -o de otro tipo-, que serían mantenidos a resguardo de curiosos, con unas cotas de seguridad y privacidad muy altas. Y no solo de curiosos, sino también de las propias administraciones, en cuanto que los sistemas de identificación autosoberana, a diferencia de los actualmente existentes, no precisan de la intervención de entidades públicas en su funcionamiento. Pero, por la otra, el individuo, haciendo uso de su clave, podrá otorgar acceso a alguno de los datos que le sean precisados al relacionarse con la Administración en el marco de un procedimiento administrativo o para la recepción de un servicio público, incluso simplemente sirviendo para identificarse de forma fehaciente o para otorgar consentimiento válido a alguna petición que se le realice. Precisamente esta iniciativa, que podría dar

21. Zyskind *et al.* (2015).

22. Disponible en: <https://politiquesdigitals.gencat.cat/ca/tic/identicat/> (última consulta: 13/10/2021).

frutos tan interesantes, es la que se ha visto cercenada por lo previsto en la disposición adicional sexta del Real Decreto-ley 14/2019²³.

El uso de *blockchain* como sistema de identificación digital permite que los interesados controlen su información de tal manera que los ciudadanos únicamente darán acceso a que los poderes públicos -y también privados- manejen aquellos datos que se hayan configurado como necesarios para el cumplimiento de sus funciones, manteniéndose la confidencialidad de los restantes datos personales del individuo. De este modo se otorga al ciudadano una libertad real sobre el uso de sus propios datos, como bienes que le pertenecen y cuyo uso puede gestionar y controlar a partir del sistema sustentado en esta tecnología.

En definitiva, la tecnología de registro distribuido, por sus propias características técnicas, cuenta con la ventaja de que, pese a su transparencia, la privacidad de los usuarios puede garantizarse, eso sí, siempre y cuando haya una correcta definición y delimitación jurídica de lo que sea necesario compartir y de lo que sea necesario proteger, de tal forma que es posible asegurar un mayor nivel de control respecto a un uso de la información que aporten para obtener determinados servicios que sea acorde con el principio de finalidad para el que se aportan los datos. Estas posibilidades, bien declinadas y correctamente articuladas jurídicamente, pueden suponer por ello un empoderamiento del ciudadano y un avance sin precedentes en la gestión de su información personal, que permite un uso más seguro y garantista de esta.

La prestación de servicios en ciudades inteligentes constituye uno de los sectores en los que esta tecnología puede emplearse para cumplir con la doble dimensión esgrimida, en la medida en que la información captada por los sensores u objetos requerirá de un archivo. Sin embargo, esta información captada por tales sensores podría ser traducida de forma sesgada. Por ello es necesario que los algoritmos que rigen la misma sean transparentes también, de modo que si se ha introducido alguna disonancia cognitiva en los mismos esta sea susceptible de ser identificada. Y es que igual pueden existir intereses subyacentes bajo la utilización de esos algoritmos sesgados según la finalidad para la que se empleen o poner en riesgo determinadas garantías o derechos de los ciudadanos, lo que la transparencia del sistema ayudaría a detectar.

En cualquier caso, aunque las transacciones sean transparentes, las personas son dueñas de su información y pueden emplear esta con la finalidad

23. Boix Palop (2019: 23-24).

que quieran. Pueden además hacerlo anónimamente o con un seudónimo, e incluso con una anonimización parcial -solo dando acceso a determinados datos de su identidad-. Lo habitual en el internet tradicional es que los prestadores e intermediarios pueden conocer los datos de los individuos que operan en la red sin que estos puedan ejercer su derecho a la autodeterminación informativa respecto a aquellos. Sin embargo, las redes *blockchain* pueden articularse de forma que sus transacciones sean anónimas, aunque ello requiera de esfuerzos adicionales en su diseño.

5. Colisiones entre la utilización de la tecnología *blockchain* y la regulación en materia de protección de datos personales

En el presente punto del trabajo nos ocuparemos de analizar las colisiones que podrían producirse entre los derechos de protección de datos previstos en el Reglamento General de Protección de Datos (RGPD)²⁴ y el uso de la tecnología *blockchain*. Cabe adelantar ya que, *a priori*, los conflictos que pudieran plantearse tendrán una más sencilla solución en redes privadas y permissionadas que en las públicas sin permisos. Esto se debe al mayor nivel de control al que es posible someter las primeras, que permiten una identificación más sencilla del responsable y una intervención en el diseño de la red para que se acomode a los requerimientos de privacidad exigibles según el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD). En cuanto que en las redes privadas siempre existe una organización que gestiona y controla la participación y la ejecución del consenso, esta podría ser una Administración pública o un ente con el que mantenga vinculación o sobre el que tenga algún tipo de control. En el caso de las permissionadas, aunque no existe esta centralización en la gestión, la participación se encuentra restringida a quien posea los permisos necesarios para ello, lo que permite articular una red *blockchain* integrada solo por entidades de confianza fundamentalmente públicas, pero también privadas. En cambio, en lo que concierne a las redes públicas difícilmente un Gobierno local que opte por hacer uso de ellas podrá de algún modo intervenir en el diseño previo de la red, lo que pone en jaque el ejercicio de los derechos de supresión, rectificación, oposición, limitación del tratamiento e incluso, según cuál sea su configuración de la privacidad, el derecho de acceso.

24. 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.

5.1. El problema de la identificación de la responsabilidad por el tratamiento de la información

Uno de los principales problemas a los que se tiene que enfrentar el uso de la tecnología *blockchain* es la identificación del responsable del tratamiento de los datos. La cadena de bloques está formada por una red descentralizada de nodos, por lo que resulta complicado reconocer quién es el responsable específico del tratamiento que se haga de los datos que se validan o custodian a través de esta tecnología. En este sentido es necesario apuntar que pueden existir distintas opciones, dada la diversa configuración con la que pueden contar estas redes, así como indicar que en muchos casos, inevitablemente, a efectos jurídicos el responsable del tratamiento será aquel que haya sido responsable del diseño de la red en cuestión, en la medida en que el mismo se haya hecho de modo que continúe teniendo el control efectivo sobre los datos clave del diseño en registro distribuido. Este no es sino un ejemplo adicional de la relevancia jurídica, de cariz normativo, del diseño y programación de las aplicaciones informáticas que puedan emplear los poderes públicos en el futuro²⁵ y que exige de una concreción previa de las finalidades y los objetivos que se pretenden conseguir, así como de las garantías jurídicas que pudiesen estar en juego. Entre ellas, la identificación de la responsabilidad ante cualquier problema que se pudiera suscitar como consecuencia de un funcionamiento inadecuado de la aplicación informática. En lo que concierne a la presente exposición, nos detendremos en la distinción entre redes privadas y permissionadas por una parte, y redes públicas por la otra.

5.1.1. Redes privadas y permissionadas

En este tipo de redes la identificación del responsable del tratamiento de datos es *a priori* más sencilla. Hay que tener en cuenta que los sujetos que integran la red están predeterminados y son conocidos, de forma que la atribución de la responsabilidad por el tratamiento de datos se supone que corresponderá, siempre y en todo caso, a uno de los miembros, y que, además, todo ello es conocido y aceptado por el resto de sujetos que participan en la misma.

En consonancia con lo señalado por la *Commission Nationale de l'Informatique et des Libertés* (CNIL), lo importante en estos casos, como es lógico, es que el órgano responsable quede fijado previamente a la realización de operaciones en la

25. Boix Palop (2020: *in toto*, pero especialmente 234-249).

red²⁶. Este podría consistir en uno de sus miembros, designado desde el inicio, o, si se prefiriese que la responsabilidad se compartiese entre varios sujetos, podría crearse una persona jurídica o agrupación con intereses comunes de diversos miembros que podría recibir la consideración de titular del tratamiento de los datos. De no cumplirse con esta atribución, se estaría incumpliendo lo previsto en el artículo 26 RGPD, que obliga a que la responsabilidad sea atribuida de forma transparente y por mutuo acuerdo de forma que cualquier sujeto afectado sepa con quién tiene que contactar -y ante quién presentar alegaciones- a efectos de proteger el uso que se hace con sus datos. Existiría el peligro de que, para cualquier reclamación, no haya un órgano específico que responda ante estas obligaciones. Por ello, si no se quisiera incumplir el deber de identificación de un responsable del tratamiento de datos al que obliga el RGPD, será preciso, previamente a la implementación definitiva de la red, que se especifique dicha cuestión. Si bien, en caso de que no se haya fijado a quién corresponde la responsabilidad, sería necesario precisar algunos criterios que le dieran respuesta.

Por otra parte, cabe apuntar otra posibilidad adicional: que la tecnología *blockchain* no se limite a la identificación digital o al registro, sino que se articulen mecanismos automatizados a través de los denominados contratos inteligentes²⁷. En estos casos el responsable debería ser el desarrollador de los algoritmos de la aplicación que realizan el tratamiento automatizado de datos personales, en la medida en que retiene el control sobre los mismos. Si bien, habría que acordar si esa responsabilidad se limitaría a su grado de intervención en el procedimiento o si pudiera tener carácter absoluto. El desarrollador debería haber tenido acceso a los datos personales. Y no hay que olvidar que el empleo de técnicas como el *machine learning* puede acabar desembocando en actuaciones por parte de la máquina incluso desconocidas para los desarrolladores, de forma que los datos podrían terminar por tratarse de un modo o con una finalidad que no era necesariamente la al inicio prevista.

En cualquier caso, la atribución de la responsabilidad en el tratamiento de los datos no es suficiente si no existen mecanismos jurídicos que permitan hacer operativos los derechos que la normativa reconoce a los ciudadanos en materia de protección de datos personales, a la vez que tengan en cuenta el contexto tecnológico e imbricarse en él, dando lugar a una normatividad donde lo jurídico y la programación de la herramienta han de ir de la mano y en ocasiones se confunden. Para ello será necesario que se adopten algunas

26. Commission Nationale Informatique & Libertés (2018: 1-4).

27. Pereiro Cárceles (2019a).

de las soluciones técnicas que planteamos en los subepígrafes sucesivos, lo que es necesario a efectos de que el ejercicio de la responsabilidad no acabe quedando desdibujado.

5.1.2. Redes públicas no permissionadas

En estos casos es más complejo identificar al responsable, dado que cualquier ciudadano que tuviera la suficiente capacidad computacional podría descargar el *software* pertinente y participar en la verificación y validación de transacciones de las redes de este tipo, así como formar parte de ellas introduciendo información en las mismas. Sin embargo, conforme a las exigencias del artículo 26 RGPD, entre la generalidad de sujetos que intervienen en la red, sería preciso atribuir a alguno de estos sujetos la responsabilidad por el tratamiento de los datos.

Una de las opciones que podrían barajarse sería la de considerar como responsables del tratamiento de datos personales a los desarrolladores de los propios protocolos *blockchain*, siempre y cuando estos se correspondan con una persona específica o una agrupación concreta, lo cual no es estrictamente necesario -no debemos olvidar que el creador del bitc in, Satoshi Nakamoto, es an nimo y ha mantenido su identidad oculta bajo un pseud nimo-. Una primera intuici n podr a llevarnos a pensar que lo m s razonable es que el sujeto responsable del tratamiento de datos en una red *blockchain* sea quien cre  la red. Sin embargo, a poco que conozcamos el funcionamiento de las aplicaciones sustentadas en esta tecnolog a nos dar amos cuenta de que ello no tendr a mucho sentido. Supondr a atribuir al creador de un protocolo las consecuencias producidas por un *software* concreto que funciona conforme a esta tecnolog a, pero en cuyo uso y finalidad no interviene. Y es que *blockchain* no es un *software* ni programa inform tico espec fico. Su creador no recibe compensaciones econ micas directas por los esfuerzos acometidos en el dise o de una aplicaci n novedosa que se sustente en esta tecnolog a. Simplemente esta servir a como fundamento para que las transacciones se realicen adecuadamente en las distintas aplicaciones, como son los *smart contracts*, en las que se les d e uso. Hay que apuntar, sin embargo, que para usos de estas posibles redes por parte de administraciones p blicas en las que ellas retengan cierto control, y para el ejercicio de actuaciones administrativas o de inter s p blico, esta soluci n puede tener sentido si son efectivamente responsables del c digo y de la programaci n de la red.

Otra hipótesis que cabría plantearse sería la atribución de la responsabilidad por el tratamiento de datos a los mineros²⁸, opción esta que debería descartarse conforme apunta el CNIL²⁹. Esta posibilidad supondría otorgar tal función a los nodos, lo que no tiene mucho sentido dado que ellos no son los que determinan el propósito con el que se realiza el tratamiento de datos, que simplemente verifican y validan para el correcto funcionamiento del sistema. Los mineros únicamente se limitan a ejecutar un protocolo, resolviendo cálculos matemáticos para validar las transacciones y obteniendo a cambio una recompensa económica. Contribuyen a la estabilidad del sistema y no dependen de intermediarios externos, pero no intervienen en la toma de decisión de la finalidad con la que se transmiten o emplean los datos, por lo que esta opción no parece del todo plausible.

¿Quiénes serían los responsables entonces? Parece que lo más lógico es pensar que serán quienes introduzcan los datos personales en la red, al menos mientras se trate de una persona jurídica o de una persona física que desempeña una actividad profesional o económica, aunque también podría plantearse que lo fueran los usuarios que firman y envían transacciones siempre y cuando realicen los envíos de información personal como parte de su actividad comercial. En cambio, quedarán excluidos como responsables aquellos que realicen transacciones de datos personales en la red con fines domésticos, en aplicación de lo previsto en el artículo 2.2.c) RGPD.

5.2. La exigencia de consentimiento expreso

Una de las principales novedades que el RGPD ha contemplado es una nueva forma de otorgar el consentimiento necesario para el tratamiento de datos personales que es distinta a la que se contenía en la anterior regulación. En concreto, su artículo 4.11 señala que el consentimiento debe ser libre, específico, informado e inequívoco, teniendo que ser realizado mediante una declaración o acción afirmativa. Dicha previsión, desarrollada a nivel estatal en el artículo 6.1 LOPD, se ve complementada por el artículo 7 de la misma Ley, en el que se especifica que el tratamiento de datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando su edad sea superior a los catorce años, de modo que cuando no la alcancen se requerirá el consentimiento de sus padres o tutores legales.

28. Conforme a la denominación que emplea Ibáñez Jiménez (2018: 34), los mineros son los nodos que participan en el registro de datos en los bloques a cambio de una recompensa económica.

29. Commission Nationale Informatique & Libertés (2018: 2).

Las administraciones públicas no quedan ajenas a estas previsiones en el manejo de inmensas cantidades de información pública de la que hacen uso. Como sabemos, las administraciones cada vez están llevando a cabo más actuaciones automatizadas (artículo 41 LRJSP) para cuyo ejercicio se precisa de un tratamiento de datos que cumpla con las exigencias que establece la normativa en materia de protección de datos, de forma que no haya dudas de que cualquier ciudadano al que pertenezca el dato al que se refiera dicha información haya prestado claramente su consentimiento.

Debido a sus características intrínsecas, *blockchain* ofrece las suficientes garantías técnicas para cumplir con la obligación de expresar el debido consentimiento. Y es que cuando cada usuario verifica y valida la transacción acometida en la red, por ejemplo, aportando determinada información propia, automáticamente está dando consentimiento para que los datos aportados sean utilizados por aquel al que se le ha autorizado para ello de acuerdo con el principio de finalidad para el que se han solicitado. Conforme funcionan los sistemas de identificación digital soberana, si no hay una acción clara como es la de otorgar el acceso, que solo puede ser llevada a cabo por el propio titular de los datos, no será posible que otro sujeto los conozca ni utilice, por lo que la existencia de voluntad expresa del individuo para aportar los datos que sean estrictamente necesarios para el cumplimiento de las funciones para las que se facilitan está completamente garantizada. En consonancia puede afirmarse que el historial de transacciones de datos que recopila *blockchain* actúa como una prueba de consentimiento para su tratamiento, de tal forma que mediante su consulta resultaría posible verificar su otorgamiento.

5.3. Compatibilidad con el derecho de acceso a los datos personales

El artículo 13 LOPD contempla el derecho de acceso del ciudadano a dirigirse al responsable del tratamiento para conocer si está tratando o no sus datos de carácter personal y obtener así cuanta información estime precisa relacionada con ese eventual tratamiento. La cuestión consiste aquí en identificar si este derecho puede encajar o no con el uso de la tecnología *blockchain*, que, como sabemos, suele suponer un tratamiento de los datos que se introducen en la red.

A esta cuestión ha dado respuesta la CNIL, que se ha apresurado a subrayar que el ejercicio del derecho de acceso a la información que posibilita una estructura transparente como es la de *blockchain* es perfectamente

compatible con las previsiones legales contenidas en el RGPD³⁰. El sistema se puede configurar de forma que se proporcione la información requerida a la parte interesada, lo que exigirá previamente que la solicitud determine el objeto en términos claros y no ambiguos para que, una vez registrada esta, se efectúen las transacciones necesarias para la entrega de los datos de carácter personal para que sean facilitados una vez los mineros hayan procedido a su validación. Ello no impide tener en cuenta las dificultades que podrían existir para identificar a la persona responsable de la gestión de la información en este procedimiento de acceso, conforme ya se ha comentado en el subepígrafe correspondiente.

5.4. Compatibilidad con el derecho de portabilidad

El derecho a la portabilidad, previsto en el artículo 20 RGPD, constituye uno de los derechos que desde el 25 de mayo de 2018 resulta aplicable a sujetos privados y públicos que manejen datos personales y realicen operaciones de transferencia con los mismos. De forma complementaria al derecho de acceso, su ejercicio permite que los datos personales que un usuario ya ha entregado a otro sujeto puedan a su vez transmitirse a un tercero sin necesidad de que aquel vuelva a disponer de ellos para hacer el intercambio.

En este sentido, los sistemas de identificación digital autosoberana que funcionan con *blockchain* permiten al ciudadano estar en conocimiento de qué información ha sido entregada y a quiénes, así como su facilitación a un tercero. De este modo, el ciudadano contaría con la posibilidad de acceder o denegar al acceso del tercero a esta información, al mantener el control de lo que ocurre con sus propios datos. Por consiguiente, el ejercicio del derecho a la portabilidad de datos es perfectamente compatible con el tratamiento de datos en redes *blockchain*, lo que además ha sido expresamente confirmado por la CNIL³¹.

5.5. Compatibilidad con el derecho de rectificación

El derecho de rectificación, contemplado respectivamente en los artículos 16 RGPD y 14 LOPD, es uno de los derechos que apriorísticamente más claramente podrían contravenir el rasgo de inmutabilidad que caracteriza la

30. Commission Nationale Informatique & Libertés (2018: 8).

31. Commission Nationale Informatique & Libertés (2018: 8).

tecnología *blockchain*. Y es que no hay ninguna circunstancia bajo la que sea posible modificar el contenido de una transacción que haya quedado registrada en un bloque, ya que hacerlo supondría alterar su *hash* y, por consiguiente, romper la propia cadena. Conforme a su funcionamiento, una vez una información ha quedado registrada, esta pasa a formar parte siempre de la red *blockchain*, siendo susceptible de ser conocida si no se adoptan las soluciones técnicas necesarias para evitarlo.

No obstante, cumplir con la exigencia de que se rectifiquen sin dilación los datos personales por existir alguna inexactitud es una tarea que puede tener solución en la práctica sin necesidad de complicadas medidas técnicas. Bastará simplemente con que la nueva información corregida se introduzca en un nuevo bloque de la cadena a través de una transacción. Bien es cierto que de este modo la información primigenia no desaparecerá, ya que el bloque anterior no podrá borrarse, pero sí se podrá ocultar conforme a los medios técnicos que existen para ello, lo que supone unas altas cotas de seguridad para que la información incorrecta no vuelva a ser conocida, quedando subsanado el error. Además, en caso de cualquier contradicción entre varios datos introducidos en la red, el contenido inscrito en un bloque posterior prevalecerá sobre cualquier otro que se recoja en un bloque anterior en el tiempo. Por lo tanto, existen soluciones técnicas para afirmar que el uso de la tecnología *blockchain* es compatible con el ejercicio del derecho de rectificación.

5.6. Compatibilidad con el derecho de supresión

El derecho de supresión, también denominado “derecho al olvido”, contemplado en el artículo 17 RGPD e incorporado en el ordenamiento estatal también a través del artículo 15 LOPD, constituye uno de los derechos de más complicada conciliación con el uso de la tecnología *blockchain* para el tratamiento de datos. Debido a la inmutabilidad y la permanencia de la información que caracterizan *blockchain*, el borrado de información cuya difusión pública no tiene interés resulta una tarea imposible de desarrollar en estas redes, por lo que, en puridad, sería imposible dar cumplimiento a las exigencias legales de supresión total de la información cuestionada.

Para dar respuesta a esta cuestión sería necesario atender a la finalidad de este derecho, que no es otra que evitar el conocimiento público y el uso de una información que no debería estar en poder de terceros, pero que no aspira en ningún caso a “borrar” o hacer desaparecer el pasado, ni siquiera de las redes. Recordemos, de hecho, que tanto la articulación actualmente

vigente del derecho al olvido como su origen tienen que ver no tanto con lograr el borrado de ciertas informaciones o ciertos datos ya no actualizados o relevantes, lo que supondría una evidente colisión con ciertas libertades informativas básicas, como con dificultar su recuperación o acceso, por medio de la no indexación, lo que es bien distinto³². En este sentido, cualquier tecnología que se diseñe y programe con la intención de realizar tratamientos de datos personales deberá cumplir con tales exigencias si no se quiere que su actividad quede al margen de lo previsto en el ordenamiento jurídico.

Desde este punto de vista, si prescindimos de la rígida exigencia de que la información deba ser necesariamente borrada, existen mecanismos técnicos para hacer inaccesible esa información, a efectos de que quien no se encuentre legitimado para ello no pueda conocerla, que equivalen sustancialmente a la forma en que se instrumenta el ejercicio efectivo del derecho al olvido. Como sabemos, no hay un solo diseño de tecnología *blockchain*, sino que esta se encuentra en constante avance, siendo posible establecer configuraciones de privacidad avanzadas que permiten ocultar información en la red. Por tanto, existen alternativas que permiten, si no borrar la información, sí aproximarse a una situación análoga a esta. En particular, desde el punto de vista técnico, las dos posibilidades más conocidas y que mayor grado de extensión tienen son las siguientes:

- El *hashing* criptográfico. Esta técnica consiste en almacenar la información de carácter personal de forma ajena a la cadena de bloques, es decir, en bases de datos externas. De esta manera será posible superar la inmutabilidad de la cadena de bloques con pleno respeto de la información más sensible, que podría requerir de supresión si se dieran los requisitos normativamente exigidos para ello. En estos casos el responsable del tratamiento de datos será el que se encargue de custodiar los bloques externos, quien eliminará la información de carácter personal que hubiera en los mismos si existiese algún conflicto por el que tuviese que hacerlo. Mediante esta técnica no se logra borrar el *hash* de la original transacción a través de la que se introdujeron los datos originales, pero sí se consigue su transformación en una serie de valores aleatorios que impedirán el acceso a la información que contenían.
- Canales privados. Esta solución técnica supone añadir a la tecnología *blockchain* técnicas de criptografía adicionales que permitan una conciliación entre la permanencia de la información en la red y su

32. Boix Palop (2015).

cancelación. Los canales privados son medios de transmisión de datos creados por dos o más nodos de la red que quieren compartir información entre ellos sin el conocimiento del resto de sus integrantes. En estos supuestos la información será solo accesible por los nodos miembros de este canal secundario privado que se generaría, de forma que la información estaría encriptada para los otros miembros. Esta técnica permite dar respuesta al ejercicio del derecho al olvido en redes *blockchain*, al poder los nodos que conocen el *hash* de ese canal secundario eliminar la clave criptográfica. De esta forma, el acceso a la información personal quedará bloqueado para siempre, al menos mientras la robustez técnica actual de *blockchain* en términos de ciberseguridad no pueda ser destruida por futuros avances tecnológicos que permitieran acceder a la información atrapada en esos bloques.

5.7. Anonimización de datos personales

La última cuestión relevante que necesita ser resuelta es la consistente en discernir si *blockchain* permite la anonimización de datos a efectos de conseguir que su tratamiento no vulnere las exigencias de privacidad personal que imponen el RGPD y, a nivel estatal, la LOPD, y que han sido convenientemente precisadas por la Agencia Española de Protección de Datos en su documento “Orientaciones y garantías en los procedimientos de anonimización de datos personales”³³. En general, es importante no solo que las técnicas de anonimización sean lo suficientemente robustas como para impedir la identificación del individuo al que pertenecían los datos originarios, sino también que el proceso de anonimización sea irreversible. Dicho de otra manera, no debería ser posible reanonimizar los datos originales. Cualquier información que no cumpla con tal propósito podría ser calificada como seudonimizada, pero en ningún caso estaremos ante una información completamente anónima.

Los datos seudonimizados se encuentran definidos en el artículo 4.5 RGPD. Concretamente, según se contempla en el precepto, se corresponden con aquella información que sin referirse de forma directa a datos nominativos potencialmente podría, a través de su asociación con información adicional, dar lugar a averiguar quién es el titular original al que pertenecen los mismos. Si bien el RGPD fomenta la seudonimización de los datos por su utilidad para reducir los riesgos de privacidad de los ciudadanos, estos continúan

33. Agencia Española de Protección de Datos (2016).

recibiendo la consideración de datos personales (considerando 28), por lo que aún se encontrarán obligados a cumplir con las obligaciones que se prevén para los mismos. Este es el caso de las claves públicas de *blockchain*, que reciben la consideración de datos seudonimizados.

Como ya hemos repetido insistentemente, la inmutabilidad es uno de los principales rasgos característicos de la cadena de bloques. Si mediante su uso nosotros queremos proteger la privacidad de la información de carácter personal, lo adecuado será utilizar algún tipo de encriptación adicional que permita que los datos permanezcan ocultos al resto de individuos que accedan a la red. Con este fin cobra especial sentido la aplicación del principio “*privacy by design*” previsto en el artículo 25.1 RGPD, según el cual la minimización de riesgos de privacidad en la utilización de datos personales será tenida en cuenta por el programador en el propio diseño de la plataforma que emplea *blockchain*. Sin embargo, la utilización de esta tecnología sí choca con el principio “*privacy by default*” contemplado en el apartado 2 del artículo 25 RGPD. *Blockchain* es una tecnología de configuración primigenia transparente que requiere de soluciones técnicas adicionales para garantizar la privacidad de datos de especial relevancia o de uso sensible que pudieran manejarse en la red.

El *European Union Blockchain Observatory and Forum* -una iniciativa de la Comisión Europea para acelerar la innovación de la cadena de bloques y desarrollar un ecosistema de transformación en la UE sustentado en esta tecnología- ha aportado algunos requerimientos con los que deben cumplir algunas técnicas criptográficas que deberían ser usadas para proteger el acceso a la información de carácter personal en las redes *blockchain*. Concretamente menciona que su diseño e implementación deberá previamente contar con una evaluación de los siguientes riesgos³⁴:

- A) Riesgo de reversión. Ocurre cuando es posible revertir el proceso y reconstituir los datos personales originarios. Bajo determinadas condiciones, en cadenas de bloques con un pequeño número de miembros es factible desencriptar los *hashes* probando a usar un descifrado de fuerza bruta. En este sentido, la clave pública usada para hacer transacciones en *blockchain* es considerada un dato seudonimizado.
- B) Riesgo de vinculación. Examinando patrones de uso, contextualizando o comparando los datos con otras piezas de información, los datos encriptados podrían ser vinculados a una persona concreta. La

34. European Union Blockchain Observatory and Forum (2018: 19).

técnica de cifrado de la información que se utilice debería tener el propósito de minimizar este riesgo.

En la misma línea, el Grupo de Trabajo del artículo 29 (ahora llamado *European Data Protection Board*) señalaba en su Dictamen 05/2014 tres aspectos que tienen que ser verificados para asegurar que la anonimización se ha realizado de forma correcta, a los cuales deberá atenderse para encriptar los datos personales que se manejen en una red *blockchain*³⁵. El primero de ellos es la singularidad de los datos resultantes, es decir, si es posible extraer de ellos información que permita identificar a la persona natural a la que pertenecen los mismos. El segundo es la vinculación -o vinculabilidad-, según la cual hay que averiguar si pueden conectarse varias transacciones o registros de información que puedan producir que se atribuyan dos o más de ellas a un mismo individuo -lo que, por ejemplo, puede ocurrir cuando se vincula la clave pública de *blockchain* con el perfil de una red social-. Y el tercero es la inferencia, que se encarga de determinar si es posible deducir o no con una significativa probabilidad el valor de un atributo al que no se tiene acceso a partir de los valores de un conjunto formado por otros atributos a los que sí.

Teniendo en cuenta la evitación de estos riesgos, el *European Union Blockchain Observatory and Forum* ha propuesto algunas técnicas de anonimización de datos personales en redes *blockchain* que podrían cumplir con lo dispuesto en el RGPD. En primer lugar, menciona la ofuscación de direcciones personales, que trata de dificultar la desanonimización de los datos a partir de los patrones de comportamiento y vinculaciones que se detectan del uso de la clave pública. Existen dos técnicas de este tipo³⁶: el servicio de direccionamiento de terceros, consistente en pedir a un tercero que agregue transacciones en la red empleando su propia clave pública; y la firma de anillos, según la cual un conjunto de sujetos firma la transacción, de forma que un tercero ajeno al traspaso de la información desconocerá cuál de las partes es el firmante legítimo. En segundo lugar, las técnicas de anonimización pueden consistir en un cifrado de los datos personales que según cómo se realice tendrá un mayor o menor riesgo de reversibilidad -para mitigarlo se aplican unas técnicas denominadas *salting* y *peppering*, encargadas de agregar información adicional a los *hashes* para que no puedan revertirse³⁷. En tercer lugar, explica una serie

35. Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2014).

36. European Union Blockchain Observatory and Forum (2018: 20).

37. European Union Blockchain Observatory and Forum (2018: 21 y 22).

de técnicas criptográficas más avanzadas como son las pruebas *ZKP* o de conocimiento cero, la encriptación homomórfica y la agregación de datos personales.

En definitiva, cuando como consecuencia de la actividad que se realiza en las redes *blockchain* se efectúa un tratamiento de datos personales lo ideal es que, en el propio diseño de la red *blockchain*, se tengan en cuenta los requerimientos de privacidad que van a necesitarse para proteger la información de las transacciones que se introduzcan en la misma. En el caso de que ello no haya sido posible se procurará mantener la información fuera de la cadena de bloques (*hashing* criptográfico) y, de no ser posible, se aplicarán técnicas criptográficas que permitan dificultar el acceso a la identidad de los individuos a los que pertenece la información con la que se realizan transacciones. Si ello no fuera posible, la información de carácter personal será subida a la red *hasheada* o en bruto, aunque en cualquiera de los dos casos ese tratamiento incumpliría con las previsiones contenidas en el RGPD. Como puede verse, las soluciones técnicas para lograr una conciliación con lo previsto por las normas existen, pero han de ser analizadas e implementadas desde el primer momento. Así, es necesario tener en cuenta estas consideraciones desde el mismo diseño de cualquier red de *blockchain*, herramientas que son un ejemplo de la pertinente y necesaria hibridación de las soluciones normativas/jurídicas con la programación del concreto registro distribuido que se haga en cada caso (que se concreta así en la solución "normativa" de tipo tecnológico que ha de integrar a la primera y estar definida de modo que respete las previsiones y garantías jurídicas establecidas en materia de protección de datos).

5.8. La prohibición de adopción de decisiones individuales automatizadas en el uso de *smart contracts*

Por último, como cierre de esta exposición, consideramos idóneo preguntarnos por la compatibilidad que pudiera o no existir entre el uso de contratos inteligentes y el derecho a la limitación del tratamiento de datos del que disponen las personas físicas previsto en el artículo 18 RGPD. El dilema que aquí se plantea es si las decisiones totalmente automatizadas que se rigen por la tecnología *blockchain* admiten o no una limitación en el tratamiento de datos.

La adopción de decisiones automatizadas no se encuentra prohibida en todos los casos, de forma que si esta fuera necesaria para la celebración o ejecución de un contrato o se basara en el consentimiento explícito del interesado -recordemos que, como ya hemos expuesto, el acceso que otorga el ciudadano al dato puede entenderse como una acción informativa- su utilización sería conforme al artículo 22 RGPD. Sin embargo, es cierto que esta clase de supuestos son infrecuentes en el ámbito administrativo, razón por la cual su uso debería regularse mediante norma, estableciéndose las medidas necesarias de salvaguarda de derechos y libertades que pudieran entrar en juego³⁸. En este sentido, sería perfectamente posible que el *smart contract* limitara el tratamiento de datos planificando el programa informático a esos efectos. Y para los usos públicos, la programación del registro distribuido en cuestión debiera ser entendida como un elemento normativo al que aplicar las garantías exigidas en cada caso, que deberían quedar incorporadas al concreto diseño de la red.

En cualquier caso, como no puede ser de otra manera, el interesado no puede quedar completamente desprotegido ante la decisión adoptada de forma automatizada, de modo que lo apropiado será que cuente con la posibilidad de solicitar una explicación u oponer una reclamación ante la decisión de forma que la respuesta que reciba sí que requiera de intervención humana, conforme a lo que se establece en el apartado 3 del artículo 22 RGPD. Adicionalmente, y en la medida en que se vaya avanzando en la consideración de que las actuaciones de este tipo se conforman a partir de una programación de la cadena de bloques que determina efectos normativos para los ciudadanos afectados por su funcionamiento, estas posibles decisiones automatizadas basadas en el mismo habrían de incorporar derechos y garantías más allá de esta explicación en caso de ser solicitada. Y, de igual manera, deberían incorporar más transparencia respecto del funcionamiento de la herramienta, dando incluso total acceso al código que permite entender su funcionamiento en algunos casos, así como medidas de recurso y garantía frente a los resultados aplicativos³⁹. Ello, no obstante, requeriría de una revisión de las normas de transparencia para que facilitasen criterios claros de publicación o acceso a los algoritmos que tuvieran en cuenta la necesidad de proteger los derechos de los ciudadanos por el uso de sistemas automatizados.

38. Valero Torrijos (2019: 90).

39. Boix Palop (2020: 249-261).

6. Bibliografía

- Agencia Española de Protección de Datos (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. Disponible en: <https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf> (última consulta: 14/10/2021).
- Alamillo Domingo, I. (2019a). Las tecnologías de registro distribuido (*blockchain*) y la transformación del procedimiento administrativo. *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, 1, 57-65.
- (2019b). El RDL 14/2019: una extraordinariamente urgente e innecesaria reforma del régimen de identificación y firma electrónica en la LPAC. *El Consultor de los Ayuntamientos*, 12, 112-123.
- Alonso Suárez, L. (2021). La aplicación de la tecnología *blockchain* en las ciudades inteligentes: hacia una gestión urbana descentralizada e inteligente. *European Review of Digital Administration & Law*, 2 (1), 107-126.
- Barrero Rodríguez, C. (2014). Transparencia: ámbito subjetivo. En E. Guichot Reina (coord.). *Transparencia, Acceso a la Información Pública y Buen Gobierno. Estudio de la Ley 19/2013, de 9 de diciembre* (pp. 63-96). Madrid: Tecnos.
- Bernal Blay, M. Á. (2018). *Blockchain, Administración y contratación pública*. Observatorio de Contratación Pública. Disponible en: <http://www.obcp.es/opiniones/blockchain-administracion-y-contratacion-publica> (última consulta: 13/10/2021).
- Boix Palop, A. (2015). El equilibrio entre los derechos del artículo 18 de la Constitución, el “derecho al olvido” y las libertades informativas tras la Sentencia Google. *Revista General de Derecho Administrativo*, 38.
- (2019). Reforma jurídico-administrativa, procedimiento electrónico y administración local. *Revista galega de Administración pública*, 58, 29-73.
- (2020). Los algoritmos son reglamentos: La necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones. *Revista de Derecho Público: Teoría y Método*, 1, 223-269.
- (2021). El Reial decret llei 14/2019, el constreyniment de les comunitats autònomes en matèria d'utilització d'eines digitals i electròniques i l'increment del control administratiu de l'opinió i de la informació en xarxes. *Revista catalana de dret públic*, 61, 14-29.

- Cerrillo i Martínez, A. (2016). ¿Cómo facilitar el ejercicio de los derechos de los ciudadanos en la administración electrónica? En A. M. Delgado García y R. T. Borge Bravo (coords.). *Nuevas tendencias en Internet, Derecho y Política* (pp. 175-194). Barcelona: Huygens.
- Commission Nationale Informatique & Libertés (2018). *Blockchain. Solutions for a responsible use of the blockchain in the context of personal data*. Disponible en: https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf (última consulta: 12/10/2021).
- European Union Blockchain Observatory and Forum (2018). *Blockchain and the GDPR*. Disponible en: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (última consulta: 14/10/2021).
- Federación Española de Municipios y Provincias (2017). *Comentarios sobre aspectos clave en materia de acceso a la información pública*. Cizur Menor (Navarra): Thomson Reuters-Aranzadi.
- Gamero Casado, E. (2021). *Compliance* (o Cumplimiento Normativo) de desarrollos de Inteligencia Artificial para la toma de decisiones administrativas. *Diario La Ley*, 50.
- Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2014). *Dictamen 05/2014 sobre técnicas de anonimización*. Disponible en: <https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf> (última consulta: 14/10/2021).
- Hernández San Juan, I. (2019). Tecnología *blockchain* y regulación de la trazabilidad: la digitalización de la calidad y seguridad alimentarias. *Revista General de Derecho de los Sectores Regulados*, 4, 1-29.
- Ibáñez Jiménez, J. W. (2018). *Blockchain: Primeras cuestiones en el ordenamiento español*. Madrid: Dykinson.
- Jiménez Serranía, V. (2020-2021). La Blockchain como medio de protección del diseño: “Design blockchain by design”. *Cuadernos del Centro de Estudios en Diseño y Comunicación*, 106, 181-199.
- Martín Delgado, I. (2020). Innovación tecnológica e innovación administrativa en la contratación pública. En I. Martín Delgado y J. A. Moreno Molina (dirs.). *Administración electrónica, transparencia y contratación pública* (pp. 19-54). Madrid: Iustel.
- Merchán Murillo, A. (2019). Identidad digital: su incidencia en el *blockchain*. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 50, 1-19.
- Pereiro Cárceles, M. (2019a). La utilización del blockchain en los procedimientos de concurrencia competitiva. *Revista General de Derecho Administrativo*, 50.

- (2019b). Usos de la tecnología “blockchain” en la Administración pública. En B. Puentes Cociña y A. Quintiá Pastrana (dirs.). *El derecho ante la transformación digital. Oportunidades, riesgos y garantías* (pp. 141-154). Barcelona: Atelier.

Pereiro Cárceles, M. y Doménech Pascual, G. (2019). Artículo 3. Otros sujetos obligados. En J. J. Díez Sánchez y R. García Macho (eds.). *Comentarios a la Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana* (pp. 30-45). Madrid: Reus.

Tejedor Bielsa, J.C. (2020). Transformación digital, "blockchain" e inteligencia artificial en la administración pública. *Revista Española de Derecho Administrativo*, 209, 111-138.

Valero Torrijos, J. (2015). La trasposición en España de la normativa europea sobre contratación pública electrónica: una oportunidad para la innovación tecnológica. En M. Almeida Cerredá e I. Martín Delgado (dirs.). *La nueva contratación pública* (pp. 29-45). Toledo-Santiago de Compostela: Red Internacional de Derecho Europeo.

- (2019). Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. *Revista catalana de dret públic*, 58, 82-96.

Velasco Rico, C. (2019). La ciudad inteligente: entre la transparencia y el control. *Revista General de Derecho Administrativo*, 50, 1-29.

Vivas Augier, C. (2017). Aplicaciones transversales de la blockchain. En A. Preukschat (coord.). *Blockchain: la revolución industrial de internet* (pp. 119-129). Barcelona: Gestión 2000.

Zyskind, G., Nathan, O. y Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE CS Security and Privacy Workshops*, 180-184.

***Blockchain* y contratación pública: análisis general e implicaciones en el ámbito local**

María Hernando Rydings

*Profesora contratada doctora de Derecho Administrativo.
Universidad Rey Juan Carlos*

SUMARIO. 1. Introducción: qué es el *blockchain*. 2. Desafíos a la integridad en la contratación pública. 3. Proyección de la tecnología del *blockchain* en el ámbito de la contratación pública. 3.1. Utilización del *blockchain* y de los *smart contracts* en los procedimientos de adjudicación de contratos públicos. 3.1.1. El procedimiento abierto supersimplificado como marco idóneo para la utilización del *blockchain*: breve recordatorio. 3.1.1.1. Ámbito de aplicación. 3.1.1.2. Tramitación del procedimiento. 3.1.2. ¿Cómo funcionan el *blockchain* y los *smart contracts* en la presentación de ofertas y la adjudicación de un contrato? 3.2. Acreditación de los requisitos del contratista y Registro de Licitadores. 3.3. Ejecución de contratos. 3.4. Algunos supuestos prácticos. 4. Estado actual de la regulación relativa a la utilización de los sistemas que conlleven *blockchain*. 5. Bibliografía.

1. Introducción: qué es el *blockchain**

En los últimos años, se viene atribuyendo un considerable protagonismo al fomento de la utilización de la tecnología *blockchain* por las administraciones

* Este trabajo ha sido realizado en el marco del Grupo de Excelencia de la Universidad Rey Juan Carlos, “Derecho y política económica” (GEDYPE), y del Grupo de Investigación de la Universidad Complutense de Madrid 931089, “Las transformaciones del Estado y la autonomía local: organización institucional, servicios públicos y democracia participativa”, en los que colaboro como miembro.

públicas aprovechando la obligatoriedad de la utilización de la administración electrónica. También es habitual que al hablar de la tecnología *blockchain* se haga referencia a los *smart contracts*. En estas páginas hablaremos de ambas realidades, de manera que puede ser útil caracterizarlas de manera inicial, para después centrarnos en su aplicación al sector de la contratación pública.

En este sentido, con la expresión *blockchain*, se hace referencia a una tecnología de registro distribuido o sistema de identificación que funcionaría como un registro virtual o base de datos, permitiendo identificar de manera fehaciente al usuario y la operación o transacción que se está realizando a través de la misma, y almacenándolas de manera permanente¹. La novedad que presentaría esta tecnología respecto de otras ya utilizadas en las plataformas tradicionales, es que la información que se aloja en esa base de datos se encuentra encriptada en bloques a disposición de todos los miembros que forman parte de ella, que serán los encargados de verificar las transacciones realizadas sin necesidad de que participe una entidad de control centralizada².

La denominación de *blockchain* proviene de su modo de funcionamiento, ya que se basa, como decimos, en la creación de una cadena de bloques sellados, que resulta imposible de falsificar y a la que tienen acceso todos los usuarios de la cadena. Cada bloque, a su vez, incorpora la información relativa a las operaciones, transacciones o datos que tengan que ver con el procedimiento en el que esté incurso. Además, todos los usuarios disponen de igual información en tiempo real, siendo imposible la alteración de los datos, ya que la modificación de la citada información que se incluye en los bloques requiere el consenso de todos los dispositivos que están en la red³. Tampoco resulta necesaria, como decimos, la existencia de intermediarios que tengan que realizar la labor de

1. *Blockchain* ha sido definido por Berryhill *et al.* (2020) como “una herramienta tecnológica que posibilita un sistema de contabilidad distribuido digital que actúa como un registro abierto, compartido y de confianza que realiza transacciones entre las partes y no se almacena por una autoridad central y sigue manteniendo el enfoque tradicional”. Por su parte, Pereiro Cárceles (2019: 3) define *blockchain* como “una herramienta tecnológica que permite registrar información en una base de datos, almacenando de modo permanente las transacciones que se realizan en una red”. En este sentido también, la Proposición de Ley de Transformación Digital presentada por el Grupo Parlamentario Popular y publicada en el Boletín Oficial de las Cortes Generales de 26 de julio de 2021 incluye una definición del *blockchain* en los siguientes términos: “Tipo de libro de registros distribuido, de todas las operaciones que se realizan en la red en un tiempo determinado. Funciona como una base de datos descentralizada y administrada por computadores pertenecientes a una red de punto a punto o P2P (peer-to-peer). Los mecanismos de consenso y la criptografía garantizan la seguridad de la red, no pudiendo eliminar ni modificar nada sin el consenso de la mayoría de los participantes de la red”.

2. En ese sentido se pronuncia Pereiro Cárceles (2019: 3).

3. Al respecto, *vid.* Ibáñez Jiménez (2019).

identificar a los usuarios de la cadena de bloques⁴: así concebida, todos ellos se convierten en “supervisores” de la cadena de bloques, lo que determina también que ese papel ya no sea exclusivo de la Administración.

Por otro lado, hay que precisar también que no todas las redes *blockchain* aparecen configuradas del mismo modo, lo que determinaría la necesidad de que la Administración deba elegir la que mejor responda a sus necesidades⁵. En este sentido, y en función del tipo de acceso que se requiera a los usuarios para poder acceder a la red, cabe diferenciar entre redes públicas y privadas. En una red pública puede participar cualquier usuario, por cuanto su acceso es abierto. En cambio, para poder participar en una red privada se requiere una invitación. De este modo, y para que la Administración pueda realizar las labores de supervisión de las operaciones que se vayan realizando en la cadena de *blockchain*, sería preferible que en los procedimientos administrativos que se tramitaran utilizando este tipo de tecnología se utilizaran redes privadas⁶.

De este modo, la tecnología *blockchain* ofrece una serie de ventajas que parecen hacer aconsejable su utilización en ciertos sectores del derecho, como la contratación pública: garantiza la inmutabilidad e integridad de la información; es un medio seguro de identificación de los usuarios; y logra incrementar la seguridad jurídica en las operaciones y actuaciones llevadas a cabo por agentes públicos y privados, así como una mayor integridad y transparencia de los mismos⁷.

Por otro lado, resulta muy habitual, como decíamos antes, que se haga referencia a los *smart contracts* al tratar el *blockchain*. Los *smart contracts*

4. De este modo, el *blockchain* puede concebirse como una base de datos de la que existen múltiples copias idénticas distribuidas entre varios participantes, las cuales se actualizan de manera sincronizada por consenso de las partes. Así lo define Romero Ugarte (2018).

5. Bernal Blay (2018a) señala al respecto que esta circunstancia permite hablar de un “Blockchain by design”.

6. En este sentido, Pereiro Cárceles (2019) señala que “mediante la utilización de la red privada se renuncia a la desintermediación en la gestión administrativa, al ser necesario que exista un órgano de control que autorice los accesos a la red, de tal manera que el grado de simplificación administrativa que se alcanza es menor que en una red pública. En la red privada se reduce notablemente la descentralización”.

7. Pereiro Cárceles (2019: 3) apunta que esta herramienta también conlleva ciertas limitaciones que dificultan su utilización, y como se ha puesto de manifiesto “su uso nunca será efectivo si no se dedican ingentes recursos materiales, económicos y personales a un tratamiento avanzado de la información que permita que la información esté disponible en formatos adecuados que posibiliten su registro en esta red. Las dificultades que la Administración pública vive para digitalizar documentos adecuadamente e intercambiarlos en sistemas interoperables y seguros constituyen, junto con el coste energético que conlleva *blockchain*, los principales problemas a los que la implantación de esta tecnología tendrá que hacer frente”.

pueden ser definidos, siguiendo a Pereiro Cárceles, como “programas de software que, verificando el cumplimiento de determinadas condiciones, se ejecutan automáticamente”. En este sentido, se rigen bajo la fórmula “si X, ocurre Y”, desencadenando una serie de consecuencias a partir de una serie de observaciones. No hay acción humana en este proceso, más allá del algoritmo que marca el funcionamiento del *smart contract*, ni tampoco intermediarios⁸. Y ambas herramientas aparecen ligadas, por cuanto el *smart contract* basa la automatización de su funcionamiento en la tecnología *blockchain*.

Con esta carta de presentación, y como decía antes, parece que ambas herramientas -*blockchain* y *smart contracts*-, con las debidas cautelas, pueden ser utilizadas por las administraciones públicas, y de manera particularmente aconsejable en procedimientos de concurrencia competitiva en los que se vayan a configurar actuaciones administrativas automatizadas, como puede ser el de la contratación pública. Lo cierto es que ya se ha realizado en este sector una utilización pionera de las mismas: en el País Vasco, para operar sobre el Registro de contratistas, y en Aragón, en el seno de diversos procedimientos abiertos abreviados. De ello se hablará más adelante. No obstante, deviene necesario analizarlas desde una perspectiva crítica, por cuanto la especialización y formación que requiere su aplicación va a impedir su utilización generalizada en el ámbito de la Administración pública y muy especialmente en el ámbito local, el cual carece, con carácter general, de los medios personales y reales que requiere la aplicación de este tipo de sistemas. Y es que resulta evidente que poco tienen que ver los medios y las necesidades de las entidades locales con los que precisan las administraciones de mayor envergadura. Por ello, no parece que vaya a resultar sencilla la extensión de la utilización de este tipo de sistemas al ámbito local.

8. Así los define Pereiro Cárceles (2019: 4), el cual además diferencia entre los *smart code contracts* y los *smart legal contracts*. Al respecto aclara que la tecnología *blockchain* se utiliza en los primeros. El citado autor también apunta a las dificultades que presenta la utilización de los *smart contracts*, y así señala que habría que guardar la debida cautela al determinar los procedimientos que se van a someter a ejecución automática para que no se pongan en peligro determinados derechos de defensa del particular, como el derecho a presentar alegaciones. De este modo, hay que asegurar el cumplimiento de las garantías procedimentales. Pero, además, la utilización de los *smart contracts* no sería posible en relación con los procedimientos que conlleven la toma de decisiones discrecionales. De este modo, como afirma el citado autor, en la medida en que la valoración dependa de distintos intereses generales no identificables a través de datos concretos, no será posible utilizar los *smart contracts* en la fase de valoración de un procedimiento administrativo. Así ocurrirá en aquellos procedimientos de evaluación en los que se realicen juicios de valor o se adopten decisiones conforme a criterios fijados mediante conceptos indeterminados cuyo significado no sea fácilmente calculable siguiendo algoritmos matemáticos. Ahora bien, también entiende Pereiro que en la práctica administrativa es difícil identificar decisiones puramente discrecionales en las que no hayan sido tenidos en cuenta elementos reglados, cuya localización e identificación podría realizar de forma automática *blockchain*.

Por otro lado, y a pesar del fomento en su utilización que se ha venido propugnando desde diversos foros, en la actualidad el *blockchain* no ha sido objeto de regulación, ni parece que se pretenda que lo sea a corto plazo. En este sentido, la única referencia que se realiza a este tipo de tecnología es la que se contiene en la disposición adicional sexta de la Ley 39/2015, del Procedimiento Administrativo Común (en adelante LPAC), para prohibir su regulación/utilización por parte de las comunidades autónomas en la normativa que desarrolle las prescripciones de la citada norma. Esta prohibición resulta llamativa, como analizaremos también más adelante, al resultar dudosa la posibilidad de que el Estado pueda proscribir en una norma básica esta opción. Por su parte, la única referencia que se hace implícitamente a los *smart contracts* en la normativa administrativa es la contenida en el artículo 41 de la Ley 40/2015, de Régimen Jurídico del Sector Público, al referirse a las actuaciones administrativas automatizadas: en su virtud, se prevé la posibilidad de que haya determinados trámites de la Administración que sean automatizados, en los que no intervenga de forma directa un empleado público. No obstante, resulta necesario que se asegure el cumplimiento de las garantías procedimentales correspondientes, so pena de invalidez de los mismos.

Partiendo de las diversas cuestiones que han quedado apuntadas, y tratando de analizar a continuación la utilización de la tecnología *blockchain* en el ámbito de la contratación pública, procederemos, en primer lugar, a recordar cuáles son algunos de los desafíos que amenazan la integridad en la contratación pública para poder concretar, en segundo lugar, cómo se aplica la citada tecnología a este sector y determinar si con ello quedan subvertidos los desafíos que se apuntaron en un primer momento. Todo ello al hilo del análisis de los casos en los que ya se ha utilizado el *blockchain*. Por último, se hará referencia al derecho positivo que se ocupa de la misma.

2. Desafíos a la integridad en la contratación pública

Uno de los mayores desafíos a los que se enfrenta la contratación pública en general, consiste en la necesidad de garantizar la transparencia y la efectiva concurrencia en la adjudicación de los contratos públicos. Conforme al documento *Análisis sobre la contratación pública en España: oportunidades de mejora desde el punto de vista de la competencia*, publicado por la Comisión Nacional de los Mercados y la Competencia, con fecha de 5 de febrero de 2015, y al Informe anual de supervisión de la contratación pública en España (2020), dicha contratación representa entre el 10 y el 20 % del PIB en nuestro

país, y se ha calculado que en ausencia de presión concurrencial se pueden originar desviaciones medias, al alza, del 25 % del presupuesto de la contratación pública. En España, esto podría implicar hasta un 4,6 % del PIB anual, aproximadamente 47 500 millones de euros/año⁹.

Más recientemente, en otro *Informe sobre los procedimientos de adjudicación*, realizado por el mismo organismo, se recogen dos importantes conclusiones¹⁰. Por un lado, se sostiene que la elección del procedimiento de contratación no es neutral para la eficiencia en la adjudicación, en términos de coste, en la contratación pública¹¹. Y ello porque se obtiene una relación negativa entre la selección del procedimiento abierto (el más competitivo de todos) y el precio de adjudicación que paga la Administración por la licitación, ya que, “de media, la Administración paga un 9,9 % menos en los contratos en los que utiliza el procedimiento abierto en vez de un procedimiento no abierto (negociados, restringidos y diálogos competitivos)”.

En segundo lugar, se defiende claramente la utilización del procedimiento abierto, al sostener que el mismo permitiría obtener ahorros significativos en las licitaciones¹².

Esta amenaza a la integridad en la contratación pública como consecuencia de la falta de competencia y de transparencia que afecta a este sector, también ha sido subrayada por la Unión Europea¹³, y es una de las claves de bóveda

9. *Vid. Análisis sobre la contratación pública en España: oportunidades de mejora desde el punto de vista de la competencia*, publicado por la Comisión Nacional de los Mercados y la Competencia, con fecha de 5 de febrero de 2015, p. 6, y el Informe anual de supervisión de la contratación pública en España (2020), de la Oficina Independiente de Regulación y Supervisión de la Contratación.

10. Informe *Radiografía de los procedimientos de contratación pública en España*, publicado por la CNMC, con fecha de 7 de febrero de 2019.

11. En este sentido, se afirma que “la intensidad de la competencia en el aprovisionamiento público es reducida, como revela el elevado porcentaje de licitaciones con un único participante (en casi un 34 % de los contratos estatales hay un único participante, y en un 66 % de los contratos estatales hay 3 o menos participantes)”. Pero además se señala que “en los contratos de importe reducido se recurre con mucha frecuencia al procedimiento negociado sin publicidad, y estos contratos tienen un peso significativo en el total de contratos (el 50 % de los contratos estatales tienen un presupuesto inferior a 92 389 €)”.

12. Al respecto, se señala que, si hubiera sido posible la utilización de procedimientos abiertos en todas las licitaciones, el coste de la contratación pública habría sido, como mínimo y bajo criterios muy conservadores, unos 1700 millones de euros inferior en el periodo 2012-2016 (Informe *Radiografía de los procedimientos de contratación pública en España*, publicado por la CNMC, con fecha de 7 de febrero de 2019, p. 50).

13. Así, entre otros, puede citarse el Informe monográfico de la Comisión al Consejo y al Parlamento Europeo sobre la lucha contra la corrupción en la Unión Europea en 2014.

de las directivas de contratación pública actualmente vigentes¹⁴ y que se implementaron en virtud de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (en adelante, LCSP), y el Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales (en adelante, LSE)¹⁵.

En este sentido, la LCSP, en la que centraremos nuestro análisis al incluir la regulación sustantiva de la adjudicación de los contratos públicos, incluye, como uno de sus principales objetivos, lograr una mayor transparencia, integridad y eficiencia en el ámbito de la contratación pública¹⁶. Así, la Ley introduce diversas medidas que buscan dar cumplimiento al citado objetivo, entre las que cabe citar, a modo de ejemplo, las previsiones relativas a la lucha contra la corrupción y los conflictos de intereses, mediante la imposición al órgano de contratación de la obligación de tomar las medidas adecuadas para luchar contra el fraude, el favoritismo o la corrupción; la regulación de las prohibiciones para contratar o una regulación, más exhaustiva, del perfil de contratante, el cual viene a desempeñar un papel protagonista como instrumento de publicidad de los distintos actos y fases de la tramitación de los contratos¹⁷. En el ámbito de los procedimientos de adjudicación, también se incluyeron medidas destinadas a fomentar una mayor transparencia, como ocurre con la

14. Son las directivas 2014/23/UE, relativa a la adjudicación de contratos de concesión; 2014/24/UE, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE; y 2014/25/UE, relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales y por la que se deroga la Directiva 2004/17/CE.

15. La citada LCSP fundamentalmente traspuso las dos primeras directivas (2014/23 y 2014/24), aunque, tal y como advierte el propio Preámbulo de la Ley, esta también resulta de aplicación a los contratos que liciten las administraciones públicas en los conocidos como sectores excluidos (agua, energía transporte y servicios postales). Sobre las directivas pueden consultarse, entre otras, las siguientes referencias: Gimeno Feliu (2013: 39) y Moreno Molina (2013: 115). Por otro lado, la LCSE traspuso parte de la Directiva 2014/25.

16. Concretamente, tal y como señala el Preámbulo, en su apartado II, *in fine*, uno de los objetivos primordiales de la norma consiste en articular un “sistema de contratación pública, más eficiente, transparente e íntegro, mediante el cual se consiga un mejor cumplimiento de los objetivos públicos, tanto a través de la satisfacción de las necesidades de los órganos de contratación, como mediante una mejora de las condiciones de acceso y participación en las licitaciones públicas de los operadores económicos”. No obstante, además de la anterior, la referencia a la búsqueda de la transparencia e integridad es muy recurrente a lo largo del citado Preámbulo, y por ello esta se configura realmente como uno de los pilares de la nueva LCSP.

17. Se ha ocupado de analizar cómo puede fomentarse una mayor transparencia e integridad en la contratación pública, entre otros, Gimeno Feliu (2017), que ha analizado la importancia de los principios de integridad y transparencia en la contratación pública, proponiendo, a su vez, un decálogo de propuestas de mejora que deberían incluirse en la legislación de contratación pública. Véanse también Gimeno Feliu (2010), Malaret (2016), Cerrillo i Martínez (2012), o Medina Arnáiz (2014).

eliminación del procedimiento negociado sin publicidad por razón de la cuantía, del protagonismo que en el ámbito de los procedimientos con negociación se atribuye a esta última, con las importantes limitaciones que se prevén respecto de los contratos menores o con la inclusión de dos nuevas vertientes en el procedimiento abierto: la simplificada y la simplificada abreviada.

De este modo, y detectada la necesidad de lograr articular adjudicaciones de contratos públicos que garanticen el cumplimiento de los principios que informan la contratación pública, y muy especialmente el de la integridad y la transparencia, se han incluido diversas medidas en nuestra normativa de contratación pública con el objetivo de lograr lo anterior. No obstante, y de conformidad con los datos publicados en el *Informe sobre la contratación pública de 2021*, emitido por la OIRESCON, las irregularidades en la adjudicación de contratos constituyen la primera causa de las denuncias que se formularon a lo largo del año 2020 en las distintas agencias antifraude¹⁸. Es por ello por lo que podría pensarse en la procedencia de aplicar medidas adicionales, como las que ofrece el *blockchain*, que pudieran contribuir a garantizar la consecución de estándares más elevados de integridad.

3. Proyección de la tecnología del *blockchain* en el ámbito de la contratación pública

Los sistemas electrónicos de registro distribuido, del que *blockchain* forma parte, como decíamos, “permiten el almacenamiento de información, o su representación digital mediante huella electrónica, de manera permanente, simultánea y sucesiva en una base de datos distribuida de manera que quede garantizada la inmutabilidad de dicha información y se permita la auditoría de su integridad”¹⁹.

A su vez, por medio de los *smart contracts*, como también señalamos antes, se puede lograr la adopción de una decisión administrativa automatizada, sin necesidad de la intervención de un agente público.

Ambas herramientas pueden resultar de aplicación en el ámbito de la contratación pública y ser utilizadas -como ha destacado Bernal Blay, entre

18. *Informe anual de supervisión de la contratación pública. Módulo IV: La prevención y lucha contra la corrupción en la contratación pública. 2021*, de OIRESCON.

19. La citada definición se recogía en la disposición adicional cuarta del Proyecto de Ley de organización y uso estratégico de la contratación pública en Aragón, publicado en el Boletín Oficial de las Cortes de Aragón núm. 266, de 1 de agosto de 2018, el cual no ha tenido ulterior desarrollo.

otros-, en primer lugar, para registrar ofertas y adjudicar un contrato, siempre que el procedimiento de adjudicación no requiera la realización de juicios de valor ni la intervención de agentes públicos. Pero también para la acreditación de la solvencia (siendo un atributo de la identidad digital del empresario), así como, en tercer lugar, para la automatización de los pagos a los contratistas, o, por último, para el mejor control en la ejecución de los contratos²⁰.

No obstante, a día de hoy, este tipo de tecnología ha tenido una aplicación muy limitada en nuestro país y solo se ha utilizado, como apuntamos antes, en el País Vasco, para la construcción de una aplicación para la consulta de los datos de su Registro de contratistas, y por parte del Gobierno de Aragón, que licitó un servicio de registro distribuido de ofertas para contratos públicos que permitiese posteriormente su evaluación automatizada, utilizando para ello el procedimiento abierto simplificado abreviado.

En cualquier caso, conviene analizar con mayor detalle cómo se aplicarían estas herramientas en los ámbitos apuntados: en el ámbito de la adjudicación de un contrato por medio de un procedimiento abierto simplificado abreviado, en relación con el Registro de Licitadores, y, en tercer lugar, en relación con el pago a contratistas o la ejecución de contratos. Por último, haremos referencia también a la aplicación práctica que han tenido las citadas tecnologías.

3.1. Utilización del *blockchain* y de los *smart contracts* en los procedimientos de adjudicación de contratos públicos

La presentación electrónica de ofertas y solicitudes de participación, como es sabido, constituye una obligación, de conformidad con la disposición adicional decimoquinta.3 de la LCSP, la cual solo puede exceptuarse en los casos previstos en la propia disposición²¹.

20. Bernal Blay (2018b: 136).

21. Las citadas excepciones son las siguientes: “Cuando, debido al carácter especializado de la contratación, el uso de medios electrónicos requeriría herramientas, dispositivos o formatos de archivo específicos que no están en general disponibles o no aceptan los programas generalmente disponibles; cuando las aplicaciones que soportan formatos de archivo adecuados para la descripción de las ofertas utilizan formatos de archivo que no pueden ser procesados por otros programas abiertos o generalmente disponibles o están sujetas a un régimen de licencias de uso privativo y el órgano de contratación no pueda ofrecerlas para su descarga o utilización a distancia; cuando la utilización de medios electrónicos requiera equipos ofimáticos especializados de los que no disponen generalmente los órganos de contratación o cuando los pliegos de la contratación requieran la presentación de modelos físicos o a escala que no pueden ser transmitidos utilizando medios electrónicos”.

Pero, además, es preciso que el empleo de medios electrónicos, informáticos y telemáticos en los procedimientos de adjudicación de contratos del sector público dé cumplimiento a las exigencias contenidas en las disposiciones adicionales decimosexta y decimoséptima de la citada norma.

Pues bien, partiendo de que la tecnología *blockchain* cumple con las citadas exigencias, como se ha puesto de manifiesto por especialistas en esta materia²², esta se podría utilizar, en primer lugar, fundamentalmente para una fase concreta del procedimiento de adjudicación de contratos, que sería la correspondiente a la de recepción de ofertas en los casos en que el procedimiento de adjudicación que se estuviera tramitando cumpliera también con unos determinados requisitos, que, como hemos dicho, parecen remitirse al abierto simplificado abreviado. A su vez, y en el marco del citado procedimiento, la valoración de las ofertas y su adjudicación también podrían realizarse de manera automatizada, por medio de un *smart contract*, sin necesidad, por tanto, de que haya intervención directa de un empleado público²³. Y decimos que el procedimiento idóneo para ello sería el simplificado abreviado por la propia configuración del mismo, la cual recordaremos brevemente a continuación para analizar con detalle después cómo se aplicarían ambas herramientas en la recepción y valoración de ofertas.

3.1.1. El procedimiento abierto supersimplificado como marco idóneo para la utilización del *blockchain*: breve recordatorio

La LCSP introdujo, en el ámbito del procedimiento abierto, dos nuevas vertientes denominadas simplificada y simplificada abreviada, que pretendían garantizar una mayor transparencia y eficiencia en la adjudicación de los contratos²⁴. También tenían como objetivo lograr reconducir los contratos

22. Pereiro Cárceles (2019).

23. Art. 41 de la Ley 40/2015, de Régimen Jurídico del Sector Público.

24. Esta nueva vertiente que, como decimos, no trae causa de las directivas comunitarias, sí había sido regulada con anterioridad a la LCSP, tanto en la Ley Foral 6/2006, de 9 de junio, de Contratos Públicos de Navarra, como en la Ley 3/2011, de 24 de febrero, de medidas en materia de Contratos del Sector Público de Aragón, y al parecer se han aplicado con bastante éxito. Resultan interesantes, en este sentido, los datos publicados por el Registro de Contratos del Sector Público respecto del número de contratos y procedimientos de adjudicación licitados en el ámbito del Estado, comunidades autónomas y entidades locales, en el año 2016. Tanto en Aragón como en Navarra, ambas con vertientes simplificadas del procedimiento abierto, la utilización del mismo supera a la utilización de los demás procedimientos: en Aragón se licitaron un total de 1076 contratos por medio del abierto y 949 a través de otros procedimientos, y en Navarra, 312 y 119, respectivamente, a diferencia de lo

que con anterioridad se adjudicaban mediante el procedimiento negociado sin publicidad por razón de la cuantía a estas nuevas vías simplificadas, que además de ser ágiles, como lo era el negociado sin publicidad, proporcionan la necesaria publicidad y transparencia en el procedimiento de licitación del contrato. Consideramos, además, que ambas vertientes del procedimiento simplificado resultan especialmente interesantes en el ámbito local, como consecuencia de las limitaciones que se han incluido en la aplicación de los contratos menores y en los procedimientos negociados sin publicidad, y de que las cuantías máximas que permiten la aplicación del procedimiento abierto simplificado y del supersimplificado son considerablemente elevadas.

La LCSP lo regula en el artículo 159.6, al que haremos referencia de manera telegráfica para poder dejar constancia de las principales características de la vertiente supersimplificada, que es la que nos interesa de cara a la ulterior concreción de la aplicación del *blockchain* en el mismo. Para ello, haremos referencia a su ámbito de aplicación y a la tramitación del procedimiento.

3.1.1.1. Ámbito de aplicación

El artículo 159.6 de la LCSP prevé que cabe acudir a esta tramitación *abreviada* del procedimiento simplificado en el caso de que se trate: bien de un contrato de obras, de valor estimado inferior a 80 000 €, o bien de un contrato de suministros o servicios, de valor estimado inferior a 35 000 €, a excepción de los que tengan por objeto prestaciones de carácter intelectual, que no pueden acudir a la aplicación de esta vertiente del simplificado.

También podrá ser de aplicación la tramitación prevista en el citado artículo 159.6 de la LCSP a los contratos de obras de valor estimado inferior a 200 000 €, y a los contratos de suministros y servicios de valor estimado inferior a 100 000 € que se vayan a financiar con fondos procedentes del Plan de Recuperación, Transformación y Resiliencia, excepto los que tengan por objeto prestaciones de carácter intelectual²⁵.

que ocurre en otras comunidades autónomas que no cuentan con la vertiente simplificada. Sobre la regulación de los procedimientos de adjudicación de contratos, puede consultarse Hernando Rydings (2019).

25. Y ello de conformidad con el artículo 51 del Real Decreto-ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia.

3.1.1.2. Tramitación del procedimiento

En primer lugar, se incluye un breve plazo de presentación de proposiciones, el cual no podrá ser inferior a diez días hábiles, a contar desde el siguiente a la publicación del anuncio de licitación en el perfil de contratante. No obstante, si se trata de compras corrientes de bienes disponibles en el mercado, el plazo se reduce a cinco días hábiles.

Por otro lado, se exige a los licitadores de la acreditación de la solvencia económica y financiera y técnica o profesional. Este aparente deseo del legislador de que se confíe en el mercado puede determinar la aparición de posibles problemas con el licitador que resulte adjudicatario, en el caso de que este no cumpla con unos estándares mínimos de solvencia, que, al no solicitarse, son desconocidos por el órgano de contratación en el momento de adjudicar el contrato²⁶.

En tercer lugar, y en relación con los criterios de adjudicación, estos deben ser cuantificables mediante la mera aplicación de fórmulas, y solo se presenta un sobre o archivo electrónico.

Lo anterior determina, a su vez, que la valoración de las ofertas se va a realizar, o bien automáticamente mediante un dispositivo informático, o bien con la ayuda de una unidad técnica que colaborará con el órgano de contratación. A su vez, un dispositivo electrónico deberá garantizar que no se procede a la apertura de las ofertas hasta que no haya finalizado el plazo de presentación de las mismas, y por ello no se exige que esta tenga lugar en acto público. Por otro lado, se requiere que todas las ofertas y la documentación presentada sean accesibles de forma abierta por medios informáticos y sin restricciones desde el momento en que se notifique la adjudicación del contrato.

Por último, no se requiere constituir garantía definitiva, y la formalización del contrato podrá realizarse mediante la firma de aceptación por el contratista de la resolución de adjudicación.

Estas características, como apuntábamos antes, convierten a este procedimiento en el idóneo para la utilización de la tecnología *blockchain*.

26. Quizá sería aconsejable entender que se permite la solicitud de la acreditación de la personalidad jurídica del licitador y de que el objeto social del mismo coincide con el objeto de la prestación que se licita, logrando evitar de esta forma riesgos y posibles dilaciones innecesarias.

3.1.2. ¿Cómo funcionan el *blockchain* y los *smart contracts* en la presentación de ofertas y la adjudicación de un contrato?

En términos generales, la aplicación de la tecnología *blockchain* al procedimiento de adjudicación de un contrato, como ha precisado Bernal Blay, podría funcionar, en términos generales, del siguiente modo: “se solicitaría a los licitadores la confección de su oferta en formato electrónico siguiendo un modelo normalizado y facilitado junto al pliego de cláusulas administrativas particulares que haya de regir la licitación. El licitador se identificará en el sistema que, a través de un servicio web, calculará la huella electrónica (*hash*) de la oferta del licitador, la presentará al sistema antes de que finalice el plazo de presentación de ofertas y la enviará para su registro a una red de registro distribuido. Una vez finalizado el plazo de presentación de ofertas, los licitadores deberán enviar su oferta en formato electrónico. El sistema tras volver a calcular la huella electrónica de la oferta, comprobará su coincidencia con la registrada previamente en la red de registro distribuido. En caso de darse esa coincidencia, la oferta sería admitida a la licitación y se procedería a su valoración”²⁷.

De este modo, la utilización de la tecnología *blockchain* en la fase de presentación de ofertas se llevaría a cabo en dos fases: en una primera se produce el registro de la huella electrónica, y en una segunda se envía la oferta. Esta posibilidad viene contemplada en la disposición adicional decimosexta de la LCSP, la cual prevé lo siguiente:

“En los procedimientos de adjudicación de contratos, el envío por medios electrónicos de las ofertas podrá hacerse en dos fases, transmitiendo primero la huella electrónica de la oferta, con cuya recepción se considerará efectuada su presentación a todos los efectos, y después la oferta propiamente dicha en un plazo máximo de 24 horas. De no efectuarse esta segunda remisión en el plazo indicado, se considerará que la oferta ha sido retirada”.

Veámoslo con mayor detalle.

Así, en primer lugar, se solicitaría a los licitadores la confección de su oferta en formato electrónico siguiendo un modelo normalizado y facilitado junto al pliego de cláusulas administrativas particulares que haya de regir la licitación. El licitador se identificará en el sistema, anunciando su oferta, y el

27. Bernal Blay (2018b: 135-136).

citado sistema, a través de un servicio web, generará la huella electrónica²⁸ de la oferta del licitador, la presentará al sistema antes de que finalice el plazo de presentación de ofertas y la enviará para su registro a una red de registro distribuido. En este sentido, se genera en el sistema un registro del momento exacto en el que la oferta ha sido presentada, tanto para el órgano de contratación como para el resto de licitadores. De este modo, una vez anunciada la oferta, y generada la huella electrónica, esta se volcará en el sistema *blockchain*, e incluirá información que permita distinguir al licitador que realiza la oferta, pero sin identificarlo, el contrato para el que presenta la oferta, y la fecha y hora de recepción de la solicitud en el sistema. De este modo, toda la red conoce de inmediato la presentación de las ofertas, pero no la oferta en sí²⁹.

Con posterioridad, los licitadores deberán enviar su oferta en formato electrónico, y ello “en un plazo máximo de 24 horas”, tal y como prevé la disposición adicional decimosexta.1.h) de la LCSP³⁰. El sistema, tras volver a calcular la huella electrónica de la oferta, comprobará su coincidencia con la registrada previamente en la red de registro distribuido. En caso de darse esa coincidencia, la oferta sería admitida a la licitación y se procedería a su valoración³¹.

Este sistema, según se ha apuntado, mejora la integridad y trazabilidad del procedimiento, siendo su presentación más sencilla y rápida, y no dándose problemas con la carga de archivos por su tamaño.

Una vez presentadas y admitidas, en su caso, las ofertas que cumplieran con los requisitos exigidos en la convocatoria, se procedería a su valoración. La utilización de un *smart contract* para realizarla solo sería posible si los criterios de adjudicación fueran cuantificables mediante la mera aplicación de fórmulas, y fuera posible realizar la valoración de las ofertas automáticamente mediante un dispositivo informático³². En este sentido, el *smart contract*

28. En este sentido, conviene aclarar también que, de conformidad con lo señalado en la citada disposición adicional decimosexta de la LCSP: “Se entiende por huella electrónica de la oferta el conjunto de datos cuyo proceso de generación garantiza que se relacionan de manera inequívoca con el contenido de la oferta propiamente dicha, y que permiten detectar posibles alteraciones del contenido de esta garantizando su integridad”.

29. Bernal Blay (2018b: 135).

30. No obstante, hay quien ha apuntado, como Quintana Cortés, que esta previsión debería modificarse para incluir la posibilidad de que se puedan enviar ofertas hasta el momento de apertura de las mismas.

31. Bernal Blay (2018b: 135-136).

32. Y ello, como se ha apuntado, dado el estado inicial en que se encuentra el proceso de maduración de esta tecnología, como recuerda Muñoz Carmona (2018).

estaría programado para que, una vez finalizara el plazo de presentación de ofertas, seleccionara de forma automatizada la que obtuviese una mayor puntuación de acuerdo con las fórmulas previamente establecidas. Así, el *smart contract* estaría realizando la función de valoración (aunque fuera automática) atribuida al órgano de contratación, el cual se limitaría a suscribir la adjudicación realizada por medio del *smart contract*. Por esta razón decíamos que posiblemente el procedimiento abierto simplificado abreviado, al ser el de tramitación más sencilla, sería el apropiado para poder albergar la utilización de ambas herramientas. Recordemos que la utilización de aquellas no sería posible en relación con ofertas que dependan de criterios cualitativos o juicios de valor.

No obstante, rápidamente se habrá caído en la cuenta de los problemas que podría suscitar la utilización de las adjudicaciones automatizadas. En este sentido, parece difícil justificar que el órgano de contratación pudiera apartarse de la adjudicación que hubiera realizado el *smart contract*. Ello, a su vez, exige que la determinación de los parámetros o algoritmos que deban seguirse para poder valorar ofertas y adjudicar el contrato se haya realizado correctamente, ya que lo contrario determinaría que el procedimiento de adjudicación estuviera viciado. Lo que, por tanto, resulta claro es que la utilización de este tipo de herramientas no puede conllevar una merma de los derechos y garantías de los administrados en el seno de los procedimientos en que sean utilizadas.

Por otro lado, y a pesar de que la aplicación del procedimiento abierto simplificado resulte especialmente interesante en el ámbito local, como consecuencia, como se apuntó antes, de las limitaciones que se han incluido en la aplicación de los contratos menores y en los procedimientos negociados sin publicidad, y de que las cuantías máximas que permiten la aplicación del procedimiento abierto simplificado y del supersimplificado son considerablemente elevadas, la especialización y la complejidad de la tecnología *blockchain* y de los *smart contracts* quizá impidan su utilización generalizada en este ámbito. En este sentido, parece prudente que no se exija a las asfixiadas administraciones locales el cumplimiento de nuevos objetivos, como son las tecnologías de las que hablamos, si no van acompañados de la correspondiente dotación de medios personales y reales. Solo así se podría comenzar a considerar la posibilidad de que el mundo local pueda ir dando cumplimiento a las exigencias técnicas que plantea el insaciable ámbito de la contratación pública.

3.2. Acreditación de los requisitos del contratista y Registro de Licitadores

La configuración de los registros por medio de tecnologías *blockchain* es otro de los ámbitos en los que se ha señalado la utilidad y eficacia de las mismas, al garantizar su inmutabilidad, trazabilidad y transparencia³³.

Así, en el ámbito de la contratación pública, se podría aplicar en el Registro Oficial de Licitadores y Empresas Clasificadas (en adelante, ROLECE), al que se hace referencia en los artículos 337 y ss. de la LCSP. La citada inscripción, como es sabido, tiene por objeto simplificar el trámite de acreditación del cumplimiento de los requisitos previos, ya que esta permite acreditar la personalidad jurídica del licitador, su habilitación profesional o empresarial, la representación y acreditación de no estar incurso en prohibiciones para contratar, así como su solvencia económica y financiera (art. 96.1 y 2 LCSP). De este modo, se evita la necesidad de tener que acreditar la misma al concurrir al procedimiento de adjudicación de un contrato.

Si el ROLECE funcionara por medio de la citada tecnología sería posible que los *smart contracts* se conectaran al mismo para que se pudiera comprobar, de forma automatizada y eficaz, la capacidad de los distintos licitadores³⁴. Incluso se podría incorporar al citado Registro el historial de relaciones contractuales con el sector público, lo cual podría prevenir problemas futuros y detectar, por ejemplo, si ha incurrido en retrasos en la ejecución del contrato, en posibles incumplimientos, o en resolución culpable de los contratos³⁵.

Pero, además, la tecnología *blockchain* podría ser de utilidad, tal y como se apunta, para la certificación de los requisitos que debe cumplir una entidad para ser contratista, ya que “una gestión avanzada de la información, disponible en una red *blockchain*, integrada por todas las administraciones públicas, permitiría una comprobación fácil y eficaz del cumplimiento de las condiciones de capacidad que podría ser consultada por cualquier Administración que actúe como nodo en la red”³⁶. De este modo, sería posible también que por medio de un *smart contract* se accediera y verificara la información necesaria para acreditar la solvencia económica y financiera y técnica, lo que además

33. *Vid.*, entre otros, García Meilán (2019).

34. Así lo apunta Muñoz Carmona (2018).

35. En este sentido, García Meilán (2019: 4).

36. Así se pronuncia Pereiro Cárceles (2019), que considera, además, que la automatización en el proceso permitiría bloquear la participación en el procedimiento de sujetos que incurran en causas de incompatibilidad o incapacidad, o cualesquiera otras que impidiesen el cumplimiento de los requisitos legales.

determinaría que no fuese necesario aportar documentos que ya tuviera la Administración³⁷.

Por último, también se ha señalado la posibilidad de utilización de la citada tecnología para simplificar la constitución del aval o garantía en los casos en que se exija para poder ser licitador de un contrato público. En este sentido, se ha afirmado que “el *blockchain* hace factible la creación de un registro que almacenase el importe total de las garantías que un sujeto ha puesto a disposición de la Administración pública. De este modo, esa cuantía podría ser utilizada en cualquier procedimiento público en que el licitador participe, sin necesidad de que constituya una garantía por cada uno de los procedimientos en los que concurre. Para ello, la red debería tener acceso a dichos recursos, procedentes de cualquiera de las vías señaladas en el artículo 108 de la LCSP”³⁸.

3.3. Ejecución de contratos

El uso del *blockchain* también podría extenderse a la fase de ejecución del contrato, aunque parece que actualmente su aplicación quedaría reducida a la automatización de la ejecución de prestaciones mediante la comprobación de hechos objetivos y fácilmente comprobables a través de la citada red, sin poder realizar aún tareas que conlleven la aplicación de juicios de valor³⁹.

Así, por un lado, podría utilizarse para la ejecución de ingresos y pagos sin necesidad de intermediarios, lo que además podría determinar una reducción de los plazos de pago de la Administración. Y también se

37. Pereiro Cárceles (2019) realiza un análisis detallado de cómo sería posible proceder a acreditar el cumplimiento de las distintas solvencias que se exigen a los contratistas. Así, el citado autor entiende que la solvencia económica y financiera podría acreditarse mediante el acceso a las cuentas de ahorro y a los activos financieros que un titular posee, previo aviso al mismo de que se va a realizar el citado acceso. Por otro lado, para acreditar la solvencia técnica, sería preciso verificar los medios humanos con que se cuenta para la ejecución del contrato. Así, los datos que consten en un certificado público o hubieran sido presentados en otros procedimientos administrativos, en inspecciones laborales o para el cumplimiento de obligaciones contables y económicas de la entidad, serían accesibles de forma automatizada por el *smart contract*.

38. Pereiro Cárceles (2019). Continúa señalando el citado autor que el *smart contract* permitiría además que el ingreso fuera automático, extrayendo el importe directamente de la cuenta asociada al registro para mantenerlo en reserva de forma segura hasta que se decidiese el adjudicatario. Una vez perfeccionado el contrato, se produciría también de forma automática la devolución de la garantía o el aval a los correspondientes licitadores.

39. *Vid.*, en este sentido, Pereiro Cárceles (2019).

ha señalado la posibilidad de controlar la ejecución mediante la conexión a objetos inteligentes, verificando, por ejemplo, el cumplimiento de los objetivos estipulados en el contrato⁴⁰.

No obstante, quizá el estado de inmadurez de este tipo de tecnología, que impide que sea utilizada para operaciones que requieran la realización de juicios de valor, no termina de aconsejar aún su utilización, y posiblemente sería necesario esperar a que se pudiera contar con sistemas de inteligencia artificial.

3.4. Algunos supuestos prácticos

Las dos principales iniciativas que han tenido lugar en nuestro país de uso de la tecnología *blockchain* en el ámbito de la contratación pública, han tenido lugar en Aragón y en el País Vasco.

Aragón puso en marcha en 2018 un registro distribuido de ofertas de contratos públicos. Este actúa como un sistema de presentación de ofertas que se sirve de la tecnología *blockchain*⁴¹. La licitación fue adjudicada a la propuesta conjunta de Open Canarias e IA Sof de entre las diez empresas que concurrieron a la licitación. Este sistema se ha utilizado en 24 concursos públicos, y mediante el mismo, que se ha utilizado en el marco del procedimiento abierto simplificado abreviado, se logra validar la presentación de ofertas, y automatizar la elección del licitador. En este sentido, los licitadores incorporan la huella electrónica de *blockchain* a la oferta, al presentar la propuesta. Al finalizar el plazo de presentación de ofertas, los licitadores presentan sus documentos de oferta en formato electrónico ante las autoridades de contratación. A continuación, mediante *smart contract* se valoran automáticamente las ofertas correspondientes.

Por otro lado, hace pocos meses, en mayo de 2021, fue publicado el anuncio de licitación para la adjudicación de un contrato de servicios para la contratación del desarrollo y evolución del sistema de licitación electrónica con tecnología de registro distribuido (*blockchain*) de la Comunidad Autónoma de Aragón, el cual fue finalmente adjudicado, mediante procedimiento abierto, a OESIA Networks, por algo de más 400 000 euros.

40. Pereiro Cárceles (2019).

41. Quintana Cortés (2020: 166).

También en Euskadi se ha licitado un contrato de servicios para el uso de *blockchain* en el registro de contratistas. Fue adjudicado a la mercantil ODEI S.A., en enero de 2018, por 24 000 euros.

Por otro lado, y aunque no ha sido en el marco de la contratación pública, existen iniciativas relacionadas con *blockchain* en diversas comunidades autónomas. Así, en Aragón se ha creado el *Blockchain Aragón*; en Galicia, la *Comunidade Blockchain de Galicia*; en Euskadi, *Blockchain Euskadi*; y en Cataluña se ha creado el *Observatorio de Contratación Pública*, promovido por la Generalitat de Cataluña. También, a nivel nacional, cabe citar al consorcio multisectorial Alastria, promovido por empresas e instituciones. No obstante, la mayoría de estas agrupaciones tienen por objeto el análisis de la aplicación de la citada tecnología en el sector privado, y escasamente hacen referencia al público, el cual aún está pendiente de desarrollo.

4. Estado actual de la regulación relativa a la utilización de los sistemas que conlleven *blockchain*

Actualmente no existen referencias directas al *blockchain* en la normativa básica estatal en materia de contratación pública. En cambio, sí encontramos una referencia en la normativa básica de procedimiento administrativo, concretamente en la disposición adicional sexta de la LPAC, como se apuntó al principio de este texto. La citada referencia trae causa de la reforma operada en la misma por el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Aunque el análisis detallado de la misma exceda con creces el objeto del presente estudio, sí haremos unas breves consideraciones que pueden ser de utilidad también en el ámbito de la contratación pública.

Y es que el artículo 3 del citado Real Decreto-ley incorporó una disposición adicional sexta a la LPAC, la cual dispone que en las relaciones de los interesados con las administraciones públicas: “no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificaciones basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del derecho de la Unión Europea”.

Además, la nueva disposición adicional sexta establece que “cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal deberá contemplar que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública”.

De este modo, se prohíbe temporalmente la utilización del *blockchain*, y se impide la identificación del ciudadano con sistemas basados en *blockchain* ante las administraciones públicas hasta que haya regulación europea. Esta prohibición resulta llamativa, ya que, por un lado, no es del todo evidente que el Estado pueda proscribir en una norma básica esta posibilidad. Pero, además, también se plantearía la duda de si la prohibición de su utilización se extendería a sectores concretos de actividad como puede ser el ámbito de la contratación pública.

En relación con la primera posibilidad, habrá que esperar a los correspondientes fallos del Tribunal Constitucional, pues han sido admitidos a trámite dos recursos de inconstitucionalidad. Por un lado, el recurso de inconstitucionalidad n.º 718-2020, promovido por la Generalitat de Cataluña contra determinados artículos del citado Real Decreto-ley 14/2019, entre los que se encuentra precisamente el 3. Y también el presentado por el Gobierno Vasco contra las disposiciones correspondientes de la citada norma.

Mientras tanto, y a la espera del fallo del Tribunal Constitucional, se han ido articulando regulaciones y propuestas por parte de algunas comunidades autónomas, como ocurre en el caso de Cataluña o Aragón.

Así, en Cataluña, se aprobó el Decreto 76/2020, de 4 de agosto, de administración digital, el cual, en el artículo 55.3, dispone lo siguiente: “La identificación de las personas físicas se puede realizar mediante los sistemas establecidos en las oficinas de asistencia en materia de registro y otros sistemas basados en un registro distribuido de identidades”.

Por su parte, Aragón también ha articulado una propuesta para la utilización de los citados sistemas de registro distribuido con las cautelas precisas para, aparentemente, no vulnerar la normativa básica de la disposición adicional sexta de la LPAC. Esta se prevé en el artículo 52 de la Ley 1/2021, de 11 de febrero, de simplificación administrativa de Aragón. En este sentido, el citado artículo dispone lo siguiente: “Podrán utilizarse sistemas electrónicos de registro distribuido para asegurar la aportación, acreditación e integridad de los datos y documentos en cualquier expediente, procedimiento o registro, sin perjuicio de lo establecido en el

artículo anterior respecto de identificación y firma⁴². 2. Podrán también utilizarse sistemas electrónicos de registro distribuido, con plena validez legal, para la realización de tramitación administrativa automatizada conforme a la normativa básica estatal y, en particular, en cualesquiera procedimientos de contratación pública. 3. A los efectos establecidos en esta Ley, tendrá la consideración de sistema electrónico de registro distribuido el que permita el almacenamiento de la información, o su representación digital mediante huella electrónica, de manera permanente, simultánea y sucesiva en una base de datos distribuida, de manera que quede garantizada la inmutabilidad de dicha información y se permita la auditoria de su integridad”.

Por último, también ha sido publicada recientemente, en el Boletín Oficial de las Cortes Generales de 26 de julio de 2021, la Proposición de Ley de Transformación Digital presentada por el Grupo Parlamentario Popular. En ella se hace referencia a la tecnología *blockchain* y a su uso por las administraciones públicas, en el artículo 52. En este sentido, propugna que las administraciones públicas, en el ámbito de sus competencias, fomentarán la implantación de plataformas digitales, tecnología *blockchain*, contratos inteligentes y otras formas de automatización para la transparencia, simplificación, seguridad y trazabilidad en el comercio⁴³, y prevé también su utilización en diversos sectores, como pueda ser el de los alimentos⁴⁴, centros sanitarios⁴⁵ o respecto de los medicamentos⁴⁶.

42. Dispone el artículo 51.1 lo siguiente: “La sede electrónica y sedes asociadas de la Administración de la Comunidad Autónoma de Aragón utilizarán como plataforma de identificación y firma de los usuarios Cl@ve, plataforma de identificación y firma electrónica utilizada por la Administración General del Estado, o un sistema equivalente, garantizando de esta manera la identificación y firma mediante certificado electrónico reconocido conforme a lo establecido en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. *En particular, podrán considerarse sistemas equivalentes de identificación y firma los basados en un registro distribuido de atributos de identidad aceptados por el órgano administrativo ante el que el interesado pretenda identificarse, de conformidad con lo establecido en la normativa estatal sobre procedimiento administrativo*”.

43. Se dispone en la citada Proposición que las administraciones públicas, en el ámbito de sus competencias, impulsarán un marco de identidad digital distribuida basada en *blockchain* para personas físicas y jurídicas.

44. Respecto de los productos alimentarios se señala que pueden contar con un pasaporte en el que se asigne una etiqueta asociada a cada producto con información codificada en una cadena de bloques personal, intransferible e inalterable, para que quede constancia de su paradero, y se utilizará el sistema *blockchain* para su trazabilidad de principio a fin.

45. Los centros sanitarios podrán usar la tecnología *blockchain* con el fin de ofrecer una mayor trazabilidad en las decisiones y los procesos médico-hospitalarios, así como en las gestiones de equipos valiosos de hospitales o expedientes médicos que impliquen decisiones de diferentes especialistas. En esos casos, el paciente será el propietario de su historial digital y decidirá a quién permite el acceso.

46. Y respecto de los medicamentos, se señala que las administraciones públicas, en el ámbito de sus competencias, impulsarán medidas para garantizar la autenticidad de medica-

5. Bibliografía

- Bernal Blay, M. Á. (2018a). Blockchain, Administración y contratación pública. *OBCP*.
- (2018b). El desarrollo autonómico de la normativa sobre contratos públicos. *Monografías de la Revista Aragonesa de Administración pública*. Zaragoza.
- Berryhill, J., Bourgerly, T. y Hanson, A. (2018). Blockchain unchained: blockchain technology and its use in the public sector. *OECD Working papers on public governance*, 28.
- Cerrillo i Martínez, A. (2012). *El principio de integridad en la contratación pública*. Cizur Menor: Aranzadi.
- García Meilán, J. C. (2019). *Blockchain y smart contracts* para la transparencia y confidencialidad de los contratos públicos. *Actualidad Administrativa*, 1.
- Gimeno Feliu, J. M.^a (2010). La Ley de Contratos del Sector Público: ¿una herramienta eficaz para garantizar la integridad? Mecanismos de control de la corrupción en la contratación pública. *REDA*, 147.
- (2013). Las nuevas directivas –cuarta generación- en materia de contratación pública. Hacia una estrategia eficiente de compra pública. *Revista Española de Derecho Administrativo (REDA)*, 159.
 - (2017). Medidas de prevención de corrupción y refuerzo de la transparencia en la contratación pública. *Revista de Estudios de la Administración Local y Autonómica*, 7.
- Hernando Rydings, M.^a (2019). Procedimientos de contratación y su incidencia en las entidades locales: principales novedades. *Anuario del Gobierno Local 2018*. IDP - Fundación Democracia y Gobierno Local.
- Ibáñez Jiménez, J. (2019). Tecnología *blockchain* en las administraciones públicas: aplicación y cuestiones legales. *Actualidad Administrativa*, 7.
- Malaret, E. (2016). El nuevo reto de la contratación pública para afianzar la integridad y el control: reforzar el profesionalismo y la transparencia. *Revista Digital de Derecho Administrativo*, 15.

mentos, mediante el establecimiento de tecnología *blockchain* en los centros farmacéuticos que registre y garantice el seguimiento, desde que el fármaco se crea en el laboratorio hasta que llega al consumidor final.

- Medina Arnáiz, T. (2014). Instrumentos jurídicos frente a la corrupción en la contratación pública: perspectiva europea y su incidencia en la legislación española. En AA. VV. *La contratación pública a debate: presente y futuro*. Cizur Menor: Civitas.
- Moreno Molina, J. A. (2013). La cuarta generación de directivas de la Unión Europea sobre contratos públicos. *Observatorio de Contratos Públicos 2012*. Thomson Reuters Aranzadi.
- Muñoz Carmona, A. (2018). *Implicaciones jurídicas del uso de blockchain en la Administración pública*. Trabajo Fin de Master en Investigación Avanzada y especializada en Derecho. Disponible *online*.
- Pereiro Cárceles, M. (2019). La utilización del *blockchain* en los procedimientos de concurrencia competitiva. *Revista General de Derecho Administrativo*, 50.
- Quintana Cortés, J. L. (2020). La tecnología *blockchain* y su pretendida aplicación a la contratación pública como mecanismo para lograr una mayor integridad. *Revista Española de Control Externo*, 64.
- Romero Ugarte, J. L. (2018). Tecnología de registros distribuidos (*DLT*): una introducción. *Banco de España, Boletín Económico 4/2018*. Banco de España.

Servicios locales y *blockchain*¹

Andrea Garrido Juncal

Profesora contratada doctora de Derecho Administrativo.

Universidad de Santiago de Compostela

SUMARIO. 1. Introducción. 2. Retos a abordar por las entidades locales interesadas en desarrollar una estrategia de I+D+i. 2.1. La identificación y definición de las necesidades de los municipios. 2.2. El desarrollo de las consultas preliminares de mercado y la influencia de sus resultados en la actuación de la Administración. 2.3. Barreras y factores que desincentivan la innovación en la contratación pública. 2.4. La posible colisión entre los principios que orientan la actuación administrativa y los intereses de los operadores económicos y agentes vinculados a la innovación. **3. Conclusiones para la implantación del *blockchain* en el ámbito de los servicios locales. 4. Bibliografía.**

1. Introducción

Deben realizarse, desde un principio, dos observaciones. En primer lugar, a pesar de que en la actualidad la tecnología *blockchain* despierta un gran interés, en España carecemos de un marco normativo que regule específicamente

1. Trabajo realizado en el marco de actividades del Grupo GI-1876 “Empresa y Administración”, Grupo de Referencia Competitiva del Sistema Universitario de Galicia - ED431C 2019/15.

su uso. Por regla general, la ausencia de normas genera incertidumbre y ello podría estar favoreciendo que los poderes públicos estuvieran descartando la posibilidad de convertirse en usuarios de esta tecnología².

En segundo lugar, es posible que el despliegue de la tecnología de cadena de bloques en la prestación de los servicios públicos no dependa tanto de que esta cuestión esté más o menos regulada, sino más bien del papel que, hasta ahora, nuestras administraciones han asumido respecto a la innovación. El propósito de este trabajo no es difundir la importancia ni la repercusión de las políticas innovadoras, pues numerosos y prolijos trabajos ya se han ocupado de ello. Ahora bien, sí que estimamos conveniente aludir aquí sumariamente, al menos, a tres ideas.

- a) Si comparamos España con otros países, la partida destinada a I+D+i (investigación, desarrollo e innovación) en los presupuestos públicos podría calificarse como insuficiente³.
- b) Los casos de innovación que se divulgan para tomar como ejemplo son promovidos con frecuencia por la Administración estatal, las administraciones autonómicas, las diputaciones provinciales o los municipios de gran población.

2. Es más, el manejo de esta tecnología se prohíbe en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. La disposición adicional sexta de este texto legal declara: “1. No obstante lo dispuesto en los artículos 9.2 c) y 10.2 c) de la presente Ley, en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. 2. En todo caso, cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal a que hace referencia el apartado anterior deberá contemplar asimismo que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública”. Desde el punto de vista de D. Tapscott y A. Tapscott, “no conviene ni regular de más ni no regular nada. Jurisdicciones en las que vale todo, como las de Bielorrusia o Ucrania, tendrán serios problemas. Pero prohibir el bitcoin, las ofertas iniciales de moneda, las ofertas de tokens de valor y el comercio de criptomonedas, como está planteándose hacer muchos países, perjudicará la innovación durante décadas. Esta es sólo una de las muchas cuestiones de regulación, no siendo la menos importante la fiscal” (Tapscott y Tapscott, 2017: 90-91).

3. Según los datos del Instituto de Estadística de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), recogidos en el portal de datos abiertos del Banco Mundial, los diez países que más recursos destinan a I+D son: Israel (4,95 %), Corea del Sur (4,81 %) Suiza (3,37 %), Suecia (3,34 %), Japón (3,26 %), Austria (3,17 %), Alemania (3,09 %), Dinamarca (3,06 %), Estados Unidos (2,84 %) y Bélgica (2,82 %). España ocupa el puesto treinta y uno (1,24 %). Disponible en: https://datos.bancomundial.org/indicador/GB.XPD.RSDV.GD.ZS?end=2018&locations=IL-KR-CH-SE-JP-AT-DE-DK-US-BE-ES&most_recent_value_desc=true&start=1996&type=shaded&view=chart.

- c) La modernización de la gestión pública, a través de la utilización de las tecnologías, no se caracteriza por ser barata; al contrario, la misma exige asignar una gran cantidad de recursos económicos a ese fin y, como prueba irrefutable de lo anterior, todos podemos recordar lo que ha costado implantar la administración electrónica. En relación con esto último, no puede pasar inadvertido que, en el supuesto de que una entidad local se embarque en actuaciones tendentes a promover la innovación, el origen de los fondos empleados (la financiación externa) condiciona su forma de obrar y, en particular, los tiempos en los que los trabajos deben ejecutarse⁴.

Tras cuanto queda expuesto puede parecer un atrevimiento hablar del impacto de la tecnología *blockchain* en la prestación de los servicios locales, en especial si pensamos en municipios de mediano o pequeño tamaño⁵. Debido a la imposibilidad de analizar lo que no se aplica de forma generalizada en estos momentos, convendrá notar que el objetivo de este capítulo se limitará a dar respuesta al siguiente interrogante: ¿Qué pueden hacer los Gobiernos locales para propiciar la innovación y, singularmente, la tecnología *blockchain*?

Con el ánimo de no caer en demasiadas vaguedades y ambigüedades en la exposición del mencionado tema, se ha optado por someter a estudio SMARTIAGO, un proyecto diseñado por el Ayuntamiento de Santiago de Compostela cuya máxima pretensión es responder a diferentes retos apostando por la innovación tecnológica.

La decisión de investigar esta experiencia y no otra se justifica en que SMARTIAGO es un programa pionero en la gestión de políticas de I+D+i dirigido por una Administración de reducido tamaño, en el que la colaboración público-privada está proporcionando excelentes resultados, hasta el punto de lograr la nominación a varios premios que valoran la transferencia de

4. En los pliegos de contratación del proyecto SMARTIAGO se aclara normalmente que “la determinación del plazo máximo de ejecución de los trabajos tiene en cuenta no solo las prestaciones contratadas, sino las características de la financiación del proyecto SMARTIAGO”, o “la naturaleza de las prestaciones contratadas y las condiciones de financiación en las que se desarrolla no aconseja ni habilita la posibilidad de prórrogas al mismo, con lo que no existe la posibilidad”.

5. “Independientemente de cuándo, o incluso de si alguna vez, la tecnología de cadena de bloques pase a ser de uso general, es algo que merece nuestra atención. Después de todo, ¿acaso la computadora personal, el internet y las redes sociales, hoy en día de uso corriente, no fueron alguna vez tecnologías emergentes que tenían un futuro incierto?” (EquiSoft, 2017).

soluciones innovadoras al mercado⁶. La amplia información accesible a todo el público sobre cómo se ha ejecutado este proyecto, la posibilidad de intercambiar opiniones con las personas al frente de SMARTIAGO⁷ o incluso la procedencia de la autora de este trabajo, han sido posiblemente otros factores que han determinado e influido en esta elección. Sea como fuere, insistimos en que el propósito que se persigue al elaborar este estudio es, a partir del análisis de un caso real, abordar algunos de los principales desafíos a los que se enfrentaría cualquier entidad local que estuviera interesada en desarrollar una estrategia de I+D+i, pues partimos de que esta es una premisa fundamental para que la tecnología *blockchain* irrumpa con fuerza y de una vez por todas en la prestación de servicios públicos.

2. Retos a abordar por las entidades locales interesadas en desarrollar una estrategia de I+D+i

2.1. La identificación y definición de las necesidades de los municipios

Para comprender mejor SMARTIAGO y los tres retos sobre los que este pivota, consideramos oportuno tener en cuenta algunas cifras. Según datos del Padrón municipal de 2020, 97 848 personas figuran censadas en este municipio. En el curso 2018-2019 la Universidad de Santiago de Compostela alcanzó los 25 432 estudiantes matriculados. En el 2019 se registraron 1 466 282 pernoctaciones en los hoteles de la ciudad y, conforme a los registros del Instituto Nacional de Estadística (INE), solo dos localidades, Tarifa y Santiago de Compostela, lograban en julio de 2021 mejorar los datos de ocupación del mismo mes del año 2019, es decir, antes de la pandemia.

6. En octubre de 2021 SMARTIAGO era seleccionado como finalista de los premios Procura + Awards, en la categoría de "Compra pública e innovación del año", junto a Praga, la capital de la República Checa. Los premios Procura + Awards están gestionados y coordinados por ICLEI - Gobiernos Locales para la Sostenibilidad; una red global de más de 2500 Gobiernos locales y regionales comprometidos con el desarrollo urbano sostenible.

El septiembre de 2021 SMARTIAGO fue también seleccionado como uno de los finalistas de los Premios Europeos de Adquisición de la Innovación (EUIPA) 2021. Estos premios, otorgados por el programa Horizon Europe, con el apoyo del Consejo Europeo de Innovación, reconocen los casos más destacados en toda Europa de promoción de la adquisición de innovación por parte de compradores públicos y privados, destacando además la colaboración entre el comprador (en este caso, el Ayuntamiento de Santiago de Compostela) y los proveedores de innovación para llevar las soluciones innovadoras al mercado.

7. Quiero agradecer de forma expresa la ayuda de Gumersindo Guinarte Cabada, concejal responsable de Presidencia, Relaciones Institucionales y Turismo.

A la luz de lo expuesto, no puede sorprender a nadie que el acceso y la movilidad de vehículos, especialmente en el casco histórico, sean un auténtico caos. De esta manera, el reto, que se ha denominado “Reto 1: Movilidad inteligente y sostenible”, se fundamenta en “desarrollar una solución innovadora para la racionalización del modelo actual de carga y descarga, para la reducción de congestión y emisiones y para la evolución del control de acceso y estacionamiento; para evitar daños en pavimentos históricos y bloqueo de vías de servicio público”. En la actualidad, el control de la actividad de los medios de transporte se basa en el control humano y en la instalación de elementos físicos no integrados en el patrimonio.

Tampoco nos debería extrañar que el elevado volumen de basura que se genera en Santiago de Compostela constituya un grave problema ambiental, el cual se ve además agravado por un porcentaje muy bajo de recogida selectiva de residuos (13 %), que está bastante alejado de los objetivos de reciclaje y preparación para la reutilización fijados por la Unión Europea: 50 % en 2020 y 65 % en 2030. Con vistas a revertir esta situación, se plantea el “Reto 2: Gestión Sostenible e Inteligente de Residuos Sólidos Urbanos (RSU)”, cuyo núcleo central es “impulsar soluciones innovadoras para un nuevo modelo de depósito y tratamiento descentralizado de la fracción orgánica de los residuos, que posibilite alcanzar los objetivos marcados por la UE; para una nueva forma de relación con la ciudadanía que premie el comportamiento adecuado en cuanto a depósito de RSU y limpieza viaria, aumentando la corresponsabilidad y la transparencia y para un nuevo modelo de fiscalización de la calidad de servicio, especialmente en cuanto a recogida y limpieza viaria en el centro y casco histórico”.

Por otra parte, en una Ciudad Patrimonio de la UNESCO con elevada afluencia turística, es obvio que la iluminación supone un valor añadido y que la conservación y el mantenimiento de elementos del patrimonio implican importantes gastos recurrentes. El cometido del “Reto 3: Alumbrado ornamental inteligente para conservación del patrimonio” se centra en “el desarrollo de una solución innovadora para mejorar la eficiencia energética, con luminarias sostenibles, diseñadas y fabricadas bajo el modelo de economía circular y poner en valor el patrimonio a través de la iluminación ornamental, reduciendo a su vez los costes de su mantenimiento y conservación”.

Volviendo al interrogante que nos planteábamos al principio, ¿qué pueden hacer los Gobiernos locales para favorecer la innovación en la prestación de sus servicios? Si examinamos la experiencia de este municipio gallego, la

respuesta sería, primero, realizar una consulta preliminar de mercado y, a continuación, dar el salto a la compra pública innovadora, si fuera conveniente.

2.2. El desarrollo de las consultas preliminares de mercado y la influencia de sus resultados en la actuación de la Administración

De acuerdo con lo establecido en el artículo 115 de la LCSP, el 21 de noviembre de 2019 el Ayuntamiento de Santiago de Compostela inició el proceso de consulta preliminar de mercado con el objeto de, por un lado, recopilar la información necesaria para preparar una eventual contratación pública de innovación, y, por otro, informar a los operadores económicos acerca de sus planes y requisitos de contratación.

Cuando un órgano de contratación no tiene la seguridad sobre si el mercado puede ofrecerle una solución que requiere para solventar una necesidad pública, o carece de información contrastada y actualizada sobre las condiciones de calidad de dichas soluciones, el tiempo requerido para llegar a un grado de desarrollo adecuado, el precio del producto final, en el que hay que incluir el pago de las fases de investigación y desarrollo, la proporcionalidad de determinados requisitos de solvencia o el cronograma del desarrollo de un producto, por poner algunos ejemplos, será muy positivo que, antes de iniciar la fase de preparación del contrato, se realice una consulta preliminar de mercado⁸.

Las consultas preliminares de mercado no son un instrumento exclusivo de la compra pública de innovación, sino que se trata de un instrumento horizontal, que se puede utilizar para la preparación de cualquier tipo de procedimiento o contrato. No obstante, es en el ámbito de la compra pública de innovación donde las consultas cobran un especial sentido⁹.

Solo si estandarizamos el mecanismo de consulta preliminar de mercado haremos que estas consultas proliferen. Si complicamos el proceso de consulta todo seguirá igual que ahora (consultando con los empresarios cercanos o fomentando las corruptelas en donde los empresarios podrán verse tentados a pagar por estar bien posicionados y actuar como prescriptores). Así, las consultas preliminares de mercado no solo tienen que ver con la innovación, sino también con la eficiencia, la integridad y la lucha contra la corrupción¹⁰.

8. Guerrero Manso (2020: 436).

9. Bernal Blay (2017: 88).

10. Vázquez Matilla (2019).

Si leemos detenidamente el artículo 115 de la LCSP, comprobamos que la Administración tiene un amplio margen de libertad a la hora de dirigirse al mercado; es ella la que decide qué se pregunta y cómo se pregunta, mientras que, como es lógico, el mercado ajustará también sus respuestas en función de sus intereses.

El legislador impone únicamente dos exigencias. La primera, la obligación de publicitar que se va a llevar a cabo una consulta preliminar de mercado, así como los resultados recabados tras su desarrollo. La segunda, la imposibilidad de que la participación en la consulta comporte ventajas respecto de la adjudicación del contrato.

En esta línea, el legislador establece: “De las consultas realizadas no podrá resultar un objeto contractual tan concreto y delimitado que únicamente se ajuste a las características técnicas de uno de los consultados”¹¹. Aunque, de manera paralela, se dispone que “el resultado de las consultas debe concretarse en la introducción de características genéricas, exigencias generales o fórmulas abstractas que aseguren una mejor satisfacción de los intereses públicos”.

Teniendo en cuenta que no existe ninguna limitación sobre el tipo de información que puede requerir el órgano de contratación en las consultas preliminares de mercado, ni tampoco existe forma específica de solicitar dicha información¹², explicaremos cómo se desarrolló la consulta preliminar de mercado en el marco del proyecto SMARTIAGO, por si pudiera servir de inspiración para otras administraciones.

La participación de personas físicas o jurídicas se llevó a cabo mediante la presentación de propuestas innovadoras, destinadas a dar respuesta a una serie de retos mediante el empleo de tecnologías que superasen las prestaciones existentes actualmente en el mercado. Se admitió la presentación de varias propuestas por una misma persona física o jurídica, ya fuese individualmente o en forma conjunta con otras, aclarando que el Ayuntamiento no estaba obligado a financiar ni a aceptar las propuestas presentadas en la convocatoria. En este sentido, parece conveniente aclarar que el artículo 115 de la LCSP no recoge la

11. La previsión de que de las consultas realizadas no resulte un objeto contractual tan concreto y delimitado que únicamente se ajuste a las características técnicas de uno de los consultados viene también regulada con carácter general en el art. 126.6 de la LCSP (Batet Jiménez, 2021).

12. Guerrero Manso (2020: 439).

posibilidad de compensar económicamente a los participantes en la consulta. En todo caso, esto no impediría que se pudieran establecer compensaciones por los gastos generados a los operadores económicos participantes en la consulta.

Se anunció que el análisis de las ideas propuestas se efectuaría en base a los siguientes criterios: a) adaptación de la propuesta a la necesidad descrita en el proyecto; b) plazo de ejecución de la propuesta de solución; c) escalabilidad; y d) novedad que aporta respeto al estado del arte, es decir, el carácter innovador de la propuesta. Ahora bien, ello no debería inducir a error. No hay que confundir la consulta preliminar del mercado con un elemento de la fase de preparación del contrato. Las empresas deben responder a la consulta presentando una idea o propuesta y no una oferta¹³.

El Ayuntamiento de Santiago de Compostela no se comprometió a responder individualmente sobre la valoración de las propuestas, aunque se puntualizó que ello no impedía que pudiera convocar una reunión para clarificar puntos de una propuesta, sin significar esa reunión una selección de la misma, ni considerarse tampoco esta más interesante que las restantes. Las reuniones servirían para completar información sobre la propuesta o solicitar matizaciones sobre su contenido.

Ante el volumen de propuestas recibidas en la consulta y la diversidad tecnológica de las mismas, el Ayuntamiento de Santiago de Compostela decidió recurrir al asesoramiento de expertos, de conformidad con lo previsto en el artículo 115.1 de la LCSP. Estos asesores expertos acompañaron al equipo del proyecto en las reuniones con las entidades, aportando su conocimiento y experiencia en el ámbito de la compra pública de innovación y la aplicación de las nuevas tecnologías.

El Ayuntamiento de Santiago de Compostela resaltó la amplia respuesta y el interés mostrado por el mercado en proporcionar soluciones. A mayor abundamiento, se constató que todos aquellos que participaron disponían de soluciones, algunas incluso en el mercado, aunque estas no siempre cumplían totalmente con las necesidades recogidas en los retos, de forma que se contempló la necesidad de que existiera algún tipo de integración, adecuación específica y/o desarrollo tecnológico para la ejecución del proyecto. Por este motivo, se consideró adecuado iniciar un procedimiento de compra pública precomercial en el caso del alumbrado, al mismo tiempo que se hizo hincapié en

13. Guerrero Manso (2020: 438).

la importancia de ofrecer una solución llave en mano, con un alcance completo sobre todos los requerimientos especificados en los retos. Lo anterior requeriría aunar diferentes tecnologías, tales como *big data*, *cloud*, inteligencia artificial, visión artificial, *machine learning*, etc., y áreas de conocimiento en un mismo sistema que, coordinado, le diera solución¹⁴. Por ello, a juicio del Ayuntamiento de Santiago de Compostela, serían de una gran utilidad las uniones temporales de empresas y, en su suma, la fusión de diferentes capacidades y conocimientos para la propuesta de una solución integral.

En la compra pública de innovación la consulta preliminar tiene una especial relevancia, puesto que nos va a servir también para saber si el objeto del contrato ya existe en el mercado o existe alguna patente al respecto y ayudará a identificar el procedimiento de contratación adecuado, dependiendo de si necesitamos de I+D o no se precisa. Además, asociaciones, universidades, operadores económicos y otras entidades relacionadas con el producto o servicio podrán aportar información relevante para preparar los pliegos de condiciones¹⁵.

Una vez que se ha sistematizado cómo se podría desarrollar la consulta preliminar del mercado gracias al examen de la experiencia SMARTIAGO, ha de subrayarse que la identificación exacta de cuáles son las necesidades de las Administración, y el conocimiento de cuáles son las soluciones que el sector privado puede proporcionar para satisfacerlas, son la base sobre la que cualquier proceso de compra pública innovadora con visos de éxito debe fundamentarse. De cara a lograr una mayor implantación del *blockchain* en la prestación de servicios públicos, creemos que es esencial que los agentes que se dediquen a esta tecnología presenten sus propuestas.

Con independencia de la opinión que nos merezca la introducción de la consulta preliminar de mercado en la LCSP desde el punto de vista de la defensa de la libre competencia, una cosa está clara y es evidente: los informes finales de las consultas nos pueden valer para extraer algunas conclusiones técnicas, como la siguiente: la tecnología *blockchain* no ha acaparado un gran

14. En las licitaciones publicadas en el marco del proyecto SMARTIAGO se observa que se rechaza la división en lotes, aspecto que en principio perjudicaría la participación de las pymes. La adopción de esta medida se justifica indicando que “una eventual división del objeto del contrato en lotes y su adjudicación a una pluralidad de contratistas dificultaría la correcta ejecución del mismo al entorpecer la necesaria coordinación de la ejecución de las diferentes prestaciones intrínsecamente conectadas. En conclusión, no procede la división en lotes”.

15. Batet Jiménez (2021).

protagonismo en las propuestas recibidas por el Ayuntamiento de Santiago de Compostela. La mayoría de los proponentes ofrecía abordar los retos de SMARTIAGO recurriendo a otras tecnologías, como *big data*, inteligencia artificial, *machine learning*, visión artificial, etc.

Sin entrar en mayores detalles, podríamos intuir que ello podría obedecer a lo que se refleja en el informe *Estado del arte de Blockchain en la empresa española*. En este informe se indica: “Entre el 89,1 % de empresas que todavía no utilizan *blockchain*, el 41 % manifiestan que todavía no entienden en qué puede ayudarles *blockchain* a la hora de transformar sus negocios y el 32 % añade que sus actuales procesos ya están definidos sin incluir *blockchain*”¹⁶. Asimismo, se declara que España sigue la tendencia marcada por la zona Europa Occidental, siendo el sector financiero el que lidera la inversión en *blockchain*¹⁷. A partir de la constatación de esta realidad, solo nos quedaría interiorizar la importancia de construir un ecosistema propicio a la innovación en todos los ámbitos. Interiorización que posiblemente surgirá de repente y a marchas forzadas, pues los fondos de la Unión Europea, destinados a contribuir a la reparación de los daños causados por la pandemia, darán prioridad al gasto ecológico y digital¹⁸.

La tecnología *blockchain* está ahí, podría jugar un papel fundamental en la prestación de servicios locales en un futuro no muy lejano, y cualquier Administración podría beneficiarse de todo el potencial de su uso y, por extensión, los ciudadanos¹⁹.

Tal y como muestra la *Estrategia España Nación Emprendedora*, un documento presentado en febrero de 2021 y que pretende cimentar las bases productivas de la economía española, “hay grandes oportunidades de innovación en frentes como el uso de vehículos autónomos y eléctricos, en la automatización en los procesos a través de la robótica, el análisis y uso de grandes volúmenes de datos para mejorar la gestión de cargas y fomentar la eficiencia en el uso de combustible y la cantidad de trayectos y sus rutas; el

16. AMETIC con la colaboración de REALSEC e ICEX (2019: 17).

17. AMETIC con la colaboración de REALSEC e ICEX (2019: 24).

18. En opinión de Guerra Fariña, “si la crisis de 2007 acabó con el modelo de crecimiento económico basado en la construcción, esta nueva crisis sanitaria y económica del COVID19, debe servir para demostrar que una economía basada en el turismo tal y como lo conocemos, también ‘se ha agotado’ y que hay que apostar por un crecimiento basado en la investigación y desarrollo promoviendo también un ‘turismo inteligente’” (Guerra Fariña, 2020).

19. Con la finalidad de impulsar el uso del *blockchain*, las instituciones públicas están comenzando a reaccionar. Para conocer los potenciales usos de esta tecnología en la Administración, nos remitimos a Pereiro Cárceles (2019: 147-152).

uso de *blockchain* para mejorar la trazabilidad de las mercancías, el uso de drones para cierto tipo de repartos poco pesados y la búsqueda de eficiencia en las entregas a través de inteligencia aplicada a las rutas y los horarios de reparto y el uso cada vez más popular de terminales automatizados para el envío y recogida de paquetería²⁰.

En fin, la tecnología *blockchain* no solo podría irrumpir en el ámbito de la movilidad, sino que su empleo se está testando también en la actualidad en la recogida de residuos. Desde principios de 2021, Getxo, municipio situado en Vizcaya, participa en un proyecto piloto para la recogida de aparatos electrónicos y eléctricos. A partir de técnicas de *blockchain*, inteligencia artificial y reconocimiento de imagen, unas máquinas bautizadas como contenedores inteligentes son capaces de reconocer y clasificar los dispositivos que se van almacenando, así como de asignar unas recompensas a los ciudadanos, llamadas eco-créditos, que les proporcionan descuentos en compras o se pueden donar para promover la plantación de árboles en parques. En línea con lo expuesto, debe señalarse que, según Stefan Junstrand, “gracias a la tecnología *blockchain*, es posible elaborar un registro público y transparente de datos que no solo permitiría cobrar tasas por la generación y recogida de diferentes residuos, sino también recompensar el buen hacer de los ciudadanos que menos residuos generen o mejor reciclen”²¹.

En lo que atañe a la iluminación, el grupo Iberdrola ha puesto en marcha un proyecto piloto basado en el uso del *blockchain* para garantizar en tiempo real que la energía que se suministra y consume es 100 % renovable. Con el apoyo de esta tecnología, la compañía ha conseguido unir las plantas donde se produce la electricidad con los puntos de consumo y trazar así su origen, lo que incrementa la transparencia y, en última instancia, favorece el uso de la energía renovable²².

Aun corriendo el riesgo de ser insistente, recalcaré que las consultas preliminares de mercado, si bien pueden despertar ciertas reticencias, tienen un valor extraordinario como herramienta de planificación. Las ideas de soluciones innovadoras recogidas en el proceso de consulta ayudan a la Administración a definir el tipo de contrato, a determinar el plazo máximo de ejecución de los trabajos contratados o a elegir el procedimiento de adjudicación, por ejemplo.

20. Presidencia del Gobierno, Gobierno de España (2021: 64).

21. Junstrand (2017).

22. Noticia disponible en: <https://www.iberdrola.com/innovacion/blockchain-energia>.

Gracias a esa relación con el mercado, y, por supuesto, con el apoyo de asesores externos, el Ayuntamiento de Santiago de Compostela descubrió que no existían soluciones tecnológicas viables que respondieran al “Reto 3: Alumbrado ornamental inteligente para conservación del patrimonio”, de manera que en ese caso se optó por la compra pública precomercial y no por la compra pública de tecnología innovadora.

2.3. Barreras y factores que desincentivan la innovación en la contratación pública

Se ha defendido con fervor que la contratación pública innovadora representa una herramienta idónea para estimular la innovación. La Administración realiza una compra inteligente, mejorando sus resultados, soluciones y/o servicios a través de los beneficios de la I+D+i, a la vez que fomenta la innovación del tejido empresarial²³. Otro aliciente que aporta este modelo de contratación es que permite a las empresas desarrollar innovaciones y probarlas en entornos reales, acercando a las administraciones a nuevas soluciones a sus necesidades, que, de otra manera, no podrían ser satisfechas²⁴.

La contratación pública innovadora marca un antes y un después en la relación entre el sector privado y las administraciones. Se pasa de una Administración que subvenciona a una Administración que contrata, consiguiendo mejorar la gestión de servicios públicos y creando un entramado económico ligado a la innovación. Este papel del sector público como promotor de nuevas ideas que posteriormente se convierten en productos y servicios parece más relevante en las regiones menos innovadoras, debido a las menores capacidades de otros agentes. Por ello, y actuando principalmente desde la demanda, pero también coordinando con la perspectiva de la oferta, el sector público tiene un importante papel dinamizador en las áreas menos innovadoras de cara a contribuir al desarrollo de esas capacidades²⁵.

Sin embargo, las grandes alabanzas sobre esta modalidad de compra pública estratégica no vienen respaldadas por su uso masivo, ni mucho menos. En octubre de 2021 se publicaba un informe que alertaba sobre lo siguiente: “Tan solo trece comunidades autónomas han apostado por la compra pública

23. Agencia Valenciana de la Innovación (2019: 12).

24. Beaz (2020: 15).

25. Sánchez Carreira *et al.* (2019: 82).

de innovación. Por número de casos, destacan Andalucía con 17, Cataluña con 14, Madrid con 12, Galicia con 10 y el País Vasco con 9 casos²⁶.

Aunque la identificación de las razones por las cuales la compra pública innovadora no ha calado en las instituciones públicas merecería un estudio aparte y más a fondo, comentaremos a continuación algunas de las barreras que podrían estar obstaculizando su consolidación.

- a) La adquisición de bienes y servicios altamente innovadores requiere dinero.

El importe total del proyecto SMARTIAGO asciende a 6 180 000 €, de los que un 80 % (4 944 000 €) son aportados por el Programa Operativo Plurirregional de España (POPE) 2014-2020, a través del Convenio firmado con el Ministerio de Ciencia, Innovación y Universidades; otro 10 % (618 000 €) son financiados por la Axencia Galega de Innovación, y otro 10 % proviene de recursos propios del Ayuntamiento de Santiago de Compostela.

- b) La compra pública innovadora no exige solo tener dinero, sino que obliga a contratar poniendo en tela de juicio los pilares clásicos de la contratación pública.

Como ha destacado J. A. Carrillo Donaire, no se siguen las pautas ordinarias de la contratación del sector público. En palabras de este autor, “tanto la preparación y adjudicación del contrato como su ejecución (...) cuestionan los principios clásicos de la contratación: objeto cierto, precio determinado, inmediatez y corto plazo, riesgo y ventura del empresario, etc., evolucionado hacia modelos en los que prima la negociación con el mercado y el reparto de riesgos ante la incertidumbre que inevitablemente conlleva la adquisición de innovación y la apuesta por la investigación aplicada²⁷”.

El camino hacia el afianzamiento de la compra pública innovadora no está exento de dificultades. Sin ánimo de exhaustividad, cabe apuntar que, de acuerdo con Horizonte 2020, la compra pública innovadora se materializa en dos categorías: la compra pública de tecnología innovadora y la compra pública precomercial²⁸. En consecuencia, una primera decisión compleja a adoptar por el gestor pú-

26. Corporación Tecnológica de Andalucía (CTA) y el bufete Cremades & Calvo-Sotelo (2021: 11).

27. Carrillo Donaire (2021: 39).

28. No obstante, tampoco es inusual que los tipos de compra en los que interviene la innovación se clasifiquen en tres categorías: la compra pública precomercial, la compra pública de tecnología innovadora y la compra pública regular de innovación. Para conocer la diferencia entre ellas, nos remitimos, por ejemplo, a Ayuntamiento de Madrid (2018).

blico consistirá en la elección del instrumento adecuado para llevar a cabo su proyecto de innovación. Y en este sentido, ya avanzamos que, dependiendo del mecanismo por el que se decante, la normativa de contratos públicos se aplicará o no.

Debe repararse en que la tipología de compra pública innovadora se determina atendiendo al nivel de madurez de la tecnología que se desea obtener a través del proceso. Para ello, se emplean los TRL – Technology Readiness Level. TRL es un concepto que surgió en la NASA, pero que más tarde se generalizó para aplicarse a cualquier proyecto y no necesariamente a los aeronáuticos o espaciales, desde su idea original hasta su despliegue comercial²⁹.

La compra pública precomercial se circunscribe exclusivamente a la compra de servicios de I+D dirigidos a conseguir unos resultados innovadores respecto a lo existente en ese momento en el mercado, remunerados íntegramente por el órgano de contratación. Este órgano comparte con las empresas adjudicatarias los riesgos y beneficios de la investigación científica y técnica necesaria para desarrollar soluciones innovadoras que superen las disponibles en el mercado. El objetivo primordial de esta tipología de contratación son servicios de investigación y desarrollo en un proceso que permita filtrar los riesgos tecnológicos de soluciones no existentes en el mercado antes de abordar una compra de los mismos. Este tipo de contratos cubre hasta la obtención de prototipos validados en un entorno real más o menos extenso.

La contratación pública precomercial pivota sobre tres elementos: su ámbito son los servicios de I+D; los riesgos y beneficios se comparten en condiciones de mercado; la contratación no entraña ninguna suerte de ayuda. La circunstancia de que la Administración no retenga los resultados de la actividad de I+D puede llegar a ser el principal atractivo para que las empresas dediquen tiempo y efectivos a la tarea de I+D que es objeto del contrato, al poder las empresas contratistas servirse de los resultados con otros clientes³⁰.

La compra pública de tecnología innovadora consiste en la compra pública de un bien o servicio que no existe en el momento de la

29. La elección del procedimiento de contratación va a depender de determinados factores. Especialmente, el nivel de conocimiento del mercado, el porcentaje de trabajos de I+D, la posibilidad o no de determinar las prescripciones técnicas, la necesidad o no de adquisición de la solución a escala comercial (es decir, más allá de un prototipo), el número de potenciales proveedores y la estructura del mercado, y el plazo y los recursos disponibles para la contratación (Vázquez Matilla, 2019).

30. Núñez Lozano (2016: 129).

compra, pero que puede desarrollarse en un período de tiempo razonable. Dicha compra requiere el desarrollo de tecnología nueva o mejorada para poder cumplir con los requisitos demandados por la entidad contratante. A diferencia de la compra pública precomercial, no se contrata una actividad de I+D, sino que el objeto del contrato son obras o servicios que la Administración adquiere para la satisfacción de sus necesidades, si bien es precisa con carácter previo una actividad I+D que forma parte del mismo contrato.

Antes de continuar, es necesario recalcar que, a través de la compra pública precomercial, el sector público busca soluciones innovadoras que no existen en el mercado. Esto hace previsible que las tareas de I+D que deban llevarse a cabo se dilaten en el tiempo, al menos más que en la compra pública de tecnología innovadora. Que la compra pública precomercial promueva la investigación para el desarrollo de soluciones inexistentes en un horizonte temporal no excesivamente inmediato, explica que esta modalidad de compra de innovación se excluya de la legislación de contratos³¹.

En efecto, la compra pública precomercial está excluida del ámbito de aplicación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014³². Sin embargo, su adjudicación está sujeta tanto a los principios del TFUE como a los principios de la contratación pública³³.

Como pone de manifiesto M.^a C. Núñez Lozano, el hecho de que la contratación pública precomercial no cuente con un régimen jurídico “codificado” entraña un problema³⁴. Serán los órganos de contra-

31. Valcárcel Fernández (2018).

32. El art. 8 de la LCSP establece:

"Quedan excluidos de la presente Ley los contratos de investigación y desarrollo, excepto aquellos que además de estar incluidos en los códigos CPV 73000000-2 (servicios de investigación y desarrollo y servicios de consultoría conexos); 73100000-3 (servicio de investigación y desarrollo experimental); 73110000-6 (servicios de investigación); 73111000-3 (servicios de laboratorio de investigación); 73112000-0 (servicios de investigación marina); 73120000-9 (servicios de desarrollo experimental); 73300000-5 (diseño y ejecución en materia de investigación y desarrollo); 73420000-2 (estudio de previabilidad y demostración tecnológica) y 73430000-5 (ensayo y evaluación), cumplan las dos condiciones siguientes:

a) Que los beneficios pertenezcan exclusivamente al poder adjudicador para su utilización en el ejercicio de su propia actividad.

b) Que el servicio prestado sea remunerado íntegramente por el poder adjudicador".

33. Jaramillo Villacís (2020).

34. Núñez Lozano (2016: 129).

tación los que en cada caso deban diseñar *ad hoc* el procedimiento de adjudicación que deba seguirse para seleccionar a quienes lleven a cabo las actividades de I+D. Los pliegos o documentos de la licitación determinarán el régimen general que deba regir en cada contrato, especificando cómo se materializan los principios de concurrencia competitiva, publicidad, transparencia e igualdad entre los participantes durante todo su desarrollo³⁵.

La compra pública de tecnología innovadora está plenamente sometida a la normativa de contratación pública, pero no se configura como una nueva forma de adjudicar contratos ni licitar. La característica que la convierte en un instrumento interesante es su finalidad: servir de apoyo a la actividad innovadora del sector privado para satisfacer las necesidades de un organismo público. Se consigue, por tanto, que la demanda del sector público dirija la actividad innovadora y no se vean obligados a amoldarse a los nuevos productos o servicios desarrollados por el sector privado, sino que sea de manera contraria. Así, en función del objeto contractual al que se refiera la innovación (obras, servicios o suministros), se celebrará el contrato típico que corresponda de acuerdo con la naturaleza de las prestaciones que deban acometerse. Eso sí, con la particularidad no menor de que la prestación principal del contratista es algo innovador, lo que afectará a la forma a través de la que se define el objeto, dado que habrá que recurrir a la utilización de especificaciones funcionales o en términos de rendimiento³⁶.

Por otra parte, el art. 167 de la LCSP sugiere, en el apartado b), el empleo de procedimientos de licitación con negociación cuando “la prestación objeto del contrato incluya un proyecto o soluciones innovadoras”. Sin embargo, nada impide que en estos casos el procedimiento de adjudicación elegido sea el abierto. De hecho, en SMARTIAGO se optó por esa vía, alegando que “las consultas preliminares del mercado desarrolladas con antelación al inicio del presente expediente han permitido esclarecer al órgano de contratación todos los apartados técnicos del contrato junto a los operadores económicos, tal y como se refleja en el alto grado de detalle del pliego de prescripciones técnicas, siendo innecesario, en opinión de la Oficina Técnica de Apoyo, abordar un nuevo proceso de diálogo con los licitadores”.

35. Valcárcel Fernández (2018).

36. Valcárcel Fernández (2018).

- c) Las reservas a la hora de lanzarse a la compra pública innovadora pueden también fundamentarse en que la misma recomienda la formación de equipos multidisciplinares, en los que los profesionales de las ciencias jurídicas estén dispuestos a colaborar estrechamente con los expertos en las áreas técnicas. Es evidente que esto conlleva la creación de nuevas dinámicas de trabajo y la asunción de una nueva cultura en la Administración local.
- d) A menudo se alega que la Administración que tenemos sigue anclada en el pasado y que es incapaz de afrontar la necesaria modernización de sus estructuras, procesos y servicios. Siendo este un argumento muy utilizado entre aquellos que recriminan la inacción de nuestro sector público en numerosos ámbitos, es posible que, en esta ocasión, la inexperiencia sea uno de los mayores obstáculos a superar. No estamos ante una práctica muy extendida en el ámbito local, ni siquiera en otros niveles administrativos, por lo que el desconocimiento y la inexperiencia pueden actuar como frenos. Pero cuesta aún más plantear la implantación de esta compra pública estratégica en las ciudades históricas.

La simple insinuación de que se van a adquirir productos y servicios innovadores va a ser acogida, casi con toda probabilidad, con desconfianza. Se debatirá si las instalaciones con las tecnologías más punteras impactan en la imagen de ciudad histórica; se insistirá en la importancia de que estos elementos, si bien no pueden pasar desapercibidos, no perturben ni descontextualicen el espacio urbano histórico; se reclamará que, en la medida en que la tecnología lo permita, los modelos que se compren tengan un tamaño reducido y sus acabados tengan un pulido o color que no sea ni brillante, ni llamativo ni reflectante; se instará al aprovechamiento máximo de las instalaciones existentes de redes de alumbrado público, semaforicas y de fibra óptica, minimizando todo lo posible el número de tendidos aéreos, y se pedirá que el número de elementos verticales a instalar sea el menor posible, dentro de las necesidades a cubrir y procurando integrar todos ellos en un mismo soporte, para reducir el número de postes o columnas en la vía pública³⁷. Consiguientemente, para el impulso de la compra pública innovadora en los territorios con patrimonio cultural e his-

37. Véase el “Contrato de suministro, instalación e posta en funcionamento dunha serie de actuacións relacionadas coa mobilidade no marco do proxecto SMARTIAGO”, publicado el 15/05/2020 en la Plataforma de Contratación del Estado.

tórico, será aconsejable que en los equipos de trabajo se integre la Comisión Asesora de la Ciudad Histórica u órgano equivalente, tal y como se ha hecho en SMARTIAGO.

Desde el 25 de octubre de 2021 la Casa do Cabildo, en la Plaza de Platerías, disfruta de un sistema pionero de iluminación inteligente, que previsiblemente reducirá el consumo de energía en un 80% y ayudará a combatir la colonización biológica de sus fachadas. Se trata del primer resultado tangible de SMARTIAGO y, a la espera de que se confirmen en un entorno real los excelentes y prometedores datos obtenidos en el laboratorio, sus promotores destacan que con esta innovación “ahorramos en luz y ganamos en arte”, aunque algunos pueden aceptar esto con cierto resquemor, pues entienden que la fachada de un monumento histórico sin musgo pierde identidad o resulta artificial. Por tanto, otra esfera de acción de la entidad local debería concentrarse en la labor de concienciación y sensibilización de la ciudadanía, de manera que esta comprendiera las ventajas que comporta apostar por la innovación.

2.4. La posible colisión entre los principios que orientan la actuación administrativa y los intereses de los operadores económicos y agentes vinculados a la innovación

Otro foco de problemas es cómo se pueden conciliar los intereses de la Administración con los intereses de los operadores económicos y agentes vinculados a la innovación, pues el respeto de unos y otros se antoja complicado, cuando no imposible, por momentos.

La actuación administrativa debe estar guiada por los principios de transparencia, igualdad de trato y no discriminación, pero no puede olvidarse que aquí estamos hablando de hacer realidad nuevas ideas. Por tanto, los sujetos pueden decidir no participar en la consulta por miedo a las filtraciones de información a sus competidores.

En muchos casos los operadores económicos serán reticentes a participar en la consulta por el temor a las filtraciones de información. Si los operadores económicos no tienen la plena seguridad de que sus soluciones no van a transmitirse a los otros participantes, ya sea directa o indirectamente, no correrán el riesgo de participar en la consulta y preferirán esperar y participar en la futura licitación (si es que se lleva a cabo), con un claro perjuicio para el

órgano de contratación, que carecerá de información relevante para preparar el pliego³⁸.

Para asegurar la transparencia, la disponibilidad de la mayor información posible y el intercambio eficaz de experiencias y opiniones, el Ayuntamiento de Santiago de Compostela insta a los participantes a que hagan constar expresamente su conformidad para que la Administración mantenga accesible y actualizada la información necesaria, total o parcial, sobre sus propuestas, sin perjuicio de aquella que haya sido marcada como confidencial. Para ello, los participantes deben indicar la documentación o la información técnica o comercial de su propuesta que tiene carácter confidencial, no siendo admisible que efectúen una declaración genérica o declaren que toda la información tiene carácter confidencial. Este carácter confidencial protege, en particular, los secretos técnicos o comerciales y los aspectos confidenciales de las soluciones. El artículo 115.3 de la LCSP prohíbe al órgano de contratación cualquier revelación a los participantes en el proceso de consultas relativa a las soluciones propuestas por los otros participantes, siendo las mismas solo conocidas íntegramente por él.

El Ayuntamiento de Santiago de Compostela especifica que la información que le ha proporcionado el mercado no es vinculante y que su uso se limita exclusivamente a su posible inclusión en las especificaciones funcionales o técnicas de un eventual procedimiento de contratación posterior, en concordancia con el artículo 115.3 de la LCSP, que establece: “Con carácter general, el órgano de contratación al elaborar los pliegos deberá tener en cuenta los resultados de las consultas realizadas; de no ser así deberá dejar constancia de los motivos en el informe”.

En otro orden de consideraciones, debe añadirse que la compra pública innovadora implica invertir en hacer realidad nuevas ideas, tanto por parte de la Administración como por la de las entidades proveedoras del producto o servicio. Los riesgos derivados de proyectos innovadores suelen ser muy elevados y los beneficios económicos no siempre son proporcionales al esfuerzo desplegado. Por esta razón, se comparten riesgos y beneficios entre el órgano de contratación y los adjudicatarios, cobrando así una especial relevancia todo lo relacionado con la protección de la propiedad industrial e intelectual que pudiera derivarse de la ejecución de los trabajos contratados. Como nota adicional, cabe remarcar que en SMARTIAGO el reparto y el valor de los *royalties* se configuran como criterio de adjudicación.

38. Guerrero Manso (2020: 442).

Teniendo en cuenta el artículo 8 de la LCSP, el Ayuntamiento de Santiago de Compostela presta atención a todo lo relacionado con la protección de la propiedad industrial e intelectual que pudiera derivarse de la ejecución de los trabajos contratados. Las bases de dicha regulación fueron las siguientes: “Cada Parte mantendrá la titularidad de los conocimientos previos tanto propios como de terceros, debiendo, en todo caso, el contratista mantener al órgano de contratación indemne frente a cualquier reclamación de terceros en relación con una infracción debida al uso de los conocimientos previos. El contratista deberá informar al órgano de contratación de cualquier resultado nuevo generado. La titularidad de los derechos de propiedad nacidos bajo el ámbito del contrato pertenecerá a las partes en los porcentajes y alcance que se establezcan, estando sujetos dichos porcentajes a un criterio de adjudicación de la licitación. El contratista será responsable de la preparación, solicitud, gestión y mantenimiento de los derechos de propiedad nuevos generados en relación a los resultados, y correrá con todos los gastos relacionados. En el caso de infracción de cualquiera de los derechos de propiedad generados bajo el contrato por un tercero, las partes cooperarán y harán los esfuerzos razonables para detener tal infracción”.

3. Conclusiones para la implantación del *blockchain* en el ámbito de los servicios locales

Algunos auguran que la tecnología actual, especialmente la inteligencia artificial unida a *blockchain*, producirá una gigantesca convulsión en nuestros actuales sistemas económicos, de forma que aquellos países, sectores, empresas y ciudadanos que se posicionen correctamente tendrán ventajas muy relevantes, mientras que los más conservadores quizá eludan algunos riesgos, pero serán más dependientes³⁹.

Otros ponen el acento en que *blockchain* ofrece el potencial de redefinir la relación entre el Gobierno y el ciudadano en términos de intercambio de datos, transparencia y confianza; por lo que pronto seremos testigos de una revolución en la prestación de servicios públicos del siglo XXI, de la misma forma que internet revolucionó la comunicación a finales del siglo XX⁴⁰.

En efecto, la tecnología *blockchain* ofrece una serie de características técnicas y oportunidades que, sin lugar a dudas, pueden contribuir a conseguir un sector público en el que la interoperabilidad, la automatización,

39. Pedreño Muñoz (2018).

40. Lafont Déniz (2018: 321-322).

la transparencia y, especialmente, los derechos de los administrados queden perfectamente garantizados por el propio sistema⁴¹.

Ahora bien, y con todos los respetos a los firmes defensores del *blockchain*, estamos más próximos a aquellos que se muestran más cautelosos, señalando que la tecnología de cadenas de bloques puede ser usada para una gran cantidad de asuntos, pero a causa de sus limitaciones intrínsecas (de naturaleza tanto jurídica como técnica) hay que preguntarse de manera honesta, caso por caso, si su aplicación aporta algún valor añadido en comparación con las tecnologías existentes, si resulta la mejor opción⁴².

Para desarrollar y validar la tecnología *blockchain* en la prestación de los diferentes servicios públicos, la compra pública innovadora se erige como un instrumento idóneo, al permitir a las empresas que desarrollen un prototipo de sus tecnologías y comprueben cuál es su funcionamiento y viabilidad en un entorno real, superando así una de las principales dificultades con las que se encuentran las empresas innovadoras⁴³.

España, y otros países de habla hispana, tienen una magnífica oportunidad para desarrollar y utilizar la tecnología *blockchain* y posicionarse en este incipiente mercado global. Según Preukschat, tenemos el talento, las infraestructuras y el capital para lograrlo, pero nos falta tener una predisposición por invertir, experimentar e innovar con *blockchain*. Se necesita un marco regulatorio favorable y proactivo que permita que estos proyectos puedan nacer y desarrollarse en España y Latinoamérica porque, de lo contrario, lamentablemente tendrán que emigrar⁴⁴.

La implementación de la compra pública innovadora, que se enmarca dentro de las llamadas políticas de demanda para promoción de la innovación, exige construir un nuevo esquema mental que oriente las compras de las entidades locales no solo al cumplimiento de sus fines, sino al establecimiento de objetivos estratégicos de segundo nivel que busquen el fomento de la innovación y el desarrollo tecnológico en las empresas, al tiempo que se mejoren los servicios públicos⁴⁵.

41. Muñoz Carmona (2018).

42. Delgado Báidez (2018).

43. Ministerio de Ciencia e Innovación, Gobierno de España (2021: 59).

44. Preukschat (2017a: 11).

45. Sinde Cantorna (2018).

En último lugar, tampoco creemos que repetir como un mantra “comprar lo más barato siempre puede salir más caro” o “la innovación más cara de hoy puede ser la más barata mañana” sea la estrategia más acertada para impulsar la compra pública innovadora, ya que su despegue definitivo depende de múltiples elementos. Más allá de los eslóganes, lo que es indiscutible es que la innovación pide imperiosamente asignar una gran cantidad de recursos económicos a ese fin y que algunas innovaciones ahorrarán costes inmediatamente a las autoridades públicas locales, mientras que otras necesitarán una fuerte inversión inicial para obtener ganancias a largo plazo.

4. Bibliografía

- Agencia Andaluza del Conocimiento (2019). *Estrategia para el impulso y consolidación de la Compra Pública de Innovación (CPI) en la Administración Pública de la Junta de Andalucía*.
- Agencia Valenciana de la Innovación (2019). *Guía Práctica del Proceso de Compra Pública de Innovación para Organismos Públicos de la Comunitat Valenciana*.
- AMETIC con la colaboración de REALSEC e ICEX (2019). Informe *Estado del arte de Blockchain en la empresa española*.
- Ayuntamiento de Madrid (2018). *Guía de contratación pública de innovación del Ayuntamiento de Madrid*.
- Batet Jiménez, M.^a P. (2021). La compra pública de innovación. *Contratación administrativa práctica*, 175, 11-19.
- Beaz (2020). *Guía dual de Compra Pública de Innovación para la demanda pública y la oferta tecnológica: Impulso de la I+D+i en el Territorio Histórico de Bizkaia*.
- Bernal Blay, M. Á. (2017). Compra pública de innovación: una aproximación pro-competitiva. En J. Guillén Caramés y M.^a Hernando Rydings (coords.). *Contratación, competencia y sostenibilidad: últimas aportaciones desde el derecho administrativo* (pp. 83-105). Navarra: Civitas.
- Carrillo Donaire, J. A. (2021). La compra pública de innovación: retos y oportunidades para el desarrollo de la I+d+i desde la demanda pública. *IUS ET VERITAS*, 62, 38-59.
- Corporación Tecnológica de Andalucía (CTA) y el bufete Cremades & Calvo-Sotelo (2021). *Compra Pública de Innovación: informe de situación y perspectivas*.

- Delgado Báidez, J. M.^a (2018). Blockchain e identidad soberana en relación con el derecho del interesado a no aportar documentos que ya obren en poder de las administraciones públicas. Comunicación presentada en las *Jornadas para empresas y emprendimiento*, celebradas en la Facultad de Derecho de la Universidad de Murcia el 7 y 8 de noviembre.
- EquiSoft (2017). Informe *La cadena de bloques (blockchain). Una tecnología disruptiva con el poder de revolucionar el sector financiero*.
- Guerra Fariña, M.^a R. (2020). Los procedimientos de adjudicación en la Compra Pública de Innovación desde la entrada en vigor de la Ley 9/2017. *Contratación administrativa práctica*, 170, 3-10.
- Guerrero Manso, C. de. (2020). ¿Compra pública de innovación en tiempo de COVID-19? En C. de Guerrero Manso (coord.) y J. M.^a Gimeno Feliú (dir.). *Observatorio de los contratos públicos 2019* (pp. 433-458). Madrid: Aranzadi.
- Jaramillo Villacís, A. L. (2020). *Compra Pública Pre-Comercial: ¿qué abarcan los servicios de I+D?*. Observatorio de Contratación Pública.
- Junestrand, S. (2017). Smart Cities en la era blockchain. En A. Preukschat (coord.). *Blockchain: La revolución industrial de internet* (pp. 103-111). Barcelona: Planeta.
- Junta Consultiva de Contratación Administrativa del Estado (2011). *Informe 37/11, de 28 de octubre de 2011. "Guía sobre compra pública innovadora"*.
- Lafont Déniz, R. (2018). Hacia una identidad digital basada en blockchain dentro de la Administración pública. En R. Vilarroig Moya y C. Pastor Sempere (dirs.). *Blockchain: Aspectos Tecnológicos, Empresariales y Legales* (pp. 321-338). Madrid: Aranzadi.
- Ministerio de Ciencia e Innovación, Gobierno de España (2021). *PEICTI. Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2023*.
- Muñoz Carmona, A. (2018). Implicaciones jurídicas del uso de blockchain en el sector público. Comunicación presentada en las *Jornadas para empresas y emprendimiento*, celebradas en la Facultad de Derecho de la Universidad de Murcia el 7 y 8 de noviembre.
- Núñez Lozano, M.^a C. (2016). La contratación pública innovadora: compras comerciales y compras precomerciales. En F. Lorenzo Hernández (coord.). *El impacto de la crisis en la contratación pública: España, Italia y Francia* (pp. 107-144). Madrid: Aranzadi.
- Pedreño Muñoz, A. (2018). Blockchain: ¿un nuevo patrón económico? En R. Vilarroig Moya y C. Pastor Sempere (dirs.). *Blockchain: Aspectos Tecnológicos, Empresariales y Legales* (pp. 25-31). Madrid: Aranzadi.

- Pereiro Cárceles, M. (2019). Usos de la tecnología "blockchain" en la Administración Pública. En B. Puentes Cociña y A. Quintiá Pastrana (dirs.). *El derecho ante la transformación digital. Oportunidades, riesgos y garantías* (pp. 141-154). Atelier: Barcelona.
- Presidencia del Gobierno, Gobierno de España (2021). *Estrategia España Nación Emprendedora*.
- Preukschat, A. (2017a). Prólogo a la versión en español. En P. Champagne. *El Libro de Satoshi*. Disponible en: <http://www.libroblockchain.com/satoshi/>
- (coord.). (2017b). *Blockchain: La revolución industrial de internet*. Barcelona: Planeta.
- Procurement of Innovation Platform (2018). *Guía para autoridades públicas sobre la Contratación Pública de Innovación*.
- Sánchez Carreira, M.^a del C., Varela Vázquez, P. y Peñate Valentín, M.^a C. (2019). A compra pública de innovación: análise da experiencia de Galicia no ámbito sanitario. *Revista Galega de Economía*, 28 (2), 71-86.
- Sinde Cantorna, S. (2018). La compra pública de innovación como herramienta transformadora de las entidades locales innovadoras. El gran reto de las entidades locales es gestionar la innovación en lo público y aprovechar el potencial de la compra pública de innovación. *El Consultor de los Ayuntamientos*, 3, 55-63.
- Tapscott, D. y Tapscott, A. (2017). *La revolución blockchain*. Barcelona: Deusto.
- Valcárcel Fernández, P. (2018). La innovación como objeto prestacional en los contratos del sector público. La Compra Pública de Innovación. *Contratación administrativa práctica*, 153, 56-68.
- Vázquez Matilla, F. J. (2019). Compra pública de innovación. Avanzando hacia la compra pública estratégica. *Contratación administrativa práctica*, 159.
- Xunta de Galicia (2016). *Guía de buenas prácticas para favorecer la Contratación Pública de Innovación en Galicia*.

Democracia local y tecnología *blockchain*

Patricia García Majado

*Profesora ayudante doctora de Derecho Constitucional.
Universidad de Oviedo*

Miguel Ángel Presno Linera¹

*Catedrático de Derecho Constitucional.
Universidad de Oviedo*

SUMARIO. 1. Presentación. 2. ¿De qué hablamos cuando hablamos de democracia local? 3. Los procesos participativos en el ámbito local: oportunidades y riesgos. 4. Pautas de actuación de los poderes públicos en relación con los procesos participativos locales. 5. Procesos participativos en el ámbito local. 5.1. La iniciativa popular sobre ordenanzas y reglamentos locales. 5.2. La participación ciudadana en la elaboración de los presupuestos de las entidades locales. 5.3. Las consultas populares de ámbito local. 5.4. Otros instrumentos de participación ciudadana. 6. Tecnología, *blockchain* o no, y procesos participativos locales. 7. ¿Conclusiones? 8. Bibliografía.

1. Presentación

En este capítulo expondremos, en primer lugar, la potencialidad de los ámbitos locales como espacios para el desarrollo de diferentes instrumentos de participación ciudadana en el gobierno de la comunidad, que van más allá de

1. Patricia García Majado es autora de los epígrafes 1 a 5; Miguel Ángel Presno Linera de los epígrafes 6 y 7 y de la bibliografía.

Estudio elaborado en el marco del proyecto de investigación “Partidos políticos: origen, función y revisión de su estatuto constitucional” (ref.: DER2017-84733-R).

la mera intervención en la elección de un determinado número de representantes políticos, pues se tendrán en cuenta otros procesos participativos que buscan ampliar las oportunidades de la ciudadanía para influir en las decisiones públicas. A nuestro juicio, la intervención en estos procesos tendría que incluir, siempre que sea posible, las siguientes facultades: el acceso a toda la información pública cuyo conocimiento facilite el ejercicio de la participación, el derecho a iniciar o promover esos procesos participativos en los términos previstos en cada uno de ellos, el derecho a realizar aportaciones durante su desarrollo y el derecho a recibir respuesta de las administraciones y entidades locales a las iniciativas y aportaciones realizadas en los diferentes procesos participativos.

Los procesos participativos que se tendrán en cuenta serán, además de los propiamente electorales, la iniciativa popular en el ámbito local, la participación ciudadana en la elaboración de los presupuestos, las consultas populares, los foros ciudadanos y los jurados ciudadanos.

En una suerte de segunda parte de este capítulo analizaremos si, en el estado actual de conocimiento de las cosas, la tecnología *blockchain* contribuye a mejorar la calidad de los antedichos procesos participativos, es decir, si garantizando requisitos esenciales del derecho de participación -que se ejerza de manera universal, libre, igual, directa y secreta-, facilita su ejercicio y aporta más transparencia y confianza a la ciudadanía, “con el fin de ampliar el debate político y favorecer una mejor y más legítima adopción de las decisiones políticas” [Principio n.º 6 del Anexo a la Recomendación del Comité de Ministros del Consejo de Europa a los Estados miembros sobre la democracia electrónica (e-democracia), adoptada el 18 de febrero 2009], sin olvidar que más y mejor tecnología no conduce por sí misma a más y mejor democracia (Principio n.º 49)².

En esta línea, la Resolución del Parlamento Europeo, de 16 de marzo de 2017, sobre la democracia digital en la Unión Europea: posibilidades y retos [2016/2008(INI)]:

“1. Subraya las potenciales ventajas de la democracia digital, que se define como el apoyo y el refuerzo de la democracia tradicional por medio de las tecnologías de la información y la comunicación (TIC) y que puede complementar y reforzar los procesos democráticos añadiendo elementos de empoderamiento de los ciudadanos a través de diversas

2. Nos hemos ocupado antes en Presno Linera (2016, 2020).

actividades en línea que incluyen, entre otras cosas, la administración pública electrónica, la gobernanza electrónica, la deliberación electrónica, la participación electrónica y la votación electrónica; acoge con satisfacción que las nuevas tecnologías de la información y la comunicación (TIC) permitan a un número de ciudadanos cada vez mayor participar en los procesos democráticos;

(...)

3. (...) señala que la democracia digital por sí misma no garantiza la participación política y que también debe abordarse un entorno no digital al objeto de procurar la participación política de los ciudadanos en paralelo a la democracia digital;

4. Señala la importancia de la votación electrónica y de la votación a distancia por internet como sistemas capaces de ampliar la inclusión de los ciudadanos y facilitar la participación democrática, en particular en zonas geográfica y socialmente más marginadas, al ofrecer numerosas ventajas potenciales, en particular para los jóvenes, las personas con movilidad reducida, las personas mayores y las personas que viven o trabajan permanente o temporalmente en un Estado miembro del que no son nacionales o en un tercer país, siempre que se respeten las normas más exigentes en materia de protección de datos; recuerda que, al implantar la votación a distancia por internet, los Estados miembros deben garantizar la transparencia y la fiabilidad del escrutinio y respetar los principios de igualdad y secreto de la votación y de acceso a la misma, y de libertad de sufragio;

(...)

9. Recuerda el primer ejemplo europeo de votación en línea, que tuvo lugar en Estonia en las elecciones jurídicamente vinculantes de 2005, pero afirma que, para que la introducción de una posible votación electrónica en otros Estados miembros sea un éxito, habrá que evaluar si se puede garantizar la participación efectiva de toda la población, así como los beneficios, los retos y las repercusiones de los diferentes o divergentes enfoques tecnológicos; hace hincapié en que la existencia de conexiones a internet seguras y de alta velocidad y de infraestructuras seguras de identificación electrónica son requisitos previos importantes para el éxito de la votación electrónica; subraya la necesidad de aplicar las ventajas de las nuevas tecnologías a los actuales procesos de votación presencial y considera que se pueden realizar avances significativos mediante el intercambio de buenas prácticas y la investigación a todos los niveles políticos;

(...)

35. Destaca la necesidad de proteger, con carácter prioritario, la intimidad y los datos personales cuando se utilicen herramientas de democracia digital, y de fomentar un entorno más seguro en internet, en particular por lo que se refiere a la seguridad de la información y de los datos, incluido el ‘derecho al olvido’, así como de ofrecer garantías frente al *software* de vigilancia y la verificabilidad de las fuentes; pide, además, un mayor uso de los servicios digitales basados en habilitadores clave, como una identidad digital segura y encriptada de conformidad con el Reglamento eIDAS; aboga por la creación de registros públicos digitales seguros y la validación de las firmas electrónicas para evitar interacciones fraudulentas múltiples, en consonancia con las normas de derechos humanos europeas e internacionales y con la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea; subraya, por último, que los problemas de seguridad no deben convertirse en un elemento disuasorio para la inclusión de individuos y grupos en los procesos democráticos;

36. Insiste en la necesidad de mejorar la democracia a través de la tecnología, que debe usarse en un entorno seguro que esté a salvo del mal uso de las herramientas tecnológicas (por ejemplo, robots para el envío de correo basura, elaboración anónima de perfiles y usurpación de identidad), y recuerda la necesidad de respetar las normas jurídicas más exigentes;
(...)”.

Poco después, se aprobó la Recomendación CM/Rec(2017)5 del Comité de Ministros del Consejo de Europa, de 14 de junio de 2017, sobre los estándares para la votación electrónica, entre los que queremos destacar los siguientes:

“1. La interfaz del votante de un sistema de voto electrónico deberá ser fácil de entender y utilizar por todos los votantes.

2. El sistema de voto electrónico estará diseñado, en la medida de lo posible, para que las personas con discapacidades y con necesidades especiales puedan votar de forma independiente.

3. A menos que los canales de voto electrónico a distancia sean universalmente accesibles, serán solo un medio adicional y opcional de votación.

(...)

14. El sistema de voto electrónico avisará al votante si emite un voto electrónico inválido.

15. El votante deberá poder comprobar que el voto ha entrado en la urna electrónica sin ser alterado. Cualquier influencia indebida que haya modificado el voto deberá ser detectable.

16. El votante recibirá la confirmación por parte del sistema de que el voto ha sido emitido con éxito y de que se ha completado todo el procedimiento de votación.

17. El sistema de voto electrónico deberá proporcionar una prueba sólida de que cada voto auténtico se incluye con precisión en los respectivos resultados electorales. Las pruebas deben ser verificables por medios independientes del sistema de voto electrónico.

(...)

19. La votación electrónica se organizará de manera que se garantice el respeto del secreto del voto en todas las etapas del procedimiento de votación.

20. El sistema de voto electrónico procesará y almacenará solo los datos personales necesarios para el desarrollo de la elección electrónica.

(...)

25. El voto electrónico garantizará el secreto de las opciones anteriores registradas y borradas por el votante antes de emitir su voto definitivo.

26. El proceso de voto electrónico, en particular la fase de recuento, se organizará de tal manera que no sea posible reconstruir un vínculo entre el voto y el votante. Los votos son, y deben seguir siendo, anónimos.

27. Los Estados miembros que introduzcan el voto electrónico lo harán de forma gradual y progresiva.

28. Antes de introducir el voto electrónico, los Estados miembros introducirán los cambios necesarios en la correspondiente legislación pertinente.

29. La legislación pertinente deberá regular las responsabilidades del funcionamiento de los sistemas de voto electrónico y garantizar que el organismo de gestión electoral tenga el control de los mismos.

30. Cualquier observador podrá observar el recuento de los votos. El organismo de gestión electoral será responsable del proceso de recuento.

(...)

32. La ciudadanía —y en particular los electores— deberá ser informada, con suficiente antelación al inicio de la votación, en un lenguaje claro y sencillo, sobre: los pasos que un votante puede tener que dar para participar y votar; la utilización y el funcionamiento correctos del sistema de voto electrónico; y el calendario de la votación electrónica, incluyendo todas las etapas.

33. Los componentes del sistema de voto electrónico se divulgarán a efectos de verificación y certificación.

34. Cualquier observador, en la medida permitida por la ley, podrá observar y comentar las elecciones electrónicas incluyendo la compilación de los resultados.

35. Se utilizarán estándares abiertos para permitir la interoperabilidad de varios componentes o servicios técnicos.

36. Los Estados miembros desarrollarán los requisitos técnicos, de evaluación y de certificación, que reflejen plenamente los principios jurídicos y democráticos pertinentes. Los Estados miembros mantendrán los requisitos al día.

37. Antes de la introducción de un sistema de voto electrónico y a intervalos apropiados después, y en particular tras cualquier cambio significativo en el sistema, un organismo independiente y competente evaluará la conformidad del sistema de voto electrónico y de cualquier componente de tecnología de la información y la comunicación con los requisitos técnicos.

(...)

39. El sistema de voto electrónico deberá ser auditable. El sistema de auditoría deberá ser abierto y exhaustivo e informar activamente sobre los posibles problemas y amenazas.

40. El organismo electoral competente será responsable del respeto y cumplimiento de todos los requisitos, incluso en el caso de fallos y ataques. El organismo de gestión electoral será responsable de la disponibilidad, fiabilidad, usabilidad y seguridad del sistema de voto electrónico.

41. Solo las personas autorizadas por el organismo de gestión electoral tendrán acceso a la infraestructura central, a los servidores y a los datos electorales.

42. Antes de que se celebren las elecciones electrónicas, el organismo de gestión electoral se asegurará de que el sistema funciona correctamente.

(...)

45. Los votos y la información de los votantes se mantendrán sellados hasta que comience el proceso de recuento.

46. El organismo de gestión electoral deberá manejar todo el material criptográfico de forma segura.

(...)

49. El sistema de voto electrónico identificará los votos afectados por una irregularidad”.

2. ¿De qué hablamos cuando hablamos de democracia local?³

Es probable que no haya mejor forma de empezar un texto sobre la democracia local que recordando lo ya proclamado por la Carta Europea de Autonomía Local, hecha en Estrasburgo el 15 de octubre de 1985 y ratificada por España el 20 de enero de 1988. En su Preámbulo proclama, entre otras cosas, que las entidades locales son uno de los principales fundamentos de un régimen democrático; que el derecho de los ciudadanos a participar en la gestión de los asuntos públicos forma parte de los principios democráticos comunes a todos los Estados miembros del Consejo de Europa; que en este nivel local este derecho puede ser ejercido más directamente...

En su artículo 3.2 define el derecho a la autonomía local como el que “se ejerce por Asambleas o Consejos integrados por miembros elegidos por sufragio libre, secreto, igual, directo y universal y que pueden disponer de órganos ejecutivos responsables ante ellos mismos. Esta disposición no causará perjuicio al recurso a las asambleas de vecinos, al referéndum o a cualquier otra forma de participación directa de los ciudadanos, allí donde esté permitido por la Ley”.

Por todo ello, a la hora de valorar el grado de democracia que existe en un determinado ámbito social y político, como el de los entes locales, no se puede reparar solo en el número de personas que votan en las elecciones, sino que deben tenerse en cuenta también el respaldo a iniciativas populares, la demanda de consultas ciudadanas y la participación en las mismas, la apertura de foros de debate...

Habrà, pues, que tener en cuenta todos estos elementos para saber si se puede hablar, parafraseando a Pierre Rosanvallon, del mito del “ciudadano pasivo” en los entes locales⁴. Y es que la participación ciudadana en la vida política, económica, social y cultural de estas entidades constituye, como diría Kelsen, la esencia y el valor de la democracia⁵. Esta democracia participativa se contrapone a la “democracia inactiva”, donde el papel de la ciudadanía se limita a la intervención en el proceso mediante el que se selecciona a quienes gobernarán las entidades políticas.

3. Estudiamos parcialmente estas cuestiones en Presno y García (2019).

4. Rosanvallon (2006: 24 y ss.).

5. Kelsen (2006).

La propia Constitución Española (CE) ha descartado esa vertiente inactiva de la democracia local al proclamar en su Preámbulo la voluntad de alcanzar una sociedad democrática avanzada, algo que se ve confirmado al establecer en el artículo 9.2 un mandato claro dirigido a los poderes públicos, a los que corresponde, en palabras textuales, “promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social”. No estamos, por tanto, ante una potestad discrecional de los poderes públicos, que puedan, o no, desarrollar, sino, como ya se ha dicho, ante un mandato de hacer: “facilitar la participación”.

Esta exigencia constitucional se dirige a todos los poderes públicos; por tanto, también a las entidades locales. Tales disposiciones generales se ven complementadas en otros preceptos donde se reconoce la participación de determinados colectivos. Así, por ejemplo, el artículo 48 CE establece que “los poderes públicos promoverán las condiciones para la participación libre y eficaz de la juventud en el desarrollo político, social, económico y cultural”.

En esta última línea se inscriben disposiciones supranacionales que también nos obligan, como la Carta de Derechos Fundamentales de la Unión Europea, donde se dispone:

“Artículo 25

(...)

La Unión reconoce y respeta el derecho de las personas mayores a llevar una vida digna e independiente y a participar en la vida social y cultural.

Artículo 26

(...)

La Unión reconoce y respeta el derecho de las personas discapacitadas a beneficiarse de medidas que garanticen su autonomía, su integración social y profesional y su participación en la vida de la comunidad”.

Y, volviendo a la normativa española, cabe mencionar también lo previsto en algunos estatutos de autonomía, que atribuyen competencias a las comunidades autónomas para legislar en materia de procesos participativos locales. Así, el artículo 29.6 del Estatuto de Autonomía de Cataluña dice que “los ciudadanos de Cataluña tienen derecho a promover la convocatoria de consultas populares por parte de la Generalitat y los ayuntamientos, en materia de las competencias respectivas, en la forma y las condiciones que las leyes

establecen”, y, de acuerdo con el artículo 122, “corresponde a la Generalitat la competencia exclusiva para el establecimiento del régimen jurídico, las modalidades, el procedimiento, la realización y la convocatoria por la propia Generalitat o por los entes locales, en el ámbito de sus competencias, de encuestas, audiencias públicas, foros de participación y cualquier otro instrumento de consulta popular, con excepción de lo previsto en el artículo 149.1.32 de la Constitución”; por su parte, el artículo 78 del Estatuto andaluz dispone que “corresponde a la Junta de Andalucía la competencia exclusiva para el establecimiento del régimen jurídico, las modalidades, el procedimiento, la realización y la convocatoria por ella misma o por los entes locales en el ámbito de sus competencias de encuestas, audiencias públicas, foros de participación y cualquier otro instrumento de consulta popular, con la excepción del referéndum”.

Pues bien, esta participación a la que se apela en los textos jurídicos necesita de instrumentos que regulen los diferentes procesos, concretando qué personas son las titulares del derecho de participación, en qué condiciones se puede participar, hasta dónde alcanza la participación, etc.

3. Los procesos participativos en el ámbito local: oportunidades y riesgos

En un estudio de los profesores Patricia García-Espín y Manuel Jiménez Sánchez⁶ se analizan los procesos participativos como reformas institucionales que buscan ampliar las oportunidades de la ciudadanía para influir en las decisiones públicas. Recuerdan los autores que esos procesos han venido siendo considerados como herramientas para fortalecer la sociedad civil, empoderar a los grupos asociativos (generando nuevos recursos) y establecer pautas de interacción con los poderes públicos basadas en la autonomía, la transparencia y la horizontalidad. No obstante, la práctica evidencia que, a veces, estos procesos están bajo un sesgo institucional y no dejan de ser mecanismos que propician la instrumentalización y la legitimación del *statu quo*.

En ese estudio se analiza, en primer lugar, si los procesos participativos establecen espacios institucionales (“arenas políticas”) que propician las interacciones y las iniciativas de coordinación entre individuos y actores

6. García-Espín y Jiménez (2017).

asociativos que de otro modo serían difíciles. Si fuera así, funcionarían en la sociedad civil como los “arrecifes de coral” lo hacen en la vida marina.

Pues bien, según los autores: “Una vez resueltos los problemas iniciales de coordinación, los procesos participativos pueden incrementar la probabilidad de que la acción colectiva se mantenga en el tiempo y tome cuerpo en grupos más o menos formalizados. Las expectativas de acceso a recursos (de influencia, por ejemplo) pueden actuar como un factor impulsor para grupos que no estaban previamente organizados. Así como los arrecifes de coral fomentan la diversidad de especies, el aumento en el número de grupos puede conducir a una mayor diversidad o pluralidad de participantes. Por el contrario, si son percibidos como costosos, las expectativas reducidas, o los resultados son frustrantes, los nuevos participantes potenciales pueden abstenerse y otros pueden abandonar (potencialmente, reduciendo la diversidad dentro de las redes de políticas). En algunas ocasiones, la salida puede implicar una forma de expresar desacuerdo o rechazo del nuevo escenario político”⁷.

Estos procesos pueden activar mecanismos de intermediación entre grupos (no conectados previamente), ya que implican convocatorias más o menos amplias a la participación, promoviendo la convergencia y, eventualmente, futuras colaboraciones y acciones conjuntas. Por el contrario, un sesgo en la selección de los participantes, intencionado o no, podría desencadenar un mecanismo de cierre, limitando el flujo de información e incluso reduciendo el universo de actores conectados.

En segundo lugar, García-Espín y Jiménez recuerdan que los procesos participativos empoderan a los grupos asociativos: pueden implicar cambios en la cantidad y variedad de recursos organizativos disponibles, favorecer innovaciones en su estilo organizativo (metodologías, agendas, repertorios de acción) y, finalmente, promueven la aparición de (nuevos) sentimientos de eficacia política entre los actores asociativos. Pero se advierte que cuando se espera que estos procesos aumenten los sentimientos de eficacia política (“podemos tener voz”), el efecto contrario (frustración de expectativas y sentimientos de ineficacia política externa) resulta frecuente.

En tercer término, se analiza si los procesos participativos democratizan los patrones de interacción entre los grupos asociativos y las

7. García-Espín y Jiménez (2017: 124-125).

autoridades. Y es que estos procesos pueden conducir a la incorporación o al mantenimiento de nuevos actores asociativos previamente excluidos, pero también pueden activar mecanismos de cierre, reduciendo el número de voces que acceden a las redes políticas o ubicándolas en posiciones marginales.

Además, un efecto clave de los procesos participativos se relaciona con la institucionalización de prácticas de transparencia; por ejemplo, los cambios en los flujos de información, provocados por la formalización y publicidad de las interacciones, pueden reducir el ejercicio del poder discrecional por parte de las autoridades y actores asociativos, y pueden aumentar la capacidad de influencia de quienes carecen de poder.

En la misma línea, los procesos participativos pueden proporcionar nuevas oportunidades políticas para influir en las decisiones; así, por ejemplo, un proceso de toma de decisiones compartida en un área de política específica puede ser replicado en otras áreas. El riesgo es que estas dinámicas acaben sirviendo más bien para fomentar la cooptación y el clientelismo político.

A modo de conclusión y a los efectos que nos interesan en este texto, consideramos fundamental tener en cuenta lo siguiente: los procesos participativos en el ámbito local deben propiciar las interacciones y las iniciativas de coordinación entre individuos y actores asociativos; si dichos procesos son percibidos -en sentido amplio- como costosos, las expectativas son reducidas o los resultados frustrantes, fracasarán sin duda; los mecanismos de participación deben conducir a la incorporación de actores previamente excluidos, aumentar el número de voces que acceden a las redes políticas y ubicarlas en posiciones no marginales; en cuarto lugar, los procesos participativos deben conectarse a la institucionalización de prácticas de transparencia, favoreciendo así el control sobre el poder discrecional de las autoridades. Finalmente, los procesos participativos tienen que articularse de manera que se reduzca al mínimo posible el potencial de cooptación y clientelismo político.

Pues bien, todas estas exigencias deberían ser tenidas en cuenta a la hora de optar por el empleo de herramientas electrónicas y, en particular, de la tecnología *blockchain* en los procesos participativos.

4. Pautas de actuación de los poderes públicos en relación con los procesos participativos locales

Como ya se ha anticipado al principio, la intervención en estos procesos tendría que implicar, al menos, las siguientes facultades:

a) el acceso a toda la información pública cuyo conocimiento facilite el ejercicio de la participación, sin más limitaciones que las previstas en la legislación sobre transparencia;

b) el derecho a iniciar o promover esos procesos participativos en los términos previstos en cada uno de ellos;

c) el derecho a realizar aportaciones durante el desarrollo de los procesos participativos con arreglo a lo establecido en los mismos;

d) el derecho a recibir respuesta de las administraciones y entidades locales a las iniciativas y aportaciones realizadas en los diferentes procesos participativos.

La primera de estas cuatro concreciones del derecho de participación se vincula a la legislación sobre transparencia, estatal y autonómica, y se orienta a hacer posible una participación informada, valga la teórica redundancia; la segunda alude al impulso de los procesos participativos, la tercera a la intervención en los mismos una vez iniciados y la cuarta a la información que ha de recibirse de las actuaciones anteriores.

Y en esos procesos participativos locales, los poderes públicos y los organismos y entidades de ellos dependientes tendrían que actuar de conformidad con los siguientes principios:

a.- universalidad, fomentando la participación de todas las personas y de los grupos en los que se integran en los asuntos públicos, con la obvia exigencia de respetar lo que hubieran establecido al respecto las correspondientes disposiciones;

b.- transparencia, poniendo a disposición de todas las personas, de conformidad con lo previsto en la respectiva legislación estatal y autonómica, toda la información pública necesaria para el desarrollo de los procesos participativos;

c.- igualdad de oportunidades y accesibilidad universal para garantizar la intervención efectiva y sin exclusiones de todas las personas en los procesos participativos;

d.- coordinación, promoviendo iniciativas que favorezcan la actuación conjunta de las personas legitimadas para intervenir en los procesos participativos;

e.- publicidad y rendición de cuentas, en virtud de las cuales se darán a conocer los resultados de los diferentes procesos participativos y la incidencia de los mismos en las políticas públicas.

5. Procesos participativos en el ámbito local

Los procesos participativos, que se describirán de manera muy sucinta, podrían ser, entre otros, los siguientes -al margen de los procesos electorales sobradamente conocidos⁸:- la iniciativa popular sobre ordenanzas y reglamentos locales, la participación ciudadana en la elaboración de los presupuestos locales, las consultas populares y los foros y jurados ciudadanos.

Algunos de estos procesos han sido incorporados de manera expresa en diversas normas legales. Así, a título de ejemplo, cabe mencionar, en primer lugar, el artículo 108 del Estatuto de Autonomía de Canarias -“Corresponde a la Comunidad Autónoma de Canarias la competencia exclusiva para regular: a) El régimen jurídico, las modalidades, el procedimiento, la realización y la convocatoria por ella misma o por los entes locales, en el ámbito de sus competencias, de encuestas, audiencias públicas, foros de participación y cualquier otro instrumento análogo de consulta popular, con la excepción del referéndum. (...)”-, y, de modo más preciso, la Ley 7/2017, de 27 de diciembre, de participación ciudadana de Andalucía, cuyo artículo 12 enuncia los siguientes procesos de participación ciudadana: “a) Deliberación participativa. b) Participación ciudadana en la elaboración de presupuestos. c) Participación ciudadana mediante consultas populares. d) Participación ciudadana en la proposición de políticas públicas y elaboración de normas. e) Participación ciudadana en el seguimiento y evaluación de las políticas públicas y de la prestación de los servicios públicos”⁹.

8. Font (2001) y Font y Blanco (2006).

9. Sobre esta Ley, Ruiz Magaña (2020).

Y, por lo que tiene que ver con el uso de las herramientas tecnológicas modernas, la Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana, ya prevé que “la Administración de la Generalitat y su sector público desarrollarán, entre otros, los medios telemáticos adecuados y accesibles para informar a la ciudadanía de las iniciativas de actuaciones públicas y de los resultados de la gestión, potenciando la implementación progresiva de procesos de participación ciudadana a través de medios electrónicos” (artículo 45)¹⁰.

5.1. La iniciativa popular sobre ordenanzas y reglamentos locales

Las entidades locales, en los términos previstos en la legislación sectorial, deben articular procesos de participación ciudadana para la elaboración de los anteproyectos de ordenanzas y reglamentos locales. Así, de acuerdo con el artículo 18.1 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL), es un derecho y un deber de los vecinos: “b) Participar en la gestión municipal de acuerdo con lo dispuesto en las leyes y, en su caso, cuando la colaboración con carácter voluntario de los vecinos sea interesada por los órganos de gobierno y administración municipal”; y el artículo 70 bis 1. y 2 dispone lo siguiente:

“1. Los ayuntamientos deberán establecer y regular en normas de carácter orgánico procedimientos y órganos adecuados para la efectiva participación de los vecinos en los asuntos de la vida pública local, tanto en el ámbito del municipio en su conjunto como en el de los distritos, en el supuesto de que existan en el municipio dichas divisiones territoriales.

2. Los vecinos que gocen del derecho de sufragio activo en las elecciones municipales podrán ejercer la iniciativa popular, presentando propuestas de acuerdos o actuaciones o proyectos de reglamentos en materias de la competencia municipal.

Dichas iniciativas deberán ir suscritas al menos por el siguiente porcentaje de vecinos del municipio:

- a) Hasta 5000 habitantes, el 20 por ciento.
- b) De 5001 a 20 000 habitantes, el 15 por ciento.
- c) A partir de 20 001 habitantes, el 10 por ciento.

Tales iniciativas deberán ser sometidas a debate y votación en el Pleno, sin perjuicio de que sean resueltas por el órgano competente por razón de la materia. En todo caso, se requerirá el previo informe de legalidad del secretario del ayuntamiento, así como el informe del interventor cuando

10. Ampliamente sobre estas cuestiones, Castellanos Claramunt (2020).

la iniciativa afecte a derechos y obligaciones de contenido económico del ayuntamiento. En los municipios a que se refiere el artículo 121 de esta Ley, el informe de legalidad será emitido por el secretario general del pleno y cuando la iniciativa afecte a derechos y obligaciones de contenido económico, el informe será emitido por el interventor general municipal.

Lo dispuesto en este apartado se entiende sin perjuicio de la legislación autonómica en esta materia.

Tales iniciativas pueden llevar incorporada una propuesta de consulta popular local, que será tramitada en tal caso por el procedimiento y con los requisitos previstos en el artículo 71”.

A nuestro juicio, es necesario, si se quiere realmente fomentar la participación, reducir el número de firmas requerido para presentar una iniciativa popular local: el 20 % de los habitantes en los municipios de hasta 5000 habitantes y el 15 % en los que tengan menos de 20 000 son cifras extraordinariamente altas y que pueden generar un auténtico efecto de desaliento por la dificultad que supone alcanzarlas. Téngase en cuenta que en la iniciativa legislativa popular prevista en la CE (artículo 87.3) se prevé una cantidad ya muy alta en términos comparados -500 000 firmas frente a las 50 000 exigidas en Italia-, pero que es poco más del 10 % de la población española.

5.2. La participación ciudadana en la elaboración de los presupuestos de las entidades locales

Como es bien conocido, se trata de la intervención ciudadana en lo que es el instrumento anual clave de la política local: el presupuesto, que se ha definido, en términos amplios, como “un mecanismo (o un proceso) por el cual la población define o contribuye a definir el destino de todo o una parte de los recursos públicos”¹¹. Es también sabido que surgió en la ciudad brasileña de Porto Alegre en 1989 y luego se ha extendido por ciudades de diferentes continentes¹². En la legislación española aparecen mencionados, por lo que al ámbito local se refiere, en la citada Ley andaluza de participación ciudadana (artículo 24):

“1. Las entidades locales, conforme a sus competencias y atribuciones, podrán iniciar procesos de participación ciudadana, como presupuestos participativos, para llevar a cabo una priorización sobre aspectos determinados de sus presupuestos.

11. Cabannes (2004: 20) y Cabannes y Lipietz (2015).

12. Gómez del Peso (2014).

2. La finalidad de estos procesos es que la asignación de gasto por parte de las entidades locales se haga teniendo en cuenta las prioridades manifestadas en un proceso participativo en el que se hayan oído previamente las opiniones, criterios y sensibilidades de la ciudadanía.

3. La Junta de Andalucía fomentará la promoción y difusión de procesos de presupuestos participativos con base en los principios de universalidad y autorreglamentación.

4. La Junta de Andalucía colaborará en el impulso y promoción de los presupuestos participativos desarrollados por las entidades locales, a través de acciones positivas, información, formación y sensibilización”.

5.3. Las consultas populares de ámbito local

El artículo 18.1.f) LBRL reconoce, como uno de los derechos de los vecinos, “pedir la consulta popular en los términos previstos en la ley”, y el artículo 71 de la misma norma prevé que, “de conformidad con la legislación del Estado y de la comunidad autónoma, cuando esta tenga competencia estatutariamente atribuida para ello, los alcaldes, previo acuerdo por mayoría absoluta del pleno y autorización del Gobierno de la nación, podrán someter a consulta popular aquellos asuntos de la competencia propia municipal y de carácter local que sean de especial relevancia para los intereses de los vecinos, con excepción de los relativos a la Hacienda local”¹³.

Además, y relacionado con el asunto que nos ocupa, en el artículo 70.bis.3 LBRL se preceptúa que, “asimismo, las entidades locales y, especialmente, los municipios, deberán impulsar la utilización interactiva de las tecnologías de la información y la comunicación para facilitar la participación y la comunicación con los vecinos, para la presentación de documentos y para la realización de trámites administrativos, de encuestas y, en su caso, de consultas ciudadanas. Las diputaciones provinciales, cabildos y consejos insulares colaborarán con los municipios que, por su insuficiente capacidad económica y de gestión, no puedan desarrollar en grado suficiente el deber establecido en este apartado”.

Por su parte, y en relación con las previsiones de la LBRL, tras las reformas llevadas a cabo en el presente siglo, diversos estatutos de autonomía han incorporado a su articulado estas consultas populares como

13. Véanse al respecto, entre otros, los estudios de Ibáñez Macías (2005, 2013), Martínez-Alonso Camps (2011), Tur y Sanjuán (2018) y Expósito Gómez (2019).

instrumentos de participación ciudadana: así, el de la Comunidad Valenciana (artículo 50.8), el de Cataluña (artículo 122), Islas Baleares (artículo 31.10), Andalucía (artículo 78), Aragón (artículo 71.27.^a), Castilla y León (artículo 71.15), Extremadura (artículo 9.50) y Canarias (31.3 y 108), lo que, a su vez, ha dado lugar a leyes autonómicas que desarrollan dichas consultas, como algunas de las ya mencionadas. No obstante, ya existían previsiones al respecto bien en la normativa autonómica de régimen local o, incluso, en leyes específicas como, en Andalucía, la Ley 2/2001, de 3 de mayo, de regulación de las consultas populares locales en Andalucía y, en Navarra, la Ley Foral 27/2002, de 28 de octubre, reguladora de consultas populares en el ámbito local.

En todo caso, si algo parece claro es la infrautilización de este mecanismo a lo largo de la reciente historia democrática española: a fecha 1 de enero de 2018, y de acuerdo con una respuesta parlamentaria del Gobierno, desde 1985 a 2017 se efectuaron 50 consultas populares locales autorizadas por el Gobierno. Esta es una cantidad ridícula si se piensa en los más de ocho mil municipios españoles, el tiempo transcurrido y, cosa nada desdeñable, la pérdida de legitimidad de muchas decisiones tomadas por los órganos locales y que, teniendo como destinatarios inmediatos a sus vecinos y pudiendo conocer su opinión, han sido adoptadas al margen de este instrumento de participación y de legitimación democráticas.

5.4. Otros instrumentos de participación ciudadana

Existen otros mecanismos de deliberación y participación que adoptan formas como los foros y los jurados ciudadanos. En términos generales, un foro ciudadano tiene como finalidad debatir sobre la oportunidad de llevar a cabo una concreta política pública y acerca del contenido de la misma, y, en teoría, esta forma de participación puede crearse a iniciativa de la entidad local, a propuesta de un determinado número de personas titulares del derecho de participación o de varias entidades asociativas de participación ciudadana. Cada foro ciudadano estaría formado por un mínimo relativamente reducido de personas elegidas por sorteo. Por su parte, los jurados ciudadanos, de modo similar a los foros, se componen de un número reducido de personas elegidas por sorteo con la finalidad de realizar una valoración de los resultados que ha producido un concreto programa, proyecto o intervención de la entidad local. Los foros intervendrían en una fase previa, a propósito de una iniciativa y su contenido, y los jurados después, para enjuiciar la iniciativa.

Encontramos referencias normativas a estos instrumentos tanto en las disposiciones estatutarias como legales. Así, el artículo 122 del Estatuto catalán (“Consultas populares”) dispone: “Corresponde a la Generalitat la competencia exclusiva para el establecimiento del régimen jurídico, las modalidades, el procedimiento, la realización y la convocatoria por la propia Generalitat o por los entes locales, en el ámbito de sus competencias, de encuestas, audiencias públicas, foros de participación y cualquier otro instrumento de consulta popular, con excepción de lo previsto en el artículo 149.1.32 de la Constitución”; el artículo 78 del Estatuto andaluz (también “Consultas populares”) prevé: “Corresponde a la Junta de Andalucía la competencia exclusiva para el establecimiento del régimen jurídico, las modalidades, el procedimiento, la realización y la convocatoria por ella misma o por los entes locales en el ámbito de sus competencias de encuestas, audiencias públicas, foros de participación y cualquier otro instrumento de consulta popular, con la excepción del referéndum”; el 71.27.^a del Estatuto de Aragón atribuye a la Comunidad competencia exclusiva sobre: “Consultas populares, que, en todo caso, comprende el establecimiento del régimen jurídico, las modalidades, el procedimiento, la realización y la convocatoria por la Comunidad Autónoma o por los entes locales en el ámbito de sus competencias de encuestas, audiencias públicas, foros de participación y cualquier otro instrumento de consulta popular, con excepción de la regulación del referéndum y de lo previsto en el artículo 149.1.32.^a de la Constitución”; y, por no extendernos más, conforme al artículo 108 del Estatuto de Canarias: “Corresponde a la Comunidad Autónoma de Canarias la competencia exclusiva para regular: a) El régimen jurídico, las modalidades, el procedimiento, la realización y la convocatoria por ella misma o por los entes locales, en el ámbito de sus competencias, de encuestas, audiencias públicas, foros de participación y cualquier otro instrumento análogo de consulta popular, con la excepción del referéndum”.

Por su parte, según la Ley de participación ciudadana de Andalucía, los foros de participación “son espacios de debate, creados por iniciativa de la Administración pública, que tienen por objeto debatir y reflexionar sobre los efectos de una política pública, así como elaborar análisis valorativos de los efectos reales de dichas políticas en la ciudadanía”, y los jurados “son grupos creados por la Administración pública que tienen como finalidad analizar los efectos de una determinada acción, proyecto o programa llevado a cabo por la misma” (artículo 26.c y e).

Previamente, la Ley catalana 10/2014, de 26 de septiembre, de consultas populares no referendarias y otras formas de participación ciudadana, incluye

foros y jurados como “foros de participación” (artículo 55), que “se organizan como espacios de deliberación, análisis, propuesta y evaluación de las iniciativas y las políticas públicas”¹⁴.

Y la Ley 8/2015, de 25 de marzo, de transparencia de la actividad pública y participación ciudadana de Aragón, contempla (artículo 53.b y d) los foros de consulta, que “son espacios de debate, creados por iniciativa de la Administración, que tienen por objeto debatir y reflexionar sobre los efectos de una política pública, así como elaborar análisis valorativos de los efectos reales de dicha política en la calidad de vida de la ciudadanía”, y los jurados ciudadanos, “entendidos como grupos creados por la Administración pública que tienen como finalidad analizar los efectos de una determinada acción, proyecto o programa llevado a cabo por la misma”.

6. Tecnología, *blockchain* o no, y procesos participativos locales

En un trabajo anterior nos ocupamos de las “premisas para la introducción del voto electrónico en la legislación electoral española”¹⁵, y ya hemos mencionado las recomendaciones del Parlamento Europeo y del Comité de Ministros del Consejo de Europa en relación con los procesos participativos electrónicos. Volveremos sobre ellas a lo largo de este epígrafe, pues, en la medida en que nos parecen también adecuadas a lo que aquí tratamos, aplicaremos

14. “(...) Los foros de participación pueden tener carácter temporal o permanente. 2. Los foros están integrados por un conjunto de ciudadanos y representantes de entidades cívicas seleccionados por la Administración como muestra representativa de un sector o colectivo directamente concernido por la iniciativa o política pública. También pueden incluir a expertos en la materia independientes. 3. Los foros pueden tener las siguientes finalidades: a) Deliberar sobre la idoneidad de una iniciativa pública que se quiere poner en práctica y prever los efectos sobre el sector al que va dirigida. b) Efectuar el seguimiento de las políticas públicas y proponer medidas para su mejora, especialmente en cuanto a la prestación de servicios. c) Analizar y evaluar los resultados de las políticas públicas. 4. Para la efectividad de lo establecido en este artículo, la Generalidad y las entidades locales deben crear y regular un registro de participación en el que pueden inscribirse voluntariamente las personas, entidades y organizaciones cívicas representativas que lo deseen, para formar parte y ser parte activa de los foros. 5. La composición de los foros que se constituyan debe determinarse mediante una elección entre las personas y entidades inscritas en el registro de participación, salvo que la naturaleza especializada del proceso de participación aconseje efectuar su designación. En este último caso, la selección debe realizarse de la forma más plural posible y de acuerdo con los demás principios establecidos en el artículo 2”.

15. Presno Linera (2016, 2020); también, entre otros, los trabajos de González de la Garza (2008), Barrat y Fernández (2011), Guglielmi e Ihl (2017), y, sobre participación y gobierno a través de internet, entre otros estudios de la doctrina española, Cotino Hueso (2006), Ramírez Nárdiz (2010: 158 y ss.), Cebrián Zazurca (2012) y Castellanos Claramunt (2020: 251 y ss.).

dichas premisas y recomendaciones a la hora de valorar una eventual aplicación de la tecnología *blockchain* a la participación política en el ámbito local. Lo que sea dicha tecnología, incluida su potencialidad en términos jurídicos, ha sido objeto de atención en este mismo libro por parte del coordinador del mismo, el profesor Gustavo Manuel Díaz González, por lo que no insistiremos en cuestiones que él ha explicado¹⁶.

En cuanto a la exigencia obvia de que dicha participación deba consistir en un acto de libertad, entendida como su ejercicio sin sujeción a coacciones de ningún tipo, creemos que no hay motivos sólidos para sostener que la persona que participa a través de un dispositivo electrónico, sea o no con tecnología *blockchain*, está más expuesta a intimidaciones que menoscaben su derecho, que la persona que interviene, por correspondencia postal o presencialmente, en unas elecciones, en una consulta popular o en un foro ciudadano.

Sí encontramos mayor fundamento en las cautelas que inciden en la vulnerabilidad de la votación electrónica no *blockchain* a distancia en materia de secreto de voto, pues es bien conocida la posibilidad de interferencias maliciosas en el manejo de cualquier dispositivo informático. Aquí, además del riesgo de que se pueda conocer el sentido de la voluntad de quien participa, lo que en sí mismo no menoscaba necesariamente su libertad, lo que más preocupa es la alteración de esa voluntad ya emitida o su bloqueo para que no sea contada. Con todo ello, estaría seriamente dañada la confianza en el proceso en el que está interviniendo.

A este respecto, son claros los estándares previstos por las instituciones europeas: la votación electrónica se organizará de manera que se garantice el respeto del secreto del voto en todas las etapas del procedimiento de votación; el votante deberá poder comprobar que el voto ha entrado en la urna electrónica sin ser alterado. Cualquier influencia indebida que haya modificado el voto deberá ser detectable; el votante recibirá la confirmación por parte del sistema de que el voto ha sido emitido con éxito y de que se ha completado todo el procedimiento de votación.

Y, por citar un ejemplo conocido, uno de los proyectos más ambiciosos en materia de voto electrónico a distancia, el *Secure Electronic Registration and Voting Experiment* (SERVE), promovido por el Gobierno de Estados Unidos y

16. Hemos manejado también algunas de las referencias bibliográficas que cita el profesor Díaz González: García Mexía (2018), González-Meneses (2017), Magnuson (2020), y también la tesis doctoral de Benítez Martínez (2020).

pensado para permitir el voto de los ciudadanos de ese país que viven fuera del mismo y para el personal militar destinado en el extranjero, fue abandonado ante los numerosos fallos de seguridad que presentaba y que, en palabras de algunos de los más prestigiosos expertos en esta materia, podían resumirse en los siguientes: especial vulnerabilidad a los ataques informáticos en sus múltiples variantes, tanto por personas vinculadas al sistema informático como por sujetos ajenos al mismo, insuficiente garantía de la confidencialidad del voto¹⁷,...

Como contraste a este proyecto fallido cabe mencionar un ejemplo de voto electrónico exitoso un poco posterior en el tiempo: el *i-Voting* articulado en Estonia, el país que realizó la primera experiencia “real” de sufragio electrónico a distancia en unas elecciones legislativas, las de 4 de marzo de 2007. Este sistema se introdujo en 2002 para las elecciones locales, entre otros motivos, para incrementar la participación, sobre todo, de las personas jóvenes. El Tribunal Constitucional avaló su compatibilidad con la norma fundamental y su carácter no discriminatorio, algo a lo que no fue ajeno el hecho de que la población estonia está muy preparada para el uso de las tecnologías de la información y el país cuenta con una infraestructura adecuada para que nadie se sienta excluido del proceso.

Entre los numerosos beneficios que, según la Administración estonia, ha supuesto este sistema, cabe destacar, entre otros, los siguientes: es muy cómodo de usar y de gran ayuda en el supuesto de que el elector esté fuera del país por motivos temporales o porque viva en el extranjero, aunque también resulta de utilidad para quienes no tienen un colegio electoral cerca de su lugar de residencia; supone un ahorro de gasto (mucho menos uso de papeletas y, por tanto, descenso de los envíos y de los consiguientes costes postales), de tiempo real para votar (la mediana de la duración de la sesión de voto electrónico fue de 1:29, 1:21 y 1:36 minutos en 2013, 2014 y 2015) y de horas de trabajo dedicadas al ejercicio del sufragio (unos 11 000 días laborables en 2011).

En Estonia, el voto electrónico tiene lugar durante siete días y comienza diez días antes de la jornada electoral presencial, momento a partir del cual, a través de una tarjeta de identificación, se puede ingresar en el sistema electrónico y emitir el voto, que se podría modificar posteriormente quedando anulado el voto previo. El carácter secreto del sufragio se garantiza con la eliminación electrónica de la identidad del votante antes del escrutinio.

17. Jefferson *et al.* (2004).

Desde 2015, la Administración electoral debe ofrecer al votante la posibilidad de comprobar la integridad del voto registrado¹⁸. En las elecciones de 2015 usaron este sistema 176 329 personas, 185 871 en las elecciones locales de 2017 y 247 232 en las generales de 2019, en este último caso con votantes que ejercieron su derecho desde 145 países.

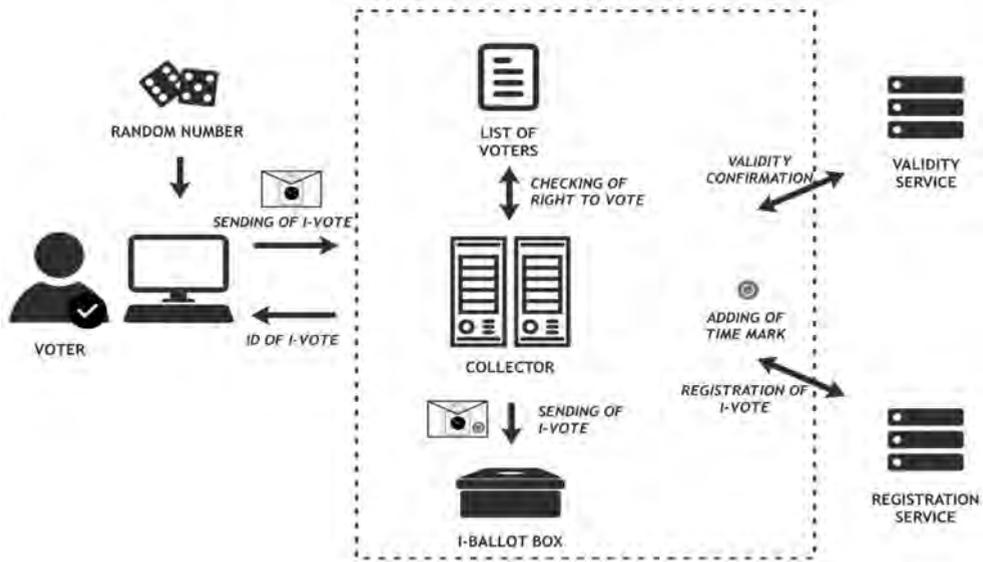


Gráfico tomado de *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*

En España esta confianza institucional y legal en la tecnología electrónica como herramienta al servicio de los procesos participativos ha sido asumida en los últimos años, al menos como objetivo a alcanzar, en el ámbito normativo autonómico, sin que se haya llegado a especificar, quizás por los rápidos cambios inherentes a esa tecnología, qué tipo concreto sería, aunque sí las exigencias que tendría que cumplir para garantizar su carácter democrático. Así, por ejemplo, lo ha hecho el Parlamento de Cataluña, que ya en la Ley 4/2010, de 17 de marzo, de consultas populares por vía de referéndum, incluyó un Título V con la rúbrica: “De la utilización de los medios electrónicos”, y un precepto, el 56, con los “principios generales”, “de acuerdo con la Recomendación del Comité de Ministros del Consejo de Europa relativa a los estándares legales, operacionales y técnicos para el voto electrónico” (según proclama en el Preámbulo):

18. State Electoral Office of Estonia (<https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf>). *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*.

“1. Cuando se establezca un sistema de votación electrónica, el canal electrónico de votación debe tener siempre un carácter facultativo y excluyente, de modo que cualquier ciudadano o ciudadana pueda escoger entre votar con una papeleta o hacerlo electrónicamente.

2. La utilización de medios electrónicos y el *software* electoral aplicable a las consultas populares por vía de referéndum deben respetar los principios democráticos generales, los derechos de los ciudadanos y las garantías de la legislación electoral, y deben garantizar la fiabilidad y seguridad del sistema, la transparencia y, especialmente:

a) La plena identificación del votante o la votante, de modo que el canal de votación garantice que quien vota es realmente la persona legitimada para hacerlo.

b) El secreto del voto, de modo que no pueda establecerse un vínculo entre el sentido del voto y la persona que lo ha emitido.

c) La libertad de voto, de modo que se excluya cualquier coerción o influencia externa al votante o la votante que determine la orientación de su voto.

d) La posibilidad de que el votante o la votante audite y verifique la emisión de su voto.

e) La emisión de un solo voto por persona.

f) La presentación equitativa y fidedigna de las preguntas y de las opciones correspondientes.

g) El carácter público de todo el proceso electoral por medios electrónicos. Para garantizarlo, el Gobierno y la junta electoral ordenan y controlan todo el proceso, tienen disponibilidad sobre el *software* electoral utilizado y acceso a las instalaciones de las empresas prestadoras del servicio y pueden consultar la documentación relevante en caso de inspección.

h) La seguridad técnica contra adiciones, sustracciones o manipulaciones del sistema o de los votos.

i) La accesibilidad y el conocimiento del hardware y el software electorales, de modo que la Administración pública, los partidos políticos y los ciudadanos puedan comprobar la objetividad del sistema y la fiabilidad de los resultados”¹⁹.

19. El Título incluye otros tres artículos:

“Artículo 57. Recogida de firmas por medios electrónicos.

1. La recogida de firmas puede hacerse por medios electrónicos siempre y cuando se garantice la identificación fehaciente del ciudadano o ciudadana por medio de la firma electrónica y que la voluntad que expresa por medio de la firma sea inequívoca.

2. La recogida electrónica de firmas debe observar garantías similares a las establecidas por el artículo 25.1 respecto al conocimiento y la precisión del objeto de la consulta.

En la misma línea, la Ley 10/2014, de 26 de septiembre, de consultas populares no referendarias y otras formas de participación ciudadana, contempla la utilización de medios electrónicos (artículo 28)²⁰.

Por su parte, la Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana, dispone (artículo 46.2): “La participación y colaboración ciudadanas se podrán hacer efectivas por medio de cualquier mecanismo que sirva para favorecer la implicación de la ciudadanía en los asuntos públicos y, especialmente, por medio del uso de las nuevas tecnologías”²¹.

3. Las entidades prestadoras del servicio de certificación deben certificar la identificación de los firmantes que utilicen la firma electrónica.

4. Corresponde al Gobierno la regulación reglamentaria del sistema y el procedimiento de recogida de firmas por medios electrónicos para las consultas populares por vía de referéndum, de acuerdo con lo establecido por el presente artículo.

Artículo 58. Plataforma única.

El Gobierno debe poner a disposición de los entes locales una plataforma tecnológica común que permita la implantación homogénea del sistema de voto electrónico.

Artículo 59. Garantías y transparencia.

1. Una entidad, pública o privada, externa e independiente, prestadora de servicios de auditoría y certificación de voto electrónico, designada por la administración convocante, debe certificar la corrección del sistema de voto electrónico antes de que se utilice, por medio de un informe que debe entregar a la Administración convocante y al Gobierno. Corresponde al Gobierno autorizar, en función de estos datos, el uso de medios electrónicos en las consultas populares por vía de referéndum de ámbito municipal.

2. Una comisión formada por seis expertos, dos designados por el Parlamento, dos designados por el Gobierno y dos designados por las asociaciones representativas de los entes locales, debe tener acceso a toda la información técnica, incluido el informe de la entidad externa e independiente, y debe entregar al Parlamento un informe anual en que se evalúe la adecuación a la normativa electoral de los sistemas de voto electrónico utilizados. El Parlamento debe hacer público este informe.

3. Los partidos políticos con representación en el ámbito territorial afectado deben recibir toda la información técnica relativa al sistema de votación electrónica, incluido el informe emitido por la entidad externa e independiente”.

20. “1. La participación en las consultas populares no referendarias puede realizarse por medios electrónicos, siempre que se garantice: a) La seguridad en la identificación del participante. b) La no duplicidad o multiplicidad de participación de una misma persona. c) El secreto del voto, de modo que no pueda establecerse vínculo alguno entre la opinión expresada y la persona que la ha emitido. d) La seguridad del voto electrónico para impedir la alteración de la participación o de los votos emitidos. e) La suficiente transparencia para que los actores interesados puedan llevar a cabo una observación y supervisión independiente y fundamentada. 2. El voto electrónico puede ser presencial o telemático. 3. Los medios electrónicos, además de utilizarse para la participación en las consultas, también pueden utilizarse para la recogida de firmas en el caso de la iniciativa ciudadana, siempre que se garantice la seguridad en la identificación de los firmantes. 4. El Gobierno debe regular por reglamento el sistema de participación electrónica de acuerdo con lo establecido en este artículo. Esta regulación debe incluir el establecimiento de una plataforma tecnológica común para permitir su implantación homogénea en el ámbito local”.

21. “A este efecto, la Generalitat: a) Promoverá el diálogo electrónico con los ciudadanos y las ciudadanas y participará en las redes sociales y otros instrumentos de comunicación social en internet. b) Promoverá el acceso a las herramientas, conocimientos y recursos tec-

Finalmente, y yendo más lejos, la varias veces citada Ley 7/2017 de participación ciudadana de Andalucía contempla la existencia de un sistema público de participación digital (artículo 65):

“1. La Administración de la Junta de Andalucía creará un sistema público de participación digital para la puesta en marcha de los procesos contenidos en esta Ley.

2. El centro directivo competente en materia de dirección, impulso y gestión de la política digital en lo concerniente a las nuevas tecnologías aplicadas al gobierno abierto asumirá las funciones, con carácter transversal para la Administración de la Junta de Andalucía, de dirección técnica y desarrollo de las plataformas de participación ciudadana basadas en el uso de las tecnologías de la información y la comunicación (TIC) necesarias para la materialización del derecho a la participación ciudadana, en el marco de lo establecido en la presente Ley.

3. Dicho sistema contará con el desarrollo de una plataforma de participación, en *software* libre, provista de herramientas y funcionalidades que cubran las necesidades informativas de deliberación, de voto y de seguimiento de las iniciativas a las que dé soporte.

4. El método de autenticación garantizará que cada persona usuaria registrada corresponda efectivamente con algunos de los sujetos previstos en

nológicos necesarios para el desarrollo de este enfoque. c) Escuchará proactivamente, tanto por los canales electrónicos como telefónicos, las opiniones de los ciudadanos y las ciudadanas, responderá a sus peticiones con celeridad y eficacia y valorará sus opiniones en la toma de decisiones. A este efecto, se podrá promover sobre determinadas actividades públicas, cuando así se considere oportuno, la realización de encuestas. d) Promoverá la comunicación y la interacción con la ciudadanía a través de dispositivos de telecomunicaciones móviles, e impulsará la utilización en sus relaciones con la Administración. 3. En los procesos participativos que se realicen a través de medios tecnológicos, con el fin de comprobar la identidad de las personas que participan, así como los diferentes requisitos de edad, vecindad administrativa o cualquier otro que se disponga en las disposiciones normativas, la ciudadanía prestará su autorización expresa a la Generalitat para la verificación de los datos requeridos. 4. En las iniciativas de participación y colaboración ciudadana que afecten a los derechos de grupos con especial protección, se elegirá el instrumento de participación que resulte más adecuado para cada uno de ellos, y se pondrá a su disposición la información de apoyo en formato accesible”.

Conforme al artículo 47, “sin perjuicio del trámite de audiencia e información pública previsto en la legislación, la Administración de la Generalitat y su sector público podrá someter, simultánea o consecutivamente a aquel, a consulta pública las normas, planes, procedimientos, instrumentos de planificación o políticas públicas relevantes, de acuerdo con el siguiente procedimiento: 1. Los órganos administrativos o entidades competentes que consideren oportuno abrir un proceso de participación pública, publicarán en el Portal de Transparencia el proyecto de norma, plan, procedimiento o instrumento administrativo, junto a la documentación complementaria necesaria para su comprensión y valoración. 2. Se informará sobre los plazos y mecanismos de participación que serán preferentemente electrónicos, así como sobre el estado de tramitación del proyecto”.

el artículo 6, asegurando el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

5. El portal de la Junta de Andalucía será el punto de acceso general a las plataformas web de participación ciudadana.

6. El centro directivo proponente del proceso participativo asumirá la gestión del propio proceso en cualquiera de las plataformas de participación desarrolladas de acuerdo con lo establecido en el presente artículo.

7. La Administración de la Junta de Andalucía facilitará el acceso al sistema público de participación digital en edificios y dependencias públicas, contando con unidades móviles a fin de acercar a toda la ciudadanía en igualdad de condiciones el uso de estos instrumentos de participación”.

Y precisamente en Andalucía se realizó, entre 2018 y 2019, la primera “prueba de concepto” para definir las necesidades del Sistema Público de Participación de Andalucía²², y en ella se planteó usar y/o adaptar el sistema CONSUL, *software* libre y publicado bajo licencia Affero GPL v3, lo que permite instalarlo, usarlo y modificarlo sin tener que pagar por ello. Según se informa, cuenta con un sistema de registro que garantiza la privacidad y la neutralidad de la participación y puede integrarse con sistemas de padrón o censo existentes. Entre otras cosas, permite la gestión de procesos participativos presupuestarios, intervenir en la elaboración de normas o servir para votaciones. Este sistema se está aplicando en diversas ciudades españolas (Alicante, Valencia, A Coruña, Oviedo, Madrid...) y de otros países (Buenos Aires, Porto Alegre, Quito, Lima, Montevideo, Bogotá, Nueva York o Turín)²³.

Vemos, pues, que parece posible articular un sistema de votación electrónica “seguro” -dicho lo de seguro con las obligadas cautelas en este ámbito- e, incluso, introducir sistemas electrónicos que sirvan para gestionar las diversas fórmulas participativas locales de las que hemos hablado antes. A este respecto, la tecnología *blockchain* también podría contribuir a fortalecer el carácter secreto de la voluntad manifestada (en elecciones, consultas, foros...) y la intangibilidad del acto de participación pues, en principio, al estar basada en la capacidad para crear registros muy difíciles de modificar, se potenciaría la autenticidad, su carácter confidencial, su inalterabilidad y, en última instancia, la confianza ciudadana en el proceso. En primer lugar, la persona titular del derecho podría verificar lo que ha hecho y, en segundo, se

22. <https://enreda.coop/proyectos/sistema-participacion/> (a 29 de septiembre de 2021).

23. <https://consulproject.org/es/index.html> (a 29 de septiembre de 2021).

podría llevar a cabo una auditoría del proceso y de la plataforma de gestión sin que eso supusiera menoscabar, en su caso, el carácter secreto de la decisión.

Apunta el profesor Rubio Núñez que para ello sería necesario desarrollar un código abierto a fin de que cualquiera pudiera auditar la aplicación y contribuir a mejorar su seguridad. El carácter público y compartido de los datos en la cadena permitiría, además, la verificación de la integridad de la información por parte de cualquier persona²⁴.

En realidad, si estas premisas de la tecnología *blockchain* se cumplieran se estaría avanzando mucho en el logro de los citados estándares europeos sobre participación electrónica. Además de los ya mencionados en relación con el voto electrónico no *blockchain*, se permitiría que cualquier persona pudiera no solo observar el recuento, sino también comentar las elecciones electrónicas, incluyendo la compilación de los resultados, algo que hasta ahora no se puede hacer con el voto electrónico. También se favorecería el uso de estándares abiertos para permitir la interoperabilidad de varios componentes o servicios técnicos y la auditoría del proceso.

No obstante estas ventajas, y parafraseando el final de *Con faldas y a lo loco*, nada es perfecto, como también ha puesto de relieve la doctrina que se ha ocupado de estas cuestiones. Parece que ni el ya descrito *i-Voting* estonio²⁵ ni la tecnología *blockchain* garantizan la inmutabilidad absoluta de las transacciones, con lo que asumimos que, en este estado de la cuestión, no cabe mantener que la seguridad sobre una información tan sensible esté fuera de todo riesgo²⁶, al menos del riesgo asumible sin que pueda quedar en cuestión la legitimidad del proceso.

En segundo lugar, cabe preguntarse para qué tipo de votaciones podría suponer una mejora respecto a lo que tenemos ahora el empleo de la tecnología *blockchain*. Nos parece evidente que en España la participación efectiva y sin trabas, el carácter secreto del sufragio y su inalterabilidad, además de la transparencia, están plenamente garantizados con el vigente sistema de votación presencial²⁷, algo que, consideramos, no se puede decir con el

24. Rubio Núñez (2018: 222 y ss.).

25. Nurse *et al.* (2016).

26. Rubio Núñez (2018: 222 y ss.).

27. Conforme al artículo 86 LOREG: “1. El voto es secreto. 2. Los electores solo pueden votar en la sección, y dentro de esta en la Mesa Electoral que les corresponda salvo lo dispuesto en el apartado 1.º del artículo 79. Los electores se acercarán a la Mesa de uno en uno, después de haber pasado, si así lo desearan, por la cabina que estará situada en la misma habitación, en

mismo convencimiento del sufragio por correo de los nacionales residentes en el extranjero: leyendo los debates parlamentarios correspondientes a la elaboración de la Ley Orgánica 2/2011 de reforma de la LOREG se constata, entre otras cosas, que la extensión del voto rogado a los procesos electorales autonómicos, a las Cortes y al Parlamento Europeo respondió a la preocupación de evitar prácticas fraudulentas relacionadas con la identidad de los electores²⁸.

Esta preocupación por el fraude consistente en la suplantación de la identidad del elector no carecía de fundamento pues, como es conocido, la falta de recepción personal de la documentación hacía posible tal suplantación. Y, como resultado de la reforma, tenemos, por lo que ahora interesa, la introducción del voto rogado en los referendos y en todas las elecciones en las que pueden participar los nacionales residentes en el extranjero y la opción de que los electores puedan entregar personalmente la papeleta en las Oficinas o Secciones Consulares en las que estén inscritos o en los lugares que a tal efecto se habiliten para ello o, de manera alternativa, puedan enviarla por correo postal a una de las citadas dependencias.

un lugar intermedio entre la entrada y la Mesa Electoral. Dentro de la cabina el votante podrá elegir las papeletas electorales e introducirlas en los correspondientes sobres. 3. Cada elector manifestará su nombre y apellidos al Presidente. Los Vocales e interventores comprobarán, por el examen de las listas del censo electoral o de las certificaciones aportadas, el derecho a votar del elector, así como su identidad, que se justificará conforme a lo dispuesto en el artículo anterior. Inmediatamente, el elector entregará por su propia mano al Presidente el sobre o sobres de votación cerrados. A continuación este, sin ocultarlos ni un momento a la vista del público, dirá en voz alta el nombre del elector y, añadiendo ‘Vota’, entregará el sobre o sobres al elector quien los depositará en la urna o urnas. 4. Los Vocales y, en su caso, los Interventores que lo deseen anotarán, cada cual en una lista numerada, el nombre y apellidos de los votantes por el orden en que emitan su voto, expresando el número con que figuran en la lista del censo electoral o, en su caso, la aportación de certificación censal específica. Existirá una lista numerada por cada una de las Cámaras de las Cortes Generales y, en su caso, de las Asambleas Legislativas de las Comunidades Autónomas, Corporaciones Locales o Parlamento Europeo que corresponda elegir. Todo elector tiene derecho a examinar si ha sido bien anotado su nombre y apellidos en la lista de votantes que forme la Mesa para cada urna”.

28. Así, en palabras del diputado socialista Benegas Haddad, “en cuanto al contenido concreto de la reforma, respecto al voto de nuestros compatriotas residentes en el extranjero, hemos pretendido garantizar una mayor transparencia y evitar vías de fraude... Van a poder seguir votando en elecciones autonómicas, elecciones generales, europeas y referéndums y el sistema será de voto rogado para garantizar la máxima transparencia del proceso...”. En la misma línea, el diputado del Grupo Popular Bermúdez de Castro apuntó que “el nuevo procedimiento de voto de los españoles que residen en el exterior... va a eliminar cualquier sombra de duda o de sospecha sobre dichos sufragios. Es un procedimiento más garantista basado en tres principios: el de personalidad para evitar suplantaciones, el de transparencia para evitar manipulaciones y el de efectividad para garantizar que sus votos se contabilicen en el escrutinio, introduciendo por primera vez en la historia la previsión del voto en urna en consulado, que era una antigua reivindicación de nuestros compatriotas en el exterior y que con esta reforma ha sido atendida. Más garantías en el voto en el exterior y más control y transparencia en la definición y elaboración del censo electoral...”.

No nos detendremos aquí en el hecho, constatado, de que esa reforma permitió alejar muchas de las dudas o sombras sobre la “personalidad” del votante, evitando suplantaciones, pero no cabe decir, más bien al contrario, que haya introducido el principio de efectividad del sufragio, pues es evidente el reiterado descenso en la participación²⁹. La cuestión ahora, no obstante, es que en las elecciones locales -no en vano estamos hablando de democracia en ese ámbito- el derecho de sufragio activo está reservado a personas residentes en nuestro país³⁰ y no a españoles residentes en el extranjero. Esta precisión es relevante porque si tiene sentido el voto electrónico, con tecnología *blockchain* o sin ella, es como alternativa al voto por correo y no al voto presencial que en España, como ya se ha dicho, ha funcionado bien, sin opacidades, se contabiliza con mucha rapidez y ya permite la intervención ciudadana en su control. No en vano, las urnas son transparentes, el escrutinio es público (artículo 95.2 LOREG) y quienes integran las mesas electorales “son designados por sorteo público entre la totalidad de las personas incluidas en la lista de electores de la Mesa correspondiente...” (artículo 26.2 LOREG).

29. Así, en las elecciones a las Cortes Generales de 10 de noviembre de 2019, según la información que facilita el Ministerio del Interior, el CERA lo formaban 2 130 754 personas, fueron aceptadas 226 050 solicitudes de voto y se computaron 145 908 sufragios (el 6,85 %); en los comicios de abril de ese mismo año había en el CERA 2 099 463 y votaron 118 357 (5,64 %). En las elecciones generales de junio de 2016 el censo CERA llegaba a 1 924 021 personas, se aceptaron 169 658 solicitudes de voto y se emitieron 121 277 (6,3 %). El porcentaje más bajo de votantes tuvo lugar en las elecciones de 2011: con un censo CERA de 1 482 786 personas hubo 138 037 solicitudes de voto y, finalmente, 73 361 votantes (4,95 %). Por contraste, en las elecciones generales de marzo de 2008, anteriores a la reforma de 2011 y con un censo CERA de 1 205 329 personas, votaron 382 568 (31,74 %) y en las de marzo de 2004, con un censo de 1 113 754 personas, hubo 304 685 sufragios (27,36 %); sobre estas cuestiones, García Mahamut (2012), Mateos Crespo (2019) y Presno Linera (pendiente de publicación).

30. El artículo 190 de la LOREG, que regulaba el voto en las elecciones locales de los españoles residentes en el extranjero, fue derogado por la Ley Orgánica 2/2011, de 28 de enero; antes disponía: “1. Los españoles residentes ausentes que vivan en el extranjero y deseen ejercer su derecho de voto en las elecciones del municipio en el que estén inscritos, según el censo electoral, deben comunicarlo a la correspondiente Delegación Provincial de la Oficina del Censo Electoral, no más tarde del vigésimo quinto día posterior a la convocatoria. Dicha comunicación debe realizarse mediante escrito al que se adjuntará fotocopia del Documento Nacional de Identidad o Pasaporte. 2. Recibida dicha comunicación, la Delegación Provincial envía al interesado un certificado idéntico al previsto en el artículo 72, una papeleta de votación en blanco, cuyo formato se determinará reglamentariamente, copia de la página o páginas del ‘Boletín Oficial’ de la provincia en el que figuren las candidaturas proclamadas en el municipio, el sobre de votación, así como un sobre en el que debe figurar la dirección de la Mesa Electoral que le corresponda. Con estos documentos se adjunta una hoja explicativa. 3. Dicho envío debe realizarse por correo certificado y no más tarde del trigésimo segundo día posterior a la convocatoria. 4. El elector escribirá en la papeleta el nombre del partido, federación, coalición o agrupación a cuya candidatura desea votar y remitirá su voto conforme a lo dispuesto en el artículo 73, párrafo 3. El Servicio de Correos actuara en este supuesto conforme a lo previsto en el párrafo cuarto de dicho artículo”.

¿Cabría acudir a la tecnología *blockchain* para sustituir al voto por correo en las elecciones y referendos locales o en cualquier proceso participativo en ese ámbito que culmine en una votación?

Si hablamos de elecciones, referendos o consultas populares, la eventual aplicación de ese voto tecnológico sería para sustituir al voto por correspondencia nacional -ya se ha dicho que no pueden participar las personas españolas residentes en el extranjero-. Por ello, tendría, *a priori*, un uso minoritario -para el sufragio de las personas que no pueden o quieren hacerlo presencialmente ni tampoco a través del correo postal-. Tal cosa no constituye una objeción, pero habría que tener en cuenta el hecho de que su implantación supondría un coste adicional (económico, medioambiental...) sin que, probablemente, ello supusiera una eliminación del vigente voto por correo postal. Para muchas personas, este podría ser un método más cómodo, fácil y confiable que el voto tecnológico *blockchain* que, como se ha dicho también, puede ser fácil y cómodo para quien no esté afectado por brechas tecnológicas, pero tampoco está exento de riesgos.

A este respecto, y si acudimos a los estándares europeos en la materia, nos encontramos con que la interfaz del votante de un sistema de voto electrónico deberá ser fácil de entender y utilizar por todos los votantes -algo que está por ver con la tecnología *blockchain*- y, a menos que los canales de voto electrónico a distancia sean universalmente accesibles, serán solo un medio adicional y opcional de votación, con lo que esta tecnología tendría que seguir conviviendo con la votación presencial y con la votación por correo postal.

En tercer lugar, la introducción de ese nuevo sistema de votación exigiría un cambio legislativo, pues habría que modificar la LOREG y la normativa de referéndum sobre consultas populares locales, además de la aprobación de normas autonómicas que contemplasen todo el protocolo *blockchain*. Todo ello presupone un amplio acuerdo político y un estudio detallado de las ventajas e inconvenientes, acuerdo y estudio que no existen en la actualidad.

También sería preciso llevar a cabo campañas de difusión del nuevo procedimiento e, incluso, de facilitación tecnológica para que no hubiera algún tipo de exclusión derivada de la falta de conocimiento y/o de confianza. Y es que estas exigencias forman parte, como ya se ha anticipado, de los estándares europeos en la materia: “antes de introducir el voto electrónico, los Estados miembros introducirán los cambios necesarios en la legislación pertinente; la ciudadanía, y en particular los electores, deberá ser informada, con suficiente

antelación al inicio de la votación, en un lenguaje claro y sencillo, sobre: -los pasos que un votante puede tener que dar para participar y votar, -la utilización y el funcionamiento correctos del sistema de voto electrónico, -el calendario de la votación electrónica, incluyendo todas las etapas...”.

En cuarto término, la eventual introducción de la tecnología *blockchain* tendría que hacerse contando, en todo caso, con la necesaria presencia y supervisión de una Administración electoral, algo que está previsto en España tanto en la normativa de participación estatal³¹ como en la autonómica³², y que viene contemplado también en los estándares europeos varias veces mencionados: “la legislación pertinente deberá regular las responsabilidades del funcionamiento de los sistemas de voto electrónico y garantizar que el organismo de gestión electoral tenga el control de los mismos... el organismo de gestión electoral será responsable del proceso de recuento... el organismo electoral competente será responsable del respeto y cumplimiento de todos los requisitos, incluso en el caso de fallos y ataques. El organismo de gestión electoral será responsable de la disponibilidad, fiabilidad, usabilidad y seguridad del sistema de voto electrónico... solo las personas autorizadas por el organismo de gestión electoral tendrán acceso a la infraestructura central, a los servidores y a los datos electorales... antes de que se celebren las elecciones electrónicas, el organismo de gestión electoral se asegurará de que el sistema funciona correctamente... el organismo de gestión electoral deberá manejar todo el material criptográfico de forma segura...”.

En esta línea, y recordando las conceptualizaciones apuntadas por el profesor Díaz González y la bibliografía que él menciona, entendemos que habría que optar por una red de distribución *blockchain* “privada”, que se

31. De acuerdo con el artículo 8 LOREG: “1. La Administración electoral tiene por finalidad garantizar en los términos de la presente Ley la transparencia y objetividad del proceso electoral y del principio de igualdad. 2. Integran la Administración Electoral las Juntas Electorales, Central, Provincial, de Zona y, en su caso, de Comunidad Autónoma, así como las Mesas Electorales. (...)”.

32. Así, por ejemplo, el artículo 14 de la Ley catalana 10/2014, de consultas populares no referendarias y otras formas de participación ciudadana, prevé: “La Comisión de Control es el principal órgano encargado de velar por que las consultas populares no referendarias se ajusten a los principios, reglas y requisitos que establece esta Ley y por que se lleven a cabo con pleno respeto al procedimiento establecido y a las reglas específicas de la convocatoria. (...) 3. La Comisión de Control se compone de siete juristas y politólogos de reconocido prestigio. El Pleno del Parlamento los designa mediante acuerdo adoptado por mayoría de tres quintas partes de los diputados. Estas designaciones deben efectuarse dentro de los tres meses siguientes al inicio de la legislatura. En cualquier caso, la mayoría de miembros de la comisión deben ser juristas”.

caracteriza por la imposición de restricciones tanto al acceso a la información contenida en la cadena de bloques como a la posibilidad de inclusión de nuevas transacciones en la misma. Estas restricciones son coherentes con la propia titularidad del derecho a intervenir en los procesos participativos en el ámbito local que, por muy amplia que sea, no será, en ningún caso, totalmente universal, y estará condicionada por diversos factores como la residencia en el término municipal, la edad, en su caso haber sido elegido para intervenir en el foro o jurado ciudadano...

Y, si eso es así, nos encontramos con que el carácter privado de la red limita la virtualidad de los principios de distribución y descentralización que se atribuyen a la tecnología *blockchain*, toda vez que las redes privadas son administradas por una o varias autoridades centrales, a las que se atribuye con carácter exclusivo la facultad para asegurar que intervienen las personas que tienen derecho a ello.

Partiendo, por tanto, de que debe tratarse de una red privada, debe ser, necesariamente, una red “permisionada”, pues la capacidad para intervenir en el proceso vendrá determinada por las reglas del respectivo proceso participativo (no serán las mismas para unas elecciones locales que para la iniciativa de reforma de una norma municipal o para un jurado ciudadano), y, conforme a dichas reglas, la autoridad central -la Administración electoral competente- estaría obligada a bloquear la entrada a quien no tuviera derecho a ello³³.

Por todo ello, y como recuerda asimismo Díaz González, parece que “las redes *blockchain* de carácter privado presentan un impacto tecnológico limitado, en la medida en que se asimilarían al modelo, ya muy extendido,

33. Lage Serrano (2017: 88-89) se muestra mucho más proclive al carácter público de una red electoral *blockchain*: “El carácter descentralizado de la *blockchain* permite dar respuesta a una de las mayores deficiencias de las plataformas actuales, que al estar basadas en sistemas centralizados y gobernados por una única fuente no garantizan la inalterabilidad de la intención del voto, por lo que cualquier manipulación en la base de datos podría suponer un cambio drástico en los resultados de una votación *online*. En un sistema así es obligado que todas las partes confíen en el administrador central. En cambio, la *blockchain* lo que hace es descentralizar dicha responsabilidad y dispersarla entre todos los nodos participantes, que son los que logran el consenso sobre los datos albergados en la base de datos. A esta gran ventaja hay que sumar otra: la auditabilidad que la *blockchain* ofrece frente a los sistemas tradicionales. Gracias a esta tecnología sería posible incluir nodos públicos, nodos de auditores e incluso nodos de comunicación, que podrían auditar todo el proceso y, si la regulación lo permite, comunicar los resultados del mismo en tiempo real a los interesados —ciudadanos o asociados— sin que ello comprometa la seguridad del sistema. Todo ello, sumado al anonimato que ofrece por diseño, postula a la *blockchain* como la tecnología base de la participación y votación *online* del futuro”; véase también Tapscott y Tapscott (2019: 386-392).

de la intranet”³⁴, con lo que, también en ese aspecto, se podrían formular objeciones a su eventual introducción.

Adicionalmente, Benítez Martínez propone un “modelo tokenizable de la eParticipación”, en el cual, “una vez que el voto esté encriptado, el bloque se agregará a la *blockchain* dentro de la arquitectura BaaS utilizada y, a su vez, el bloque agregado genera el *token* que otorgará al elector una serie de ventajas y/o derechos de uso en la ciudad, ofrecidos por la carta de servicios que la institución local ha desarrollado para este proceso”. Esta propuesta “pretende utilizar estos nuevos *tokens* para premiar la participación y la cogestión de proyectos de valor público...”³⁵.

En nuestra opinión, el ejercicio del derecho de participación en cualquiera de los procesos de ámbito local a los que nos hemos referido es dudosamente compatible con algún tipo de “premio” o “ventaja”. Y, desde luego, nos parece incompatible, si se tratase de procesos electorales o de referéndums, con una configuración constitucionalmente adecuada del derecho fundamental de participación política, que entre el haz de facultades que garantiza está la de “no participar”, con lo que el ejercicio del derecho a través de la no participación no podría implicar desventaja o trato desfavorable alguno en el acceso y disfrute de los servicios públicos.

Por todo lo dicho, y teniendo en cuenta el estado actual de desarrollo de la tecnología *blockchain*, con sus fortalezas y debilidades, la existencia de otros desarrollos tecnológicos alternativos, las exigencias jurídico-democráticas precisas en cualquier proceso participativo, así como la necesidad de seguir manteniendo instrumentos de participación presenciales y a distancia tradicionales y no electrónicos, llegamos a la conclusión de que la opción *blockchain* no es, por el momento, la panacea para los problemas existentes. Más todavía, pensamos que no es la mejor alternativa para el único escenario en el que se nos antoja deseable el desarrollo de mecanismos de participación electrónica –el ejercicio del derecho de voto a distancia–, pues caben otras fórmulas electrónicas ya contrastadas en la práctica, como el sistema de voto aplicado en Estonia, y/o la mejora sustancial del actual sistema de votación por medio del correo postal.

En todo caso, también entendemos que sí cabría continuar desarrollando experiencias vinculadas a la tecnología *blockchain* en el ámbito municipal,

34. También García Mexía (2018: 29).

35. Benítez Martínez (2020: 281-287).

como se está haciendo en la actualidad en diversas entidades locales, pues no en vano ofrecen un ámbito adecuado, por su tamaño y por la proximidad física y administrativa entre instituciones y ciudadanía, para el desenvolvimiento gradual de herramientas que sirvan para mejorar la calidad de la democracia local³⁶.

7. ¿Conclusiones?

Mencionamos al principio de estas páginas que los procesos participativos en las democracias del siglo XXI, en particular en el ámbito local, precisan de reformas institucionales que amplíen las oportunidades de la ciudadanía para influir en las decisiones públicas, estableciendo al efecto pautas de interacción y espacios –“arenas políticas”- de encuentro de la ciudadanía con los poderes públicos que estén basadas en la autonomía, la transparencia y la horizontalidad. A este respecto, las herramientas electrónicas ya se vienen usando para, por citar algunos ejemplos, agilizar el recuento de cualquier proceso electoral o de consulta popular o facilitar la recogida de firmas en una iniciativa ciudadana, pero hasta la fecha en España, a diferencia del conocido y, diríamos, excepcional caso de Estonia, no existe un sustrato suficiente, ni desde el punto de vista tecnológico ni tampoco en los planos jurídico o sociológico, para que estos instrumentos funcionen en nuestra democracia como los “arrecifes de coral” lo hacen en la vida marina.

El propio voto electrónico, y no digamos uno basado en la tecnología *blockchain*, no ha generado de momento expectativas amplias ni parece augurar resultados que sean, en términos participativos, mucho mejores que los mecanismos ahora existentes, a pesar de la manifiesta necesidad de paliar las importantes carencias que presenta hoy el voto por correo postal.

A la mejora de este panorama no contribuye un cierto sesgo elitista asociado al manejo de herramientas cuyo uso no está suficientemente generalizado en el ámbito de la participación política ni, quizá, lo necesario en otros espacios, con lo que la pretensión de sustituir los vigentes mecanismos basados en la presencialidad por otros de índole exclusivamente electrónica no parece que fuese a contar con el respaldo político y social necesario para alcanzar la imprescindible legitimidad, y, como ya se ha dicho, se corre el riesgo, no trivial

36. Véase Arteaga Moralejo (2018); con carácter más general, VV. AA. (2020).

ni infundado, de que procesos dirigidos a aumentar los sentimientos de eficacia política (“podemos tener voz”) acaben generando el efecto contrario (frustración de expectativas y sentimientos de ineficacia política externa), reduciendo el número de voces que acceden a las redes políticas o ubicándolas en posiciones marginales.

En esta línea, y aunque la tecnología *blockchain* se ha venido relacionando con la institucionalización de prácticas de transparencia y la reducción del ejercicio del poder discrecional por parte de las autoridades, aumentando la capacidad de influencia de quienes carecen de poder, nos parece que en los procesos participativos, al menos con el diseño normativo actual, es imprescindible seguir contando con la presencia de autoridades -Administración electoral- e instituciones públicas, lo que rebaja las expectativas que puede ofrecer alternativamente aquella tecnología.

No obstante, y como se ha dicho un poco más arriba, parece oportuno continuar desarrollando experiencias vinculadas a la tecnología *blockchain* en el ámbito municipal, pues ofrecen un ámbito adecuado, por su tamaño y por la proximidad física y administrativa entre instituciones y ciudadanía, para el desenvolvimiento gradual de herramientas que sirvan para mejorar la calidad de la democracia local.

8. Bibliografía

- Arteaga Moralejo, J. (2018). *Blockchain* en procesos de participación ciudadana: Innovando desde la práctica en el Ayuntamiento de Alcobendas. En C. Güemes, J. Resina y C. Cruz (eds.). *Participación ciudadana: Experiencias inspiradoras en España* (pp. 147-158). Madrid: CEPC.
- Barrat i Esteve, J. y Fernández Riveira, R. M.^a (coords.). (2011). *Derecho de sufragio y participación ciudadana a través de las nuevas tecnologías*. Cizur Menor: Civitas.
- Benítez Martínez, F. L. (2020). *Un modelo de gobernabilidad para procesos de eDemocracia basados en una red neuronal de blockchain* [tesis doctoral]. Universidad de Granada.
- Cabannes, Y. (2004). *¿Qué es y cómo se hace el Presupuesto Participativo? 72 respuestas a Preguntas Frecuentes sobre Presupuestos Participativos Municipales*. Quito: UN-Hábitat. Disponible en: http://www.socioeco.org/bdf_fiche-outil-54_es.html
- Cabannes, Y. y Lipietz, B. (2015). *The Democratic Contribution of Participatory Budgeting. Working Paper Series 2015*, 15-16. Londres: London School of Economics.

- Castellanos Claramunt, J. (2020). *Participación ciudadana y buen gobierno democrático. Posibilidades y límites en la era digital*. Madrid: Marcial Pons.
- Cebrián Zazurca, E. (2012). *Deliberación en internet: una propuesta de modelo de participación política*. Zaragoza: Fundación Manuel Giménez Abad.
- Cotino Hueso, L. (coord.). (2006). *Libertades, democracia y gobierno electrónico*. Granada: Comares.
- Expósito Gómez, E. (2019). La paulatina reforma del marco legal sobre consultas populares locales: ¿un mismo plato con distintos aliños? En C. Garrido López y E. Sáenz Royo (coords.). *Referéndums y consultas populares en el Estado autonómico* (pp. 151-183). Madrid: Marcial Pons.
- Font, J. (coord.). (2001). *Ciudadanos y decisiones públicas*. Barcelona: Ariel.
- Font, J. y Blanco, I. (2006). *Polis, la ciudad participativa: participar en los municipios: ¿quién?, ¿cómo? y ¿por qué?: experiencias de participación ciudadana*. Barcelona: Diputació de Barcelona/Xarxa de Municipis.
- García Mahamut, R. (2012). La reforma electoral (LO 2/2011) y el voto de los españoles en el exterior (CERA). La ineffectividad del derecho de sufragio de los españoles en el exterior. Una necesaria revisión. *Teoría y Realidad Constitucional*, 30, 259-289.
- García Mexía, P. (2018). Introducción general. En P. García Mexía (dir.). *Criptoderecho. La regulación de Blockchain* (pp. 23-35). Las Rozas: Wolters Kluwer.
- García-Espín, P. y Jiménez, M. (2017). Los procesos participativos como potenciadores de la democracia. Explorando los efectos, mecanismos y evidencias en la sociedad civil. *Revista de Estudios Políticos*, 177, 113-146.
- Gómez del Peso, J. L. (2014). *Los presupuestos participativos: dimensiones analíticas y líneas de debate en la experiencia española* [tesis doctoral]. Universidad Carlos III de Madrid.
- González de la Garza, L. M. (2008). *Voto electrónico por Internet. Constitución y riesgos para la democracia*. Madrid: Edisofer.
- González-Meneses, M. (2017). *Entender Blockchain. Una Introducción a la tecnología de registro distribuido*. Cizur Menor: Aranzadi.
- Guglielmi, G. J. e Ihl, O. (dirs.). (2017). *El voto electrónico*. Madrid: Centro de Estudios Políticos y Constitucionales.

- Ibáñez Macías, A. (2005). *El referéndum local en España: régimen jurídico*. Cádiz: Servicio de Publicaciones de la Universidad de Cádiz.
- (2013). Los referendos regional y local en el Estado Autonómico. Sus bases y límites constitucionales. *Revista Vasca de Administración Pública*, 97, 97-138.
- Jefferson, D., Rubin, A. D., Simons, B. y Wagner, D. (2004). *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*. Disponible en: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.366.9223&rep=rep1&type=pdf>
- Kelsen, H. (2006). *De la esencia y valor de la democracia*. Oviedo: KRK.
- Lage Serrano, Ó. (2017). Participación ciudadana y voto electrónico. En A. Preukschat (coord.). *Blockchain: La revolución industrial de internet* (pp. 87-89). Disponible en: https://www.academia.edu/36701339/Blockchain_La_revoluci%C3%B3n_industrial_de_internet_Alexander_Preukschat
- Magnuson, M. (2020). *Blockchain Democracy. Technology, Law and the Rule of the Crowd*. Cambridge: Cambridge University Press.
- Martínez-Alonso Camps, J. L. (2011). Las consultas populares municipales: consideraciones sobre el marco normativo y su identificación como referéndum. *Anuario del Gobierno Local 2010*, 447-486.
- Mateos Crespo, J. L. (2019). La implantación del voto rogado en España: el perjudicial límite a la participación electoral de los españoles residentes en el extranjero a punto de enmendarse. *Teoría y Realidad Constitucional*, 441-470.
- Nurse, J. R. C. et al. (2016). An Independent Assessment of the Procedural Components of the Estonian Internet Voting System. *Cyber Studies Programme, Working Paper Series* – No. 6. Oxford.
- Presno Linera, M. Á. (2016). Premisas para la introducción del voto electrónico en la legislación electoral española. *Revista de Estudios Políticos*, 173, 277-304.
- (2020). Sobre la posible introducción del voto electrónico en la legislación electoral española. En L. A. Fernández Villazón (coord.). *Derecho y nuevas tecnologías* (pp. 641-660). Oviedo: Thomson Reuters/Universidad de Oviedo.
 - (pendiente de publicación). *Procedimiento (o procedimientos) de voto (identificación, emisión y escrutinio) en el sistema CERA. Propuestas y posibilidades*.
- Presno Linera, M. Á. y García Majado, P. (2019). Una democracia local para el siglo XXI. En M.^a C. Campos Acuña et al. (dirs.). *III Informe Red Localis: Retos de las entidades*

- locales ante la transformación digital de la gestión pública* (pp. 267-283). Madrid: Wolters Kluwer.
- Ramírez Nárdiz, A. (2010). *Democracia participativa. La democracia participativa como profundización de la democracia*. Valencia: Tirant lo Blanch.
- Rosanvallon, P. (2006). *La contra-démocratie. La politique à l'âge de la défiance*. París: Éditions du Seuil.
- Rubio Núñez, R. (2018). *Blockchain: Gobierno y Democracia*. En P. García Mexía (dir.). *Criptoderecho. La regulación de Blockchain* (pp. 217-249). Madrid: Wolters Kluwer.
- Ruiz Magaña, I. (2020). Consultas populares y entidades locales: a propósito de la Ley 7/2017, de 27 de diciembre, de Participación Ciudadana de Andalucía. *Revista de Estudios de la Administración Local y Autonómica*, 13, 47-74.
- Tapscott, D. y Tapscott, A. (2019). *La revolución blockchain. Descubre cómo esta nueva tecnología transformará la economía global*. Barcelona: Deusto.
- Tur Ausina, R. y Sanjuán Andrés, F. J. (2018). Las consultas populares municipales. Instrumentos de la autonomía local para la mejora de la calidad democrática. *Cuadernos Manuel Giménez Abad*, 15, 169-187.
- VV. AA. (2020). *Gobernanza participativa local. Construyendo un nuevo marco de relación con la ciudadanía*. Madrid: FEMP. Disponible en: <http://femp.femp.es/files/3580-1936-fichero/GOBERNANZA%20PARTICIPATIVA%20LOCAL.pdf>

Subvenciones locales, *blockchain* y actuación administrativa automatizada

Antonio Bueno Armijo

Profesor titular de Derecho Administrativo.

Universidad de Córdoba¹

SUMARIO. 1. Conclusión: la escasa utilidad de la tecnología *blockchain* para la actividad administrativa subvencional, y la necesidad, a pesar de todo, de ocuparse de ella. 1.1. Un *hype* global con limitados efectos administrativos. 1.2. Una nueva materia necesitada de análisis jurídico-administrativo. 1.3. El singular atractivo de la actividad subvencional para el estudio de la tecnología *blockchain* aplicada a la Administración pública. **2. Las revolucionarias ventajas del uso de la tecnología *blockchain* en las relaciones entre privados y su limitado valor añadido para las administraciones públicas.** 2.1. La generación de confianza entre amplios grupos de personas sin necesidad de intermediarios. 2.2. La irrelevancia del poder desintermediador de *blockchain* para la actividad administrativa: la Administración no desaparecerá. 2.3. Una posible ventaja del uso de *blockchain* en la Administración: la inmutabilidad de los documentos. 2.3.1. La tecnología *blockchain* como herramienta de lucha contra la corrupción. 2.3.2. La dificultad de desplegar redes de *blockchain* útiles en los procedimientos de concesión de subvenciones. **3. El uso de *blockchain* como base para el desarrollo de otras tecnologías en la administración digital: *smart contracts* y actividad administrativa automatizada.** 3.1. Los *smart contracts* basados en *blockchain* como forma de automatizar la actuación administrativa. 3.2. La actividad administrativa

1. Grupo de investigación de la Junta de Andalucía SEJ-196. Proyecto PGC2018-093760 (MCIU/FEDER, UE).

automatizada más allá del uso de *smart contracts*. **4. Las posibilidades del uso de *blockchain* y de automatización de la actividad administrativa en la gestión de subvenciones.** 4.1. Requisitos para la incorporación de actividades administrativas automatizadas a la tramitación de subvenciones. 4.2. Actividades materiales automatizadas en materia de subvenciones. 4.3. Fase de iniciación del procedimiento de concesión de subvenciones. 4.3.1. La convocatoria del procedimiento de concesión de subvenciones. 4.3.2. Presentación de solicitudes y acreditación de requisitos. En especial, el uso de herramientas de *Self-Sovereign Identity* basadas en *blockchain*. 4.4. Fases de instrucción y resolución del procedimiento de concesión de subvenciones. 4.4.1. La concesión directa de subvenciones. Remisión. 4.4.2. La concesión de subvenciones mediante concurrencia competitiva. 4.5. El control administrativo y financiero de subvenciones. 4.6. La iniciación del procedimiento de reintegro de subvenciones y del procedimiento administrativo sancionador. **5. Bibliografía.**

1. Conclusión: la escasa utilidad de la tecnología *blockchain* para la actividad administrativa subvencional, y la necesidad, a pesar de todo, de ocuparse de ella

La conclusión de este trabajo es que la tecnología de cadena de bloques o *blockchain*, en el momento actual y por sí sola, resulta de escasa utilidad para la actividad subvencional de las administraciones públicas. Puede resultar extraño que este trabajo comience con una conclusión, en lugar de terminar con ella, pero este hecho obedece a una estricta coherencia: con la aplicación de la tecnología *blockchain* al ámbito de actuación de las administraciones públicas parece haberse empezado por el final, en lugar de por el principio; y lo mismo hace este trabajo.

1.1. Un *hype* global con limitados efectos administrativos

Se ha desatado una pasión por la tecnología *blockchain* que va bastante más allá de la exageración². Pero lo cierto es que, en el ámbito de la Administración pública y del Derecho Administrativo, la tecnología *blockchain* solo es

2. Como recoge Gallone (2019: 190), algunos autores han definido esta tecnología nada menos que como “el protocolo de Dios” (Casey y Vigna, 2018a), mientras que otros, más modestamente, solo consideran que estamos ante una revolución comparable o incluso superior a la que supuso la aparición de internet (Tapscott y Tapscott, 2016) o, simplemente, ante una innovación fundamental en el progreso de la humanidad, comparable a la *Magna Charta* o al descubrimiento de la piedra Rosetta (Swan, 2015).

actualmente una solución en busca de problemas; cuando no algo peor³. De hecho, si resulta discutible que la tecnología *blockchain* sea siempre y necesariamente útil en las relaciones privadas, aún más dudoso es que lo sea en el ámbito de la Administración pública⁴. En particular, y por cuanto afecta a la actividad administrativa subvencional, cabe adelantar que el problema que viene a resolver la tecnología *blockchain* (la necesidad de ofrecer seguridad, sin acudir a un intermediario, en los intercambios entre sujetos privados e iguales que desconfían entre sí) no existe como tal.

Este apasionamiento por una nueva tecnología no constituye, sin embargo, una situación absolutamente inédita. El lógico entusiasmo por las inmensas posibilidades de desarrollo que ofrece la digitalización de la Administración ya ha podido llevar, en sus distintas oleadas, a la falsa creencia de que nos encontramos ante una revolución que cambiará radicalmente a la Administración y al Derecho Administrativo, o de que la Administración electrónica es una Administración distinta; cuando no lo es⁵. En el mejor de los casos, será una Administración más eficaz en la satisfacción de los intereses generales, y más eficiente en el uso de medios públicos, pero seguirá siendo la misma Administración: una organización de medios materiales y humanos orientada al único fin de servir con objetividad los intereses generales (artículo 103.1 CE).

3. Cuesta trabajo expresarlo en términos más gráficos que los de Quintana Cortés (2020: 164): “tenemos ante nosotros una potente solución tecnológica y estamos ávidos de encontrar problemas a los que la misma pueda aplicarse [en el ámbito de la Administración pública]”. Por eso, con sabia cautela, este y algunos otros autores han advertido de que el ciego deseo de encontrar a toda costa aplicaciones de la tecnología *blockchain* en la actuación administrativa podría obedecer a una más de las modas que periódicamente sacuden al mundo tecnológico o digital o a un *hype* resultado de inteligentes campañas de *marketing* (Quintana Cortés, 2020: 153, remitiéndose, a su vez, a García Melián, 2019: 6). Ciertamente, no son pocos ya los giros copernicanos basados en nuevas tecnologías que se nos han anunciado en los últimos años (v. gr., realidad virtual, realidad aumentada, impresoras en 3D o, más recientemente, el metaverso), sin que, al menos hasta ahora, se hayan materializado esos revolucionarios cambios vinculadas a estas tecnologías.

4. Se han lanzado advertencias similares en las relaciones privadas y, particularmente, en el ámbito empresarial: “*blockchain technology is not the solution to every problem. Entrepreneurs should not assume that using blockchain automatically makes an application more secure or cheaper, or that it automatically equates to data protection or privacy*” (EU Blockchain Observatory and Forum, 2018: 29). De hecho, existen desde hace algunos años interesantes estudios advirtiendo de usos ineficientes e innecesarios de redes de *blockchain*, y ofreciendo metodologías estructuradas que ayudan a las organizaciones a decidir cuál es la solución tecnológica más adecuada a sus necesidades concretas, como en el ejemplar trabajo de Wüst y Gervais (2018).

5. Véanse Tarrés Vives (2012: 448) y Martín Delgado (2009a: 355 y 358-366), quien deduce de ello y explica con especial acierto que la actuación administrativa automatizada, de la que nos ocuparemos más adelante, no altera la teoría del órgano ni el concepto actualmente predominante de acto administrativo, frente a lo que había sido sugerido por otros autores.

Por ello, debe recelarse del empeño en aplicar a toda costa nuevas tecnologías al ámbito de la Administración pública cuando con ello se confunden medios y fines: el uso de nuevas tecnologías por parte de la Administración no es un fin en sí mismo, sino un medio para mejorar la eficacia y la eficiencia de su actividad y de sus relaciones con los ciudadanos, con miras a la satisfacción del interés general⁶. La implantación de nuevas tecnologías en la actuación administrativa, por impresionantes que sean, como ciertamente es el caso de la tecnología *blockchain*, debe desconfiar de modas o tendencias promovidas por grandes empresas tecnológicas, y basarse en un análisis sosegado de las ventajas y los inconvenientes que puede acarrear⁷.

1.2. Una nueva materia necesitada de análisis jurídico-administrativo

En cualquier caso, el sano escepticismo y la razonable cautela no deben ir más lejos de lo ya expresado. Las dudas sobre el carácter revolucionario y casi mesiánico de la tecnología *blockchain* aplicada a la Administración pública no justifican que sea ignorada. Antes al contrario.

Estas dudas obligan, en primer lugar, a un análisis de esta actividad cuando es desarrollada por sujetos privados, en la medida en que podría generar situaciones de desequilibrio entre las partes o provocar daños o perjuicios en sujetos desprotegidos, lo que exigiría la intervención de los poderes públicos (por ejemplo, en relación con la gestión automatizada de datos personales). Es decir, deben ser objeto de atención para el caso en que fuera necesario proceder a su regulación⁸. Piénsese a este respecto, por cuanto afecta al ámbito que nos ocupa, en la posibilidad de que entidades puramente privadas (la Fundación Santander, por emplear un ejemplo real) decidan utilizar redes de *blockchain* para conceder a estudiantes universitarios las ayudas que actualmente otorgan a través de las Universidades; o que elaboren perfiles a partir de un tratamiento automatizado de sus datos personales; o que empleen algoritmos para la selección de sus beneficiarios⁹.

6. Extensamente sobre ello, Martín Delgado (2009b: 359).

7. En este mismo sentido, en relación con la implantación de robots software y la automatización de la actividad administrativa, Cerrillo i Martínez (2021: 303-304).

8. Es lo que Gallone (2019: 196) llama “ordenación en materia de *blockchain*” (*blockchain governance*) por oposición a la “ordenación mediante el uso de *blockchain*” (*governance by blockchain*), de la que, propiamente, nos ocuparemos en este trabajo.

9. El uso de algoritmos en las relaciones entre privados y los problemas que ello puede conllevar, por ejemplo, en materia de discriminación, han sido ya expresamente objeto de atención en el ámbito laboral. Véase, sobre el particular, Sáez Lara (2020a, 2020b).

En segundo lugar, estas mismas dudas exigen un análisis cuidadoso de cuáles son las ventajas reales que ofrece esta tecnología y de si tales ventajas podrían darse también en el ámbito de la Administración pública. Ese es el objeto del presente trabajo, en el que se analizará, en particular, la posible aplicación de la tecnología *blockchain* a la actividad subvencional. Nuestra conclusión, ya adelantada, es que esta tecnología no parece ofrecer grandes ventajas a los modelos actualmente existentes. Al menos no con carácter específico¹⁰. No obstante, en la medida en que pueda ayudar a la automatización de la actividad administrativa, la tecnología *blockchain* sí podría resultar de utilidad.

Finalmente, la aplicación de la tecnología *blockchain* a la actividad administrativa subvencional no puede analizarse aisladamente, como un fenómeno singular al margen del resto de desarrollos digitales en los que se encuentra inmersa la Administración pública. En efecto, la tecnología de cadena de bloques es solo uno más de los espectaculares avances que se están produciendo en la sociedad digital, ayudando no solo a su consolidación, sino a su propia construcción. En consecuencia, todo análisis de esta tecnología estará incompleto si no se pone en relación con las demás tecnologías (internet, *smart contracts*, actuaciones administrativas automatizadas, inteligencia artificial o, más ampliamente, uso de algoritmos, etc.). Ello obliga a que la perspectiva más adecuada para el análisis de estos fenómenos sea la que se centra en la idea de ecosistema digital, entendido como el conjunto de tecnologías de la información que se encuentran conectadas entre sí y que evolucionan conjuntamente. Es desde esta idea de ecosistema digital desde la que el presente trabajo abordará el posible impacto de la tecnología *blockchain* en la actividad subvencional, poniéndolo en relación con el uso actual y las posibilidades de desarrollo de otras tecnologías digitales.

1.3. El singular atractivo de la actividad subvencional para el estudio de la tecnología *blockchain* aplicada a la Administración pública

Cabe hacer un último apunte sobre el interés de nuestro objeto de estudio: el hecho de que el presente trabajo se circunscriba a la actividad subvencional no es un dato anecdótico o irrelevante. Al contrario, ofrece la posibilidad de estudiar el uso de tecnologías potencialmente peligrosas por parte de la Administración en un sector más bien inocuo o seguro. En efecto, muchos

10. Como habrá ocasión de exponer, el uso más prometedor de la tecnología *blockchain* en el ámbito de la actividad subvencional se produciría mediante la identidad autogestionada (*SSI* o *Self-Sovereign Identity*, por sus siglas en inglés). Sin embargo, este tipo de herramienta no constituiría, ni remotamente, algo limitado a (o propio de) la actividad subvencional.

de los riesgos detectados y de las cautelas expresadas en relación con el uso de nuevas tecnologías digitales se orientan a evitar que, con su actuación, la Administración pueda adoptar decisiones desfavorables o desarrollar actuaciones vulneradoras de derechos de los ciudadanos.

Sin embargo, la situación se plantea en términos muy distintos cuando la actividad desarrollada por la Administración se traduce en actuaciones favorables para los ciudadanos. Así puede ocurrir, paradigmáticamente, en el ámbito de la actividad administrativa de fomento y, específicamente, en relación con las subvenciones¹¹. En estos casos se produce una relajación del principio de legalidad y de otros límites u obligaciones impuestos a la Administración, por ejemplo, en materia de motivación¹².

De alguna forma, la Administración gozaría de menos constricciones en este ámbito para hacer uso de las nuevas tecnologías, al poder experimentar con ellas y comprobar su alcance y efectos sin grandes riesgos para los derechos de los ciudadanos. Dicho en otros términos, podríamos hallarnos ante uno de los *sandboxes* o espacios de pruebas seguros reclamados por la doctrina, en los que resulta posible probar nuevas técnicas y regulaciones sin incurrir en riesgos excesivos¹³.

11. Estas afirmaciones, naturalmente, deben tomarse con las debidas cautelas. Es cierto que, en rigor, la actividad administrativa de fomento siempre tiene un contenido favorable para su destinatario. No obstante, como he tenido ocasión de explicar y como ha reconocido la jurisprudencia, ello no obsta a que también puedan desprenderse efectos desfavorables para otros sujetos (Bueno Armijo, 2011: 45). La consecuencia es que la relajación del principio de legalidad, por ejemplo, no puede ser total y que, en todo caso, debe asegurarse el respeto a ciertas garantías mínimas para los derechos subjetivos e intereses legítimos de los ciudadanos. Por ilustrarlo con un ejemplo: el simple establecimiento de un programa de prestaciones sociales sin incidencia en el mercado (ni, por tanto, en la competencia) tendrá casi necesariamente carácter favorable; no obstante, la resolución por la que se conceden estas prestaciones a algunos solicitantes y no a otros, tras tramitar el oportuno procedimiento de concurrencia competitiva, tendrá carácter favorable para los primeros, pero desfavorable para los últimos.

12. La relajación del principio de legalidad permite que en el ámbito de la actividad administrativa de fomento se produzcan con especial facilidad fenómenos de autoatribución de potestades administrativas mediante la adopción de simples normas reglamentarias y sin necesidad de acudir a normas con rango de ley (Bueno Armijo, 2019: 95). Esto explica, precisamente, la posibilidad de establecer subvenciones mediante simples normas reglamentarias, lo que resulta especialmente importante en el ámbito local (*cf.*: artículo 17.2 LGS). Respecto a la obligación de motivar, *cf.*: artículo 39.1.a) LPAC, *a contrario*, lo que puede tener una especial relevancia en relación con las dificultades para ofrecer explicaciones comprensibles de la actuación administrativa en casos de uso de aplicaciones capaces de implementar algoritmos de aprendizaje profundo (*deep learning*), lo que conduce al problema de las “cajas negras” (*black boxes*), al que nos referiremos más adelante.

13. En relación con los *regulatory sandboxes*, o “entornos supervisados para aplicar experimentalmente la regulación (...) donde se pueda experimentar a pequeña escala y de manera empírica nuevos instrumentos de regulación”, véase Cerrillo i Martínez (2019: 12).

Esta perspectiva de actuaciones administrativas favorables (o, en el peor de los casos, inocuas) permitiría igualmente levantar otras cautelas, como la necesidad de establecer una “reserva de humanidad” en el ejercicio de potestades discrecionales por parte de sistemas de actuación administrativa automatizada, planteada ya por algún autor¹⁴, o revisar algunos de los límites en materia de datos personales a la creación de perfiles y la adopción de decisiones automatizadas que produzcan efecto jurídicos en los interesados o les afecten significativamente de modo similar (artículo 22 RGPD)¹⁵. Es más, al tratarse de un ámbito en el que difícilmente se producirán daños a los interesados, precisamente por el carácter favorable de las actuaciones administrativas, perderían importancia las dudas actualmente existentes sobre el alcance de la responsabilidad patrimonial de la Administración por el uso de algoritmos¹⁶.

Esta situación de cierta (y siempre limitada) “despreocupación” es, de hecho, la que se ha producido en la práctica en la actividad administrativa de la Seguridad Social respecto a la concesión de prestaciones. En 2009 se reguló la tramitación electrónica de procedimientos en materia de protección por desempleo y, desde entonces, se venían desarrollando con cierta tranquilidad otras actuaciones administrativas automatizadas¹⁷. Estas actuaciones administrativas automatizadas se fueron extendiendo a otras prestaciones sin concitar una gran preocupación en la doctrina. Solo recientemente, con la previsión de que esta automatización pueda extenderse al ámbito de las decisiones recaudatorias y sancionadoras, se ha considerado que la inteligencia artificial muestra “su cara menos amable”, y han comenzado a expresarse cautelas y a exigirse garantías¹⁸.

Sobre el sentido de la aplicación del principio de legalidad a la administración electrónica, Martínez Gutiérrez (2009: 254-256).

14. Sin perjuicio de su análisis posterior, cabe adelantar que Ponce Solé (2019: 33) plantea la necesidad de esta reserva como “el ejercicio humano de empatía en la diligente ponderación de hechos, derechos e intereses en que consiste la buena administración de potestades discrecionales”.

15. Aunque la idea también será objeto de desarrollo posterior, debemos dejar ya indicada la advertencia de que la prohibición de incorporar al tratamiento automatizado datos de categorías especiales (artículo 22.4 RGPD) podría ir directamente en contra del interés de grupos sociales desfavorecidos, para los que se podrían diseñar sistemas de ayudas específicos. Ello justificaría una interpretación tan amplia como fuera posible de las excepciones previstas en el artículo 9.2 RGPD y, muy especialmente, de la contemplada en la letra h).

16. Véanse, entre otros, Cerrillo i Martínez (2019: 28), Asís Roig (2018: 52), Marongiu (2018: 407-411) y Valero Torrijos (2019: 92-93).

17. Disposición adicional 46.^a introducida en el TRLGSS entonces vigente a través del Real Decreto-ley 10/2009, de 13 de agosto, por el que se regula el programa temporal de protección por desempleo e inserción.

18. Goerlich Peset (2021: 31), en relación con las modificaciones introducidas por el Real Decreto-ley 2/2021, de 26 de enero, de refuerzo y consolidación de medidas sociales

2. Las revolucionarias ventajas del uso de la tecnología *blockchain* en las relaciones entre privados y su limitado valor añadido para las administraciones públicas

¿Para qué sirve *blockchain*? ¿Cuál es su valor añadido? O, dicho de otra forma, ¿por qué una organización invertiría sus recursos económicos y humanos en implantar la tecnología *blockchain* como parte de sus actuaciones? Estas cuestiones ya han sido objeto de un detenido estudio en otros trabajos incluidos en el presente volumen, por lo que no procede ahora detenerse nuevamente en ellas. Resulta preciso, sin embargo, recordar cuáles son las principales características, los requisitos de funcionamiento y las ventajas aportadas por esta tecnología, a fin de analizar de qué modo y con qué resultados puede resultar aplicable a la actividad subvencional.

2.1. La generación de confianza entre amplios grupos de personas sin necesidad de intermediarios

En esencia, *blockchain* es una cuestión de seguridad y confianza¹⁹. En concreto, la tecnología *blockchain* representa una forma de ofrecer seguridad y confianza en las relaciones de intercambio entre sujetos que no confían entre sí, sin tener que acudir a un tercero (un banco, un fedatario público, una Administración, etc.) que actúe como intermediario en el que todas las partes confíen. Ello es posible gracias a la utilización de la tecnología de registro distribuido (*distributed ledger technology*). En concreto, la tecnología *blockchain* ofrece información sobre la inmutabilidad de los documentos (electrónicos) incorporados a su red, así como sobre los cambios que se producen en ellos, garantizando, de esta forma, que la integridad de los datos contenidos en esos documentos (electrónicos) sea absolutamente fiable. No garantiza que los datos incorporados al documento (electrónico) sean ciertos. Lo que garantiza es que esos datos (y no otros) se incorporaron al documento, y que no se han cambiado desde que se incorporaron.

La peculiaridad de esta tecnología radica en que descansa en la cooperación de todos los que estén interesados en conocer y generar esos

en defensa del empleo, en el artículo 130 (“Tramitación electrónica de procedimientos en materia de Seguridad Social”) TRLGSS. Asimismo, Izquierdo Carrasco (2022).

19. No por casualidad, el número dedicado en mayo de 2018 a *blockchain* por la *MIT Technology Review* llevaba como subtítulo, precisamente, “The future of trust?”. Se trata de un elemento en el que todos los autores coinciden. A mero título de ejemplo, véanse Wanden-Berghe y Fernández Daza (2020: 134), o Merchán Murillo (2019: 5), quien habla gráficamente de “máquina para generar confianza”.

datos, sin intermediarios, en pie de igualdad y sin necesidad de una autoridad central. Cada uno de ellos, llamados participantes en la red o nodos, conserva los registros de todas las transacciones (cambios reflejados en los documentos), lo que permite hablar, justamente, de registro distribuido. Estos registros, por tanto, no se encuentran físicamente en un único servidor, sino en los ordenadores que conforman la red, todos ellos sincronizados con la misma información. Se derivaría de esta situación, como valor de seguridad añadido, que resulte mucho más difícil la pérdida de los datos como consecuencia de un accidente o un ataque, puesto que, aunque el accidente o el ataque pudieran comprometer los datos contenidos en un nodo de la red, la misma información se conservaría en todos los demás. Sin embargo, esta ventaja añadida, como se verá, está lejos de resultar tan fácil de alcanzar.

Asimismo, tampoco es posible proceder a la modificación de los datos contenidos en el registro si dicha modificación no es coherente con la información almacenada en la mayoría de los nodos. Ello también debería aumentar la fiabilidad de la red. Pero esta característica (sin perjuicio de sus distintas variaciones, según nos encontremos ante redes públicas, privadas o permissionadas) puede constituir un arma de doble filo, como señalaremos también más adelante al analizar su aplicación a la actividad subvencional de la Administración.

De acuerdo con lo anterior, el uso de la tecnología *blockchain* será útil cuando concurren varias circunstancias: la existencia de una pluralidad de sujetos que interactúen entre ellos; la necesidad de compartir una base de datos común, en la que se recoja información relevante para todos los sujetos y para sus interacciones; y la desconfianza entre todos los sujetos, de modo que ninguno de ellos pueda ser depositario de la confianza de los demás ni, por lo tanto, de la custodia de la base de datos común.

Como es obvio, el dato verdaderamente relevante no es la existencia de un mecanismo que ofrezca seguridad y confianza en el tráfico comercial. Esto ya existía, de muy distintas maneras, desde hace siglos, y bajo formas adaptadas al entorno digital en tiempos más recientes²⁰. El nuevo elemento que lo cambia todo es la desintermediación. Es decir, que la seguridad y la confianza en el tráfico comercial ya no necesitan de un tercero que actúe como intermediario y como garante. La tecnología ha sido capaz de desarrollar un mecanismo que,

20. *Cfr.*, en este sentido, los objetivos del Reglamento (UE) n.º 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, así como Alamillo Domingo (2019a).

cuando se reúnen ciertas condiciones, permite suprimir a esos terceros sin mermas de la seguridad y la confianza de los participantes en el sistema.

La tecnología *blockchain* no está exenta de problemas²¹, pero se entiende sin grandes esfuerzos el entusiasmo y el interés que ha despertado tanto en grandes empresas como en Gobiernos nacionales y, por supuesto, en el ámbito de la Unión Europea, dado el impacto profundo que esta tecnología tendrá en el mercado interior. La aparición de internet permitió que desaparecieran un extraordinario número de intermediarios (¿quién acude hoy día a una agencia de viajes para comprar un billete de tren?), y la tecnología *blockchain* permitirá la desaparición de un número aún mayor de ellos. Sin embargo, del mismo modo que la desintermediación operada por internet, aun siendo revolucionaria para la transformación de la economía en todo el mundo, no tuvo gran impacto en la Administración pública (porque las relaciones ya eran directas), tampoco la desintermediación que propone *blockchain* es previsible que le afecte en demasía²².

2.2. La irrelevancia del poder desintermediador de *blockchain* para la actividad administrativa: la Administración no desaparecerá

Desde postulados libertarios un poco sobreexcitados se ha dado la bienvenida a la tecnología *blockchain* como la solución final para acabar con la existencia del Estado (al fin y al cabo -se dice-, otro gran intermediador). Y, ciertamente, el primer gran éxito (en realidad, único, por el momento) de la

21. Como bien resume Tejedor Bielsa (2020: 120-121), “se basa en la duplicación ineficiente de procesos, no optimiza el consumo energético como consecuencia de la descentralización, depende de la disponibilidad de la red, puede prestarse a concentración o corrupción en la minería (...) y puede suscitar riesgos sobre protección de datos de carácter personal”. De todos estos aspectos problemáticos, el que más atención parece haber suscitado es el de su alta ineficiencia energética. En efecto, el consumo de energía en una red en continuo crecimiento y en la que la validación se consigue mediante el consenso de sus nodos es, necesariamente, cada vez mayor, lo que convierte el consumo energético en un importante problema. *Cfr.* Alonso Suárez (2018: 483) y Merchán Murillo (2019: 7).

22. Ni remotamente se pretende sugerir que internet no haya implicado cambios para la Administración pública, pero lo cierto es que la gran transformación de la Administración no se debe al uso de internet como mecanismo de desintermediación, sino a su digitalización, es decir, al abandono del soporte físico en papel, “que emplea constructos sociales como la firma, el documento soporte, la carpeta, la entrega postal, el tablón de anuncios y otros muchos, para sustentar las diferentes actividades a realizar, construyendo garantías apropiadas al funcionamiento y partiendo de las restricciones propias de dicha tecnología” (Alamillo, 2020: 226). Todo ello, sin perjuicio de que esa digitalización ha venido propiciada en muy buena medida por la existencia de internet y la normalización de las conexiones mediante redes de telecomunicaciones.

tecnología *blockchain* se ha producido sobre un elemento que afecta tanto al sector público como al sector privado: la moneda. Bitc on, *ethereum* y el resto de criptodivisas han hecho innecesaria la existencia tanto de las entidades financieras privadas como de los bancos centrales p blicos en cuanto que autoridades centrales emisoras de moneda.

Desde esta perspectiva, la tecnolog a *blockchain* permitir a sustituir a la Administraci n en algunas de las funciones que hasta ahora ven a ejerciendo en relaci n con la fe p blica o, m s en general, con la existencia de registros p blicos. De este modo, se dice que la tecnolog a *blockchain* podr a sustituir al Registro de la Propiedad, al Registro Civil o a los registros de v hculos²³: si un comprador quisiera tener la seguridad de que el vendedor de una finca es su verdadero propietario, ya no necesitar a la intermediaci n del Registro, sino que dicha confirmaci n podr a facilit rsela una red de *blockchain*. Estos registros p blicos devendr an redundantes y, por tanto, innecesarios.

Pero tales proclamas libertarias son, cuando menos, una notable exageraci n. Por un lado, porque los encargados de estos registros p blicos no tienen como  nica funci n la fe p blica, sino otras muchas entre las que destaca, especialmente, la de control de legalidad de los actos que se pretenden inscribir en ellos²⁴. Por otro lado, porque *blockchain* es, fundamentalmente, una tecnolog a que permite eliminar todos aquellos mecanismos utilizados hasta ahora como intermediarios entre operadores para garantizar la realidad y veracidad de sus intercambios. Esta tecnolog a est  pensada para sistemas en los que existen interacciones (transacciones) directamente entre una pluralidad de sujetos privados. Sin embargo, el  mbito propio de la actividad administrativa no es el de la mediaci n entre sujetos que quieren interaccionar entre s , satisfaciendo sus intereses privados. El  mbito propio de la actividad administrativa es el de la satisfacci n del inter s general, a cuyos efectos la Administraci n mantiene relaciones directas con los ciudadanos desde una posici n de superioridad. En consecuencia, la principal aportaci n de la tecnolog a *blockchain* (la eliminaci n de intermediarios en el negocio de la seguridad de los intercambios) resulta, m s bien, indiferente para la Administraci n y el administrado que mantienen una relaci n directa entre s .

23. Alonso Su rez (2018: 491), quien parece trasladar estas ideas a partir de propuestas realizadas en otros ordenamientos, en los que tambi n se propone la eliminaci n de registros p blicos de donaciones o de apuestas.

24. De hecho, desde un an lisis m s medurado, W st y Gervais (2018: 53)  nicamente ven interesante la opci n de sustituir los registros de propiedad por redes de *blockchain* en pa ses donde pueda dominar la corrupci n y donde la integridad de los documentos oficiales resulte cuestionable.

Esta afirmación se entiende con bastante claridad si nos fijamos en actos típicos de la actividad administrativa de limitación (*v. gr.*, una orden de demolición de una construcción en ruinas, o una orden de cierre de un local por razones de salubridad) o de la actividad sancionadora (*v. gr.*, la imposición de una sanción). Pero la actividad subvencional tampoco es, desde luego, una excepción a esta situación, a pesar de que algunos autores hayan afirmado justamente lo contrario²⁵.

En primer lugar, porque buena parte de la actividad subvencional se desarrolla a través de procedimientos de concesión directa, en los que las dos únicas partes de la relación son el sujeto solicitante y la Administración concedente²⁶.

En segundo lugar, porque, incluso en los procedimientos de concesión en concurrencia competitiva, lo que se produce en realidad es una pluralidad de relaciones directas y bilaterales entre la Administración y los solicitantes: aunque compitan unos con otros, estos últimos no interactúan nunca entre sí, sino únicamente con la Administración, que será la encargada de admitir o inadmitir, primero, y de valorar individualmente, después, cada una de las solicitudes, para, posteriormente, establecer una prelación entre ellas (artículo 22.1 LGS). Naturalmente, todos los solicitantes están interesados en las relaciones establecidas entre la Administración y cada uno de los demás solicitantes, puesto que el resultado de las valoraciones de sus solicitudes determinará la posición que cada uno de ellos ocupa en la prelación final. Ello les permitirá cuestionar las valoraciones recibidas por los demás y, llegado el caso, impugnar las resoluciones dictadas por la Administración en vía administrativa o contencioso-administrativa. Pero, incluso en estos casos, todas las interacciones de los solicitantes son siempre con la Administración concedente, nunca de manera directa con los demás interesados. Así, se impugnará la admisión al procedimiento de un participante rival (que es decidida por la Administración) o la valoración que reciben sus méritos (que es realizada por parte de la Administración), es decir, los únicos actos objeto de posible impugnación por parte de un participante serán los actos de la Administración, no los de los demás participantes.

25. Así, Pereiro Cárceles (2019: 22).

26. Aunque, ciertamente, el legislador básico configuró la concesión directa de subvenciones como un procedimiento excepcional, confinado casi exclusivamente a los estrechos límites del artículo 22.2 LGS, la realidad es que estos cauces se han visto ampliamente desbordados a través de los más diversos (y jurídicamente discutibles) mecanismos. Tempranamente sobre ello y, en especial, sobre el uso torticero de los convenios, Fernández Farreres (2012: 42-43). Una exposición con aspiraciones sistemáticas de todas las formas de concesión directa en Bueno Armijo (2017a).

Todo ello implica, en definitiva, que la aplicación de la tecnología *blockchain* a la actividad administrativa subvencional no tendría los deseados efectos de desintermediación, esto es, no permitiría eliminar a la Administración, por la sencilla razón de que esta no actúa como intermediaria en las relaciones entre otros sujetos, sino que ella misma es una de las partes de tales relaciones que, además, tienen el carácter de bilaterales. En consecuencia, eliminada la Administración, no se eliminaría un intermediario, sino la relación misma.

2.3. Una posible ventaja del uso de *blockchain* en la Administración: la inmutabilidad de los documentos

2.3.1. La tecnología *blockchain* como herramienta de lucha contra la corrupción

Hay, sin embargo, un elemento novedoso que sí aportaría el uso de la tecnología *blockchain* al ámbito de la Administración pública y, por extensión, a su actividad subvencional: la modificación de los documentos incorporados al procedimiento, tanto por parte de los interesados como por parte de la Administración, sería imposible²⁷.

En efecto, aunque los participantes en un procedimiento de concurrencia competitiva no establezcan propiamente relaciones entre sí, sino cada uno de ellos con la Administración, ya hemos dicho que todos ellos están interesados en las relaciones de los demás. Dicho interés no solo se extiende a las decisiones jurídicas que adopta la Administración, sino también a los documentos que le sirven de base. En particular, pueden tener un interés específico en que las solicitudes presentadas por los demás participantes en el procedimiento no sean modificadas una vez terminado el plazo legal para ello y fuera de los cauces legales que sí lo permitirían. Se trataría, por ejemplo, de evitar que pudieran presentarse solicitudes fuera de plazo (por ejemplo, antedatándolas) o alegarse méritos adicionales que no se incluyeron en la solicitud original y que mejorarían la puntuación (y, por tanto, la posición en la prelación final) del solicitante.

El interés en que dichos documentos no puedan ser modificados no solo es un interés de los sujetos privados, sino que constituye un interés general.

27. Quintana Cortés (2020: 163) habla, en este sentido, de “la inmutabilidad de los registros públicos”.

Por tal motivo, existen poderosos mecanismos para intentar evitar que ello ocurra y, en caso de que suceda, reaccionar contra ello²⁸. Pero intentar evitar que ocurra no es lo mismo que conseguir evitarlo, y la realidad es que pueden existir casos en que los funcionarios de la Administración manipulen o permitan que se manipulen tales documentos, lo que constituye la base de la corrupción.

Aquí es donde la tecnología *blockchain* podría realizar su aportación. Su aplicación a un procedimiento de concurrencia competitiva, como podría ser el de concesión de ciertas subvenciones, permitiría que toda la red conociera automáticamente la presentación de solicitudes y que ello ocurriera de manera inmediata, sin intermediación alguna. Ello maximizaría la transparencia y garantizaría la integridad de datos y documentos²⁹. De este modo, en un procedimiento cuyos documentos se hubieran incorporado a una red de *blockchain*, la información contenida en ellos no se encontraría únicamente en poder de la Administración, sino en todos los nodos (sujetos participantes) de la red. Tal es la esencia de las tecnologías de registro distribuido. La Administración, por tanto, solo podría cambiar los registros en su poder, pero no todos los demás, dado que estos cambios en los registros anteriores requerirían el consenso de la mayor parte de la red.

De esta forma, ya no se trataría solo de que la ley imponga la confianza en la Administración, de que le atribuya la ficción de la fe pública y de que se presuma que no va a alterar ni modificar (ni permitir que se alteren o modifiquen) documentos incorporados a un procedimiento. Se trataría de que la Administración o cualquier otro de los participantes, aun queriendo, no podría hacerlo o, haciéndolo, sería inmediatamente descubierto. Desde esta perspectiva, hay que aceptar que esta tecnología, al impedir, *de facto*, tales actuaciones, supone una garantía aún mayor contra posibles prácticas corruptas, lo que la convertiría en una formidable herramienta para el control del sector público y, específicamente, para la lucha contra la corrupción³⁰.

28. Como mínimo, cabe señalar la existencia de regímenes sancionadores, tanto disciplinarios [*cf.*: artículo 95.2.d) y j) TREBEP] como penales (en relación, específicamente, con las subvenciones, arts. 306 y 308 CP, además del Título XIX “Delitos contra la Administración pública” CP), que actúan con la finalidad disuasoria propia del principio de prevención. Todo ello, sin perjuicio del régimen de invalidez aplicable a estas actuaciones y de la existencia, en su caso, de responsabilidad patrimonial de la Administración.

29. Así lo indica Tejedor Bielsa (2020: 123-126), refiriéndose a un concreto procedimiento de concurrencia competitiva, el procedimiento abierto abreviado de contratación pública; y también, con carácter general, Gallone (2019: 205).

30. Entre otros, Pereiro Cárceles (2019: 13) y Quintana Cortés (2020: 164). Respecto al impacto de la tecnología *blockchain* en el control del sector público, Wanden-Berghe y

Ahora bien, estos posibles beneficios del uso de la tecnología *blockchain* deben ser matizados.

En primer lugar, según queda dicho, la inmutabilidad de los documentos es mucho más que un mecanismo de control o supervisión: es una limitación fáctica a la actuación de la Administración, que, de hecho, no podrá alterar la información contenida en los documentos incorporados a la red. Esta extrema rigidez, sin embargo, es dudoso que sea una ventaja incuestionable en todos los casos: ¿qué hacer cuando se descubre un dato erróneo (voluntario o involuntario) en un documento?; ¿qué hacer cuando es necesario retrotraer el procedimiento?; ¿cómo anular lo actuado?; ¿cómo conservar, selectivamente, algunos de los trámites posteriores al momento al que debe retrotraerse el procedimiento que puedan ser objeto de conservación?³¹

En segundo lugar, porque estas ventajas solo se darán en aquellas redes de *blockchain* que cumplan ciertas características: un gran número de nodos y un poder de validación descentralizado. Sin embargo, y como veremos más adelante, este tipo de redes no son las más adecuadas para los procedimientos de concesión de subvenciones.

2.3.2. La dificultad de desplegar redes de *blockchain* útiles en los procedimientos de concesión de subvenciones

Uno de los puntos débiles de la utilización de la tecnología *blockchain* por parte de las administraciones públicas es su dependencia de los usuarios privados que participen en estas redes. Esta dependencia se hace especialmente

Fernández Daza (2020: 134, 143). Aunque refiriéndose al ámbito de la contratación, Gallone (2019: 204-205) alude también al límite a posibles prácticas corruptas en la fase de selección y adjudicación de contratistas que puede suponer el uso de *blockchain*, en la medida, justamente, en que impediría la manipulación de las ofertas presentadas. No obstante, el mismo autor señala que el principal foco de corrupción en este ámbito se encuentra en la fase de ejecución de los contratos y, especialmente, en las modificaciones o variaciones no justificadas que permiten al operador económico recuperar las rebajas realizadas en la fase de presentación de la oferta (2019: 208-209). Frente a este tipo de prácticas, a las que hace frente el artículo 72 Directiva 2014/24/UE, poco puede ofrecer la tecnología *blockchain*.

31. El problema de la eliminación de datos o documentos incorporados a una red de registro distribuido no se produce únicamente en casos de corrección de errores, subsanación o anulación de actos administrativos, sino que puede venir determinado también por el ejercicio de sus derechos por parte de sujetos privados. Así ocurriría, como advierte Quintana Cortés (2020: 156), en los casos en que se tenga derecho a ejercer el llamado derecho de supresión o “derecho al olvido” (artículo 17 RGPD).

evidente en dos de las características básicas de esta tecnología que, en ocasiones, pasan desapercibidas.

La primera es que la pertenencia a una red de *blockchain* se basa en la voluntariedad. Incluso aunque el ingreso pueda estar condicionado a la aprobación de una autoridad central (redes privadas o permisionadas), la salida solo descansa en la voluntad de cada miembro. Los miembros de una red no siempre podrán entrar cuando quieran, pero sí podrán salir en cuanto lo deseen.

La segunda es que la fortaleza de toda red de *blockchain* (en realidad, su propia existencia) descansa en la premisa de que contará con un número suficiente de nodos (esto es, interesados en el procedimiento) y de que estos se mantendrán de manera indefinida como parte de dicha red, conservando la información y actuando, en su caso, como nodos de validación y verificación. Una red sin nodos, sencillamente, no es una red.

Se ha insinuado que la participación de sujetos privados en las redes de *blockchain* usadas por la Administración para tramitar procedimientos constituye un hito en la transformación de las relaciones entre Administración y ciudadanos que debería despertar un cierto entusiasmo en estos últimos³². Sin embargo, no es evidente que los nodos de una red tengan interés en pertenecer a ella de forma indefinida. Más bien al contrario, los sujetos privados que presten sus equipos para participar como nodos de una red de *blockchain* tendrán que asumir por sí mismos el coste energético, de datos, de *software* y *hardware* que ello conlleva³³. En consecuencia, no tendrán, normalmente, ningún motivo para:

32. Es la postura de un optimista Gallone (2019: 194 y 202), quien considera que la participación de sujetos privados en la red de bloques, compartiendo de este modo los datos contenidos en cada uno de ellos, llevaría nada menos que a la “cogestión del procedimiento”, puesto que tales sujetos “se convierten en protagonistas y no solo destinatarios de la acción administrativa, inaugurando un terreno inédito de realización del principio constitucional de subsidiariedad horizontal”.

33. Aunque no siempre se llame la atención sobre ello, las tecnologías de registro distribuido exigen que todos los miembros o nodos de la red cuenten con la capacidad suficiente para almacenar la cadena de bloques. Debe tenerse en cuenta que cada participante de la red tiene una copia completa del registro y de todos los cambios que se operen en él, por lo que deben disponer del *hardware* y del *software* adecuado y actualizado. Esto conlleva una cuestionable socialización de los costes de las redes *blockchain*. En efecto, la necesidad de contar con el *hardware* y el *software* adecuados se traduce en un coste económico, que se suma al creciente coste energético que conlleva el funcionamiento de una red de *blockchain* y al que nos referimos más atrás. Estos costes eran hasta ahora asumidos por las administraciones públicas, que se encargaban de controlar, custodiar y supervisar sus bases de datos. Pero, si estas bases de datos se sustituyen ahora por redes de *blockchain*, el coste dejaría de asumirlo la Administración y pasaría a repartirse entre los participantes de cada red.

a) Querer participar en la red cuando de ello no se desprenda ningún beneficio para ellos. Por ejemplo, es difícil imaginar qué podría mover a un sujeto privado a querer participar en una cadena de *blockchain* diseñada para tramitar un procedimiento de concesión de subvenciones en el que no tiene interés alguno en participar y cuyos resultados le son indiferentes³⁴.

b) Mantenerse en ella una vez que hayan alcanzado sus objetivos privados o que estos se hayan vuelto inalcanzables (por ejemplo, si han sido inadmitidos en el procedimiento, o una vez este ha concluido con una resolución definitiva en la que se les concede o deniega la ayuda solicitada).

No se trata tanto de que exista un riesgo de que se pierdan los datos (cabe imaginar que, al menos, el nodo de la Administración seguiría operativo a lo largo del tiempo), cuanto de que la red podría quedar reducida a un número tan pequeño de nodos que no sería imposible que estos se pusieran de acuerdo para cambiar los datos, alcanzando la mayoría suficiente para validarlos. Y el nodo de la Administración no podría evitarlo. Recuérdese que la tecnología de registro distribuido no impide la modificación de los datos registrados, sino que, más bien, exige el acuerdo de un número suficiente de nodos para proceder a dicha modificación.

Se trata de un riesgo muy real si, como vislumbran algunos autores, el desarrollo de esta tecnología en el ámbito público se realiza mediante la construcción de redes de pequeñas dimensiones, con un número limitado de nodos, vinculadas a procedimientos concretos³⁵. De hecho, ese parece ser el modelo que habría que seguir en materia de subvenciones: la creación de redes de *blockchain* para la tramitación de cada procedimiento, cuyos nodos vendrían constituidos por la Administración concedente y los interesados en el procedimiento, estos últimos en un número variable pero que podría ser adecuado para permitir conductas de concertación entre ellos y contra la Administración.

34. Del mismo modo, resulta difícil imaginar qué interés podría tener un sujeto privado en participar en una red de *blockchain* diseñada para asegurar la inmutabilidad de los libros electrónicos de registro de algunas administraciones, como los libros contables, los de actas, decretos y resoluciones de las administraciones locales. De ahí que resulte difícil imaginar que esta “oportunidad real para el aseguramiento de la integridad de los libros electrónicos de registro” en la que ha insistido Alamillo Domingo (2020: 251-252, 2019b: 64) pudiera resultar viable en la práctica. A lo sumo, cabría pensar en el establecimiento de una red de *blockchain* compartida por todas las administraciones locales, en la que cada una de ellas actuara como nodo, de tal forma que funcionaran de manera cooperativa, sirviendo de punto de almacenamiento de la información de las demás entidades y beneficiándose de la prestación de este mismo servicio por parte de las demás.

35. Tales son las previsiones de autores como Atzori (2018: 13) o Gallone (2019: 199).

Sin llegar tan lejos, la situación descrita permite llamar la atención sobre otra de las características de *blockchain*, típica de su naturaleza descentralizada y basada en el P2P: su configuración horizontal, basada en una estructura donde todos los miembros de la red actúan sin intermediarios, en régimen de igualdad y sin una autoridad central. La ausencia de una autoridad central suele verse como una ventaja. Pero entraña un serio inconveniente: nadie es responsable de los fallos o del mal funcionamiento de la red.

Situaciones como la descrita obligarían a configurar estas redes como redes privadas o permissionadas, en las que solo el nodo de la Administración pudiera dar acceso a nuevos nodos y pudiera validar las transacciones, ocupando un lugar destacado y asumiendo una mayor responsabilidad. Pero esto, justamente, eliminaría la principal aportación que podría conllevar el uso de *blockchain* en nuestro ámbito, dado que la Administración volvería a tener el pleno dominio sobre los documentos incorporados al procedimiento³⁶.

3. El uso de *blockchain* como base para el desarrollo de otras tecnologías en la administración digital: *smart contracts* y actividad administrativa automatizada

De cuanto queda expuesto, y sin perjuicio de lo que más adelante diremos en relación con la SSI, cabe concluir que las ventajas de aplicar la tecnología *blockchain* a la actividad subvencional de la Administración parecen muy reducidas y, tal vez, incluso inferiores a los riesgos que entraña. Sin embargo, es posible que la principal aportación de *blockchain* al ámbito de la Administración pública no sea la desintermediación o la garantía de inmutabilidad de los registros. Es posible que la principal aportación se encuentre, más bien, en que las redes *blockchain* permiten la creación y el desarrollo de otras tecnologías, como los *smart contracts* o “contratos inteligentes”. Es posible, incluso, que *blockchain* permita usos de los que ni siquiera se es consciente aún³⁷.

Debe tenerse en cuenta que la automatización de las actuaciones administrativas supone un proceso en auge e imparable. Ello podría

36. En efecto, como advierten Wüst y Gervais (2018: 46), si solo existe un validador en la red, *blockchain* no ofrece garantías adicionales de seguridad. En consecuencia, una simple base de datos centralizada podría ser una solución tecnológica más adecuada.

37. De hecho, autores como Casey y Vigna (2018b) subrayan que lo que resulta revolucionario en *blockchain* es la tecnología en sí, cuyas aplicaciones finales y más relevantes, de aquí a unos años, podrían estar muy lejos de los usos que se le dan actualmente como base de criptomonedas o de *smart contracts*.

facilitar el uso de *smart contracts* por parte de la Administración, puesto que estas aplicaciones suponen una forma concreta de automatización. Pues bien, en la medida en que los *smart contracts* toman como base la tecnología *blockchain*, algunos autores han adelantado la hipótesis de que la generalización del *blockchain* en el ámbito administrativo se producirá, justamente, por tratarse de un requisito necesario para el uso de *smart contracts*³⁸. Esta perspectiva obliga a analizar las posibilidades de desarrollo tanto de los *smart contracts* como, más ampliamente, de la actividad administrativa automatizada en el ámbito de las subvenciones públicas. Y -cabe adelantar- en relación con esta última las posibilidades de desarrollo sí que son enormes.

3.1. Los *smart contracts* basados en *blockchain* como forma de automatizar la actuación administrativa

Los *smart contracts* son mecanismos automatizados que ejecutan las prestaciones a las que previamente se han comprometido las partes en un contrato. Dicha ejecución tiene lugar cuando se cumple una condición o un término o incluso cuando se produce el cumplimiento de una de las partes, lo que es verificado por el propio sistema. De esta forma, su principal aportación es sustraer la ejecución de los contratos a la voluntad de las partes. Dado que es el propio sistema informático quien tiene que verificar por sí mismo el cumplimiento del evento que desencadena la ejecución del contrato, resulta esencial que las comprobaciones que realiza el sistema se produzcan en un entorno de datos confiables. Es ahí donde aparece su conexión con la tecnología *blockchain*, aunque, en rigor, se trate de elementos independientes³⁹.

38. Especialmente asertivo a este respecto se muestra Pereiro Cárceles (2019: 7), para quien “no será posible desarrollar todas las potenciales ventajas que ofrece *blockchain* a la Administración pública si no hacemos uso de esta tecnología para la creación de *smart contracts* o contratos inteligentes”.

39. A pesar de tratarse de elementos distintos e independientes, cabe señalar que la Ley italiana de 11 de febrero de 2019, n. 12, *Conversione in legge del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione*, contiene una definición legal de *smart contracts* en la que estos quedan vinculados con la tecnología de registro distribuido: “*si definisce ‘smart contract’ un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse*”. Frente a ello, Gallone (2020: 181) rastrea las primeras teorizaciones sobre *smart contracts* hasta momentos muy anteriores, remontándose, al menos, a las reflexiones de Szabo (1997), donde se discuten posibles protocolos de seguridad aplicables a importantes áreas de contratación mercantil.

Siguiendo una lógica bastante lineal, los *smart contracts* se basan en la previsión de que se producirá automáticamente una determinada acción (Q) en caso de que se verifiquen ciertos hechos (P), siguiendo un esquema lógico que, en su formulación más sencilla, sería del tipo: “Si P, entonces ocurre Q”. A partir de aquí, la peculiaridad de los *smart contracts* se encuentra en que la acción concreta (Q) se produce sin intervención humana, pues resulta posible programar una máquina que, verificando los hechos (P), puede generar la acción concreta (Q) por sí misma.

De acuerdo con lo anterior, y al igual que ocurre con la propia tecnología *blockchain*, los *smart contracts* resultan especialmente útiles en las relaciones entre privados. El motivo se encuentra en que el *smart contract* es un programa que se almacena en la misma red de *blockchain*, sumando su automatismo a la inmutabilidad. De esta forma, los sujetos privados ya no tienen que confiar en que su contraparte cumplirá con la realización de su prestación, dado que el cumplimiento se producirá automáticamente porque de él se encarga una máquina. Es decir, los *smart contracts* imponen a las partes el cumplimiento de sus obligaciones sin tener que acudir a un juez que declare, primero, la existencia de la obligación e imponga, después, su ejecución, y resolviendo por esta vía el problema de su falta de autotutela. Desde esta perspectiva, los *smart contracts* vendrían a resolver un problema que, en realidad, no existe en la Administración, dado que esta sí que goza de autotutela.

A pesar de ello, se ha postulado su extensión también al ámbito público⁴⁰ y, en particular, al ámbito de la contratación pública, donde, se afirma, su implantación tendría un “considerable potencial”: por una parte, porque al basarse en una tecnología de registro distribuido y al aplicarse en la fase de ejecución, se aumentaría la transparencia de la actuación administrativa, pudiendo funcionar como mecanismo de freno frente a prácticas corruptas; por otra parte, porque facilitaría (en rigor, eliminaría) los trámites de ejecución forzosa que debería realizar la Administración cuando su contratista se negara a cumplir con las prestaciones a las que venía obligado⁴¹.

40. Pereiro Cárceles (2019: 6-8), refiriéndose expresamente a la actividad subvencional.

41. Gallone (2020: 183-185) no solo propugna el uso de *smart contracts* en el ámbito de la contratación pública, sino que incluso considera que es el único sector de la actividad administrativa en el que, en rigor, puede producirse en el ordenamiento jurídico italiano. Así se deduciría de las profundas diferencias entre la categoría de los *smart contracts* y la de las actuaciones administrativas automatizadas, al situarse los primeros en el ámbito de la autonomía privada y las segundas en el ejercicio de potestades públicas (Gallone, 2020: 188).

En cualquier caso, una interpretación estricta del concepto de *smart contracts* impediría su uso en el ámbito de las subvenciones, en el que no existe propiamente una relación contractual ni sinalagmática entre Administración y beneficiario⁴². Por ello, resulta mucho más útil ampliar el marco y analizar el impacto y las posibilidades de desarrollo de todas las demás formas de actuación administrativa automatizada en materia de subvenciones públicas.

3.2. La actividad administrativa automatizada más allá del uso de *smart contracts*

Aunque resulte una obviedad, debemos recordar que la automatización de la actividad administrativa no se identifica con (ni se reduce a) el uso de *smart contracts*. La actividad administrativa automatizada no necesita para existir de una cadena de bloques. De hecho, la aparición de la actividad administrativa automatizada en España, en sentido estricto, suele situarse en los años 90 del pasado siglo, antes de que la tecnología *blockchain* fuese creada⁴³, y en algunos ámbitos, como el de la Seguridad Social, las últimas reformas normativas, reforzando y generalizando el uso de la actuación administrativa automatizada (que, precisamente, se originó en la gestión de ayudas y prestaciones), se perciben, más bien, como “la culminación, por ahora, de una evolución que arranca de las dos décadas anteriores”⁴⁴.

La actuación automatizada no supone, en rigor, una eliminación de tareas, sino una sustitución del ser humano que hasta ahora realizaba una actividad, por una máquina que se encarga de hacerla en adelante. En la medida en que la máquina pueda hacer dicha tarea de forma similar o, incluso, mejor y más rápidamente, la actuación administrativa ganará en eficiencia: la Administración puede realizar muchas más actuaciones de las que venía haciendo hasta ahora. De ahí que en el §.2 del Preámbulo de la

42. Cfr. artículo 2.1.a) LGS (“Que la entrega se realice sin contraprestación directa de los beneficiarios”). Entre las explicaciones sobre la ausencia de carácter contractual de las subvenciones: Fernández Farreres (2005: 12) y Bueno Armijo (2011: 57-60), con referencia expresa a cierta jurisprudencia que aparentemente venía sosteniendo lo contrario.

43. Wanden-Berghe y Fernández Daza (2020: 137). De hecho, cabe sostener que la aparición de la actividad administrativa automatizada, en sentido amplio, es muy anterior, pues desde hace décadas existen actos realizados por medios mecánicos (v. gr., un semáforo). La verdadera novedad aparecida a finales del s. XX se encuentra, más bien, en la aparición de actos administrativos *escritos* producidos de forma automatizada, sin intervención humana, tal y como apunta Tarrés Vives (2012: 453).

44. Goerlich Peset (2021: 24), refiriéndose, en concreto, a las modificaciones introducidas en el artículo 130 TRLGSS por el Real Decreto-ley 2/2021, de 26 de enero, de refuerzo y consolidación de medidas sociales en defensa del empleo.

LRJSP se califique la actuación administrativa automatizada como un medio electrónico cuya utilización “ha de ser lo habitual”.

Esta sustitución del ser humano es, justamente, la idea sobre la que descansa el concepto jurídico de actuación administrativa automatizada consagrada en el ordenamiento español, actualmente recogida en el artículo 41.1 LRJSP: “Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada *íntegramente a través de medios electrónicos* por una Administración pública en el marco de un procedimiento administrativo y en la que *no haya intervenido de forma directa un empleado público*”.

La contundencia con que está expresada la exclusión de intervención humana no ha pasado desapercibida ni para la doctrina ni para la jurisprudencia⁴⁵. Asimismo, de esta definición legal se deducen otras importantes consecuencias que, como veremos, son de especial relevancia para la actividad subvencional.

En primer lugar, la actuación administrativa automatizada puede referirse tanto a actividades jurídicas como meramente materiales⁴⁶. El precepto incluye

45. Entre las primeras y, como siempre, más autorizadas voces, Valero Torrijos (2015: 16) saludó esta redacción como una clarificación importante del concepto. Por su parte, la escasa jurisprudencia que se ha ocupado de este precepto ha realizado una interpretación muy estricta y literal de esta exigencia. La STSJ de Madrid de 29 de enero de 2021, 1038/2021, ECLI:ES:TSJM:2021:1038 (ponente: Chulvi Montaner), resolvió la impugnación de varios preceptos de la Ordenanza de Movilidad Sostenible (OMS) del Ayuntamiento de Madrid por parte de Automovilistas Europeos Asociados. En particular, y por cuanto aquí interesa, el artículo 15 OMS establecía: “El Ayuntamiento de Madrid podrá emplear *medios técnicos para la vigilancia automatizada* de la circulación y el estacionamiento, así como para la denuncia automatizada de las infracciones que se cometan utilizando, entre otros, los siguientes medios (...)”, mientras que el artículo 16 OMS disponía: “La Administración municipal establecerá mecanismos sistemáticos de control que combinen en su caso *medios técnicos de vigilancia* con la intervención de personas que actúen ejerciendo labores de control específicas y procedimientos de gestión adecuados para garantizar el cumplimiento de la normativa vigente en materia de circulación y estacionamiento”.

La posible actuación automatizada se refería en ambos casos a actuaciones de vigilancia, que en este ámbito se configuran como meras actuaciones materiales no procedimentalizadas (los procedimientos se iniciarán, en su caso, a raíz de los resultados de estas actividades de vigilancia). La sentencia no parece prestar atención a este detalle, a pesar de que, en rigor, ninguna de las actividades a las que se refieren los artículos 15 y 16 OMS se producen “en el marco de un procedimiento administrativo”. Lo que resulta determinante para la sentencia es que la OMS “no contempla actuaciones administrativas automatizadas realizadas íntegramente a través de medios electrónicos, que es lo que se refiere el artículo 41 de la Ley 40/2015”. En efecto, el artículo 15 OMS no impone el uso exclusivo de “medios técnicos para la vigilancia automatizada” y el artículo 16 OMS se refiere expresamente a que los mecanismos sistemáticos de control “combinen en su caso medios técnicos de vigilancia con la intervención de personas”. En consecuencia, la sentencia concluye que el artículo 41 LRJSP no resulta aplicable a estos supuestos.

46. Tarrés Vives (2012: 454-455). Sobre la distinción y utilidad de ambos conceptos y, en especial, sobre la relevancia jurídica de la actividad material, frecuentemente marginada, Rebollo Puig (2019: 62-63).

en el concepto a todo “acto y actuación”, lo que permitiría entender expresamente amparada la actividad material. Al menos, la realizada en el marco de un procedimiento administrativo. No obstante, aunque es posible que este tipo de actividad esté procedimentalizada, lo habitual es que se realice fuera de todo procedimiento, por lo que, en una interpretación demasiado literal del precepto, toda esa actividad material no procedimentalizada quedaría sin regulación⁴⁷.

Parece claro, como ha denunciado la mejor doctrina, que al abordar la actividad administrativa automatizada el legislador sigue privilegiando un enfoque centrado en la actuación formalizada de la Administración y, muy especialmente, en el acto y el procedimiento administrativo⁴⁸. Pero una interpretación excesivamente restrictiva del artículo 41.1 LRJSP no parece ni deseable ni justificada, especialmente a la vista de la amplísima variedad de actuaciones automatizadas que ya realiza la Administración. De hecho, buena parte de las estrategias desplegadas bajo los proyectos de *smart cities* consisten, justamente, en automatizar actividades materiales (v. gr., regulación automática de la duración de los semáforos atendiendo a la fluidez del tráfico de vehículos o al flujo de peatones). Esta variedad de actuaciones materiales automatizadas, sin duda, desborda las restrictivas previsiones del artículo 41.1 LRJSP⁴⁹. Y, por cuanto a nosotros importa, está muy presente en el ámbito subvencional.

En segundo lugar, la actuación administrativa automatizada puede descansar o no en inteligencia artificial, a la que el artículo 41.1 LRJSP no se refiere, utilizando el concepto mucho más amplio de “medios electrónicos”. Sin embargo, esta es la situación cada vez más habitual y, sin duda, la de un mayor desarrollo potencial.

La presencia de inteligencia artificial, al menos en su sentido más amplio, obliga a remitirse al uso de algoritmos por parte de la Administración⁵⁰. Pueden plantearse muy distintas clasificaciones de algoritmos, pero, a los efectos del

47. En este sentido, Martín Delgado (2009a: 368), si bien refiriéndose al derogado artículo 39 LAE, excluía expresamente que la actividad material de la Administración pudiera incluirse dentro del concepto de actuación administrativa automatizada, al entender que esta debía producirse necesariamente en el marco de un procedimiento administrativo.

48. Valero Torrijos (2019: 85).

49. Por todos, Moreno Rebato (2021: 111).

50. Como ha afirmado Cortés (2020: 57), “el algoritmo es el corazón de estas tecnologías”. La OCDE (2021: 7) ha propuesto como definición de sistema de inteligencia artificial un concepto muy amplio, conforme al cual se identificaría con “un sistema automatizado que, para un conjunto determinado de objetivos definidos por un ser humano, es capaz de hacer previsiones, formular recomendaciones o tomar decisiones que pueden influir en ambientes reales o virtuales. Los sistemas de Inteligencia Artificial son diseñados para funcionar con distintos grados de autonomía”.

presente trabajo, resulta de especial utilidad la que distingue entre algoritmos aritméticos, relacionales o lógicos, según se trate de algoritmos que ejecuten una acción compleja (aritméticos), que transmitan un resultado comparativo (relacionales) o que se adapten a la estructura natural y cognitiva del pensamiento (lógicos)⁵¹.

En la mayoría de las experiencias actuales de actuación administrativa automatizada, la actuación realizada (e incluso la decisión adoptada) responde exactamente a un conjunto de reglas, expresadas en forma de algoritmos aritméticos que siguen una lógica lineal y ordenados siguiendo la estructura: “Si P, entonces ocurre Q”, de manera idéntica a como hemos visto que funcionan los *smart contracts*. De esta forma, el resultado alcanzado digitalmente reproduce íntegramente y sin desviación alguna la voluntad humana previa que ha determinado su actuación mediante la programación de su *software*⁵².

Sin embargo, los desarrollos con mayor potencial son aquellos basados en algoritmos lógicos que permiten el “machine learning” o aprendizaje automático, de modo que los ordenadores no se limitan a aplicar las instrucciones que sus programadores les han introducido, sino que producen sus propias reglas, resultado de sus análisis, y dan lugar a actuaciones (o, mejor, modos de actuar) que no tienen que coincidir exactamente con las programadas por sus creadores humanos⁵³. Como veremos a continuación, la Administración ya ha desarrollado e implantado, para el ejercicio de su actividad subvencional, este tipo de actuaciones administrativas automatizadas en las que se utiliza, propiamente, inteligencia artificial, y que seguramente tienen sus ejemplos más visibles en los chatbots o robots conversacionales⁵⁴. Pero, junto a estos últimos, los algoritmos lógicos con capacidad predictiva también pueden utilizarse para determinar el momento más adecuado para convocar ciertas ayudas sociales, para identificar las características de aquellas personas que más podrían beneficiarse de ellas o para crear perfiles que ayuden a detectar casos de fraude, entre otros muchos ejemplos.

Es respecto a este último tipo de algoritmos lógicos cuando se genera el problema de las cajas negras o *black boxes* del que ha advertido un buen número

51. Vestri (2021: 373-374) y Moreno Rebato (2021: 117-119). Más ampliamente, Huergo Lora (2020).

52. Marongiu (2018: 395).

53. El siguiente paso en esta evolución sería el “*deep learning*” o aprendizaje profundo, basado en redes neuronales y el uso de enormes cantidades de datos. Véase, sobre todo ello, Cerrillo i Martínez (2019: 4).

54. Esto es, “sistemas autónomos, automodificables a través de aprendizaje, capaces de entablar diálogos no guiados por esquemas predefinidos, de reconocer y reproducir el lenguaje natural y la voz humana”, en la caracterización ofrecida por Marongiu (2018: 397).

de autores: los sistemas basados en mecanismos de aprendizaje autónomo acaban dando lugar a actuaciones decididas por parte de la máquina de las que no es posible saber cómo se han adoptado, puesto que las reglas que han llevado a decidir las no han sido previamente acordadas por su programador, sino que han sido desarrolladas por el propio algoritmo⁵⁵. Ciertamente, las actuaciones automatizadas se pueden completar con una actuación de un funcionario que valida la acción adoptada por el algoritmo. En especial, cuando se trata de actividades administrativas jurídicas o formalizadas y no meramente materiales. Pero cuanto más se desarrolla la inteligencia artificial, más difícil es aceptar que un empleado pueda entender y explicar la forma en que se ha adoptado la decisión que posteriormente valida⁵⁶.

Todo ello justifica que el tratamiento de los algoritmos aritméticos y relacionales, por un lado, y el de los algoritmos predictivos, por otro, deban ser debidamente diferenciados⁵⁷.

4. Las posibilidades del uso de *blockchain* y de automatización de la actividad administrativa en la gestión de subvenciones

Se ha sugerido, tal vez con cierta ligereza, que el procedimiento de concesión de subvenciones puede adecuarse con facilidad a una actuación administrativa basada en *blockchain* y *smart contracts* o, al menos, con mayor facilidad que los procedimientos de contratación pública⁵⁸. Conforme a cuanto llevamos expuesto, es dudoso que así sea. La tecnología *blockchain* ofrece pocas ventajas para su implantación en la tramitación de subvenciones. No obstante, sí podemos afirmar que la tramitación de subvenciones ofrece múltiples posibilidades para el desarrollo de actuaciones administrativas automatizadas. Esta afirmación, sin embargo, requiere una previa contextualización.

4.1. Requisitos para la incorporación de actividades administrativas automatizadas a la tramitación de subvenciones

Por comenzar con lo más obvio, tanto el uso de *blockchain* como el recurso a la automatización de la actividad administrativa en materia de subvenciones

55. Por todos, recientemente, Cerrillo i Martínez (2019: 4).

56. Valero Torrijos (2019: 90) y Goerlich Peset (2021: 38).

57. Vestri (2021: 392). También Moreno Rebato (2021: 119).

58. Pereiro Cárceles (2019: 22).

solo pueden producirse en el contexto, más amplio, de la digitalización de la Administración. En particular, solo tienen sentido en el marco de la actividad subvencional electrónica, del mismo modo que la aplicación de esta tecnología a la contratación pública solo tiene sentido respecto a la contratación pública en la medida en que se trate de contratación electrónica⁵⁹. Esta apreciación, aunque evidente, no es irrelevante, en la medida en que puede suponer un importante obstáculo en aquellos casos en que los administrados no estén obligados a relacionarse electrónicamente con la Administración y opten por no hacerlo⁶⁰. Esta situación no será en absoluto infrecuente en materia de subvenciones, en especial, en aquellas que tengan finalidades sociales o asistenciales, muy comunes en el ámbito local y dirigidas a sectores de la población a los que no cabe exigir que se relacionen telemáticamente con la Administración.

Asimismo, la actuación administrativa automatizada, sin perjuicio de sus múltiples ventajas, entraña también importantes riesgos. Ello ha determinado que el legislador haya impuesto ciertos requisitos para que la Administración pueda hacer uso de ella. Estos requisitos, recogidos esencialmente en el artículo 41 LRJSP y en el artículo 13 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, ya han recibido una notable atención por parte de la doctrina, no siempre coincidente en sus análisis.

Excedería del objeto de este trabajo hacer un análisis en profundidad de ellos, por lo que basta indicar ahora que las principales exigencias contenidas en tales preceptos, en la forma en que vienen siendo entendidos por la doctrina, serían:

59. Tejedor Bielsa (2020: 114). En el ámbito de la contratación pública, además, se cuenta con lo previsto en la disposición adicional 15.^a LCSP, que impone como regla general la presentación de ofertas de contratos públicos a través de medios electrónicos.

60. En rigor, y como explicó con especial acierto Martín Delgado (2009b: 356), es posible distinguir entre digitalización de la Administración *ad intra* (respecto a su forma de trabajo) y *ad extra* (respecto a su forma de comunicarse con los ciudadanos). De esta forma, la Administración podría automatizar actividades internas, de gestión del procedimiento, sin que esto afectara a su forma de comunicación con los ciudadanos, que podría seguir siendo analógica. Sin embargo, no siempre es posible una división clara entre ambas. Por un lado, porque la digitalización del procedimiento administrativo puede obligar a que la intervención de los ciudadanos también deba hacerse de manera digital. Esto explicaría, precisamente, que se haya impuesto a ciertas categorías de ciudadanos, cada vez más numerosas, la obligación de relacionarse electrónicamente con la Administración, puesto que, sin ello, no resulta posible (al menos, no sin grandes pérdidas de eficiencia) la tramitación electrónica del procedimiento. Por otro lado, porque algunas tecnologías difuminan la barrera que separa el interior y el exterior de la Administración, haciendo ilusoria la división entre digitalización *ad intra* y *ad extra*: es el caso, precisamente, de la tecnología *blockchain*.

a) La adopción de un acuerdo expreso en el que se contengan tanto la decisión de poner en marcha un sistema de actuación automatizada, como las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente⁶¹.

b) La publicación de dicho acuerdo⁶², sin perjuicio de que deba ser objeto de otras medidas de publicidad, vinculadas en ocasiones a las obligaciones de transparencia impuestas a la Administración pública⁶³.

c) La indicación del órgano u órganos competentes para establecer los contenidos de dicho acuerdo.

d) La indicación del órgano considerado responsable a efectos de impugnación.

Mayores dudas rodean la forma en que deben cumplirse estos requisitos y, especialmente, el procedimiento que debe seguirse para la adopción del referido acuerdo, aunque el sentir mayoritario parece orientarse hacia exigir la presencia de ciertos trámites que garanticen, al menos, la transparencia del proceso y la participación de los ciudadanos⁶⁴.

61. A pesar de que la literalidad de la norma no lo establece así (a diferencia del antiguo artículo 45 LRJPAC y del aún vigente artículo 96 LGT), la exigencia de dicho acuerdo parece unánime en la doctrina: Valero Torrijos (2019: 87), Zlotnik (2019: 30), Martín Delgado (2009a: 376), Izquierdo Carrasco (2022: 272) y Vestri (2021: 382). De hecho, Martín Delgado (2009a: 382) considera que la implantación de una actuación administrativa automatizada sin cumplir con este requisito previo sería constitutiva de vía de hecho.

62. Valero Torrijos (2019: 87) derivaba la necesidad de esta publicación de lo dispuesto en el artículo 45.1.a) LPAC. Ahora se recoge de manera expresa en el artículo 13.2 Real Decreto 203/2021.

El incumplimiento de esta obligación de publicidad daría lugar a la ineficacia del acto de aprobación y, en consecuencia, a la imposibilidad de utilizar el sistema de automatización. En el mismo sentido, Cerrillo i Martínez (2019: 23). Sin embargo, tanto el propio Valero Torrijos (2019: 92) como Martín Delgado (2009a: 383) consideran que las actuaciones automatizadas que efectivamente se produjeran por un sistema cuyas características no hubieran sido publicadas no serían necesariamente inválidas, lo que únicamente ocurriría en caso de que se generara una situación de indefensión para el ciudadano, es decir, por la afectación a la defensa de sus derechos e intereses legítimos.

63. Resulta de especial importancia la previsión del nuevo artículo 11.1.j) del Real Decreto 203/2021, en el que se establece la obligación de incluir en las sedes electrónicas la “[r]elación actualizada de las actuaciones administrativas automatizadas vinculadas a los servicios, procedimientos y trámites descritos en la letra anterior. Cada una se acompañará de la descripción de su diseño y funcionamiento, los mecanismos de rendición de cuentas y transparencia, así como los datos utilizados en su configuración y aprendizaje”. Asimismo, el sometimiento de esta información a la normativa de transparencia ha sido expresamente destacado por Ponce Solé (2019: 45) y Cerrillo i Martínez (2019: 20)

64. Ponce Solé (2019: 37-39) vincula estas garantías al derecho a la buena administración. Véanse Goerlich Peset (2021: 40) y Cerrillo i Martínez (2019: 24). Valero (2019: 88-91)

A pesar de su aparente sencillez, son muchas las dudas que estas exigencias plantean en la práctica. Ello quizá ayude a entender el acercamiento flexible propuesto por la jurisprudencia⁶⁵ y, tal vez, su frecuente incumplimiento, pues la mayoría de las administraciones públicas no formalizan la decisión de utilizar un algoritmo o no documentan sus finalidades, sus fuentes o los resultados obtenidos con ellos⁶⁶. A esto último, posiblemente, tampoco es ajeno el hecho de que la normativa no distinga entre actividades *ad intra* y *ad extra*, entre actividades formales y materiales, entre actos de trámite y resoluciones, favorables y desfavorables, o entre el uso de algoritmos lógicos o meramente aritméticos y relacionales. Sin embargo, tales distinciones son relevantes, en la medida en que permiten identificar numerosos casos en los que estas garantías apenas aportan nada a la defensa de los derechos e intereses de los ciudadanos, lo que podría justificar su inaplicación o, cuando menos, su flexibilización.

Sentado lo anterior, procedamos a analizar qué concretos aspectos de la gestión de subvenciones podrían ser adecuados para el uso de redes de *blockchain* o de actuaciones administrativas automatizadas.

4.2. Actividades materiales automatizadas en materia de subvenciones

Como ya hemos adelantado, la automatización de la actividad administrativa no tiene por qué referirse, necesariamente, a actividades jurídicas, ni tiene por qué implicar, en todo caso, la adopción de actos administrativos, sino que se extiende con naturalidad a la llamada actividad material o técnica. Aunque no constituye ninguna rareza, lo cierto es que en materia de subvenciones la Administración no solo despliega un amplio número de actuaciones materiales, sino que, además, algunas de ellas han sido objeto de regulación expresa por parte del legislador. Pueden señalarse entre ellas todas las funciones que el artículo 15 LGS permite atribuir a las entidades colaboradoras, pues, por definición, tienen carácter meramente material⁶⁷, o

aboga también por atribuir la competencia para adoptar la decisión a un órgano colegiado y por establecer un sistema especial de recursos ante un órgano experto y externo, dotado de autonomía funcional.

65. La STSJ de Madrid de 29 de enero de 2021, 1038/2021, ECLI:ES:TSJM:2021:1038 (ponente: Chulvi Montaner), en una interpretación bastante antiformalista, considera que se puede dar cumplimiento a los requisitos exigidos por el artículo 41.2 LRJSP en cualquier momento, siempre que sea “con carácter previo a realizarse la concreta actuación administrativa íntegramente automatizada que corresponda”.

66. Así lo denuncia, entre otros, Cerrillo i Martínez (2019: 18).

67. Ávila Orive (2005: 226-229) y Bueno Armijo (2019: 105).

las actuaciones de inspección y control financiero, reguladas en el problemático Título III LGS⁶⁸.

Centraremos nuestra atención, sin embargo, en otras dos formas de actividad material para las que no solo se ha especulado con su posible automatización, sino que incluso se han realizado ya algunos ensayos: el envío activo de información sobre programas y convocatorias de subvenciones y los robots conversacionales para resolver dudas⁶⁹.

En relación con el envío activo de información sobre programas de subvenciones, se emplean desde hace tiempo herramientas electrónicas, que hoy nos parecen evidentes y que permiten la difusión automatizada de avisos sobre la convocatoria de procedimientos de concesión de subvenciones. Se trata de los servicios de alerta mediante listas de correos, envío masivo de SMS o avisos mediante aplicaciones de mensajería instantánea (*WhatsApp*, *Telegram*, *Signal*, *Line*, etc.).

Sin embargo, este tipo de actuaciones, que probablemente ni necesitan ni cuentan con una cobertura normativa específica y que pueden realizarse por la simple solicitud del interesado⁷⁰, podrían beneficiarse de la aplicación de sistemas de inteligencia artificial que mejoraran enormemente su eficiencia. Cualquiera sabe, por experiencia propia, que la utilidad e impacto real de los *mailing* masivos puede ser muy limitada, dado su carácter indiscriminado. Frente a esta situación, la inteligencia artificial permitiría la elaboración de perfiles de necesidades o intereses específicos de los ciudadanos, de tal forma que resultara posible enviarles únicamente (o, al menos, destacadamente) información sobre aquellas subvenciones que pudieran ser de su específica

68. En relación, justamente, con algunos de los problemas derivados de su procedimentalización, Bueno Armijo (2013, 2017b).

69. No son, sin embargo, los únicos ejemplos. Así, Cerrillo i Martínez (2021: 274) ha sugerido, con carácter general, la posibilidad de utilizar robots software, que resultan especialmente adecuados para realizar tareas repetitivas y rutinarias, normalmente masivas, basadas en reglas sencillas, fijadas previamente y altamente formalizadas, para hacer acopio de datos que permitan una revisión de la eficiencia de la actividad administrativa, lo que en nuestro ámbito se traduciría en la revisión de los planes estratégicos y las bases reguladoras de las subvenciones (artículo 8.1 LGS y artículo 14 Real Decreto 887/206, Reglamento de la Ley General de Subvenciones): análisis estadísticos que señalen en qué líneas de subvenciones se han producido más reintegros, qué beneficiarios han incumplido más, qué tipo de obligaciones son las que más se han incumplido, etc.

70. Véase, *mutatis mutandis*, cuanto dice Valero Torrijos (2015: 20) en relación con los avisos enviados por la Administración al interesado informándole de la puesta a su disposición de una notificación en la sede electrónica correspondiente o en la dirección electrónica habilitada única, lo que ya era una práctica extendida mucho antes de su consagración en el artículo 41 LPAC.

utilidad o interés. La Administración estaría desarrollando aquí una actividad muy similar a las “sugerencias” que los usuarios ya reciben de plataformas de compra en línea, de alquiler de hoteles o viajes, de visionados de vídeos o series, etc.⁷¹.

Se trataría, en suma, de una forma de personalizar y prestar proactivamente los servicios públicos, es decir, de adaptarlos a las necesidades de cada persona y de anticiparse a ellas⁷². Personalización que podría utilizar, incluso, datos procedentes de otras fuentes que permitieran desarrollar funciones predictivas mucho más precisas, lo que podría resultar extraordinariamente útil, por ejemplo, para una correcta protección social.

Cabe indicar, además, que en este caso no sería de aplicación la prohibición contenida en el artículo 22 RGPD de adoptar decisiones basadas únicamente en el tratamiento automatizado de los datos de un usuario, dado que el envío de publicidad personalizada no constituye una decisión “que produzca efectos jurídicos en él o le afecte significativamente”⁷³.

Por su parte, los robots conversacionales o *chatbots* constituyen una herramienta capaz, entre otras cosas, de prestar servicios de atención e información para resolver dudas. Estas herramientas presentan interesantes ventajas, como la posibilidad de ofrecer un servicio de atención de 24 horas al día, 7 días a la semana, la reducción o práctica eliminación de tiempos de espera y, por supuesto, importantes ahorros de costes de personal, todo lo cual seguramente explica, al menos en parte, su uso cada vez más extendido entre las administraciones públicas, pudiendo rastrearse ya experiencias en relación

71. En efecto, del mismo modo que las plataformas electrónicas de empresas como *Casa del Libro* o *Netflix* pueden “aprender” de los gustos de sus usuarios y “sugerir” libros, películas o series que a estos podrían interesar, también las sedes electrónicas de las administraciones (o los buscadores de diarios oficiales) podrían “aprender” de los intereses de los usuarios y ofrecer información sobre convocatorias de ayudas y subvenciones (o normas, o resoluciones) que pudieran resultar de su interés.

72. Así lo expresa Cerrillo i Martínez (2019: 17), quien incluso propone la posibilidad de “iniciar de oficio procedimientos para la obtención de ayudas o subvenciones”. No obstante, dado que los procedimientos de concesión de subvenciones ya se inician habitualmente de oficio (artículo 23.1 LGS), seguramente debe interpretarse esta propuesta en el sentido de que la Administración invite expresamente a ciertos ciudadanos a que presenten sus solicitudes o concurran a tales procedimientos. Debe tenerse en cuenta que la normativa de subvenciones prevé la existencia tanto de convocatorias cerradas, con plazos de presentación de solicitudes sometidos a término [artículo 23.2.g) LGS], como de convocatorias abiertas, en las que las solicitudes pueden presentarse en cualquier momento del año (artículo 59 Real Decreto 887/2006, Reglamento de la Ley General de Subvenciones).

73. Gil González (2017: 175).

con actividades subvencionales⁷⁴. No obstante, los *chatbots* no están exentos de problemas.

En primer lugar, estos robots no siempre entienden a los ciudadanos, que con frecuencia necesitan ser guiados no solo en sus respuestas, sino en sus propias preguntas. En consecuencia, su utilización debe plantearse como un apoyo que venga a completar, no a sustituir, a los servicios de información propiamente humanos. Lo contrario no solo podría suponer una posible vulneración del principio de “simplicidad, claridad y proximidad a los ciudadanos” [artículo 3.1.b) LRJSP], sino un menoscabo del derecho de los ciudadanos a elegir el medio a través del cual se comunican con las administraciones públicas (artículo 14.1 LPAC). De hecho, la efectividad de este derecho exige que los ciudadanos sean informados de que están hablando con un robot y no con un ser humano. Si no se informara de esta situación, en muchas ocasiones el ciudadano ni siquiera sería consciente de que puede exigir su derecho a tratar directamente con un empleado.

En segundo lugar, estas herramientas solo encuentran una cierta base normativa, para el ámbito tributario, en el artículo 87.3 LGT: “Las actuaciones de información previstas en este artículo se podrán efectuar mediante el empleo y aplicación de técnicas y medios electrónicos, informáticos y telemáticos”. De hecho, la AEAT ha utilizado este tipo de asistentes para Suministro Inmediato de Información (SII) en materia de IVA. Sin embargo, fuera del ámbito tributario, el principal problema que presentan estas herramientas es que, si se dejan fuera del concepto de actividad administrativa automatizada por realizar una interpretación literalista del artículo 41 LRJSP, carecen de base normativa.

En tercer lugar, se asume, por lo general, que la información que ofrecen los *chatbots* no es vinculante⁷⁵. A pesar de ello, no cabe descartar que puedan producirse supuestos en los que resulte de aplicación el principio de

74. Cerrillo i Martínez (2021: 276, 280 y ss.) recoge un curioso abanico de ejemplos implantados por ayuntamientos de distintas ciudades para informar sobre el coronavirus (Córdoba, Alicante, Novelda), sobre datos generales de la ciudad (Málaga, Arganda del Rey), sobre dudas tributarias (Madrid), etc. También Vestri (2021: 371) presenta una curiosa lista de *chatbots* para ofrecer información en el ámbito educativo, puestos en marcha por un buen grupo de universidades públicas y, por cierto, casi siempre con nombres femeninos: Universidad de Murcia (*chatbot* Lola), Universidad de Alcalá (*chatbot* Isidra), Universidad de las Islas Baleares (*chatbot* Aina), Universidad Politécnica de Valencia (*chatbot* Pau), Universidad de Jaén (*chatbot* Ada) o Universidad Complutense de Madrid (*chatbot* Carol). Varios de estos *chatbots* de universidades facilitan en la actualidad información sobre las subvenciones tramitadas en ellas, generalmente bajo forma de becas: así ocurre, por ejemplo, cuando se les solicita información sobre cuándo se convocan becas de movilidad Erasmus+.

75. Zlotnik (2019: 31).

protección de la confianza legítima⁷⁶ o incluso en los que se pueda generar responsabilidad patrimonial si se reúnen los requisitos necesarios para ello⁷⁷. Lo que sí cabe descartar es la aplicación de la cláusula de exención de responsabilidad prevista en el artículo 34 LRJSP respecto de “los daños que se deriven de hechos o circunstancias que no se hubiesen podido prever o evitar según el estado de los conocimientos de la ciencia o de la técnica existentes en el momento de producción de aquellos”⁷⁸. En efecto, si la Administración decide utilizar estos sistemas estaría asumiendo deliberadamente los riesgos de producción de daños que una incorrecta configuración pudiera entrañar.

4.3. Fase de iniciación del procedimiento de concesión de subvenciones

4.3.1. La convocatoria del procedimiento de concesión de subvenciones

La regla general en los procedimientos de concesión de subvenciones (cuyas excepciones únicamente podrían producirse en los procedimientos de concesión directa) es su iniciación de oficio mediante el acto de convocatoria (artículo 23.1 LGS). Sin perjuicio de sus elementos reglados, el acto de convocatoria es un acto esencialmente discrecional: las bases reguladoras de las subvenciones no imponen a la Administración la obligación de convocarlas, sino que se limitan a habilitarla para poder hacerlo.

De acuerdo con la mejor y mayoritaria doctrina, este carácter discrecional excluiría la posibilidad de que el acto de convocatoria pudiera adoptarse mediante una actuación administrativa automatizada. En efecto, con carácter general, y no solo en relación con las subvenciones, la mayoría de los autores niegan que sea posible automatizar decisiones que resulten del ejercicio de potestades discrecionales⁷⁹, asumiendo, como mucho, la posibilidad de automatizar el ejercicio de potestades discrecionales de baja intensidad⁸⁰.

76. Cerrillo i Martínez (2021: 284).

77. Acosta Penco (2016). De hecho, así se ha reconocido también para la responsabilidad extracontractual entre privados ocasionada por el uso de robots, a partir de una curiosa interpretación de la Directiva 85/374/CEE y la posterior Directiva 1999/34/CE, relativa a la responsabilidad por los daños causados por productos defectuosos, según explica Marongiu (2018: 409).

78. Valero Torrijos (2019: 92).

79. Valero Torrijos (2007: 75), Cerrillo i Martínez (2019: 21), Moreno Rebato (2021: 119-122).

80. Izquierdo Carrasco (2022: 263-264) y, muy especialmente, Martín Delgado (2009a: 369-371). Cabe precisar, sin embargo, que este último autor no se refiere realmente al ejerci-

Yendo aún más lejos, Ponce Solé no se conforma con dudar de la posibilidad técnica de que una potestad discrecional pueda traducirse en una actuación automatizada, sino que incluso señala la necesidad de prohibirlo, a fin de garantizar la existencia de una “reserva de humanidad” en este ámbito⁸¹. Con indudable acierto, advierte de que todo ejercicio de una potestad discrecional exige, a fin de tener plenamente en cuenta todos los intereses en juego, una cierta empatía (no simpatía) en su titular, es decir, “tener la capacidad de ponerse en la piel de los interesados, participantes y posibles afectados por la futura decisión, pues solo así podrá ponderar correctamente, para el buen ejercicio de la discrecionalidad”. Dado que las máquinas no son capaces de empatía, el ejercicio de potestades discretionales por su parte siempre sería, por definición, defectuoso, por lo que debería prohibirse.

Esta parece ser la opción de la Ley alemana de procedimiento administrativo, que habría prohibido el uso de algoritmos para adoptar decisiones automatizadas que afecten a derechos de los ciudadanos cuando puedan tener un contenido discrecional⁸², y, dentro del ordenamiento español, lo mismo parece hacer el artículo 44.2 de la Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña.

Cabría, quizá, añadir que la empatía puede resultar un elemento irrenunciable en la adopción de decisiones con destinatarios determinados y concretos. No obstante, su relevancia podría ser menor en el caso de decisiones dirigidas a una pluralidad indeterminada de destinatarios en las que, justamente para alcanzar un carácter de generalidad, las situaciones concretas de cada ciudadano no exigen la misma atención. Casi cabría sostener lo contrario: la obligación de hacer caso omiso de situaciones concretas, precisamente para intentar adoptar una decisión tan general como sea posible. Ello abriría, tal vez, un cierto margen para el empleo de algoritmos lógicos en el ejercicio de ciertas potestades discretionales, y, por cuanto a nosotros interesa, permitiría, quizá, el uso de estos algoritmos para la determinación del momento más oportuno para adoptar el acto de iniciación del procedimiento, esto es, la convocatoria de las ayudas y la apertura del plazo para la presentación de solicitudes.

cio de potestades discretionales respecto a la adopción de la decisión, es decir, si se adopta o no una decisión y cuál debe ser su contenido, sino a la forma de apreciar si concurre o no el presupuesto de hecho marcado por la norma para poder actuar, lo que reconduce a la discrecionalidad técnica y a la posibilidad de parametrizar los criterios de valoración.

81. Ponce Solé (2019: 29-32).

82. Sobre el alcance de esta prohibición, véase Huergo Lora (2020: 79), quien estima que el uso de algoritmos sí es posible para la preparación de la decisión.

Piénsese, por ejemplo, en algunas ayudas sociales que con frecuencia establecen los ayuntamientos, como las ayudas para hacer frente a emergencias energéticas, y en la posibilidad, muy real, de que un algoritmo lógico, capaz de desarrollar procesos de aprendizaje autónomo, pudiera determinar por sí mismo en qué momento podría ser más útil convocarlas para la población, teniendo en cuenta no solo factores obvios (como el precio de la electricidad o el gas), sino también otros, nada evidentes, que pudieran revelar situaciones de necesidad social y cuya relevancia hubiera sido detectada por él mismo (v. gr., el conocido fenómeno “*lipstick*”, que permite establecer una correlación causal entre los momentos de recesión económica y el aumento en la venta de barras de labios).

A mi juicio, no sería ni técnicamente imposible ni jurídicamente inaceptable que algunas decisiones discrecionales en materia de subvenciones, como el acto de convocatoria (o, como mínimo, algunos elementos discrecionales de dicho acto), pudieran ser adoptadas mediante actuación automatizada basada en algoritmos lógicos. En especial, si se atiende a que la mayor parte del contenido de las convocatorias viene ya determinado por lo establecido en las bases reguladoras, según se deduce del mero cotejo entre los artículos 17.3 y 23.2 LGS.

4.3.2. Presentación de solicitudes y acreditación de requisitos. En especial, el uso de herramientas de *Self-Sovereign Identity* basadas en *blockchain*

Sin perjuicio de las especialidades que, nuevamente, puedan presentar algunos procedimientos de concesión directa de subvenciones, tras la convocatoria del procedimiento los interesados deberán presentar obligatoriamente sus solicitudes para participar en él (artículo 23.3 LGS). En el ámbito de la contratación pública, este es uno de los trámites donde mayor utilidad se ha encontrado al uso de tecnología *blockchain*, cuyo mejor ejemplo se encuentra, posiblemente, en el registro de las ofertas de contratos públicos del Gobierno de Aragón, que permite garantizar la integridad y la inmutabilidad de las ofertas presentadas⁸³. La presentación de las ofertas mediante su incorporación a la red *blockchain* permite que queden registradas mediante un *hash* que hace posible al resto de miembros de la red conocer la fecha y hora de presentación.

Pero, más allá del mero registro de las solicitudes, la tecnología *blockchain* podría ser utilizada para facilitar a los solicitantes el cumplimiento de otras cargas que acompañan a la presentación de sus solicitudes, como la acreditación

83. Ampliamente, Tejedor Bielsa (2020: 124-126).

de que se reúnen los requisitos necesarios para solicitar la subvención. En efecto, el artículo 13 LGS dispone que solo podrán ser beneficiarios de subvenciones las personas en quienes, por un lado, concurren las circunstancias previstas en las bases reguladoras y en la convocatoria [artículos 17.3.b) y 23.2.e) LGS], y, por el otro, no concurren las circunstancias enumeradas en los apartados 2 y 3 del mismo artículo 13 LGS (*v. gr.*, no estar al corriente en sus obligaciones con la Administración tributaria o la Seguridad Social, tener su domicilio en un paraíso fiscal, etc.). Es decir, si un ayuntamiento convoca ayudas para mujeres emprendedoras mayores de 45 años empadronadas durante más de cinco años en el municipio, las solicitantes deberán acreditar, además de su identidad, y simplemente para ser admitidas en el procedimiento, que son mujeres, emprendedoras, mayores de 45 años y que llevan más de cinco años empadronadas en dicho municipio. Igualmente, deberán acreditar que no concurre en ellas ninguna de las situaciones enunciadas en los artículos 13.2 y .3 LGS. Y deberá acreditarse, además, en la forma establecida en las bases y la convocatoria (artículo 23.3 LGS). Existe, por supuesto, el derecho a no presentar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración (artículo 28.2 LPAC). Pero, frecuentemente, ello no evitará la presentación de una abundante documentación.

Frente a esta situación, una de las más interesantes aportaciones de la tecnología *blockchain* es servir de base a sistemas de Identidad Soberana Personal o SSI – *Self-Sovereign Identity* –, cuya aplicación a este y otros tipos de procedimientos podría eliminar muchas de las cargas que se hacen recaer sobre los interesados, al ofrecer un sistema que permite acreditar la identidad y todo tipo de características de los usuarios de la red⁸⁴.

La SSI se configuraría como un archivo encriptado y descentralizado, mediante tecnología *blockchain*, en el que se guardarían para cada sujeto participante en la red (nodo) los datos generados por todo tipo de sujetos, tanto públicos como privados. Es decir, cada usuario (nodo) podría obtener e incorporar a su SSI credenciales o testimonios relativos a aspectos o datos vinculados a su identidad, sus cualidades o características, producidos por entidades que los habrían verificado previamente y que también formarían parte de la red. Además, el usuario mantendría el control sobre tales datos, pudiendo posteriormente, cuando y como lo deseara, presentarlos a terceros (o

84. Las ventajas de esta tecnología parecen ser unánimemente aceptadas. A título de ejemplo: Pereiro Cárceles (2019: 3), Alamillo Domingo (2019b: 59-62), Quintana Cortés (2020: 163) y Tejedor Bielsa (2020: 122).

permitir que los terceros pudieran acceder a ellos) para acreditar su identidad, cualidades o características. De esta forma, una SSI podría contener y acreditar todas las características que necesita conocer la Administración para determinar si alguien puede o no participar en un procedimiento, quien simplemente tendría que darle acceso a su identidad para acreditarlas⁸⁵.

Sin perjuicio de sus evidentes ventajas, la SSI presenta los mismos problemas que el resto de redes de *blockchain* y algunos propios, entre los que debe destacarse la espinosa cuestión de determinar quién puede incluir estas características en la identidad del sujeto para que tal información sea fiable. En efecto, *blockchain* asegura que los datos incluidos en un documento no han sido modificados, pero no puede asegurar que los datos sean auténticos, es decir, que sean conformes con la realidad. Simplemente son los datos que alguien ha puesto en un documento, sin más, “pero integridad no es autenticidad”⁸⁶. Esta situación requeriría que solo ciertos nodos pudieran validar las transacciones (modificaciones de los datos), lo que seguramente llevaría a que esta función fuera asumida por los nodos pertenecientes a la Administración⁸⁷. Pero esto eliminaría muchas de las ventajas de emplear redes *blockchain* y las convertiría, de hecho, en algo muy similar a otros sistemas, actualmente existentes, basados en el intercambio de datos entre administraciones. Tal es, justamente, uno de los principales fines que cumple la Base de Datos Nacional de Subvenciones, de conformidad con lo establecido en el artículo 20 LGS y en el Real Decreto 130/2019, de 8 de marzo, por el que se establece su regulación, cuyo funcionamiento no requiere nada similar a la tecnología de registro distribuido.

En cualquier caso, el uso de la tecnología *blockchain* para la identificación digital ante las administraciones públicas españolas se encuentra actualmente bloqueado, tras las modificaciones introducidas en los artículos 9.2.c) y 10.2.c) y en la disposición adicional sexta de la LPAC por parte del Real Decreto-ley

85. Alamillo Domingo (2020: 268-269) ha señalado que el derecho reconocido en el artículo 28.3 LPAC, y conocido como “*only once principle*” en la normativa europea, no parece adaptarse plenamente a la SSI. En efecto, la SSI requiere que sea el propio sujeto quien, en cada caso, dé acceso a la Administración a sus datos, lo que puede interpretarse como una nueva forma de entregarlos (en realidad, ponerlos a su disposición).

86. Pereiro Cárceles (2019: 10) y Quintana Cortés (2020: 168), quien plantea estos problemas en relación con los datos de los licitadores en la contratación pública.

87. En este sentido, Atzori (2018: 7). De hecho, con carácter general, Quintana Cortés (2020: 159) da por descontado que, al menos hasta que la tecnología alcance un grado de madurez más avanzado y exista un marco jurídico claro, las administraciones públicas se decantarán, en caso de utilizar tecnología *blockchain*, por redes privadas a efectos de controlar las validaciones y registros.

14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones⁸⁸.

Por un lado, se ha incluido en el artículo 9.2.c) LPAC la necesidad de obtener una autorización “por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior” como requisito previo para que las administraciones españolas puedan aceptar sistemas de clave concertada u otros sistemas distintos, entre los que se incluirían los sistemas basados en tecnologías de registro distribuido⁸⁹.

Por otro lado, la nueva disposición adicional sexta [“Sistemas de identificación y firma previstos en los artículos 9.2 c) y 10.2 c)”] ha establecido que “no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del derecho de la Unión Europea”. Esto es, se ha establecido una moratoria *sine die* para el uso de estas herramientas ante las administraciones públicas en tanto no se apruebe una regulación específica.

4.4. Fases de instrucción y resolución del procedimiento de concesión de subvenciones

Muchos de los actos de trámite incluidos en la fase de instrucción del procedimiento de concesión de subvenciones pueden ser y, de hecho, son en ocasiones convertidos en actuaciones administrativas automatizadas. Así puede ocurrir, por ejemplo, con la emisión automática de las resoluciones declarando el desistimiento de algunos interesados que no han subsanado sus solicitudes. Por ejemplo, cuando fueron requeridos para aportar nueva documentación y esta no se ha subido a la aplicación en plazo, lo que puede ser comprobado por la

88. Tejedor Bielsa (2020: 122) advierte, entre otros, de la incoherencia de este bloqueo frente al apoyo más abierto y decidido en el ámbito de la UE al uso de la SSI como requisito clave del mercado único digital. Tal vez por eso autores como Quintana Cortés (2020: 163) siguen expresando su confianza absoluta en que la SSI acabará imponiéndose como tecnología utilizada en las relaciones con la Administración.

89. En sentido similar se expresa también ahora el artículo 10.2.c) LPAC, si bien respecto a los sistemas de firma admitidos por las administraciones públicas.

propia aplicación sin intervención humana y generar tanto la correspondiente resolución como su notificación automática.

4.4.1. La concesión directa de subvenciones. Remisión

Como he desarrollado en otro sitio, la principal característica de la concesión directa de subvenciones, lo que permite distinguirla del procedimiento de concurrencia competitiva, se encuentra en la ausencia de competición entre los solicitantes y la correlativa ausencia de comparación entre sus solicitudes. De esta forma, en la concesión directa es posible proceder al otorgamiento de subvenciones a cada beneficiario sin tener en cuenta a los demás: todos y cada uno de los solicitantes podrán ser beneficiarios de la correspondiente subvención simplemente con cumplir los requisitos marcados por la norma, con independencia de que haya o deje de haber otros solicitantes y de sus posibles méritos, dado que ellos también recibirán (o no) su correspondiente subvención atendiendo exclusivamente a sus propias características y no a las de los demás⁹⁰.

Se deduce de esto que aquellas subvenciones que deban otorgarse mediante un procedimiento de concesión directa solo requerirán la acreditación, por parte del solicitante, y la comprobación, por parte de la Administración concedente, de que aquel reúne los requisitos establecidos por la norma para convertirse en beneficiario de la ayuda. De esta forma, el derecho a recibir la subvención se confunde, en estos casos, con el derecho a ser admitido en el procedimiento como solicitante, del que nos hemos ocupado en el apartado anterior y al que ahora debemos remitirnos. En consecuencia, en la medida en que la verificación de que se reúnen los requisitos exigidos por la norma y la convocatoria pueda realizarse automáticamente, la concesión podría ser igualmente automática. Así podría ocurrir con buena parte de las ayudas sociales.

Las principales dificultades radicarán en el uso de conceptos jurídicos indeterminados para la descripción de tales requisitos. Es la presencia de estos conceptos en la descripción del presupuesto de hecho al que se anuda esta potestad reglada lo que dificultará la automatización de esta actuación⁹¹.

90. Bueno Armijo (2017a: 278). Así debe entenderse, a pesar de los equívocos términos usados por el legislador en la exposición de motivos §.3 de la LGS, indicando que el procedimiento de concesión directa se caracteriza “por la no exigencia del cumplimiento de los principios de publicidad y concurrencia”.

91. Gallone (2019: 211).

De igual forma, la denegación de la subvención por no reunir los requisitos necesarios para convertirse en beneficiario, cuando estos puedan ser objeto de comprobación mecánica, también podría adoptarse mediante una actuación automatizada⁹².

4.4.2. La concesión de subvenciones mediante concurrencia competitiva

Frente al procedimiento de concesión directa de subvenciones, el procedimiento de concesión en concurrencia competitiva exige una tramitación más compleja, pues no basta con la simple acreditación de que se reúnen los requisitos para ser beneficiario de la subvención. Junto con ello, es necesario acreditar también que se reúnen todos o alguno de los méritos establecidos por las bases reguladoras. Tales méritos serán objeto de valoración para cada solicitante, lo que permitirá asignar una puntuación a sus respectivas solicitudes y establecer, sobre esta base, una prelación entre ellas, tal y como exige el artículo 22.1 LGS.

Las posibilidades de automatizar estas operaciones, a partir del uso de algoritmos aritméticos y relaciones, son muy reales. Así lo demuestran las experiencias desarrolladas en materia de contratación, donde cuentan con la base normativa expresa del artículo 159.6.d) LCSP para el procedimiento abierto simplificado: “La valoración de las ofertas se podrá efectuar automáticamente mediante dispositivos informáticos, o con la colaboración de una unidad técnica que auxilie al órgano de contratación”.

La principal dificultad se encuentra, nuevamente, en que la automatización exige la conversión de la realidad en datos: es decir, será necesario, en primer lugar, que la Administración compruebe la existencia de cada uno de los méritos alegados y acreditados (*v. gr.*, existencia de hijos a cargo del solicitante); en segundo lugar, que compruebe sus características (*v. gr.*, número y edad de los hijos); finalmente, que se les asigne la puntuación correspondiente de acuerdo con lo que establezcan las bases reguladoras (*v. gr.*, 2 puntos por hijos de hasta 12 años de edad; 1 punto por hijos de hasta 18 años de edad).

Una dificultad añadida para la automatización de este trámite se encuentra en la exigencia de que sea un órgano colegiado el que realice

92. Así lo acepta expresamente Tarrés Vives (2012: 461), quien usa este supuesto, justamente, como ejemplo de actuación reglada que podría traducirse en una decisión adoptada de forma automatizada.

la valoración de las solicitudes (artículo 22.1.2.º LGS). Sin embargo, esta exigencia no parece un obstáculo insuperable. Por un lado, el propio precepto permite excepcionarla atendiendo a “las especialidades que pudieran derivarse de la capacidad de autoorganización de las administraciones públicas”, lo que podría interpretarse como algo más que una simple habilitación a las comunidades autónomas para eliminar esta garantía⁹³. Por otra parte, podría bastar con que el algoritmo empleado (en rigor, algo mucho más sencillo: la fórmula aplicable) fuera validado por dicho órgano colegiado, sin perjuicio de la competencia del órgano al que hace referencia el artículo 41.2 LRJSP.

Esta validación no constituiría un mero formalismo huero, sino que supondría la confirmación de que el resultado alcanzado por el algoritmo es exactamente el mismo que el que habría alcanzado el órgano colegiado en caso de que las actuaciones materiales de valoración las hubieran realizado sus miembros personalmente. Dicho en otros términos: que no hubiera sido posible alcanzar otro resultado distinto y que, en consecuencia, es imposible que se haya podido vulnerar ninguno de los derechos subjetivos o intereses legítimos de los participantes en el procedimiento. A estos efectos, puede ser útil recordar que en el procedimiento de concesión de subvenciones en concurrencia competitiva la Administración no ejerce una potestad discrecional, sino reglada. Como hemos repetido, las dificultades se encontrarán en los juicios de valor sobre los presupuestos de hecho, lo que se vincula, más bien, a la existencia de conceptos jurídicos indeterminados y los casos de discrecionalidad técnica⁹⁴.

Aceptado lo anterior, y cuando se reunieran los requisitos necesarios, la Administración podría utilizar un algoritmo, integrado en el programa encargado de la tramitación del procedimiento, que elaborase una propuesta de resolución. De hecho, esta actuación automatizada podría sustituir tanto a la actuación del órgano colegiado (insistimos, siempre que haya validado, previamente, el algoritmo) como a la actuación del órgano instructor: de conformidad con el artículo 24.4 LGS, la intervención del órgano colegiado se limita, una vez evaluadas las solicitudes, a “emitir informe en el que se concrete el resultado de la evaluación efectuada”,

93. Silva Urién (2004: 194) y Laguna de Paz (2004: 341).

94. Quintana Cortés (2020: 171) reconoce en este sentido, refiriéndose a la valoración de ofertas de contratistas, que estas valoraciones no siempre son fácilmente reducibles a un código informático. Pero nada tiene ello que ver con el ejercicio de potestades discrecionales, como sostiene Pereiro Cárceles (2019: 7-8 y 24).

correspondiendo al órgano instructor, a la vista del expediente y del informe del órgano colegiado, formular la propuesta de resolución, que debe estar “debidamente motivada”. Ambos trámites, sin embargo, podrían quedar reducidos a uno solo.

El mismo artículo 24.4 LGS dispone que la propuesta de resolución formulada por el órgano instructor tendrá el carácter de propuesta de resolución provisional, debiendo notificarse a los interesados y abriendo un plazo de 10 días para que puedan presentar las alegaciones que estimen oportunas. Dicha notificación, que normalmente adoptará la forma de publicación, también podría hacerse automáticamente. Y, pasados esos 10 días sin que se presentara alegación alguna en la aplicación, esta podría emitir automáticamente la propuesta de resolución o, incluso, la resolución misma.

4.5. El control administrativo y financiero de subvenciones

El uso de la inteligencia artificial parece especialmente indicado para la planificación de controles administrativos que permitan detectar incumplimientos por parte de los administrados, así como malas prácticas o incluso casos de corrupción administrativa. El análisis masivo de datos sin ideas preconcebidas permite encontrar vínculos insospechados entre distintos hechos, descubrir pautas y repeticiones y, en consecuencia, formular predicciones que pueden ser muy precisas. Así ocurre desde hace años, como es conocido, en el ámbito tributario⁹⁵. De la misma manera se podría actuar en relación con el control administrativo y financiero de las subvenciones⁹⁶.

Este tipo de análisis basados en la inteligencia artificial podrían emplearse para acotar líneas de subvenciones, grupos de beneficiarios o

95. Por ejemplo, la Resolución de 19 de enero de 2021, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se aprueban las directrices generales del Plan Anual de Control Tributario y Aduanero de 2021 (BOE n.º 27, de 1 de febrero de 2021), señala: “En los últimos años, la Agencia Tributaria ha impulsado la captación de nuevas fuentes de información, las cuales, unidas a herramientas masivas de tratamiento de datos (...) han hecho posible efectuar de manera sistemática el análisis de residencia, sobre contribuyentes que figuran como no residentes en las bases de datos tributarias. Este análisis ha permitido obtener, en su caso, los indicios necesarios para poder determinar la presencia durante más de 183 días en territorio español, la existencia en nuestro país de un centro de intereses económicos relevante y operativo, así como la existencia de relaciones familiares que permitan inferir la residencia en España”.

96. Cotino Hueso (2021: 185).

tipos de prácticas en los que exista una mayor probabilidad de identificar irregularidades. De hecho, el uso de inteligencia artificial para la detección de casos de fraude o irregularidades en materia de subvenciones conoce ya un buen número de ejemplos, aunque no es seguro que sus resultados sean siempre satisfactorios⁹⁷.

Como ya adelantamos, en todo caso se trataría de actuaciones materiales situadas en un momento muy embrionario de la actuación administrativa, dado que se situarían no solo en un momento anterior al inicio de un procedimiento administrativo, sino en un momento previo, incluso, a otras actuaciones materiales que, en su caso, podrían llevar al inicio de un procedimiento administrativo. Este carácter tan previo o embrionario puede ayudar a superar el juicio de proporcionalidad respecto a la limitación de derechos que suponen estas actuaciones, que, en última instancia, cabe reconducir a la elaboración de perfiles mediante el tratamiento automatizado de datos⁹⁸. Pero no siempre será suficiente.

Así parece deducirse del asunto *SyRI* (*Systeem Risico Indicatie* o Sistema de Indicación del Riesgo)⁹⁹, en el que el Tribunal de Distrito de La Haya (Países Bajos) se pronunció, mediante su sentencia de 5 de febrero de 2020 (ECLI:NL:RBDHA:2020:865), sobre la conformidad a derecho de este programa informático, usado, sobre todo, por parte de la Administración local, para detectar distintas formas de fraude, incluyendo el fraude a las ayudas sociales y el fraude fiscal.

SyRI establecía patrones o modelos de riesgo a partir de grandes conjuntos de datos y, tras compararlos con los expedientes de personas concretas, determinaba si en tales personas concurrían riesgos de ser defraudadores fiscales o de estar percibiendo indebidamente prestaciones sociales. La sentencia, que no fue objeto de recurso por parte del Gobierno, declaró que el programa *SyRI* era contrario al artículo 8 CEDH por suponer una limitación desproporcionada del derecho a la vida privada a través del uso

97. Tal parece que fue el caso del polémico *SyRI* neerlandés, del que nos ocuparemos a continuación: una investigación periodística llevada a cabo en 2019 reveló que esta aplicación aún no había sido capaz de revelar ni un solo caso de fraude. Meuwese (2020: 211).

98. Así pareció entenderlo el Consejo Constitucional francés en su decisión de 27 de diciembre de 2019 (2019-796 DC), en relación con el artículo 154 de la Ley de Presupuestos para 2020 y el tratamiento de datos en plataformas digitales con el fin de evitar la evasión fiscal. Véanse Goerlich Peset (2021: 35) y Calderón Carrero (2020).

99. Al respecto, Moreno Rebato (2021: 67-69) y, muy especialmente, Meuwese (2020), quien destaca que la sentencia, lejos de cerrar el debate sobre el uso de este tipo de sistemas, más bien se limita a plantear los términos en los que dicho debate continuará.

de nuevas tecnologías y, en particular, porque su normativa reguladora y su funcionamiento no resultaban ni transparentes ni verificables.

En principio, el modelo considerado en abstracto, sus objetivos y sus medios, se estimaron útiles y conformes a la ley. El problema se situaba, más bien, en el funcionamiento concreto del sistema, que no pudo verificarse. Fundamentalmente, porque el Gobierno no quiso revelar al Tribunal todas las especificaciones relativas al funcionamiento de *SyRI*, los indicadores de riesgo y el modelo de riesgo que se utilizaban, argumentando que se quería evitar que los ciudadanos pudieran adaptar su comportamiento al mecanismo de control (*gaming the algorithm*). Esto impidió al Tribunal, por ejemplo, aclarar si el programa contenía sesgos que perjudicaran a clases sociales más desfavorecidas o a grupos de inmigrantes, como denunciaban las partes demandantes. A juicio del Tribunal, la opacidad de estas normas impedía a los ciudadanos conocer si sus datos se habían procesado de manera correcta, haciendo muy difícil que pudieran defenderse frente a la elaboración de informes de riesgo.

A estos efectos, resultaba irrelevante que la decisión concreta de iniciar actuaciones de inspección la realizaran funcionarios tras comprobar si los resultados del análisis de *SyRI* eran “falsos positivos” o “falsos negativos”. El problema se situaba en que no resultaba posible saber si la selección previa se había realizado correctamente o no, si contenía sesgos o no, si era discriminatoria o no.

Más allá del artículo 8 CEDH, la normativa de referencia respecto a la elaboración de perfiles mediante tratamiento automatizado de datos viene establecida por el ya citado artículo 22 RGPD. Este artículo no solo prohíbe que un interesado sea objeto de una decisión, basada en la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar (artículo 22.1 RGPD), sino que excluye que se puedan usar para elaborarlo datos de categorías especiales (artículo 22.4 RGPD), a lo que cabe sumar la prohibición, formulada en el Considerando 71 RGPD, de que estas decisiones puedan afectar a menores.

No obstante, no se trata de prohibiciones absolutas. Para empezar, estas garantías no se aplican a las personas jurídicas (artículo 1 RGPD). Asimismo, deben tenerse en cuenta las excepciones previstas en los artículos 9.2.g), 22.2 y, muy especialmente, 23.e) y h) RGPD.

Todo ello permite afirmar que el RGPD ofrece margen suficiente para la aprobación de normas que permitan desarrollar actuaciones administrativas automatizadas de control de subvenciones¹⁰⁰.

4.6. La iniciación del procedimiento de reintegro de subvenciones y del procedimiento administrativo sancionador

Basten, para concluir, unos últimos apuntes sobre las eventuales consecuencias de los incumplimientos del beneficiario, así como sobre su posible plasmación en nuevas formas de actuación administrativa automatizada. También en este ámbito cabe identificar algunos actos de trámite secundarios cuya automatización no solo es posible, sino una realidad. Tal es el caso del requerimiento previo al incumplimiento definitivo de la obligación de presentar la justificación de la subvención en plazo (artículo 70.3 Real Decreto 887/2006, Reglamento de la LGS): la superación del plazo originario sin haber subido documentación alguna a la aplicación informática permitiría a esta la emisión automática del requerimiento y la ampliación del plazo de presentación de la justificación en quince días, tal y como determina el citado precepto.

Pero, junto a ello, resulta más interesante señalar la existencia de algunas causas de reintegro cuya comprobación puede realizarse mediante una actuación automatizada, sin intervención humana, lo que permitiría dar inicio, también de manera automatizada, al procedimiento de reintegro. El mejor ejemplo sería, nuevamente, la falta de presentación de la justificación de la subvención en plazo, una vez agotado el plazo adicional de quince días [artículo 37.1.c) LGS].

Es interesante observar que aquí no existe riesgo de sesgos discriminatorios, porque la máquina no elige contra quién se dirige el procedimiento ni los motivos de hacerlo: la decisión ya fue adoptada por el legislador y el algoritmo se limita a trasladarla, sin margen alguno de apreciación.

De manera similar, es posible identificar algunas infracciones en materia de subvenciones que podrían dar lugar al inicio automático de un procedimiento

100. De especial interés, en este sentido, resulta la Ley valenciana 22/2018, de 6 de noviembre, de Inspección General de Servicios y del sistema de alertas para la prevención de malas prácticas en la Administración de la Generalitat y su sector público instrumental y, destacadamente, su modélica disposición adicional tercera.

administrativo sancionador contra sus presuntos autores. Para ello serían necesarios dos requisitos:

En primer lugar, debe tratarse de conductas que permitan, por su propia naturaleza, ser traducidas a una estructura binaria que pueda ser trasladada al lenguaje de las máquinas. Por ejemplo, ello no sería posible en el caso de la infracción consistente en la “resistencia, obstrucción, excusa o negativa a las actuaciones de control financiero”: artículo 56.g) LGS.

En segundo lugar, debe tratarse de conductas que puedan ser detectadas sin necesidad de intervención humana, esto es, que no requieran “un proceso de investigación previa e individualizada”¹⁰¹. Por ejemplo, ello no sería posible en el caso de la infracción consistente en la “presentación de cuentas justificativas inexactas o incompletas”: artículo 56.b) LGS.

Cuando ambos requisitos concurren, no sería imposible la iniciación automatizada del procedimiento. Tal podría ser el caso de la infracción leve tipificada en el artículo 56.a) LGS, consistente en la “presentación fuera de plazo de las cuentas justificativas de la aplicación dada a los fondos percibidos”; o de la infracción grave tipificada en el artículo 57.a) LGS como el “incumplimiento de la obligación de comunicar al órgano concedente o a la entidad colaboradora la obtención de subvenciones, ayudas públicas, ingresos o recursos para la misma finalidad (...)”¹⁰².

De hecho, en otros ámbitos administrativos se acepta ya la posibilidad de actuaciones administrativas automatizadas que inician expedientes sancionadores. Así ocurre en el ámbito de la Seguridad Social, donde el artículo 53.1.a) LISOS se refiere, expresamente, a la posibilidad de que existan actas de infracción de la Inspección de Trabajo y Seguridad Social “extendidas en el marco de actuaciones administrativas automatizadas”, lo que daría lugar al inicio del procedimiento sancionador¹⁰³.

101. Izquierdo Carrasco (2022: 285), en relación con el inicio automatizado de procedimientos sancionadores por la comisión de infracciones en el orden social.

102. Y, seguramente, cabe decir lo mismo respecto de la infracción tipificada en el artículo 57.c) LGS, consistente en “[l]a falta de justificación del empleo dado a los fondos recibidos una vez transcurrido el plazo establecido para su presentación”.

103. Dicho procedimiento se encuentra ahora regulado en un nuevo “Capítulo IX. Del procedimiento sancionador promovido por actuación administrativa automatizada en el ámbito de la Administración General del Estado”, introducido por el Real Decreto 688/2021, de 3 de agosto, por el que se modifica el Reglamento general sobre procedimientos para la imposición de sanciones por infracciones de orden social y para los expedientes liquidatorios de cuotas de la Seguridad Social, aprobado por el Real Decreto 928/1998, de 14 de mayo.

Aún más, a falta de presentación de alegaciones, estos actos de iniciación podrían considerarse propuesta de resolución cuando contengan un pronunciamiento preciso acerca de la responsabilidad imputada [artículo 64.2.f) LPAC].

5. Bibliografía

- Acosta Penco, T. (2016). La responsabilidad patrimonial de la Administración por información errónea en la doctrina del Consejo de Estado. *Revista Digital de Derecho Administrativo*, 15, 233-264.
- Alamillo Domingo, I. (2019a). *Identificación, firma y otras pruebas electrónicas. La regulación jurídico-administrativa de la acreditación de las transacciones electrónicas*. Cizur Menor: Thomson Reuters Aranzadi.
- (2019b). Las tecnologías de registro distribuido (*blockchain*) y la transformación del procedimiento administrativo. *El Consultor de los Ayuntamientos*, 1, 57-65.
 - (2020). El régimen jurídico de la administración digital: aspectos tecnológicos, plataformas y servicios de intermediación. En I. Martín Delgado (dir.). *El procedimiento administrativo y el régimen jurídico de la Administración pública desde la perspectiva de la innovación tecnológica* (pp. 225-276). Madrid: Iustel.
- Alonso Suárez, L. (2018). *Blockchain* en la Administración pública. En C. García Novoa y D. Santiago Iglesias (dirs.). *4.ª revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital* (pp. 477-498). Cizur Menor: Thomson Reuters Aranzadi.
- Asís Roig, R. de (2018). Robótica, inteligencia artificial y derecho. *Revista de privacidad y derecho digital*, 3 (10), 27-77.
- Atzori, M. (2018). Blockchain governance and the role of trust service providers: the trusted chain network. *The Journal of the British Blockchain Association*, 1, 1-17.
- Ávila Orive, J. L. (2005). Las entidades colaboradoras. En G. Fernández Farreres (dir.). *Comentario a la Ley General de Subvenciones* (pp. 225-261). Madrid: Thomson Civitas.
- Blockchain. The future of trust? (2018). *MIT Technology Review*, 121 (3), mayo 2018.

Específicamente sobre los problemas que tales actas plantean, véanse los acertados análisis de Izquierdo Carrasco (2022) y Goerlich Peset (2021, 27-31).

Bueno Armijo, A. (2011). *El reintegro de subvenciones de la Unión Europea*. Sevilla: Instituto Andaluz de Administración Pública.

- (2013). Los efectos de la caducidad del procedimiento de control financiero de subvenciones sobre la potestad de reintegro. *Revista española de control externo*, 15 (43), 125-144.
- (2017a). La concesión directa de subvenciones. *Revista de Administración Pública*, 204, 269-312.
- (2017b). De nuevo sobre la caducidad del procedimiento de control financiero de subvenciones y sus efectos sobre el reintegro. Nota a la STS de 2 de noviembre de 2016. *Revista española de control externo*, 19 (55), 135-150.
- (2019). La actividad administrativa de fomento. En M. Rebollo Puig y D. Vera Jurado (dirs.). *Derecho Administrativo. Tomo III. Modos y medios de la actividad administrativa*. Madrid: Tecnos.

Calderón Carrero, J. M. (2020). El encuadramiento legal y límites del uso de herramientas de inteligencia artificial con fines de control fiscal [Análisis de la decisión del Consejo Constitucional francés de 27 de diciembre de 2019 (Décision n.º 2019-796 DC), sobre la Ley de Presupuestos 2020]. *Estudios financieros. Revista de contabilidad y tributación*, 444, 119 y ss.

Casey, M. J. y Vigna, P. (2018a), *La macchina della verità. La blockchain e il futuro di ogni cosa*. Milán: FrancoAngeli.

- (2018b). In blockchain we trust. *Blockchain. The future of trust? MIT Technology Review*, 121 (3), 9 de abril.

Cerrillo i Martínez, A. (2019). El impacto de la inteligencia artificial en el derecho administrativo, ¿nuevos conceptos para nuevas realidades técnicas? *Revista General de Derecho Administrativo*, 50.

- (2021). Robots, asistentes virtuales y automatización de las administraciones públicas. *Revista Galega de Administración Pública*, 61, 271-309.

Cortés, Ó. (2020). Algoritmos y algunos retos jurídico-institucionales para su aplicación en la Administración pública. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 18, 54-63.

Cotino Hueso, L. (2021). Hacia la transparencia 4.0: el uso de la inteligencia artificial y *big data* para la lucha contra el fraude y la corrupción y las (muchas) exigencias consti-

- tucionales. En C. Ramío Matas (coord.). *Repensando la administración digital y la innovación pública* (pp. 169-196). Madrid: INAP.
- EU Blockchain Observatory and Forum. (2018). *Blockchain and the GDPR*. Disponible en: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (última consulta: 03/12/2021).
- Fernández Farreres, G. (2005). La aplicabilidad de la Ley general de subvenciones a las entidades locales y, en particular, a las diputaciones provinciales en el ejercicio de sus competencias de cooperación económica a los municipios. *Cuadernos de Derecho Local (QDL)*, 5, 7-33.
- (2012). Subvenciones y ayudas económicas en tiempos de crisis. *Revista Española de Derecho Administrativo*, 154, 19-48.
- Gallone, G. (2019). Blockchain, procedimenti amministrativi e prevenzione della corruzione. *Il Diritto dell'economia*, año 65, 100 (3/2019), 187-212.
- (2020). Public Administration and the challenge of contractual automation. Notes on smart contracts. *European Review of Digital Administration and Law*, 1 (1-2), 179-195.
- García Melián, J. C. (2019). Blockchain y contratación pública estratégica. *Contratación administrativa práctica*, 159.
- Gil González, E. (2017). Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías *big data* y de aprendizaje computacional. *Revista Española de la Transparencia*, 5, 164-179.
- Goerlich Peset, J. M.^a (2021). Decisiones administrativas automatizadas en materia social: algoritmos en la gestión de la Seguridad Social y en el procedimiento sancionador. *Labor*, 2 (2), 22-42.
- Huergo Lora, A. (2020). Una aproximación a los algoritmos desde el derecho administrativo. En A. Huergo Lora (dir.) y G. M. Díaz González (coord.). *La regulación de los algoritmos* (pp. 23-87). Thomson Reuters Aranzadi.
- Izquierdo Carrasco, M. (2022). Actuaciones automatizadas en la sanción de irregularidades en el orden social. En L. Cotino Hueso y A. Todolí Signes (coord.). *Explotación y regulación del uso del big data e inteligencia artificial para los servicios públicos y la ciudad inteligente* (pp. 261-286). Valencia: Tirant lo Blanch.
- Laguna de Paz, J. C. (2004). El otorgamiento de subvenciones. En G. Fernández Farreres (dir.). *Comentario a la Ley General de Subvenciones* (pp. 329-354). Madrid: Thomson Civitas.

- Marongiu, D. (2018). Inteligencia artificial y administración pública. En C. García Novoa y D. Santiago Iglesias (dirs.). *4.ª revolución industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital* (pp. 385-411). Cizur Menor: Thomson Reuters Aranzadi.
- Martín Delgado, I. (2009a). Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada. *Revista de Administración Pública*, 180, 353-386.
- (2009b). La administración electrónica como problema actual para la investigación y la docencia en el derecho administrativo. *Revista Aragonesa de Administración Pública*, Extra 11, 355-375.
- Martínez Gutiérrez, R. (2009). *Administración pública electrónica*. Cizur Menor: Civitas Thomson Reuters.
- Merchán Murillo, A. (2019). Inteligencia artificial y *blockchain*: retos jurídicos en paralelo. *Revista General de Derecho Administrativo*, 50.
- Meuwese, A. (2020). Regulating algorithmic Decision-making one case at the time: a note on the Dutch *SyRI* judgment. *European Review of Digital Administration and Law*, 1 (1-2), 209-211.
- Moreno Rebato, M. (2021). *Inteligencia artificial (umbrales éticos, derecho y administraciones públicas)*. Cizur Menor: Thomson Reuters Aranzadi.
- OCDE (2021). *Recommandation du Conseil sur l'intelligence artificielle*. Instruments juridiques de l'OCDE.
- Pereiro Cárceles, M. (2019). La utilización del *blockchain* en los procedimientos de concurrencia competitiva. *Revista General de Derecho Administrativo*, 50.
- Ponce Solé, J. (2019). Inteligencia artificial, derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico. *Revista General de Derecho Administrativo*, 50.
- Quintana Cortés, J. L. (2020). La tecnología *blockchain* y su pretendida aplicación a la contratación pública como mecanismo para lograr mayor integridad. *Revista Española de Control Externo*, XXII (64), 152-173.
- Rebollo Puig, M. (2019). La actividad administrativa. En M. Rebollo Puig y D. Vera Jurado (dirs.). *Derecho Administrativo. Tomo I* (pp. 61-84). Madrid: Tecnos.
- Sáez Lara, C. (2020a). Algoritmos y discriminación en el empleo: un reto para la normativa antidiscriminatoria. *Nueva revista española de derecho del trabajo*, 232, 83-126.

- (2020b). El algoritmo como protagonista de la relación laboral. Un análisis desde la perspectiva de la prohibición de discriminación. *Temas laborales: Revista andaluza de trabajo y bienestar social*, 155, 41-60.
- Silva Urién, I. (2004). Artículo 22. Procedimientos de concesión. En J. del Barco Fernández-Molina, A. Panizo García, I. Silva Urién y P. Arellano Pardo. *Comentarios prácticos a la nueva Ley General de Subvenciones* (pp. 186-195). Valladolid: Lex Nova.
- Swan, M. (2015). *Blockchain. Blueprint for a New Economy*. Sebastopol: O'Really Media.
- Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2 (9).
- Tapscott, D. y Tapscott, A. (2016). *Blockchain revolution: how the technology behind Bitcoin is changing money, business and the world*. Londres: Portfolio.
- Tarrés Vives, M. (2012). Actuación administrativa automatizada. En J. Tornos Mas (coord.). *Comentarios a la Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña* (pp. 447-465). Madrid: Iustel.
- Tejedor Bielsa, J. (2020). Transformación digital, *blockchain* e inteligencia artificial en la Administración pública. *Revista Española de Derecho Administrativo*, 209, 111-138.
- Valero Torrijos, J. (2007). *El régimen jurídico de la e-administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo común* (2.ª ed.). Granada: Comares.
- (2015). La reforma de la administración electrónica, ¿una oportunidad perdida? *Revista Española de Derecho Administrativo*, 172, 13-23.
 - (2019). Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena Administración. *Revista Catalana de Dret Públic*, 58, 82-96.
- Vestri, G. (2021). La inteligencia artificial ante el desafío de la transparencia algorítmica: Una aproximación desde la perspectiva jurídico-administrativa. *Revista Aragonesa de Administración Pública*, 56, 368-398.
- Wanden-Berghe Lozano, J. L. y Fernández Daza, E. (2020). Blockchain: instrumento de transparencia y control del sector público. *Revista Española de Control Externo*, XXII (64), 132-149.
- Wüst, K. y Gervais, A. (2018). Do you need a Blockchain? *CVCBT*, 45-54.
- Zlotnik, A. (2019). Inteligencia artificial en las administraciones públicas: definiciones, evaluación de viabilidad de proyectos y áreas de aplicación. *Boletic*, 84, 24-32.

Gestión tributaria: *blockchain* y otras nuevas tecnologías

José Pedreira Menéndez¹

Catedrático de Derecho Financiero y Tributario.

Universidad de Oviedo

SUMARIO. 1. Introducción. 2. La tecnología *blockchain* y su aplicación en el ámbito tributario. 3. La protección de la privacidad de los datos fiscales y las limitaciones al uso de la tecnología *blockchain*. 4. El uso de otras nuevas tecnologías en los procedimientos tributarios. 5. Conclusiones. 6. Bibliografía.

1. Introducción

En este capítulo vamos a analizar la influencia que las nuevas tecnologías que se están desarrollando en el ámbito de internet pueden tener sobre la gestión tributaria, entendida en un concepto amplio, y, en especial, sobre su posible aplicación en el ámbito de las Haciendas locales. Debemos partir del hecho de que la gestión tributaria local, muchas veces, está cedida a órganos administrativos de carácter supramunicipal, por los costes que conlleva y la insuficiencia de personal para poder abordarla. Las nuevas tecnologías informáticas pueden permitir una recuperación de estas competencias a los

1. Este trabajo se desarrolla dentro del marco del Proyecto de investigación financiado por el Ministerio de Ciencia e Innovación: “El desafío de la buena administración tributaria en un entorno digital” (PID2020-116096RB-I00).

ayuntamientos, aunque veremos que el proceso aún presenta una serie de condicionantes tecnológicos y jurídicos.

La obra en la que se enmarca este trabajo se centra en la tecnología DLT (*Distributed Ledger Technology*) y el *blockchain*, aunque veremos que también existen otros avances informáticos que pueden tener relevancia para la gestión tributaria local. Hasta la creación de la tecnología DLT, cualquier transacción *online* dependía de un intermediario (por ejemplo, una Administración o un banco) que asegurara de manera centralizada que la transferencia de información o activos se había efectuado correctamente, lo que suponía que un número reducido de intermediarios asumían el poder de gestionar grandes cantidades de datos personales, así como el riesgo que conlleva asegurar que el sistema central no sea víctima del “pirateo”. En consecuencia, las tecnologías DLT, en principio, surgen como una alternativa al sistema tradicional de control centralizado, permitiendo controlar las transacciones de datos de manera descentralizada a través de una red con miles de ordenadores conectados, dificultando la posibilidad de pirateo y facilitando a los usuarios interactuar a través de un sistema de transacciones persona-a-persona (*peer-to-peer* o P2P). El desarrollo de esta tecnología ha permitido el salto del internet de la información al internet del valor; ya no solo se transmite información de manera directa, sino que con este cambio puede transmitirse cualquier cosa de valor. Si bien es cierto que este sistema de transmisión de los bienes y derechos puede generar un nuevo ámbito de actividad para el derecho financiero y tributario, al tener que controlar y someter a gravamen este tipo de operaciones, en el presente trabajo no queremos analizar esto, sino cómo esta nueva tecnología también puede influir en los procedimientos tributarios y, especialmente, en los que se utilizan en el ámbito de la gestión de las Haciendas locales².

Como ya se ha indicado en anteriores apartados de esta obra, la tecnología *blockchain* puede incumplir sus postulados iniciales en cuanto a su distribución e inmutabilidad, sobre todo cuando las redes no son totalmente abiertas, de ahí que debemos tener cierta cautela sobre su utilización en el ámbito del ejercicio de potestades públicas y, sobre todo, dentro de los distintos procedimientos tributarios. Veremos que esta cautela es compartida por el legislador y supone una de las mayores limitaciones a la utilización de esta tecnología hoy en día.

Hasta la fecha, el intercambio de documentación tributaria se basa en sistemas centralizados dependientes de la Administración, con el coste de

2. Para un análisis más general de esta cuestión nos remitimos a Bilbao y Antón (2019).

almacenamiento y seguridad que ello supone. La tecnología *blockchain*, aparentemente, podría servir a la Administración, sobre todo a la local, para generar algún ahorro en estos costes, aunque veremos que la situación no está exenta de problemas jurídicos.

El *blockchain* es una técnica fundamentada en el consenso y el empleo de criptografía asimétrica, en la medida en que los nodos aceptan la validez de una determinada transacción, y la incorporan a la cadena de operaciones, quedando inmutable, lo que concede seguridad a los sujetos intervinientes en relación con la certeza de la operación³. Ahora bien, como ya hemos dicho, existen dudas sobre el carácter inmutable de la cadena, sobre todo cuando las redes no son del todo públicas, algo que en el funcionamiento de la actividad administrativa no parece que vaya a ser posible.

Hay que tener en cuenta que “solo las redes públicas sin permisos se adecuan, en principio, al paradigma ideológico originario de la tecnología *blockchain*, puesto que tan solo mediante su empleo se garantiza la implantación de los máximos niveles posibles (...) de distribución, descentralización y desintermediación”⁴. El *blockchain* público está totalmente descentralizado y cualquier persona en el mundo puede leer transacciones y participar en el proceso de consenso, lo que se compagina mal con la necesaria privacidad que ha de regir las relaciones Administración-administrado, al encontrarnos ante la necesidad de respetar un derecho fundamental como es el artículo 18.4 de la Constitución, en el que se establece lo siguiente: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

Hechas estas advertencias previas, consideramos que para comprender el funcionamiento de la tecnología *blockchain* podemos recurrir al análisis de la figura más conocida que la utiliza, como es la criptomoneda o criptoactivo conocido como bitc in.

En su web oficial (www.bitcoin.org), Bitcoin se define como: “Una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, Bitcoin es como dinero para internet”. El bitc in

3. Para un an alisis completo del funcionamiento de esta tecnolog a me remito a Vilarroig y Pastor (dirs.). (2018).

4. Sobre este particular me remito a lo ya indicado en esta obra en D az Gonz alez (2022).

fue creado en 2008 por una persona, o grupo de personas, que emplearon el pseudónimo de Satoshi Nakamoto. Es una “moneda virtual”, que solo existe como anotaciones en un libro de contabilidad almacenado en internet, siendo su respaldo una serie de reglas matemáticas y una red informática que nació con la finalidad de convertirse en un medio de pago virtual, descentralizado y seguro. Además, surge con fecha de caducidad, al alcanzar la cifra de 21 millones de bitcoins, sin que se puedan crear o generar más⁵. De un modo simplificado, el sistema Bitcoin se compone esencialmente de un software de firma electrónica, otro de red entre pares (P2P) y algoritmos y funciones criptográficas⁶.

Las redes de pares (*peer-to-peer* o P2P) son redes entre iguales. Todos son clientes y todos son servidores: a cada participante en la red se le llama *nodo*. Bitcoin es una red de pares en la que cada nodo guarda una copia de un inmenso libro mayor de contabilidad en el que están anotadas todas las transacciones que se han realizado con bitcoins desde que nació el sistema. El conjunto de nodos conforman el *blockchain*, que es un registro general de transacciones. Cuando se produce una transacción en bitcoins, queda registrada en al menos uno de estos nodos, que se la comunica a todos los demás. Existen dos tipos de nodos: los normales, a los que se llama “monederos”, que se limitan a guardar información de un usuario y enviar transacciones, y, por otro lado, los que guardan el libro de contabilidad y anotan las transacciones, que se denominan “mineros”.

Para certificar las operaciones, Bitcoin utiliza un sistema de firma electrónica doble, con clave pública y privada que están respaldadas por operaciones matemáticas complejas que sirven así para cifrar y descifrar el contenido de las transacciones realizadas.

Para ser usuario de Bitcoin hay que tener un “monedero” (*wallet*). En él se guardan bitcoins, en concreto las claves pública y privada. Cuando queramos gastar bitcoins, la cartera enviará a la red una especie de asiento contable en el que viene por un lado nuestra clave pública y por otro un mensaje compuesto por la cantidad de dinero y la clave pública del destinatario del mismo; mensaje

5. Esta limitación en la creación de moneda ha dado lugar a que surjan nuevas variantes, como el bitc  n “cash”, que ha comenzado a generarse el 1 de agosto de 2017, o el bitc  n “gold”, que lo ha hecho el 22 de octubre de 2017. El auge de estas criptomonedas y su creciente utilizaci  n como valor refugio de inversores pueden verse en las noticias de prensa. *Vid.* https://www.elconfidencial.com/tecnologia/2017-10-14/inversion-Bitcoin-subida-criptomonedas_1460809/

6. La explicaci  n t  cnica desarrollada en este apartado del trabajo se ha elaborado a partir de Rodr  guez Herrera (2015), Franco (2015) y Miras Mar  n (2017).

que estará firmado con nuestra clave privada. De este modo, todo usuario del sistema puede coger nuestra clave pública, descifrar el mensaje y comprobar los datos de la transacción. El saldo en bitcoins será el resultado de sumar todos los “ingresos y gastos” de bitcoins en los que aparezca nuestra clave pública.

Con lo indicado hasta ahora queda una cuestión por resolver: ¿Cómo se originan los bitcoins? Para responder a esto es necesario entender el funcionamiento del *blockchain* y su sistema de seguridad.

Para garantizar el registro correcto de las transacciones, cuando nuestro “monedero” lanza una transacción a la red, y previa a su anotación en el “libro de contabilidad global”, se produce un proceso de control con el fin de asegurarse de que la clave pública proporcionada es la dirección de destino de la operación anterior y de que esta misma clave pública pertenece al usuario que firmó la transacción.

Esta información se organiza en “paquetes de datos” que se transmiten por separado y se recomponen de nuevo a la recepción, el denominado *blockchain*. Con el fin de tener certeza de que no se han modificado entre emisor y receptor, se acompañan de funciones criptográficas, las funciones *hash*.

El método de confirmación de transacciones funciona del siguiente modo: cada diez minutos, cada uno de los nodos mineros intentará crear un bloque, que es el conjunto de transacciones que se han registrado en la red durante ese tiempo. En cuanto lo consiga, lo irá transmitiendo a los demás nodos de la red, que comprobarán que en este nuevo bloque no hay inconsistencias y la contabilidad sigue siendo correcta, momento en el cual lo confirmarán y añadirán un *hash* que permitirá que no se pueda alterar el registro.

Como son muchos los “mineros” trabajando a la vez, para evitar que la red se inunde con bloques igualmente válidos se incentiva su creación. Se les obliga a que el *hash* del bloque sea más pequeño que un cierto número, de modo que tienen que hacer pruebas aleatorias (prueba de trabajo o *proof-of-work*) hasta encontrar uno bueno. La mayor parte de las veces no lo consiguen y tienen que aceptar el que ha creado otro minero. Pero si lo consiguen, se llevan bitcoins de regalo (“generan bitcoins”). En definitiva, tres son los instrumentos clave en los que se sustenta su existencia: un *software* libre, una red *peer to peer* y la criptografía⁷.

7. Para un análisis del bitc on desde el punto de vista tributario, *vid.* Pedreira y  lvarez (2018).

En el ámbito de la Hacienda local debemos descartar el sistema descrito con el funcionamiento de Bitcoin; la Administración tributaria solo puede recurrir a redes *blockchain* de carácter privado, “que presentan un impacto tecnológico limitado”⁸, al no existir un acceso público, por lo que su funcionamiento sería similar a una intranet, pero con la ventaja de las descentralización de la información. Es un *blockchain* donde los permisos para escribir son mantenidos y centralizados en una organización: la Administración. Los permisos de lectura pueden ser públicos o restringidos: depende de lo que decida el gestor. Pese a las limitaciones de este modelo, sin embargo, no por ello ha de infravalorarse la relevancia de esta categoría de redes, puesto que el uso distribuido de la información puede servir para favorecer los procesos de almacenamiento de la documentación e incluso el intercambio entre administraciones. También debemos destacar como ventaja de las redes privadas que no hay que hacer ninguna labor de minería de datos, lo que agiliza las transacciones y la incorporación al *blockchain*. La Administración gestionaría el acceso y uso de la *blockchain*, seleccionando los participantes en la misma y los permisos que tendrían cada uno de ellos.

2. La tecnología *blockchain* y su aplicación en el ámbito tributario

Hasta la fecha los principales esfuerzos doctrinales de análisis de la utilización de la tecnología *blockchain* en el ámbito tributario están ligados a la gestión y al cobro de tributos indirectos, como el IVA o los derechos aduaneros.

La implantación del sistema de Suministro Inmediato de Información (SII) en el IVA a través del *Real Decreto 596/2016, de 2 de diciembre, para la modernización, mejora e impulso del uso de medios electrónicos en la gestión del Impuesto sobre el Valor Añadido, por el que se modifican el Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre, el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos, aprobado por el Real Decreto 1065/2007, de 27 de julio, y el Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1619/2012, de 30 de noviembre*, ha supuesto la generación de un flujo de información tributaria hacia la Agencia Estatal de Administración Tributaria (AEAT) por parte de los operadores económicos, que permite avanzar nuevas soluciones, como vamos

8. Díaz González (2022).

a exponer. Actualmente, se aportan a la sede electrónica de la AEAT datos de facturación que permiten ir confeccionando, casi en tiempo real, los distintos libros registro de IVA. En esencia, la AEAT dispone de un sistema cruzado de información —la proporcionada por el contribuyente y la suministrada por terceros— que le facilita el control de las obligaciones tributarias y le evita requerimientos de información al sujeto pasivo del IVA. Las ventajas de este mecanismo para el obligado tributario son, esencialmente, dos: a) reducción de las obligaciones formales, ya que queda exonerado de presentar facturas y algunas declaraciones informativas, por ejemplo, el modelo 347 de operaciones con terceros; b) acceso a un libro registro en la sede electrónica de la AEAT que le permite contrastar la información aportada por terceros que sigan este mismo sistema y, por consiguiente, conocer los datos de las facturas incluidas en los libros registro de sus clientes y proveedores.

Si el sistema descrito se sustentase en tecnología *blockchain* se podría ligar al mismo un modelo de liquidaciones tributarias automatizadas que, mediante *smart contracts* (que son acuerdos que se ejecutan automáticamente previa encriptación de los términos contractuales de la cadena de bloques), permitiera directamente realizar los cargos en las cuentas autorizadas de los contribuyentes, aligerando la carga documental de la liquidación de este tributo. Incluso, si se llegase a la emisión de la información mediante tecnología *blockchain*, se permitiría garantizar que los datos de facturas, tanto emitidas como recibidas, no van a ser alterados, facultando a la Administración para efectuar la oportuna liquidación sobre datos que están distribuidos y sobre los que no cabe la modificación por parte de los obligados tributarios.

En el mismo ámbito del IVA, pero en relación con las operaciones intracomunitarias, se podrían atajar las bolsas de fraude carrusel a través de la trazabilidad e inmutabilidad que proporciona un contrato inteligente sustentado en *blockchain*. La logística y la gestión de la cadena de distribución de mercancías es un campo especialmente óptimo para que un contrato de transporte asociado a una *blockchain* ofrezca seguridad y transparencia en tiempo real sobre los bienes porteados o almacenados, por lo que sería de gran utilidad para atajar el fraude carrusel en el IVA. El seguimiento en tiempo real que proporciona *blockchain* al tráfico de mercancías permite a los distintos actores que intervienen en dicho proceso (comprador, vendedor, transportistas, consignatarios, entidad financiera, autoridades tributarias, etc.) verificar la realidad del transporte y de las transacciones comerciales, con especial interés para la Administración en el momento de validar la repercusión y deducción del IVA. Y lo mismo podría decirse en el ámbito aduanero en las operaciones

de comercio internacional, facilitando un despacho de mercancías en aduana más ágil y seguro. Desde luego, sería conveniente que la Unión Europea estableciera un modelo de *blockchain* y lo implementara en el tráfico de mercancías, pudiendo ser inicialmente voluntario, pero estoy seguro de que las ventajas que reporta al conjunto de los operadores económicos harían que finalmente fuera adoptado por todos.

Los *smart contracts* basados en tecnología *blockchain* también pueden ser aplicados para practicar retenciones a cuenta de impuestos sobre la renta en los pagos realizados en ejecución de los mismos, al punto de que en algunos casos —dependiendo del tipo de rentas— el ingreso de las retenciones podría ser instantáneo, eliminándose así la necesidad de presentar declaraciones periódicas. El automatismo inherente a los *smart contracts* fomentaría el cumplimiento voluntario de las obligaciones tributarias, al aligerar las obligaciones de los administrados⁹.

El sistema de contabilidad distribuida identificativo de *blockchain* también puede ser utilizado por grupos multinacionales, generando un registro inalterable de sus operaciones ligadas a precios de transferencia, de modo que dando acceso a las administraciones tributarias nacionales para revisarlo, se podría tener un registro y rastreo de los bienes y servicios intragrupo y de su facturación, facilitando fijar la aplicación de los precios de transferencia y aligerando las declaraciones informativas país por país a presentar por este tipo de empresas. Las administraciones tributarias implicadas en estas operaciones podrían tener una mayor coordinación en las funciones de control, evitando resultados contradictorios, riesgo de doble imposición, conflictividad, etc.¹⁰.

Estos ejemplos de aplicación del *blockchain* en la gestión tributaria, llegado el caso, también podrían ser extrapolables al ámbito de las Haciendas locales. Un supuesto podría ser para la liquidación del impuesto de construcciones y obras. El ayuntamiento realiza la liquidación provisional sobre el proyecto de obra presentado. Si entre el promotor y el contratista existiera un sistema de intercambio de información mediante tecnología *blockchain*, por ejemplo, la liquidación de las certificaciones de obra a medida que se produce el avance de la obra, esta información podría ser compartida con la Administración, de modo que los datos no podrían ser alterados y permitirían la emisión de la liquidación definitiva a la certificación del fin de obra. De este modo se

9. Estas aplicaciones de la tecnología *blockchain* están perfectamente explicadas en el trabajo de Fernández López (2021).

10. Sobre este particular, *vid.* Gómez Requena (2018).

podrían simplificar procedimientos administrativos y trámites de liquidación tributaria.

Desde luego, esta tecnología puede facilitar la recaudación de determinados tributos y fortalecer el cumplimiento de obligaciones tributarias por parte de los contribuyentes, pero aún está en una fase de maduración de la tecnología en cuanto al funcionamiento de las redes que no son totalmente públicas¹¹. A nuestro juicio, esta tecnología permitiría variar el actual modelo de autoliquidaciones para retomar el antiguo esquema de la declaración (que en este caso estaría ligada a los *smart contracts* aplicables de forma automatizada) y posterior liquidación administrativa, frente a la que debería darse el oportuno modelo de recursos administrativos, con la especialidad de que aquí el pago o ingreso del tributo ya estaría realizado. Por tanto, habría que asegurar que estas liquidaciones fueran lo más correctas posible para evitar recursos y perjuicios económicos. Como puede apreciarse, estaríamos ante un cambio del modelo actual de relación entre la Administración y los obligados tributarios, que debería ir acompañado de las oportunas modificaciones en los procedimientos tributarios y su normativa de desarrollo. Todo ello debería llevarse a cabo en aras de facilitar la gestión tributaria a los administrados, asumiendo la Administración su capacidad para liquidar.

La situación descrita no es tan utópica si nos fijamos en el IRPF, donde millones de contribuyentes ya solo tienen que validar el borrador confeccionado por la AEAT. Aquí habría que dar un paso más y no seguir exigiendo a los contribuyentes que se responsabilicen del contenido de ese borrador, sino que sea la AEAT quien lo haga, ya que de ella parte la liquidación y, para eso, tiene el período de prescripción para revisar cualquier posible error cometido al liquidar; sobre esta cuestión incidiremos en próximos apartados, porque es hacia el modelo en el que se avanza en las administraciones tributarias forales del País Vasco.

3. La protección de la privacidad de los datos fiscales y las limitaciones al uso de la tecnología *blockchain*

Uno de los principales problemas que plantea la tecnología *blockchain* radica en que la información está descentralizada y cada uno de los nodos debe validarla, lo que puede generar una colisión con el tratamiento de los datos de

11. Esta situación no es exclusiva de España, como puede verse en Owens y De Jong (2017).

carácter personal, de ahí que las redes que manejen información tributaria no puedan ser públicas o abiertas, como ya hemos indicado.

El artículo 18.4 de la Constitución establece un derecho fundamental a la intimidad en el uso de la informática, lo que también está reconocido implícitamente en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea¹² y en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE)¹³.

La Administración debe velar por que los datos de los contribuyentes no puedan ser revelados a terceros, de ahí la limitación que tiene a la hora de descentralizar la información, por el riesgo de posibles quiebras de seguridad en la cadena.

Por otro lado, el uso de la tecnología *blockchain* por parte de la Administración tributaria debe respetar los derechos y garantías de los contribuyentes, así como la normativa general en materia de procedimientos administrativos.

Advertido esto último, debemos señalar que el recurso a la tecnología *blockchain* en el ámbito de los procedimientos tributarios se encuentra con una importante limitación, por lo establecido en la disposición adicional sexta de la *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas* (LPAC), que establece:

“1. No obstante lo dispuesto en los artículos 9.2 c) y 10.2 c) de la presente Ley, en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del derecho de la Unión Europea.

2. En todo caso, cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal a que hace referencia el apartado anterior deberá contemplar asimismo que la Administración General del Estado actuará como autoridad intermedia

12. *Vid.* DOCE C 83/389 de 30 de marzo de 2010.

13. *Vid.* DOCE C 83/47 de 30 de marzo de 2010.

que ejercerá las funciones que corresponda para garantizar la seguridad pública”¹⁴.

Hay que tener en cuenta que el artículo 9 LPAC se refiere a los sistemas de identificación de los interesados en los procedimientos administrativos. Por tanto, la disposición adicional sexta está impidiendo el recurso a la tecnología *blockchain* para la identificación de los administrados y el acceso al procedimiento¹⁵. Por su parte, el artículo 10 LPAC regula los sistemas de firma que pueden ser admitidos por las administraciones públicas dentro

14. Esta disposición ha sido introducida en el ordenamiento a través del *Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones*.

15. “Artículo 9. Sistemas de identificación de los interesados en el procedimiento.

1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.

2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘Lista de confianza de prestadores de servicios de certificación’.

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la ‘Lista de confianza de prestadores de servicios de certificación’.

c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).

3. En relación con los sistemas de identificación previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del 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, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto

de los procedimientos, negando de nuevo la utilización de la tecnología que estamos analizando¹⁶.

de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo”.

16. “Artículo 10. Sistemas de firma admitidos por las Administraciones Públicas.

1. Los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento.

2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘Lista de confianza de prestadores de servicios de certificación’.

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la ‘Lista de confianza de prestadores de servicios de certificación’.

c) Cualquier otro sistema que las Administraciones Públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

3. En relación con los sistemas de firma previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

5. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma”.

La justificación esgrimida en la exposición de motivos del Real Decreto-ley 14/2019, de 31 de octubre, para introducir esta limitación ha sido la siguiente:

“Las restricciones impuestas a los sistemas de identificaciones y firmas basados en tecnologías de registro distribuido en ningún caso suponen una prohibición general. Simplemente, se restringe puntualmente y de forma meramente provisional su uso como sistema de identificación y firma de los interesados cuando estos últimos se interrelacionan con la Administración y mientras no haya más datos o un marco regulatorio *ad hoc* de carácter estatal o europeo que haga frente a las debilidades que implica su uso para los datos y la seguridad pública. La falta de un marco regulatorio *ad hoc* sobre estas nuevas tecnologías justifica que, con carácter urgente y en ejercicio de su competencia para dictar legislación básica, el Estado intervenga sobre la materia con carácter provisional hasta que se avance en el seno de la Unión Europea en el tratamiento de este tipo de tecnologías”.

Por tanto, el recurso desde las administraciones locales al establecimiento de procedimientos tributarios basados en tecnología *blockchain* está vedado, pese a las posibles utilidades que puede tener esta tecnología, como ya hemos explicado, porque el acceso y la firma no pueden sustentarse en esta tecnología.

La Administración estatal y el legislador desconfían del funcionamiento de la tecnología *blockchain* y no quieren permitir, todavía, que las facultades de identificación de los administrados dentro de un procedimiento puedan depender de validaciones externas y no de los certificados establecidos por ellos¹⁷.

Como ya habíamos indicado, a los condicionantes técnicos que todavía existen, se unen las limitaciones jurídicas para el desarrollo de la tecnología *blockchain* dentro de los procedimientos administrativos y, especialmente, en los tributarios.

El marco regulatorio que se pueda establecer en el futuro deberá respetar los principios de buena administración en cuanto a la prudencia y proporcionalidad en la disponibilidad y utilización por la Administración tributaria de la información obtenida a través de esta tecnología. Asimismo, esta tecnología debería permitir avanzar en el principio de eficacia y

17. Sobre este particular puede verse el análisis realizado por Fernández López (2021).

transparencia de los procedimientos, pudiendo tener conocimiento de la situación de todos ellos en cualquier momento. Igualmente, debe preservarse el derecho de acceso del obligado tributario a sus datos personales, que deben ser confidenciales¹⁸.

En relación con esto último no debe olvidarse que el 14 de julio de 2021 se ha aprobado la Carta de Derechos Digitales, que, sin tener carácter normativo, ofrece un marco de referencia para garantizar los derechos de la ciudadanía en la nueva realidad digital, recogiendo un conjunto de veintiocho principios y derechos para guiar futuros proyectos normativos¹⁹. Esta Carta de Derechos Digitales viene a ser un marco de desarrollo de lo establecido en el Título X, relativo a la garantía de los derechos digitales, contenido en la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*.

En definitiva, podemos afirmar que el uso de la tecnología *blockchain* en el seno de los procedimientos tributarios todavía está en una fase de maduración tecnológica y pendiente de desarrollo normativo, aunque parece más que evidente que su uso futuro va a ser una realidad.

4. El uso de otras nuevas tecnologías en los procedimientos tributarios

Independientemente de la tecnología *blockchain*, en los últimos años han proliferado otra serie de herramientas tecnológicas que influyen en la gestión tributaria y sobre las que consideramos preciso realizar una breve exposición y reflexión.

La utilización de las nuevas tecnologías permite a la Administración tributaria abordar los procedimientos de gestión, comprobación y recaudación con nuevas herramientas que la pueden situar en una situación de prevalencia sobre el obligado tributario, desnivelando aún más a su favor la relación jurídico-tributaria. Por tanto, el uso de estas nuevas tecnologías debe ser objeto de debate y control.

Por una parte, las nuevas tecnologías pueden ayudar en la gestión tributaria a la Administración, pero también a los administrados. El

18. Grau Ruiz (2020).

19. *Vid.* file:///C:/Users/Administrador/Downloads/140721-Carta_Derechos_Digitales_RedEs.pdf

ejemplo más claro lo encontramos con el IRPF; multitud de contribuyentes solo tienen que validar el borrador de su autoliquidación facilitado por la Administración. Este modelo permite que el contribuyente tenga acceso a la información que obra en poder de la Administración, para cotejarla y darla por buena o rectificarla. Sin embargo, este proceder puede ir más allá, como ya indicamos, haciendo variar el modelo hacia auténticas liquidaciones administrativas, abandonando el excesivo recurso a la autoliquidación que se ha llevado a cabo y que, muchas veces, somete al obligado tributario a una carga de gestión adicional al tener que contar con un asesor fiscal de manera casi permanente.

Desde el Plan de Control Tributario 2018 se ha establecido recurrentemente que la investigación en internet y la obtención de información relacionada con los nuevos modelos de negocio serían una prioridad para la Agencia Estatal de Administración Tributaria (AEAT)²⁰. De hecho, así se sigue manteniendo en el vigente plan 2021²¹. Ahora bien, este recurso al análisis del *big data* y la utilización de inteligencia artificial mediante algoritmos genera una tensión entre los derechos de los contribuyentes y la actuación de la Administración, en aras de proteger el deber de contribuir consagrado en el artículo 31 de la Constitución.

Así, por ejemplo, las nuevas tecnologías ligadas a internet están permitiendo a la Administración utilizar programas informáticos para rastrear los anuncios en páginas web y ver si se están declarando las rentas por arrendamientos. No nos parece mal que se recurra a estos medios para luchar contra el fraude fiscal, pero dentro de un procedimiento con las debidas garantías.

El problema, en mi opinión, radica en cuáles son los límites a la investigación y la obtención de información en internet. Hoy en día tenemos una presencia permanente en la red, aunque no seamos conscientes de ello, lo que permite a la Administración utilizar muy distintas herramientas para hacer ese seguimiento de los obligados tributarios, tales como el *data mining*, el internet de las cosas, el *big data* y el *machine learning*. La utilización combinada de todos estos instrumentos puede permitir un seguimiento y rastreo de muchas de nuestras actividades, sin que hayamos prestado ningún

20. *Vid.* Resolución de 8 de enero de 2018, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se aprueban las directrices generales del Plan Anual de Control Tributario y Aduanero 2018. BOE núm. 20, de 23 de enero de 2018.

21. *Vid.* Resolución de 19 de enero de 2021, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se aprueban las directrices generales del Plan Anual de Control Tributario y Aduanero 2021. BOE núm. 27, de 1 de febrero de 2021.

tipo de consentimiento para el mismo. ¿Puede la Administración rastrear nuestro teléfono o la matrícula del coche en peajes de autopistas para controlar nuestros desplazamientos y saber dónde nos alojamos? ¿Controlar a través de los registros de los hoteles nuestras pernoctaciones y cómo las hemos pagado? Todos estos datos están fácilmente a su alcance, aunque no lo creamos, y más en momentos como los actuales, al amparo del rastreo de posibles brotes de COVID, en que se está recabando esta información en ficheros muchas veces al alcance de la Administración tributaria. Con esa ingente cantidad de información, oportunamente tratada, puede conocer nuestro nivel de rentas y detectar posibles pagos en metálico que puedan proceder de rentas no declaradas o de donaciones familiares no declaradas. Ahora bien, ¿en aras de la recaudación debemos ver limitada nuestra privacidad, o tiene que haber unos límites a la captación y al tratamiento de la información tributaria, algo que ahora mismo no está regulado?

Como indica Gil Cruz, el obligado tributario no solo debe conocer los datos que están utilizando los órganos administrativos y el tratamiento que se está dando a los mismos, sino también, y en base al artículo 15.1.h) del RGPD²², las consecuencias que de ello se derivan al existir decisiones automatizadas, poniendo especial empeño en aquella información que más ha incidido en la decisión final. Lo contrario, generaría inseguridad jurídica para el administrado, a la vez que pondría en peligro el derecho a la tutela judicial efectiva²³.

Esta circunstancia ya se ha producido en otros países de nuestro entorno, como Holanda, donde la Corte del Distrito de La Haya, en sentencia de 5 de febrero de 2020, anuló las normas regulatorias de un algoritmo desarrollado por el Gobierno para prevenir y combatir el fraude a la seguridad social por vulnerar el derecho a la privacidad y a la protección de datos personales, por apreciar sesgos discriminatorios en su aplicación²⁴. Como acertadamente indica Grau Ruiz, no es lo mismo un funcionario de la Administración tributaria que toma decisiones apoyándose en datos y programas ejecutados informáticamente, que un algoritmo que adopte decisiones y estas se ejecuten por un funcionario²⁵.

22. 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 (Reglamento general de protección de datos), DOUE, L 119/1, de 4 de mayo de 2016.

23. Gil Cruz (2021).

24. Navarro Egea (2021).

25. Grau Ruiz (2020).

Consideramos que hay que abogar por la defensa de nuestra intimidad, sobre todo frente a una Administración tributaria ávida de obtener información de sus contribuyentes, diríamos que casi obsesionada con ello. Deberíamos tener derecho a poder saber en cualquier momento cuál es la información que obra en poder de la Administración tributaria, por si es fiable o debe ser rectificada. No puede ampararse en que su labor de investigación es continuada para sacar información a mitad de un procedimiento inspector, sin haber puesto todas las cartas encima de la mesa desde el primer momento, como a veces ocurre. La labor de la Administración debe ser transparente para los obligados tributarios, y el rastreo de datos e información, sobre todo en la red, debe ser conocido²⁶.

Deberían existir unas nuevas garantías para los contribuyentes, como el derecho a la transparencia y publicidad de las acciones de captación de información, acceso a la información en cualquier momento y posibilidad de su rectificación, a la comunicación e información del uso de algoritmos por parte de la Administración, etc.

Los procedimientos tributarios están sufriendo un profundo cambio como consecuencia de la aplicación de estas nuevas tecnologías por parte de la Administración, y es necesario que la normativa se adecúe a los mismos para no desproteger a los administrados. Qué más da que se establezcan unos plazos máximos a los procedimientos si estos no empiezan a computar hasta que la Administración decide comunicar el inicio de los mismos, pese a que ha estado trabajando y recabando información durante muchos meses antes. Con la obtención de información digital esta situación no hace más que agravarse.

Un ejemplo de lo que estamos apuntando es la iniciativa TicketBAI (TBAI) del Gobierno Vasco y las tres diputaciones forales, que tiene como objetivo establecer una serie de obligaciones legales y técnicas, de modo que, a partir de su entrada en vigor, todas las personas físicas y jurídicas que realicen una actividad económica deberán utilizar un *software* de facturación que cumpla los requisitos técnicos solicitados.

El nuevo sistema permitirá a las Haciendas forales controlar los ingresos de las actividades económicas de las personas contribuyentes y, en particular, de aquellas actividades enmarcadas en sectores que realizan entregas de

26. Olivares Olivares (2020).

bienes o prestaciones de servicios a las y los consumidores finales, cobradas en gran medida en efectivo. Asimismo, dicha información se utilizará para facilitar a los contribuyentes el cumplimiento de sus obligaciones tributarias.

El sistema TBAI identificará cada una de las facturas y *tickets* que se emitan, de modo que las Haciendas podrán rastrear todas las transacciones realizadas y comprobar el pago de los impuestos correspondientes, o bien efectuar las liquidaciones correspondientes. El funcionamiento del sistema es el siguiente:

Por cada factura que se emita, el *software* creará un fichero XML, que enviará a la Hacienda foral que corresponda en función del domicilio del sujeto pasivo.

La Hacienda foral asignará un código QR y un código identificativo a cada factura. Una vez hecho esto, la Hacienda foral devolverá el archivo al *software* emisor para que pueda generar la imagen de la factura. Este proceso es instantáneo y, al final, el comprador tendrá su factura validada. El sistema de validación está en manos de la Administración como organismo certificador, pero nada impediría que en un futuro se utilizara algún sistema basado en tecnología *blockchain*.

TicketBAI también forma parte del Proyecto Batuz de la Hacienda Foral de Bizkaia, que tiene una finalidad más ambiciosa de lucha contra el fraude fiscal y que consiste en la presentación de libros y registros de operaciones mediante el modelo 140, el 240 y las futuras elaboraciones de los borradores de declaraciones de IVA y de IS o IRPF. A partir del 1 de enero de 2024, las personas físicas y entidades en régimen de atribución de rentas (ERAR) que desarrollen actividades económicas, los contribuyentes del impuesto sobre sociedades y los contribuyentes del impuesto sobre la renta de no residentes con establecimiento permanente, deberán llevar un libro registro de operaciones económicas (LROE) a través de la sede electrónica de la Diputación Foral de Bizkaia, en el que deberán anotar, en los plazos establecidos, los ingresos y facturas emitidas, los gastos y facturas recibidas, y las demás operaciones con trascendencia tributaria que realicen en el desarrollo de su actividad económica²⁷.

27. El procedimiento ha sido desarrollado a través de la *Norma Foral 5/2020, de 15 de julio, por la que se establece un sistema integral de control de los rendimientos de las actividades económicas, así como medidas para facilitar el cumplimiento de las obligaciones tributarias, mediante la modificación de la Norma Foral del Impuesto sobre Sociedades, la*

Desde luego, la iniciativa pretende poner fin a las prácticas fraudulentas de determinados empresarios que utilizan *software* de doble uso en sus cajas registradoras²⁸, así como a la posible utilización de facturas falsas emitidas por “moduleros”. Esta actuación es loable, pero hay que ponerla en contraposición con la información que va a obrar en poder de la Administración, ya que los datos de facturación también pueden recoger datos de los clientes o de los servicios prestados, lo que puede atentar de nuevo contra la intimidad. Consideramos que hoy en día, con tanta información generada en la red o por medios electrónicos y que llega a la Administración, esta cuestión gana mucho más peso y se hace preciso establecer una limitación al uso y manejo de la información recopilada. La tensión entre los artículos 18 y 31 de la Constitución está más presente que nunca.

5. Conclusiones

Para poder avanzar en el uso de la tecnología *blockchain* en los procedimientos tributarios es preciso un desarrollo normativo que establezca las líneas básicas por las que deban regirse los gestores y usuarios, ya que

Norma Foral del Impuesto sobre la Renta de no Residentes, la Norma Foral del Impuesto sobre la Renta de las Personas Físicas, la Norma Foral del Impuesto sobre Patrimonio y la Norma Foral General Tributaria del Territorio Histórico de Bizkaia; el Decreto Foral 82/2020, de 8 de septiembre, de la Diputación Foral de Bizkaia, por el que se desarrollan las obligaciones tributarias del proyecto Batuz, mediante la modificación del Reglamento del Impuesto sobre la Renta de las Personas Físicas, el Reglamento del Impuesto sobre Sociedades, el Reglamento del Impuesto sobre la Renta de no Residentes, el Reglamento por el que se regulan las obligaciones tributarias formales del Territorio Histórico de Bizkaia, el Reglamento de gestión de los tributos del Territorio Histórico de Bizkaia y el Reglamento por el que se regulan las obligaciones de facturación; la Orden Foral 1482/2020, de 9 de septiembre, del diputado foral de Hacienda y Finanzas, por la que se regulan las especificaciones normativas y técnicas del software garante y la declaración de alta en el registro de software garante; la Orden Foral 1578/2021, de 24 de septiembre, del diputado foral de Hacienda y Finanzas, por la que se regulan las especificaciones normativas y técnicas que desarrollan la llevanza del libro registro de operaciones económicas de las personas físicas a través de la sede electrónica de la Diputación Foral; y la Orden Foral 1582/2021, de 24 de septiembre, del diputado foral de Hacienda y Finanzas, por la que se regulan las especificaciones normativas y técnicas que desarrollan la llevanza del libro registro de operaciones económicas de los contribuyentes del Impuesto sobre Sociedades a través de la sede electrónica de la Diputación Foral, con excepción del capítulo de movimientos contables.

28. La preocupación de la Administración por esta cuestión es tal que, en la última reforma de la Ley 58/2003, de 17 de diciembre, General Tributaria (LGT), llevada a cabo por la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, se ha introducido un nuevo “Artículo 201 bis. Infracción tributaria por fabricación, producción, comercialización y tenencia de sistemas informáticos que no cumplan las especificaciones exigidas por la normativa aplicable”.

así lo ha establecido expresamente el legislador en la LPAC, al limitar el acceso e identificación, así como la firma de los expedientes administrativos.

Independientemente del *blockchain* han aparecido otra serie de tecnologías ligadas al uso masivo de información digital por parte de la Administración, que exigen un respeto a los derechos digitales de los particulares que debe estar en relación o justo equilibrio con las potestades administrativas que se utilizan para la gestión de los tributos. Todo ello con una atención especial al derecho fundamental a la intimidad reconocido en el artículo 18 de la Constitución.

En el ámbito de las Haciendas locales, las posibilidades de recurrir a la tecnología *blockchain* dentro de la gestión tributaria están muy limitadas por los condicionantes establecidos en la LPAC y la falta de un desarrollo legislativo, que no puede ser ejecutado por los ayuntamientos. En consecuencia, hasta que se produzcan avances a nivel estatal, lo que previsiblemente no se llevará a cabo hasta que la Unión Europea establezca alguna regulación, no podemos ser optimistas en cuanto al uso de esta tecnología en los procedimientos de gestión tributaria.

No obstante, otras nuevas tecnologías informáticas sí pueden ser utilizadas por las Haciendas locales para tener una gestión tributaria más eficiente. Para conseguir estos objetivos sería deseable que pudiera haber una cooperación interadministrativa, con las suficientes garantías para los obligados tributarios, a través de la que se pudieran intercambiar ficheros y datos. Por ejemplo, el intercambio de información fiscal con el catastro es fundamental, ya que buena parte de la tributación local radica en valoraciones emitidas por este organismo. Asimismo, el control de otros impuestos, como el de vehículos de tracción mecánica, se puede beneficiar de sistemas de intercambio de información con la Dirección General de Tráfico. En el momento actual la cooperación interadministrativa para acceder a ficheros y bases de datos de contribuyentes podría ser un gran adelanto para las Haciendas locales, con un coste tecnológico relativamente limitado. No obstante, debería existir una regulación clara y expresa sobre el alcance y uso de esta información, para no colisionar con el derecho a la intimidad.

6. Bibliografía

- Bilbao Estrada, I. y Antón Antón, A. (dirs.). (2019). *Retos y oportunidades de la Administración tributaria en la era digital*. Navarra: Aranzadi.
- Díaz González, G. M. (2022). *Blockchain* y administraciones públicas: una visión panorámica. En G. M. Díaz González (coord.). *Blockchain y Gobiernos locales*. Madrid: Fundación Democracia y Gobierno Local.
- Fernández López, R. I. (2021). El derecho tributario ante una nueva realidad virtual: la tecnología *blockchain* aplicada a los contratos inteligentes. *Revista Técnica Tributaria*, 132.
- Franco, P. (2015). *Understanding Bitcoin. Cryptography, Engineering and Economics* (1.ª edición). New York: Wiley.
- Gil Cruz, E. M. (2021). Derecho a la intimidad y *big data* tributarios. *Revista Técnica Tributaria*, 134.
- Gómez Requena, J. Á. (2018). ¿Se van a solucionar los problemas de asimetrías de información en los precios de transferencia con la aplicación de la tecnología *blockchain*? *Documentos de Trabajo del Instituto de Estudios Fiscales*, 10, 114-124.
- Grau Ruiz, M.ª A. (2020). Riesgos y oportunidades en la creciente digitalización fiscal. *Revista Técnica Tributaria*, 130.
- Miras Marín, N. (2017). El régimen jurídico-tributario del bitcóin. *Revista de Contabilidad y Tributación*, 406, 101-136.
- Navarro Egea, M. (2021). *Hacia un entorno digital más garantista: las relaciones tributarias electrónicas*. Navarra: Aranzadi.
- Olivares Olivares, B. D. (2020). Transparencia y aplicaciones informáticas en la Administración tributaria. *Crónica Tributaria*, 174, 89-111.
- Owens, J. y De Jong, J. (2017). Taxation on the blockchain: opportunities and challenges. *Tax Notes International*, 87 (6).
- Pedreira Menéndez, J. y Álvarez Pérez, M.ª B. (2018). Consideraciones sobre la tributación y la calificación contable de las operaciones con moneda digital (Bitcoins) en las empresas. *Quincena Fiscal*, 3, 17-50.
- Rodríguez Herrera, D. (2015). ¿Qué es Bitcoin? *La Ilustración Liberal*, 59.

Vilarroig Moya, R. y Pastor Sempere, C. (dirs.). (2018). *Blockchain: Aspectos Tecnológicos, Empresariales y Legales*. Navarra: Aranzadi.

Tecnologías emergentes aplicadas al presupuesto, el control interno y la fiscalización externa del sector público local

Roberto Fernández Llera*

*Síndico mayor de la Sindicatura de Cuentas del Principado de Asturias.
Acreditado como profesor titular de universidad*

Mariola Pérez Rodríguez*

Responsable de Informática de la Sindicatura de Cuentas del Principado de Asturias

Magdalena Cordero Valdavida*

Directora de Información, Entorno Laboral e Innovación del Tribunal de Cuentas Europeo

SUMARIO. 1. Introducción. 2. El presupuesto local. 3. La contratación pública. 4. Control económico-financiero. 4.1. Control interno: nuevos retos. 4.2. Rendición de cuentas y control externo. 4.3. Tecnologías emergentes: ¿es posible algún paso más? 5. Conclusiones y prudencias. 6. Bibliografía.

1. Introducción

Las tecnologías emergentes están transformando la sociedad. Son herramientas indispensables para seguir impulsando la modernización del sector público, y deberán, primero, ser capaces de ofrecer los servicios demandados por la sociedad; segundo, ser en sí mismas un motor de innovación y progreso; y por último, aunque no menos importante, realizar todo esto en un marco democrático de transparencia, integridad y eficiencia que permita generar garantías y, en última instancia, reforzar la confianza de la ciudadanía. Algunas de esas tecnologías emergentes tienen potencial transformador y hasta disruptivo; entre otras, la computación en la nube, el análisis de macrodatos (*big*

* Los juicios de valor son exclusivos de las personas firmantes y no necesariamente de las instituciones a las que representan.

data), la inteligencia artificial, el internet de las cosas, la automatización robótica de procesos o la cadena de bloques (*blockchain* o, de forma abreviada, BC). Cada vez más y con mayor alcance la ciudadanía interactúa utilizando las tecnologías de la información, un proceso que la pandemia de COVID-19 no ha hecho más que acelerar, pero que ya era imparable, también en el ámbito de las normas jurídicas del sector público.

El sector público local, en virtud de su mayor cercanía, es uno de los ámbitos donde se pueden encontrar más aplicaciones, gracias a una potencial carta de servicios susceptibles de verse modificados por un proceso de digitalización, o, incluso, de ser completamente digitalizados. En este proceso, la realidad física se reemplaza por una realidad virtual que deberá, no obstante, ofrecer las mismas garantías de unicidad, existencia y realidad. Los documentos ya no están en soporte papel, la identidad de los administrados es digital, la firma es electrónica y los pagos se realizan con la ayuda del teléfono o del ordenador. Las ciudades inteligentes son capaces de optimizar procesos y ofrecer servicios basándose en información recogida por una multiplicidad de sensores. Pero esta realidad digital no está exenta de riesgos: la falsificación de documentos, la usurpación de identidades, la distribución de información falsa o fraudulenta, son solamente algunos patrones.

Para el caso que nos ocupa, cabe reseñar que la tecnología BC emerge a finales de la primera década del siglo para dar soporte a las llamadas criptomonedas (Nakamoto, 2008). Lo hacía sobre la base de una motivación tan antigua como la que ya regía en el comercio desde tiempos pretéritos: otorgar confianza a la transacción, esto es, al producto y a las partes. Pero si esa confianza “tradicional” tenía una base personal y casi íntima o familiar, con el BC el paradigma es muy diferente, puesto que queda construido sobre un entorno tecnologizado, multidimensional, automatizado, universal y casi directo, sin intermediarios (López-Zambrano *et al.*, 2021). La pregunta inicial es inmediata: ¿se puede seguir hablando de confianza cuando las personas y/o las instituciones certificadoras o validadoras casi desaparecen, siendo sustituidas por máquinas y algoritmos? Las implicaciones de todo tipo, incluidas las jurídicas, las económicas, las políticas y, por supuesto, las éticas, son de primer orden (Benítez Palma, 2017; Huergo Lora, 2020).

Sin entrar en detalles muy técnicos, digamos que BC es una solución criptográfica que permite almacenar información de forma segura y distribuida. En definitiva, se trata de un registro compartido por millones de ordenadores conectados en red, donde se inscriben y archivan las transacciones en bloques

de manera verificable, permanente y anónima sin necesidad de intermediarios. Cada entrada en la base de datos está encadenada a la anterior y sirve de base para generar la siguiente, lo que permite un sellado en el tiempo inmutable. Dicho de otra forma: una alteración de uno de los bloques rompe la cadena. Por esta razón, la tecnología BC es especialmente adecuada para almacenar de forma creciente datos ordenados en el tiempo y sin posibilidad de modificación ni revisión. Es, por tanto, una herramienta para aumentar la seguridad de la información, con variados usos potenciales, que puede permitir, entre otras aplicaciones, mejorar la función de registro de documentos en las relaciones entre las administraciones públicas, la ciudadanía y las empresas. Las redes BC pueden ser públicas, privadas o híbridas, en función de la libertad con que se pueden añadir usuarios a la red.

Resulta obvio que los beneficios de utilizar BC aumentan en línea con el grado de digitalización del sector público. Entre tales beneficios podemos citar la rebaja de costes, tiempos y complejidades en los intercambios de información, la reducción de la burocracia ineficiente, la prevención del fraude y de la corrupción, o el aumento de la automatización y la transparencia de los procedimientos. Todo ello puede contribuir a reforzar el control interno y la fiscalización externa, siempre en busca del interés general y del beneficio ciudadano.

No es el fin de este trabajo detallar la exégesis ni el funcionamiento del BC, ni siquiera analizar sus debilidades y fortalezas generales, más allá de lo ya anotado. Solo añadiremos en este momento que se trata de una herramienta potencialmente valiosa, poco desplegada todavía (aunque recordemos que “las ciencias adelantan que es una barbaridad”, tomando la conocida frase zarzuelera) y, con seguridad, pendiente de ser comprendida en toda su dimensión. Todo ello nos permite aventurar que algunas expectativas quizás nunca lleguen a quedar del todo satisfechas, enfriando así algunos entusiasmos y no pocas veleidades.

Nuestro objetivo -más modesto- es explorar algunas de las eventuales aplicaciones del BC en el ámbito económico-financiero público, algunas de ellas ya esbozadas o iniciadas (Cordero Valdavidá, 2019), como la presupuestación, la contabilidad pública, los contratos, el control interno, la fiscalización externa, la gestión tributaria, el cumplimiento normativo, los registros públicos, la emisión y validación de certificados, las publicaciones oficiales o el voto digital. Se trata más bien de una reflexión analítica que de un compendio de posibles utilidades que, no obstante, ha de enmarcarse en la obligada -por ley- e ineludible -por necesidad- transformación digital a la

que ya se ha hecho referencia. Es en esta envolvente donde también viene ya operando en plenitud un conjunto de herramientas y plataformas al servicio de las esferas citadas relacionadas con el ámbito económico-financiero público. El BC no vendría a sustituirlas, sino, en todo caso, a reforzarlas y complementarlas cuando sea posible y aconsejable.

Tras esta introducción, se analiza la presupuestación en las entidades locales, la contratación pública, el control interno local y el control externo, introduciendo en cada caso los principales aspectos normativos y la eventualidad de una introducción gradual del BC. Una última sección concluye con una recapitulación y algunas cuestiones abiertas.

2. El presupuesto local

Los aspectos básicos de la presupuestación se regulan en el Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales (TRLRHL). De igual modo, es preciso acudir a otras leyes y normas básicas de aplicación¹, así como a las ordenanzas o bases de ejecución del presupuesto vigentes en cada entidad local.

El presupuesto constituye “la expresión cifrada, conjunta y sistemática de las obligaciones que, como máximo, pueden reconocer la entidad, y sus organismos autónomos, y de los derechos que prevean liquidar durante el correspondiente ejercicio, así como de las previsiones de ingresos y gastos de las sociedades mercantiles cuyo capital social pertenezca íntegramente a la entidad local correspondiente” (artículo 162 del TRLRHL). Esta definición legal, embebida en la más pura ortodoxia hacendística, contiene las funciones básicas del presupuesto como instrumento de planificación, gestión y control. De este modo, el presupuesto se configura como un documento político, con base económico-financiera, forma contable y exigentes requisitos jurídicos de tramitación.

1. Real Decreto 500/1990, de 20 de abril, por el que se desarrolla el capítulo primero del título sexto de la Ley 39/1988, de 28 de diciembre, reguladora de las Haciendas Locales, en materia de presupuestos; Ley 38/2003, de 17 de noviembre, General de Subvenciones; Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera (LOEPSF); Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP); legislaciones autonómicas homólogas de aplicación; y todas las normas reglamentarias sobre endeudamiento, suministro de información o estructura de los presupuestos, entre otras materias.

Desde el punto de vista temporal, el presupuesto reviste un carácter periódico (anual) y se enmarca en el ciclo que comienza con la fase de planificación y elaboración (a cargo de la Presidencia), prosigue con la de enmienda y aprobación (en el Pleno) y culmina con la ejecución (en las distintas áreas del Gobierno local). En medio, el control interno se sitúa en todo momento como el garante del cumplimiento de la legalidad, las normas contables y los demás principios de buena administración y buen gobierno, con unos roles destacados para la transparencia y la estabilidad presupuestaria. Como es natural, cada ciclo anual se superpone con el anterior y el posterior, por lo que cobra todo su sentido la presupuestación plurianual, no solo como principio de obligado cumplimiento (artículo 5 de la LOEPSF), sino como habitual y recomendable praxis de planificación a medio plazo, como también señala la normativa de la Unión Europea.

En definitiva, en torno al presupuesto se genera un volumen ingente y continuo de información, cuya fiabilidad es clave para generar confianza, ya que tiene implicaciones directas sobre la obtención, la aplicación, la contabilización y el control de los recursos públicos locales. Es clave para recabar los apoyos políticos necesarios, para lograr crédito suficiente en los mercados financieros y para la legitimidad democrática de las instituciones, en este caso, del sector público local.

El registro de los contenidos y/o las publicaciones presupuestarias en BC podría permitir, en todo momento y a cualquier usuario, comprobar si un concreto documento es el originalmente generado o emitido por otro usuario. También impediría que el propio emisor o el autor primigenio cometiesen fraude, remplazando contenidos o eliminándolos, ya que el nuevo tenor no se correspondería con el registrado. Por su parte, la entidad local podría publicar sus propios contenidos, a los que la ciudadanía tendría acceso en todo momento y en un entorno digital. Para tener garantías de que los documentos publicados son los originales, se precisa un mecanismo que permita al administrado comprobar la autenticidad de la información publicada. El registro en una cadena de bloques permitiría saber que los contenidos no se han alterado por ningún mecanismo interno o externo a la propia organización, lo cual, casi de forma paradójica, eleva los riesgos ligados a la ciberseguridad².

2. Se remite en este punto a las guías prácticas de fiscalización de los órganos de control externo autonómicos (GPF-OCEX), disponibles en la página web de la Asociación de Órganos de Control Externo Autonómicos (www.asocex.es). En particular, las GPF-OCEX 5311, 5312 y 5313.

Finalmente, el registro mediante BC podría aumentar la eficiencia del sistema presupuestario local, ya que los gestores públicos, como primera línea de defensa, garantizarían en todo momento la buena versión de los contenidos utilizados, elevando así el nivel de transparencia y la confianza ciudadana.

3. La contratación pública

La garantía de integridad y eficiencia de la contratación pública constituye una preocupación política, técnica y ciudadana, además de un mandato legal explícito de la LCSP. El ingente volumen de recursos movilizado a través de los contratos públicos es indiscutible e impacta de lleno en el crecimiento del PIB y del empleo (OECD, 2021). En el caso del sector público local, la licitación pública y la atribución de mercados tienen además un impacto claro y directo en la economía del territorio más cercano, al tiempo que operan como estímulo para la innovación y la sana competencia.

Las tecnologías emergentes van a seguir cambiando muchos procesos de contratación, desde la fase de planificación hasta la de ejecución, pasando por los estadios de licitación y adjudicación. Todo ello abre un campo inmenso a la mejora de los procedimientos, que puede redundar en beneficios para las personas responsables de los contratos, pero también a las empresas licitadoras y adjudicatarias y, en última instancia, a la ciudadanía.

El BC podría aportar beneficios a la contratación pública y contribuir a la transparencia total de los gastos públicos. Su uso iría desde el simple registro de la documentación de una oferta a la generación de contratos inteligentes que permitirían automatizar la atribución.

Comencemos con la licitación, donde el registro de todos los documentos digitalizados que conforman la oferta que presentan las empresas licitadoras podría hacerse a través de una cadena de bloques, garantizando la hora y la inmutabilidad de cada elemento del contenido. Cualquier añadido o modificación no sería reconocido por la cadena. También se pueden registrar, por ejemplo, los mensajes que se intercambien entre el contratante y los licitadores en este contexto. El potencial del registro en BC sería aún mayor si todos los registros administrativos estuviesen inscritos en una cadena de bloques, de tal forma que los documentos del expediente (escrituras, certificaciones u otras referencias) ya estarían registrados. Así, la participación en una licitación se reduciría a señalar unas entradas a documentos previamente registrados y a añadir a la cadena

la oferta presentada por la empresa. Está claro que estos usos facilitarían las tareas de la función de intervención y tendrían como beneficios, entre otros, la reducción de los riesgos de falta de conformidad con el proceso, el aumento de la seguridad y la transparencia, la automatización de la confirmación de fechas y plazos, o la eliminación de la necesidad de una verificación por terceras partes. Además, este procedimiento reduciría la carga de trabajo para las empresas y, a medio plazo, la de la entidad pública contratante.

El modelo basado en BC no se reduciría solo a la fase de licitación, sino que se podría extender a las demás fases del proceso, incluyendo toda la información relativa a facturas, albaranes de entrega, documentos de aceptación, o cobros y pagos. El registro en la cadena de bloques no se refiere exclusivamente a los documentos, a los que se atribuye una marca temporal, sino que cualquier metainformación que sirva para facilitar el proceso posterior puede acompañar a los documentos y, en consecuencia, quedará asociada a ellos (el código de contrato, la referencia de empresa o el tipo de documento, entre otros datos).

Para licitaciones sencillas -y, de manera singular, para contratos menores- la atribución podría automatizarse utilizando la tecnología de contratos inteligentes, esto es, contratos capaces de ejecutar reglas simples sin apenas intervención humana³.

Algunos de los documentos que acompañan a las transacciones del proceso de contratación digital ya pueden tener las características de inmutabilidad y marca temporal utilizando medios alternativos al registro en una cadena de bloques. Tal es el caso de la firma electrónica, utilizada en muchos procedimientos contractuales, no solamente para tener procedimientos cien por cien digitales, sino para dar más seguridad al procedimiento, garantizando la identidad del firmante, entre otros aspectos esenciales. En estos casos, cabe preguntarse cuál sería el valor añadido de BC, y la respuesta no es sencilla. Digamos con prudencia que son soluciones alternativas y complementarias, pero en modo alguno el BC arrasaría con técnicas y tecnologías de contratación pública más tradicionales (Quintana Cortés, 2020). El uso generalizado de la firma electrónica, su integración con las aplicaciones existentes y la confirmación de validez en cada caso requieren soluciones a problemas

3. Al respecto, destaca la iniciativa del Gobierno de Aragón para el desarrollo de una aplicación BC basada en contratos menores “inteligentes” (<https://www.blockchaineconomia.es/aragon-es-pionera-mundial-en-contratacion-publica-blockchain>) [recuperado el 1 de septiembre de 2021].

complejos. La garantía de inmutabilidad y accesibilidad a la información que da la cadena de bloques con el registro distribuido es su fuerte, pero por otro lado la falta de cobertura legal de BC en España en estos momentos hace que las soluciones en esta dirección no puedan ser más que exploratorias y que, por tanto, no podamos obtener el potencial beneficio máximo⁴.

4. Control económico-financiero

4.1. Control interno: nuevos retos

El artículo 213 del TRLRHL establece como modalidades para el ejercicio del control interno la función interventora, el control financiero –incluida la auditoría de cuentas- y el control de eficacia.

La función interventora (artículos 214 a 219 del TRLRHL) es la que goza de mayor tradición en el mundo local, tanto por su óptica de legalidad como por su acotado alcance, ya que despliega sus actuaciones con carácter previo a la adopción de un específico acuerdo o una resolución (Fueyo Bros, 2018). Tiene por objeto fiscalizar todos los actos de las entidades locales y sus organismos autónomos (no así de las empresas públicas) que den lugar al reconocimiento y liquidación de derechos y obligaciones o gastos de contenido económico (o que puedan tener repercusión financiera o patrimonial), los ingresos y pagos que de aquellos se deriven y la recaudación, la inversión y aplicación, en general, de los caudales públicos administrados, con el fin de que la gestión se ajuste a las disposiciones aplicables a cada caso, emitiendo el correspondiente informe y formulando los reparos procedentes.

El control financiero (artículo 220 del TRLRHL) tiene por objeto comprobar *a posteriori* el funcionamiento económico-financiero de los servicios de las entidades locales, de sus organismos autónomos y de las sociedades mercantiles dependientes. Su finalidad es aprobar informes para poner a disposición del gestor acerca de la adecuada presentación de la información financiera, del cumplimiento de las normas y directrices que sean de aplicación, y del grado de eficacia, eficiencia y economía en la consecución de los objetivos previstos. El control se realizará por procedimientos de auditoría pública, de

4. Sobre estos temas, en todo caso, se profundiza en el capítulo del presente volumen colectivo elaborado por María Hernando Rydings, al que en este momento hemos de remitirnos.

acuerdo con las normas técnicas nacionales e internacionales, en términos homogéneos a los desarrollados en otros ámbitos del sector público español⁵. El control de eficacia (artículo 221 del TRLRHL) ha quedado subsumido *de facto* dentro del control financiero, constituyendo su objeto la comprobación periódica del grado de cumplimiento de los objetivos, así como el análisis del coste de funcionamiento y del rendimiento de los servicios o las inversiones.

Ninguna de las modalidades de control interno es infalible ni completa, de lo cual se colige que todas ellas son compatibles y mutuamente necesarias. La gran ventaja de la función interventora y su enfoque de legalidad es que puede advertir de incumplimientos antes de que se produzcan, incluso con efectos suspensivos, evitando -o, en su caso, retrasando- el potencial quebranto o las responsabilidades administrativas, contables o penales que se pudieran producir. Por su parte, el control financiero y de eficacia resulta apropiado cuando se pretende imprimir un enfoque más ágil y autónomo de la gestión pública. Estas potenciales ventajas de cada una de las modalidades de ejercicio del control interno parecen claras, pero encierran al mismo tiempo sus propias debilidades. Así, la función interventora suele estar muy focalizada en el concreto expediente administrativo, por lo que puede no resultar adecuada para una visión de conjunto de la gestión pública, además de introducir, so pretexto de una interpretación demasiado rigorista de las normas, una excesiva ralentización de la actividad ordinaria de la entidad local. En el otro lado, el control financiero exige una cuidada planificación general de la entidad y de sus áreas de trabajo, sustentada sobre un análisis de riesgos y sobre objetivos mensurables y adaptativos, basados en indicadores transparentes que permitan su correcta evaluación y la delimitación de eventuales responsabilidades por incumplimiento. Desde otro punto de vista, la función interventora requiere de especialistas en legalidad administrativa, subvencional, contable, contractual y presupuestaria, mientras que el control financiero y de eficacia, además, exige competencias extrajurídicas y técnicas de análisis económico, auditoría pública y evaluación de políticas y sistemas de información, algo que no suele abundar en las administraciones públicas, por pura tradición en la selección de su personal.

Por todo lo anterior, parece deseable un tránsito gradual desde una función interventora hegemónica a otro modelo donde el control financiero y de eficacia vaya teniendo un mayor protagonismo, en simbiosis con la primera.

5. El control financiero no exige a las sociedades mercantiles que formen parte del sector público local de las auditorías anuales obligatorias a las que deben someterse, en los términos que dispone la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas.

No obstante, como ya se señaló en Fernández Llera y Oviedo Creo (2018), existen otros condicionantes que deben ser anotados. El primero, el tamaño de la jurisdicción, sobre todo en un mapa municipal tan atomizado como el español, con miles de municipios de tamaño demográfico ínfimo, presupuestos de mínimos y competencias que no se pueden desplegar. En estos casos (la inmensa mayoría), la única modalidad realista de control interno es la función interventora, pero, viceversa, en los mayores ayuntamientos, con gran volumen y complejidad de actividades y servicios, el control financiero y de eficacia, no solo es recomendable, sino que debería constituir una verdadera prioridad⁶. En segundo lugar, no es posible prescindir del todo de la función interventora, por la sencilla razón de que existen numerosas disposiciones legales que la convierten en un deber ineludible en materias de contratación pública, ingresos, personal o subvenciones. Como mera hipótesis, aunque el legislador decidiese desterrar este tipo de obligaciones (supuesto harto improbable), la función interventora seguiría siendo inexcusable como mecanismo para asegurar el control previo de legalidad, prevenir la corrupción y minimizar el fraude. Como corolario, se podría decir que un óptimo control interno debe pasar por la combinación entre una eficaz y diligente función interventora y un control financiero y de eficacia que permita conjugar autonomía local, responsabilidad, rendición de cuentas y cumplimiento de objetivos.

Para llegar a cumplir con esa ambiciosa meta, y en desarrollo del artículo 213 del TRLRHL, el Gobierno de España aprobó el Real Decreto 424/2017, de 28 de abril, por el que se regula el régimen jurídico del control interno en las entidades del Sector Público Local. Su objetivo es lograr un control económico-presupuestario más riguroso y reforzar el papel de la función interventora en las entidades locales, tal y como también había adelantado la Ley 27/2013, de 27 de diciembre, de racionalización y sostenibilidad de la Administración Local (LRSAL).

El nuevo reglamento declara la plena autonomía del órgano interventor local respecto de las autoridades y entidades cuya gestión sea objeto del control. A tal efecto, los funcionarios con habilitación nacional que lo realicen tendrán independencia funcional respecto de los titulares de las entidades controladas⁷. De igual modo, el Real Decreto 424/2017 también recoge la posibilidad

6. Por su relevancia, se señala el documento estratégico de 2018 de la Intervención General del Ayuntamiento de Madrid para un renovado modelo de control interno local (disponible en www.madrid.es) [recuperado el 1 de junio de 2021].

7. Al respecto, debe estarse a lo dispuesto en el Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.

de solicitar asesoramiento técnico a diversas instancias, en particular a la Intervención General de la Administración del Estado (IGAE), mediante la formalización del convenio previsto en la disposición adicional séptima de la LRSAL. En tercer lugar, el reglamento establece que las entidades locales deberán garantizar y adoptar las medidas necesarias para la defensa jurídica y la protección del personal controlador en los procedimientos que se sigan ante cualquier orden jurisdiccional, como consecuencia de su participación en actuaciones de control interno. Igualmente, se debe asegurar, “con medios propios o externos, el control efectivo de, al menos, el ochenta por ciento del presupuesto general consolidado del ejercicio mediante la aplicación de las modalidades de función interventora y control financiero”, y, en todo caso, en “tres ejercicios consecutivos y en base a un análisis previo de riesgos, deberá haber alcanzado el cien por cien de dicho presupuesto”.

En desarrollo de su tarea, el órgano interventor deberá entregar los resultados más relevantes del control a los órganos de gestión controlados y, del mismo modo, recomendará al gestor las actuaciones que resulten aconsejables⁸. También deberá dar cuenta al Pleno de los resultados que contengan una “especial trascendencia”, a su profesional juicio, informando sobre la situación de la corrección de las debilidades puestas de manifiesto y haciendo expresa mención del grado de cumplimiento de los principios del ejercicio del control interno.

Aunque son numerosas las novedades del Real Decreto 424/2017, destacamos ahora tres.

Para empezar, se establece que la Presidencia y el Pleno, ante un reparo del órgano de control interno y antes de la resolución de la discrepancia, podrán elevar la propuesta de resolución al órgano de control competente por razón de la materia de la Administración que tenga atribuida la tutela financiera (IGAE o comunidad autónoma, según el caso), concretando los extremos acerca de los que solicitan valoración. Dicho órgano deberá informar con criterio técnico de las cuestiones planteadas, aunque sin carácter vinculante⁹.

8. Por definición, las recomendaciones no son vinculantes, pero al menos deberían servir para que el gestor local motive su alejamiento, aplicando el principio de “cumplir o explicar”. En un ámbito conexo, esto ya se recoge para las recomendaciones contenidas en los informes evacuados por la Autoridad Independiente de Responsabilidad Fiscal (artículo 5 de la Ley Orgánica 6/2013, de 14 de noviembre, de creación de la Autoridad Independiente de Responsabilidad Fiscal).

9. El proyecto de reglamento sí preveía tal carácter, pero no fue recogido en la norma aprobada, tras la observación esencial contraria formulada por el Consejo de Estado en su Dictamen 795/2015.

La segunda novedad es que el órgano interventor debe elevar cada año al Pleno, con ocasión de la dación de cuenta de la liquidación, un informe de todas las resoluciones adoptadas por la Presidencia de la entidad local contrarias a los reparos efectuados o, en su caso, a la opinión del órgano competente de la Administración que ostente la tutela financiera al que se haya solicitado informe, así como un resumen de las principales anomalías detectadas en materia de ingresos. Dicho informe atenderá únicamente a aspectos y cometidos propios del ejercicio de la función fiscalizadora, sin incluir cuestiones de oportunidad o conveniencia de las actuaciones que fiscalice¹⁰.

Y la tercera, dando la posibilidad de que el Pleno de la entidad local apruebe la fiscalización limitada previa y los requisitos básicos que el órgano interventor deberá comprobar, en coherencia con lo previsto para la Administración del Estado¹¹. El Pleno podría aprobar otros extremos, pero debe asegurar que con ellos se mantienen la objetividad, la transparencia, la no discriminación y la igualdad de trato en las actuaciones públicas.

En todo caso, están sometidos a fiscalización previa todos los actos de los órganos de la entidad local y de sus organismos autónomos, cualquiera que sea su calificación, por los que se apruebe la realización de un gasto. Entre los actos sometidos a la intervención previa se consideran incluidos los actos resolutorios de recursos administrativos que tengan contenido económico, los convenios que se suscriban, y cualquier otro acto de naturaleza análoga, siempre que tenga contenido económico. Por el contrario, el reglamento declara exentos de fiscalización previa los gastos de material no inventariable, los de contratos menores, los de carácter periódico y demás de tracto sucesivo (una vez fiscalizado el gasto correspondiente al período inicial del acto o contrato del que deriven o sus modificaciones) y los menores de 3005,06 euros que, de acuerdo con la normativa vigente, se hagan efectivos a través del sistema de anticipos de caja fija. En caso de omisión de la función interventora cuando esta era preceptiva, el reglamento prevé que no se pueda reconocer la obligación, ni tramitar el pago, ni intervenir favorablemente estas actuaciones hasta que se resuelva en tiempo y forma la omisión.

Por lo que respecta al control financiero, el Real Decreto 424/2017 hace una regulación más proactiva, trasluciendo una clara intencionalidad

10. Este punto también fue controvertido durante la fase previa a la aprobación del reglamento, cuando se discutió sobre el exacto alcance de los informes del órgano interventor.

11. Se comprobarán la existencia y adecuación del crédito presupuestario, la competencia del órgano y aquellos otros extremos que se consideren trascendentes (a la fecha, los que señala el Acuerdo del Consejo de Ministros de 30 de mayo de 2008, modificado en 2010, 2011, 2018, 2019 y 2021).

sobre su impulso, tal y como ya se ha comentado. Se ejercerá sobre la administración general de la entidad local y los organismos públicos en los que se realice la función interventora, para comprobar de forma continua el ajuste de la actividad al ordenamiento jurídico y a los principios de buena gestión financiera, con el fin último de mejorar la gestión en su aspecto económico, financiero, patrimonial, presupuestario, contable, organizativo y procedimental. El ejercicio del control permanente comprende las actuaciones de control que anualmente se incluyan en el Plan Anual de Control Financiero y las actuaciones que sean atribuidas en el ordenamiento jurídico al órgano interventor.

Figura 1. Modalidades de control interno local



* Incluye el control de eficacia. Fuente: elaboración propia a partir del Real Decreto 424/2017.

Por su parte, la auditoría pública consistirá en la verificación posterior y sistemática de la actividad económico-financiera del sector público local, mediante procedimientos de revisión selectivos contenidos en las normas técnicas e instrucciones que dicte la IGAE. La modalidad específica de auditoría financiera tiene por objeto verificar si las cuentas anuales representan en todos los aspectos significativos la imagen fiel del patrimonio, de la situación financiera, de los resultados de la entidad y, en su caso, la ejecución del presupuesto de acuerdo con las normas y principios contables y presupuestarios que le son de aplicación, y si contienen la información necesaria para su interpretación y comprensión adecuada. El órgano

interventor local realizará anualmente la auditoría de las cuentas anuales de los organismos autónomos, las entidades públicas empresariales, las fundaciones obligadas a auditarse por su normativa específica, los fondos sin personalidad jurídica dotados en su mayoría desde el presupuesto local y los consorcios adscritos a la entidad local, así como también las sociedades mercantiles y las fundaciones del sector público local no sometidas a la obligación de auditarse que se hubieran incluido en el plan anual de auditorías. De otro lado, la auditoría de cumplimiento y la auditoría operativa se ejercerán sobre las entidades del sector público local no sometidas a control permanente, con el fin último de mejorar la gestión del sector público local en su aspecto económico, financiero, patrimonial, presupuestario, contable, organizativo y procedimental. La figura 1 desglosa las modalidades de control recogidas en el Real Decreto 424/2017.

La importancia de la planificación en el control financiero tiene su culmen en la obligación de un Plan Anual de Control Financiero, verdadera clave de bóveda del nuevo modelo. Este documento estratégico debe ser realizado y aprobado por el órgano interventor, como principal garantía de independencia técnica del control interno. El principio democrático queda salvaguardado con la obligación de su remisión al Pleno, a efectos informativos.

El Plan Anual de Control Financiero incluirá todas aquellas actuaciones de control permanente y auditoría pública que deriven de una obligación legal, así como las que cada año se seleccionen, sobre la base de un análisis de riesgos, consistente con los objetivos a conseguir, las prioridades de cada ejercicio y los medios disponibles.

Una vez identificados los riesgos y calibrados los recursos disponibles, será necesario asignar prioridades para seleccionar las actuaciones a realizar. De esta manera, se realizará una evaluación para estimar la importancia del riesgo -utilizando criterios cuantitativos y cualitativos- y la conveniencia de seleccionar controles con regularidad y rotación, evitando repetir controles en actividades sin riesgo y, al mismo tiempo, generar debilidades por la ausencia reiterada de control.

Con respecto a la posible colaboración público-privada en la realización de auditorías públicas, se admite que, en caso de insuficiencia de medios, mediante los oportunos convenios o contratos, podrán colaborar con las entidades locales otros órganos públicos o firmas privadas de auditoría. Para evitar una pérdida de “control sobre el control”, valga la expresión, no se debería admitir el modelo

inercial de justificación de falta de medios que asiduamente se incorpora a los expedientes y que ha cuestionado el Tribunal de Cuentas¹².

4.2. Rendición de cuentas y control externo

La relación entre el control interno local y el control externo no solo debe estar basada en colaboración, complementariedad y confianza, sino que debe sustentarse en una retroalimentación de sus respectivos trabajos, basada a su vez en el análisis y la ponderación de riesgos. Las Normas Internacionales de Entidades Fiscalizadoras Superiores adaptadas a España establecen: “ambos tipos de auditoría promueven el buen gobierno al contribuir a la transparencia y a la rendición de cuentas respecto al uso de los recursos públicos, así como sobre la economía, eficiencia y eficacia de la actuación de la Administración pública” (ISSAI-ES 100). Si antes hemos afirmado que dentro del control interno deben convivir la función interventora y la de control financiero (cada una con sus objetivos y finalidades), no es menos cierto que la coexistencia del control interno y el control externo tampoco está en discusión, reservando para este la función de supervisión sobre el primero. Así lo explicita la llamada “carta magna” de la auditoría pública, la *Declaración de Lima*, aprobada en 1977 por la Organización Internacional de Entidades Fiscalizadoras Superiores¹³: “asegurada la eficacia del órgano de control interno, ha de aspirarse a la delimitación de las respectivas funciones, a la delegación de las funciones oportunas y a la cooperación entre la entidad fiscalizadora superior y el órgano de control interno, independientemente del derecho de la entidad fiscalizadora superior a un control total”. En 2004, el Tribunal de Cuentas Europeo¹⁴ dictaminó: “un sistema eficiente y eficaz de controles internos de los ingresos y gastos de la Unión Europea ayudaría de manera significativa al Tribunal a desempeñar la función de auditor externo de la Unión Europea que le ha otorgado el Tratado”. En resumen, la pregonada convivencia entre control interno y fiscalización externa solo puede ser concebida como una secuencia eficaz de controles complementarios.

Descendiendo al ámbito local, se extrae la necesidad de que la institución de control externo disponga en todo momento de una panorámica suficiente de la entidad fiscalizada que, siguiendo a Cabeza del Salvador (2015), incluiría

12. *Informe de fiscalización de los contratos de asistencia técnica para la realización de auditorías en las entidades locales, ejercicios 2004, 2005 y 2006*, disponible en www.tcu.es [recuperado el 1 de junio de 2021].

13. INTOSAI-P 1, disponible en www.issai.org [recuperado el 1 de septiembre de 2021].

14. Dictamen 2/2004 (*Diario Oficial de la Unión Europea* del 30 de abril de 2004).

estas fases: conocimiento de la entidad; identificación de áreas críticas; conocimiento y evaluación preliminar del control interno de la entidad; identificación y valoración de riesgos; definición de la estrategia y las pruebas de auditoría; elaboración del informe de auditoría, basado en el procedimiento contradictorio, con opinión, conclusiones y recomendaciones. Este proceso debe ser permanente y recurrente, lo que exige una cuidada planificación de los trabajos para que pueda generar un sólido sustrato de conocimiento, liberando así recursos para poder ser destinados a la realización de nuevas pruebas de auditoría externa o trabajos adicionales en otras áreas.

La relación entre el control interno local y el órgano de control externo no forma parte del objeto del Real Decreto 424/2017, aunque sí se formulan algunas referencias mínimas, en la línea de colaboración que se ha descrito. En primer lugar, cuando se establece la obligación para la IGAE de gestionar “una base de datos sobre los informes emitidos en relación con las propuestas de resolución de discrepancias sometidas a su valoración, con objeto de unificar criterios y realizar el seguimiento de su aplicación”. A continuación, se regula el acceso a dicha base de datos por los órganos de control interno locales y autonómicos, el Tribunal de Cuentas y los órganos de control externo autonómicos, para coadyuvar a sus respectivas tareas. De igual modo, se reglamenta el momento en el que el órgano interventor debe remitir al control externo todas las resoluciones adoptadas por la Presidencia de la entidad local contrarias a los reparos efectuados o, en su caso, a la opinión del órgano competente de la Administración que ostente la tutela financiera al que se haya solicitado informe, así como un resumen de las principales anomalías detectadas en materia de ingresos. El reglamento vuelve a mencionar el órgano de control externo cuando se refiere a la intervención de las cuentas justificativas de los pagos a justificar y anticipos de caja fija, así como en el artículo relativo a la obtención de información, documentación y asesoramiento técnico en las actuaciones de control financiero, en el marco del deber legal de colaboración que tienen los órganos gestores con el órgano de control interno local.

En la práctica, las instituciones de control externo españolas han venido desplegando en los últimos años un notable esfuerzo para supervisar el control interno en las entidades locales. El método habitual ha sido el cuestionario elaborado por el auditor externo y girado a las personas responsables de la gestión local y a quienes tienen atribuida la función de control interno. En una segunda etapa, se comprueba la veracidad y la exactitud de las respuestas a los cuestionarios, a través de diversas pruebas de auditoría.

Un aspecto determinante en la relación descrita es la rendición de cuentas locales en plazo y forma ante las instituciones de control externo, así como la remisión de contratos y la tramitación del presupuesto local en los términos que establecen el TRLRHL, la LCSP y el resto de la normativa aplicable. El segundo aspecto práctico donde los órganos de control externo autonómicos (OCEX) y el Tribunal de Cuentas llevan años trabajando conjuntamente es el seguimiento de los acuerdos contrarios a reparos en las entidades locales, así como de la información remitida en virtud del artículo 218 del TRLRHL y del Real Decreto 424/2017.

Como ha dejado sentado el Tribunal de Cuentas¹⁵, “la rendición de cuentas constituye el mecanismo a través del cual los responsables de la entidad responden de la gestión económico-financiera desarrollada ante quienes les proporcionan sus recursos y atienden a las necesidades de información de los usuarios [de tal información...]: el parlamento nacional, el Tribunal de Cuentas, las asambleas legislativas autonómicas, los órganos de control externo autonómicos, los gestores, los órganos de control interno, los usuarios de los servicios públicos, los órganos de representación política, los acreedores, los analistas económicos y financieros, los servicios de *rating*, las organizaciones públicas nacionales o internacionales, los contribuyentes y los ciudadanos en general”.

Para facilitar el cumplimiento de ese deber general de colaboración con el control externo y de las concretas obligaciones de rendición de cuentas, de remisión de contratos y de otra información económico-financiera relevante, son variadas las medidas que se han ido desplegando en los últimos años. Algunas han incidido en los aspectos jurídicos, reforzado incentivos positivos y negativos, como cuando se vincula la percepción de subvenciones a la correcta rendición de cuentas o se introducen multas coercitivas o sanciones personales (Teré Pérez, 2015). Otras medidas más instrumentales han tenido como envolvente la inmersión tecnológica, dentro del proceso general de modernización y digitalización de la gestión pública y del control económico-financiero (Cordero Valdavidia, 2020). La combinación de todo ello, junto a un proceso general de relegitimación democrática y revalorización de la transparencia y el buen gobierno, han derivado causalmente -nada es casual- en un mejorado grado de cumplimiento en los últimos años, no obstante, situado aún lejos del óptimo deseable (Fernández Llera, 2020).

15. *Informe sobre actuaciones del Tribunal de Cuentas para promover la rendición de cuentas en el ámbito local*, disponible en www.tcu.es [recuperado el 1 de junio de 2021].

Una de las herramientas que más han contribuido a ese éxito relativo ha sido, desde su pionero lanzamiento en 2007, la plataforma telemática de rendición de cuentas locales, promovida, gestionada y financiada por el Tribunal de Cuentas y los OCEX, en lo que en sí mismo ya supone un formidable éxito de colaboración institucional¹⁶. Esta plataforma permite transferir electrónicamente la información sobre las cuentas anuales, además, en un único y simultáneo acto al Tribunal de Cuentas y al órgano de control externo autonómico (algo que en papel era inviable). Dicha transferencia se puede realizar mediante generación automatizada de un fichero de datos procedente de una aplicación de contabilidad de la entidad local, o bien mediante la entrada de datos vía una interfaz de usuario. El fichero de datos se acompaña de toda una serie de informaciones electrónicas y ficheros que completan la cuenta general, integrada por las cuentas anuales de la entidad local principal, las de sus unidades dependientes y las de los consorcios y fundaciones con adscripción a la matriz. La plataforma automatiza una serie de controles, y además en los últimos años se han añadido las funcionalidades de remisión de contratos públicos y de supervisión del control interno (resoluciones y acuerdos contrarios a los reparos formulados por el órgano interventor local, así como un resumen de las principales anomalías en materia de ingresos).

Cada entidad local debe subir a la plataforma el fichero en formato XML con la información contable, generado de manera automática por las distintas aplicaciones de contabilidad locales, cumpliendo en todo caso con el formato normalizado aprobado por la IGAE. Se dispone así de un producto de uso compartido y homologado. En el hipotético caso de que las entidades locales no dispongan aún de una aplicación contable que genere el fichero XML, la plataforma incorpora formularios para cumplimentar los datos de los distintos estados contables.

Además de facilitar la carga del fichero XML generado por la aplicación de contabilidad, la plataforma de rendición de cuentas permite incorporar los formularios necesarios para cubrir las notas de la memoria, así como adjuntar el resto de ficheros complementarios que conforman la cuenta general de la entidad local: actas de arqueo, justificantes de saldos bancarios, estado de conciliación de la entidad, PDF con los estados integrados y consolidados, PDF con la memoria justificativa del coste y rendimiento de los servicios públicos, PDF con la memoria demostrativa del grado de

16. El acceso al portal público y al área privada se realiza desde www.rendiciondecuentas.es.

cumplimiento de los objetivos, PDF con el certificado de aprobación de la cuenta general o, en su caso, de su presentación al pleno¹⁷. Con respecto a las cuentas de las unidades dependientes o adscritas, los documentos PDF que se deben adjuntar varían en función del régimen contable de aplicación (público o empresarial). Una vez que se ha subido toda la información de la cuenta general, el paso siguiente es la validación y el envío. La primera consiste en comprobar la coherencia de los datos incorporados, incluyendo comprobaciones de carácter aritmético y verificaciones de datos de cumplimiento legal (por ejemplo, sobre la fecha exacta de aprobación del presupuesto o de la liquidación).

Como ya se ha dicho, además de la rendición de la cuenta general, las entidades locales deben enviar a través de la plataforma telemática la información contractual, incluyendo las relaciones anuales de contratos y los extractos de los expedientes de contratación que señala el artículo 335 de la LCSP, en función de su tipología e importe. La relación anual de contratos incluye los menores, cuya importancia -por número y cuantía- es nuclear en el caso de las entidades locales. En caso de no haberse formalizado ningún contrato en el ejercicio, las entidades deben comunicar la certificación negativa correspondiente. De manera análoga, las entidades locales deben remitir a través de la plataforma la relación anual de convenios suscritos (o la certificación negativa, en su caso), incluyendo los extractos de aquellos cuyos compromisos económicos asumidos superen los 600 000 euros.

En el avance hacia una plena digitalización de la fiscalización, es preciso también comentar el impacto de una plataforma de auditoría en cuanto que desarrollo adicional y lógico de este proceso de modernización.

Como es sabido, dentro de la estructura organizativa de las instituciones de control externo, los trabajos de auditoría corresponden a las áreas y los departamentos de fiscalización, mientras que en las tareas de tramitación intervienen las secretarías generales o áreas administrativas, responsables de dar fe en los documentos que así lo requieran y del registro general. Para poder dar cobertura a los trabajos de fiscalización se utilizan herramientas informáticas que garantizan los principios de la auditoría, sustituyendo los papeles de trabajo tangibles por los registros de trabajo electrónicos, lo que con ironía Riera López (2015) ha resumido como “perder los papeles” (sic).

17. Desde 2021 ya no es preceptiva la aprobación plenaria, según lo dispuesto en el artículo 212.5 del TRLRHL.

En suma, la digitalización de muchos procedimientos ha supuesto que el auditor externo esté dando paso a un entorno plenamente informatizado y digital (Cordero Valdavida, 2018).

En la tramitación de un informe de fiscalización, será el expediente digital el que dé soporte a la gestión y tramitación de los documentos que han sido aprobados y firmados por los órganos competentes. También asegura las comunicaciones establecidas con los entes fiscalizados, ya sea a través de notificaciones o de comunicaciones electrónicas.

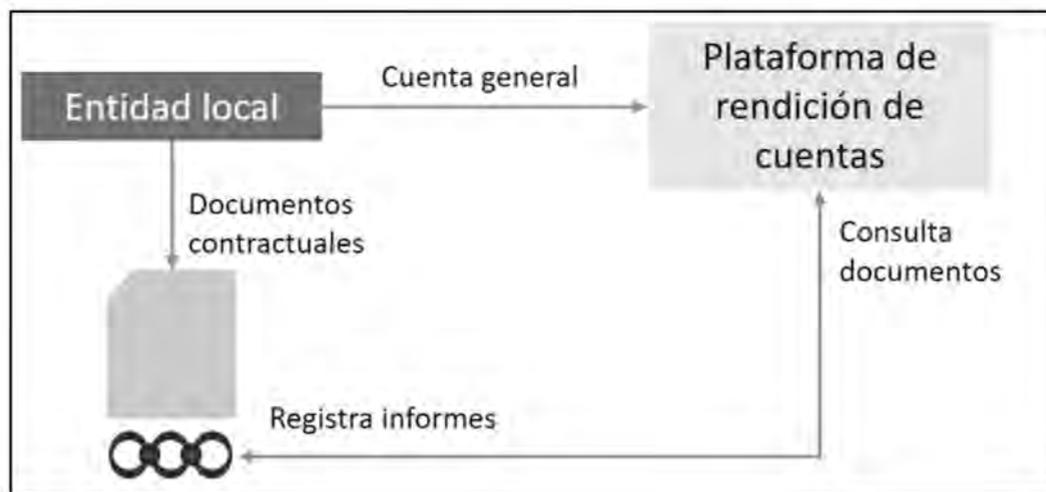
Una plataforma de auditoría tiene como finalidad facilitar el proceso completo, por lo que estas dos líneas de actuación -rendición de cuentas y trabajo de campo de la auditoría- deben ir de la mano, si bien no siempre será posible una integración al 100 % de todas las actividades administrativas. En cada una de ellas, los recursos disponibles en la institución de control externo, tanto humanos (sobre todo humanos) como tecnológicos, deben implicarse para poder completar con éxito los trabajos de auditoría, ya que un informe en el sector público no podría ver la luz sin el respaldo que otorga la tramitación administrativa del mismo.

4.3. Tecnologías emergentes: ¿es posible algún paso más?

La plataforma se ha consolidado con éxito como un elemento fundamental de transparencia, rendición de cuentas y control. En consecuencia, cabe preguntarse si BC podría contribuir a mejorar el sistema, y si lo podría hacer a un coste razonable, en términos pecuniarios y operativos, pero también analizando los nuevos riesgos potenciales. Si todas las respuestas son positivas, la siguiente cuestión sería acerca del modo de implementación del sistema resultante.

Desde un punto de vista teórico, la figura 2 indica cómo se podría hacer evolucionar la plataforma de rendición de cuentas mediante el uso de BC. En síntesis, se trataría de complementar la plataforma con una interfaz a un registro de documentos en BC. Las entidades locales, que ya habrían registrado sus documentos contractuales en la cadena de bloques, enviarían a la plataforma los documentos con garantía de fiabilidad, o incluso, simplemente, una referencia al registro. Por su lado, la plataforma también podría utilizar BC como registro para sus propios informes y resultados.

Figura 2. Posible uso de BC en conjunto con la plataforma de rendición de cuentas



Fuente: elaboración propia.

La solución debería ser única, desarrollada de forma centralizada y utilizada por todas las entidades de control. En tal caso, los potenciales beneficios de la propuesta serían varios. Primero, permitir la posibilidad de registrar una sola vez un documento y ser utilizado en todos los procesos: intervención, contratación, rendición de cuentas. Segundo, validar la unicidad y autenticidad de los documentos sujetos a intercambio electrónico, añadiendo un nivel adicional de seguridad, garantizando las fechas y los plazos de entrega. Tercero, automatizar, aún más, el proceso de control, al permitir añadir otros controles basados en la información documental. Y, finalmente, aumentar la transparencia, poniendo a disposición de la ciudadanía todos los estados contables y documentos relacionados con las cuentas.

A pesar de los mensajes positivos anteriores, hay que reconocer que la madurez de BC para su uso en el sector público es, todavía, muy baja, por lo que conviene recomendar prudencia en este punto, sobre todo cuando la tecnología en vigor (en este caso, la plataforma telemática de rendición de cuentas locales) funciona y evoluciona de forma muy satisfactoria.

Para concluir este epígrafe es preciso reflexionar sobre la pregonada extensión del control financiero y de las técnicas de auditoría pública, como

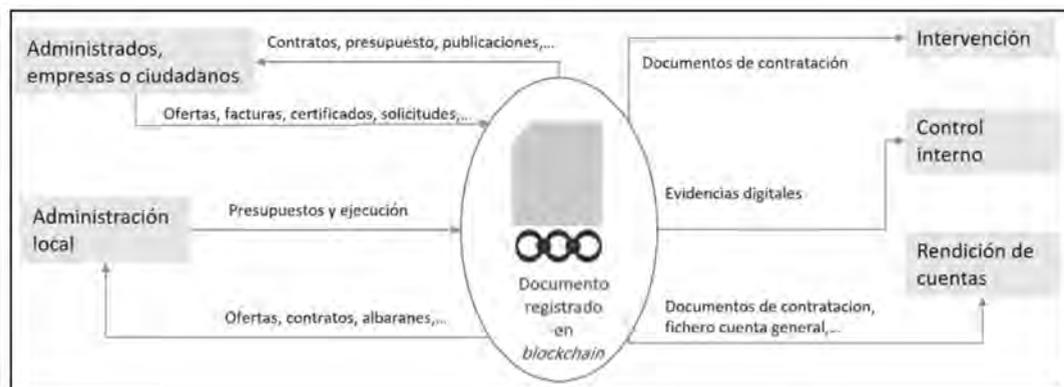
mandato normativo, pero también como necesidad frente a una creciente demanda ciudadana.

Partamos de que cuanto más se digitalizan los procesos de gestión, y en particular la gestión financiera, los hechos y las evidencias también tienen un marcado carácter digital. En este punto es relevante distinguir entre realidades digitales “nativas” (como puede ser un proceso digital de contratación de principio a fin) y realidades digitales “migradas” (procedimientos en los que el activo subyacente es físico, pero cuya gestión se ha digitalizado mediante la creación de un gemelo digital). En la segunda categoría estaría, por ejemplo, la traza que deja la presencia del personal en un edificio cuando fichan a la entrada y a la salida, permitiendo al órgano gestor y/o al controlador un análisis de la realidad sin tener una observación directa.

De otro lado, las evidencias digitales tienen que protegerse contra el fraude, también digital. De la misma forma que existen las noticias falsas, se pueden generar evidencias mendaces o transformadas que distorsionen la realidad y dificulten su control efectivo. La garantía sobre el contenido de las evidencias digitales se convierte en un reto, para el que ya existen herramientas, como la señalada firma digital que permite sellar el contenido inmutable de un documento.

La tecnología BC podría transformar el paradigma, haciendo que su incorporación en los procedimientos administrativos y demás procesos de gestión facilitase el control por diseño (Cordero Valdavidia, 2020). Si todos los contenidos quedasen registrados en la cadena de bloques, incluyendo la metainformación adecuada, el proceso de control podría automatizarse en gran medida, ya que la información almacenada en BC ofrecería una traza de evidencias lista para ser analizada por los equipos auditores. Dicha información aparecería encriptada en un sistema único, habría sido aprobada por un protocolo de consenso, estaría disponible para todos los participantes, no podría ser alterada y, en definitiva, contaría con marca temporal y huella digital exclusiva. La figura 3 presenta un esquema de los distintos actores en el proceso de presupuesto y gasto público, incluyendo algunos ejemplos de las posibles dinámicas de registro y acceso a la información.

Figura 3. Un registro en BC para las entidades locales



Fuente: elaboración propia.

Huelga decir que la auditoría de sistemas de información sería la modalidad de control *ex post* que podría recoger mejores ventajas y obtener mayores beneficios del BC, si bien, una vez más, se debe alertar de las numerosas incertidumbres que se ciernen sobre el horizonte normativo y práctico¹⁸.

5. Conclusiones y prudencias

Más allá del primigenio ámbito monetario, el BC lleva ya tiempo pidiendo paso hacia su aplicación en otras esferas de la gestión empresarial y del sector público, si bien con la misma idea subyacente de confianza, articulada ahora en torno a un “producto” (la información o, más en concreto, el valor de esa información) que unas “partes” (emisor-vendedor y receptor-consumidor, pero también múltiples usuarios e interesados ajenos) desean intercambiar en un “mercado” mundial. Haciendo un símil con la primera ley de la termodinámica, el BC no crea ni destruye la confianza (basada en personas, instituciones u organismos certificadores), pero sí la transforma en un consenso de los participantes en torno a la tecnología de grabación de la información. Se pasa de una confianza tutelada a una confianza descentralizada y distribuida (Preukschat, 2017).

El BC ya no es en puridad una nueva tecnología, dada la vertiginosa evolución en este ámbito. En cambio, sus aplicaciones cotidianas sí pueden

18. Se remite en este punto a las GPF-OCEX 5300, 5330, 5340 y 5370, disponibles en la página web de la Asociación de Órganos de Control Externo Autonómicos (www.asocex.es).

resultar muy innovadoras como integrantes del proceso de transformación digital, acelerado de forma notable en la última década y explotado con motivo de la pandemia de la COVID-19. Para ello, conviene señalar que el BC no es -ni podría serlo- un patrimonio exclusivo de una disciplina concreta o de unas pocas áreas de gestión. Antes bien, exige una combinación de saberes y técnicas, por supuesto relacionados con la informática, pero también de las matemáticas, el derecho, la economía o la sociología, entre otros.

La valoración presente de BC en su aplicación al sector público, y más específicamente a las entidades locales, ha de ser prudente. Entre otros aspectos, condicionan bastante las carencias del marco legal (Wanden-Berghe Lozano y Fernández Daza, 2020), en particular con respecto a la utilización del BC en procedimientos oficiales o a la normativa sobre protección de datos personales (que favorece las infraestructuras BC privadas frente a las de carácter público). Todo ello rompe con el concepto original de sistema abierto y multidimensional, complicando el desarrollo de las soluciones, debido al gran esfuerzo requerido de inversión en infraestructura y actualización normativa¹⁹, aunque al tiempo constituye la mejor salvaguarda o el freno más evidente frente a eventuales vulneraciones de derechos. El potencial de BC para contribuir a la transformación digital del sector público es indudable, partiendo de su conceptualización como sistema capaz de aumentar la calidad de la información y mejorar la confianza ciudadana en sus instituciones. Sin embargo, hay obvios contrapesos a colocar en el otro plato de la balanza.

La inmersión tecnológica que está en la base del proceso de digitalización no ha sido suficiente hasta el momento para que el BC explote como en su momento sí lo hicieron internet o las redes sociales. Incluso existe el riesgo de que el potencial beneficio central del BC sea superado en el ínterin por otras tecnologías emergentes derivadas de la inteligencia artificial (Mota Sánchez *et al.*, 2021).

La buena administración no es un mero desiderátum, sino un derecho fundamental de la persona, también en el ámbito digital, al que la tecnología

19. En la Unión Europea existen iniciativas como el *European Blockchain Services Infrastructure*, de cuyos resultados dependerá también su eventual utilización en el sector público local (<https://ec.europa.eu/cefdigital/wiki/display/cefdigital/ebsi>) [recuperado el 30 de septiembre de 2021].

en sus diferentes manifestaciones puede y debe contribuir²⁰. Como indica el clarificador preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, “los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales”. Incluso recomienda que “una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales”. Señala también la citada Ley Orgánica que, “en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea”. Al respecto, debe destacarse la reciente aprobación por el Gobierno de España de la Carta de Derechos Digitales (Barrio Andrés, 2021), no tanto con carácter normativo cuanto de “marco de referencia para la acción de todos los poderes públicos”, en palabras del presidente del Gobierno²¹.

En definitiva, el BC puede ser una ayuda, un complemento, una nueva vía de circulación y gestión de la información, pero cabe preguntarse si no serán demasiados los riesgos -analógicos y digitales- que se deben asumir durante la búsqueda de un beneficio potencial que no termina de concretarse. Las actuales herramientas informáticas (caso de la plataforma telemática de rendición de cuentas locales o las plataformas de auditoría digital) han demostrado su valor añadido, su operatividad y su confiabilidad, respaldada por las instituciones de control externo. Merece la pena seguir invirtiendo en su continuo desarrollo, lo cual tampoco excluye que se exploren otras vías complementarias (nunca sustitutivas) mediante tecnologías emergentes. Solo el futuro concretará lo que está por venir.

20. Baste citar el explícito artículo 41 de la Carta de Derechos Fundamentales de la Unión Europea o, de forma implícita, el artículo 9.3 de la Constitución Española cuando garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos. A su vez, el artículo 31 de la Carta Magna impone un sistema tributario justo inspirado en los principios de igualdad y progresividad, así como un gasto público equitativo basado en los criterios de eficiencia y economía.

21. Información disponible en www.lamoncloa.gob.es/presidente/actividades/Paginas/2021/140721-derechos-digitales.aspx [recuperado el 30 de septiembre de 2021].

6. Bibliografía

- Barrio Andrés, M. (2021). *Formación y evolución de los derechos digitales*. Santiago de Chile: Ediciones Olejnik.
- Benítez Palma, E. (2017). *Blockchain*, auditoría pública y confianza: un triángulo no equilátero. Comunicación presentada en los *XII Encuentros Técnicos de los Órganos de Control Externo*. Disponible en: www.sindicatura.cat [recuperado el 1 de septiembre de 2021].
- Cabeza del Salvador, I. (2015). La valoración de riesgos en las auditorías de las entidades locales. *Auditoría Pública*, 66, 19-30.
- Cordero Valdavida, M. (2018). Auditoría digital: el reto del siglo XXI. *Presupuesto y Gasto Público*, 91, 135-151.
- (2019). *Blockchain* en el sector público, una perspectiva internacional. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 16, 16-34.
 - (2020). Control por diseño en la gestión de los fondos europeos. *Presupuesto y Gasto Público*, 100, 137-158.
- Fernández Llera, R. (2020). Buen gobierno local y rendición de cuentas en España. *Retos / Revista de Ciencias de la Administración y Economía*, 19, 29-44.
- Fernández Llera, R. y Oviedo Creo, M. (2018). Un renovado control interno local. *Documento Red Localis*, 9. Disponible en: www.redlocalis.com [recuperado el 1 de julio de 2021].
- Fueyo Bros, M. (2018). Función interventora. En M. Fueyo Bros (dir.). *Reglamento de control interno local. Función interventora, control financiero permanente y auditoría pública* (2.ª edición, pp. 95-246). Cizur Menor: Aranzadi Thomson Reuters.
- Huergo Lora, A. (2020). Una aproximación a los algoritmos desde el Derecho Administrativo. En A. Huergo Lora (dir.) y G. M. Díaz González (coord.). *La regulación de los algoritmos* (pp. 23-87). Cizur Menor: Aranzadi Thomson Reuters.
- López-Zambrano, C. R., Camberos-Castro, M. y Villarreal-Peralta, E. M.^a (2021). Los determinantes de confianza y riesgo percibido sobre los usuarios de bitcoin. *Retos / Revista de Ciencias de la Administración y Economía*, 11 (22), 199-215.
- Mota Sánchez, E. M.^a, Montoro Montarroso, A., Nieto Martín, A. y Olivas Varela, J. Á. (2021). Inteligencia Artificial y el control interno en el sector público local. *Documento Red Localis*, 16. Disponible en: www.redlocalis.com [recuperado el 1 de julio de 2021].

- Nakamoto, S. (2008). *Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer*. Traducción castellana del original, disponible en: <https://bitcoin.org/es> [recuperado el 1 de julio de 2021].
- OECD (2021). *Government at a Glance 2021*. París: OECD Publishing. Disponible en: <https://doi.org/10.1787/1c258f55-en> [recuperado el 1 de septiembre de 2021].
- Preukschat, A. (coord.). (2017). *Blockchain: La revolución industrial de internet*. Barcelona: Gestión 2000.
- Quintana Cortés, J. L. (2020). La tecnología *blockchain* y su pretendida aplicación a la contratación pública como mecanismo para lograr mayor integridad. *Revista Española de Control Externo*, 64, 150-171.
- Riera López, M. (2015). El auditor pierde los papeles. *Auditoría Pública*, 66, 45-50.
- Teré Pérez, A. (2015). La rendición de cuentas y la remisión de los contratos de las entidades locales a las instituciones de control externo: la distinción entre deber y obligación. *Auditoría Pública*, 66, 93-104.
- Wanden-Berghe Lozano, J. L. y Fernández Daza, E. (2020). *Blockchain*: instrumento de transparencia y control del sector público. *Revista Española de Control Externo*, 64, 132-149.

La Serie Claves del Gobierno Local se caracteriza por desarrollar temas de interés local con un contenido jurídico, político o financiero, seleccionados por la Fundación Democracia y Gobierno Local de acuerdo con los criterios que explican su línea editorial: abordar las cuestiones más controvertidas que identifica y selecciona al hilo de su actividad de debate, análisis, seminarios y jornadas, realizada en colaboración con los Gobiernos locales.

La venta de publicaciones de la **Fundación Democracia y Gobierno Local** se realiza a través de la distribuidora **EDISOFER** (tel.: 91 521 09 24 y página web www.edisofer.com), y en librerías especializadas.

ÚLTIMAS PUBLICACIONES



La transformación digital de la Administración local.



La Agenda 2030. Implicaciones y retos para las administraciones locales.



Manual práctico sobre PROTECCIÓN DE DATOS en la ADMINISTRACIÓN LOCAL.



La Carta Europea de Autonomía Local a los treinta años de su aplicación: balance y perspectivas.



Los planes provinciales como instrumentos jurídicos necesarios en la cooperación municipal y para el ejercicio de competencias propias de las diputaciones.



Los Gobiernos locales después de la crisis. Un análisis de la evolución de las Haciendas locales en el periodo 2001-2016.



Configuración legal, actuación y funciones de las autoridades de transparencia. Algunas propuestas de mejora.



Guía del concejal 2019.

Blockchain y Gobiernos locales

Blockchain ha irrumpido con fuerza en el debate relativo a los retos de la digitalización. El desacuerdo alcanza no solo a la utilidad de esta modalidad de tecnología de registro distribuido en los respectivos sectores de actividad, sino también a sus propias características e implicaciones. En dicho contexto, han comenzado a desarrollarse importantes casos de uso en el sector público, también en nuestro país, algunos de ellos -como su empleo en el ámbito de la contratación- de todos conocidos.

La presente obra colectiva persigue contribuir al análisis de las transformaciones que podrá experimentar el ejercicio de las potestades administrativas, en general, y la actividad de los Gobiernos locales, en particular, a partir de la utilización de la tecnología *blockchain*. A tal fin, los diversos autores que colaboran en el volumen han adoptado una perspectiva que combina la reflexión teórica con el examen de aplicaciones ya implantadas y casos de uso planteados como hipótesis, e impulsados tanto por la doctrina como por diversas instituciones, nacionales y supranacionales. De esta forma, se aborda el impacto, potencial y real, de *blockchain* sobre la configuración de las ciudades inteligentes, las relaciones interadministrativas y con el ciudadano, la transparencia y la protección de datos personales, la contratación pública, la prestación de los servicios, los procesos de participación ciudadana, las subvenciones, la gestión tributaria y los mecanismos de control interno y fiscalización externa, con específica consideración, en todos los casos, de las particularidades que, en dichos contextos, presenta el mundo local.

Los autores, investigadores universitarios y profesionales especializados en los ámbitos objeto de tratamiento, han acometido su labor críticamente, huyendo de la complacencia que en ocasiones cabe advertir en los estudios sobre la materia. Ello les ha permitido no solo perfilar criterios útiles para la determinación de cuándo o en qué circunstancias resultará aconsejable la implantación de la tecnología *blockchain* en el sector público, sino también subrayar la idoneidad de la esfera local como espacio de pruebas para orientar el desarrollo de aquella hacia la satisfacción del interés general.

