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 en Derecho Administrativo.
Universitat de València

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 contractuales[1]. Como se desarrolla en este trabajo, la incidencia de esta transformación afecta además particularmente a unas administraciones muy directamente prestadoras de 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 relieve[2].

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).

ISBN: 978-84-120267-8-8

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 pública[3]. 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 inteligentes[4]. 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 de los que

3. Pereiro Cárceles (2019b: 153).
4. En relación con el de uso de *smart contracts* en la actividad administrativa automatizada, Pereiro Cárceles (2019a).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 intermediaria[5]. 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

5. Hernández San Juan (2019: 26).
6. Alamillo Domingo (2019b), Merchán Murillo (2019) y Boix Palop (2021: 23-24).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

la misma, 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 cual 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, las posibilidades y la garantía de la transparencia de la propia tecnología que emplea *blockchain* para realizar cualquier proceso pueden ser empleadas como un elemento clave para facilitar un acceso de los ciudadanos a cuanta información de su interés sea introducida en las mismas, lo que potencia 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 instaurando por medio 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 que forman parte de la red. Esto quiere decir que mediante su empleo será más sencillo detectar algunos incumplimientos que quedarían

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 oráculos[7], 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 produzcan en el marco de un procedimiento pueden ser detectados 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.

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.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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, 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,

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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

8. Velasco Rico (2019).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

hablarse de participación en el sector privado, introduciendo mecanismos de 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

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 Infraestructure*, 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

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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, redunda 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 desempeño[9]. 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

9. Cerrillo i Martínez (2016: 176).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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, pero haciéndola conciliar con la protección de datos personales u otros intereses con los que la transparencia pudiera colisionar[11]. 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 automática[12] -como sí ocurre con las causas de inadmisión contempladas en el artículo 18.1 LTBG y con los datos especialmente protegidos[13]-. En este sentido, aunque se automatizase parcialmente este procedimiento, obviando las aportaciones que respecto a la toma de decisiones podría hacer la inteligencia artificial[14], 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 pública[15] o de

10. Bernal Blay (2018).
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.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

gestión de averías[16]. De esta forma, el ciudadano podría conocer aspectos del procedimiento 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 supuestos[17], en cuanto que el uso de la tecnología *blockchain* como sistema

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 interrupciones 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.).

ISBN: 978-84-120267-8-8

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 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 materia[18] 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 administrativos[19].

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 precepto[20], 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

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).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 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

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 Pentland[21], 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 Cataluña[22]. 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

21. Zyskind *et al.* (2015).
22. Disponible en: https://politiquesdigitals.gencat.cat/ca/tic/identicat/ (última consulta: 13/10/2021).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

para identificarse de forma fehaciente o para otorgar consentimiento válido a alguna petición que se le realice. Precisamente esta iniciativa, que podría dar frutos tan interesantes, es la que se ha visto cercenada por lo previsto en la disposición adicional sexta del Real Decreto-ley 14/2019[23].

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.

23. Boix Palop (2019: 23-24).

En cualquier caso, aunque las transacciones sean transparentes, las personas son dueñas de su información y pueden emplear esta con la finalidad 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 permisionadas 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 permisionadas, 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

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.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

del tratamiento e incluso, según cuál sea su configuración de la privacidad, el derecho de acceso.

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 futuro[25] 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 permisionadas por una parte, y redes públicas por la otra.

5.1.1. Redes privadas y permisionadas

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.

25. Boix Palop (2020: *in toto*, pero especialmente 234-249).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 red[26]. 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 inteligentes[27]. 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 inicialmente 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, pero que han de tener en cuenta

26. Commission Nationale Informatique & Libertés (2018: 1-4).
27. Pereiro Cárceles (2019a).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 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 permisionadas

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 bitcóin, Satoshi Nakamoto, es anónimo y ha mantenido su identidad oculta bajo un pseudónimo-. Una primera intuición podría llevarnos a pensar que lo más razonable es que el sujeto responsable del tratamiento de datos en una red *blockchain* sea quien creó la red. Sin embargo, a poco que conozcamos el funcionamiento de las aplicaciones sustentadas en esta tecnología nos daríamos cuenta de que ello no tendría mucho sentido. Supondría atribuir al creador de un protocolo las consecuencias producidas por un *software* concreto que funciona conforme a esta tecnología, pero en cuyo uso y finalidad no interviene. Y es que *blockchain* no es un *software* ni programa informático específico. Su creador no recibe compensaciones económicas directas por los esfuerzos acometidos en el diseño de una aplicación novedosa que se sustente en esta tecnología. Simplemente esta servirá como fundamento para que las transacciones se realicen adecuadamente en las distintas aplicaciones, como son los *smart contracts*, en las que se les dé uso. Hay que apuntar, sin embargo, que para usos de estas posibles redes por parte de administraciones públicas en las que ellas retengan cierto control, y para el ejercicio de actuaciones administrativas

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

o de interés público, esta solución puede tener sentido si son efectivamente responsables del código y de la programación de la red.

Otra hipótesis que cabría plantearse sería la atribución de la responsabilidad por el tratamiento de datos a los mineros[28], opción esta que debería descartarse conforme apunta el CNIL[29]. 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

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).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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.

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,

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 RGPD[30]. 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 CNIL[31].

30. Commission Nationale Informatique & Libertés (2018: 8).
31. Commission Nationale Informatique & Libertés (2018: 8).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 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 respecto a que la información incorrecta no volverá 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.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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, cuanto con dificultar su recuperación o acceso, por medio de la no indexación, lo que es bien distinto[32]. 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 transforma-

32. Boix Palop (2015).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

ción 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 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 técnica que no cumpla con estos estándares podría considerarse información seudonimizada, pero en ningún caso estaríamos ante información completamente anónima.

Los datos seudonimizados se encuentran definidos en el artículo 4.5 RGPD. Concretamente, según se contempla en el precepto, se corresponderían

33. Agencia Española de Protección de Datos (2016).

ISBN: 978-84-120267-8-8

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 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 riesgos[34]:

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

34. European Union Blockchain Observatory and Forum (2018: 19).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 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 tipo[36]: 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

35. Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2014).
36. European Union Blockchain Observatory and Forum (2018: 20).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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 revertirse-[37]. En tercer lugar, explica una serie 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, teniéndolas en cuenta desde el mismo diseño de la red de *blockchain* en cuestión, suponiendo un ejemplo de esa hibridación de las soluciones normativas con la programación del concreto registro distribuido, convertida 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

37. European Union Blockchain Observatory and Forum (2018: 21 y 22).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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, consideramos que 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 juego[38]. 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 forma 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 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 aplicativos[39]. 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

38. Valero Torrijos (2019: 90).
39. Boix Palop (2020: 249-261).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

cuenta la necesidad de proteger los derechos de los ciudadanos por el uso de sistemas automatizados.

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.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

— (2021). 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 información 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.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8

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.

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 Cerreda 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.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 34
ISBN: 978-84-120267-8-8