



Blockchain y descarbonización: ¿El futuro de la gestión laboral?*

BLOCKCHAIN AND DECARBONIZATION: THE FUTURE OF LABOUR MANAGEMENT?

Lucía Aragüez Valenzuela

Profesora Permanente Laboral, Departamento de Derecho del Trabajo
Universidad de Málaga
L@uma.es 0000-0003-1819-5494

Recibido: 05.05.2025 | Aceptado: 30.05.2025

RESUMEN

La cadena de bloques es una tecnología novedosa que cumple con un proceso de registro de transacciones y seguimiento de activos de manera segura y transparente, reduciendo así posibles riesgos y costes para las personas interesadas. Su estructura está descentralizada, permitiendo un registro inmutable a lo largo del tiempo.

Esta tecnología está comenzando a adentrarse en el ámbito de la gestión laboral ya que, aunque en principio parezcan cuestiones divergentes, en realidad la necesidad de procesos más eficientes y transparentes ha acelerado su impulso y operatividad.

En líneas generales esta tecnología se ha venido empleando para la contratación de personal, la gestión de identidades, la automatización de nóminas, el desarrollo del talento y su evaluación, el registro de jornada e incluso la tramitación de ausencias o vacaciones.

Sin embargo, más allá de las ventajas que esta tecnología presenta –la cual resulta innegable–, hay ciertos aspectos que merecen una especial reflexión sobre su impacto en la descarbonización del empleo, posibles vacíos de justicia y cuestiones relacionadas con la privacidad en las que nos centraremos en el presente estudio para dar respuesta a si verdaderamente su implementación resulta ciertamente interesante.

ABSTRACT

The blockchain is a novel technology that fulfils a process of recording transactions and tracking assets in a secure and transparent manner, thereby reducing potential risks and costs for stakeholders. Its structure is decentralised, allowing for an immutable record over time.

This technology is beginning to enter the field of labour management because, although at first they may seem to be divergent issues, the need for more efficient and transparent processes has accelerated its momentum and operability.

PALABRAS CLAVE

Blockchain
Decarbonización
Tecnologías
Trabajo
Gestión

KEYWORDS

Blockchain
Decarbonisation
Technologies
Job
Management

* Proyecto: PID2021-124031NB-C44. IP: Antonio Márquez Prieto y María Salas Porras, financiado por el Ministerio de Ciencia, Innovación y Universidades, denominado: "Descarbonización y relaciones jurídicas de producción: políticas y acuerdos de transición justa en un contexto digital", siendo la autora miembro del equipo de investigación.

In general terms, this technology has been used for staff recruitment, identity management, payroll automation, talent development and evaluation, time recording and even absence or holiday processing.

However, beyond the advantages of this technology –which is undeniable–, there are certain aspects that deserve a special reflection on its impact on the decarbonisation of employment, possible justice gaps and privacy-related issues, which we will focus on in this study to answer the question of whether its implementation is interesting.

SUMARIO

- I. PRIMERAS APROXIMACIONES AL BLOCKCHAIN
- II. MARCO NORMATIVO
- III. BLOCKCHAIN Y GESTIÓN LABORAL
 - A. Smart Code Contract
 - B. Registro horario
- IV. CONCLUSIONES: ¿ESTÁ EL BLOCKCHAIN ORIENTADO EN MATERIA DE DESCARBONIZACIÓN?: PRINCIPALES RETOS EN EL MUNDO DEL TRABAJO Y VACÍOS DE JUSTICIA
- Bibliografía

I. PRIMERAS APROXIMACIONES AL BLOCKCHAIN

En el contexto actual la inteligencia artificial (IA) ha emergido como un motor transformador en diversas industrias, ofreciendo soluciones innovadoras que potencian la eficiencia operativa y la toma de decisiones informadas. Esta evolución tecnológica no solo ha tenido un impacto significativo en la forma en que las empresas gestionan sus recursos¹, sino que también plantean interrogantes sobre las nuevas herramientas que pueden complementar sus capacidades.

Uno de los desarrollos más destacados en este ámbito es el blockchain, una tecnología que, al operar de manera descentralizada, se posiciona como una herramienta valiosa en el proceso de gestión de información, especialmente en lo que respecta a la administración laboral. Esta técnica, sustentada en el *big data* y en sofisticados métodos de análisis, propicia una optimización en el manejo de grandes volúmenes de datos. No obstante, son muchos los riesgos que conlleva la implantación de la IA en estos procesos de toma de decisiones, y muchas las incógnitas e incertidumbres² sobre el devenir de esta tecnología.

Tradicionalmente, la confianza en el entorno laboral se basaba en la relación humana, en el entendimiento y la credibilidad entre las personas. Por el contrario, con el avance de la tecnología, esta confianza ha empezado a trasladarse hacia las máquinas y sistemas automatizados. De hecho, dentro de las propias relaciones laborales esta confianza mutua entre la persona trabajadora y la empresa se encuentra mermada

1. Herrero Jiménez, Marcial: "Gobierno corporativo e inteligencia artificial", en AA.VV.: *La privacidad en el metaverso, la inteligencia artificial y el big data*, Acedo Penco A. (Coord.), Tecnos, 2023, p. 98.

2. Herrero Jiménez, Marcial: "Gobierno corporativo e inteligencia artificial", op. cit. ibidem. 98.



debido a una excesiva instrumentalización hacia lo tecnológico. En esta difusión del carácter personal de las relaciones de trabajo basada en la confianza, parece que el sistema de blockchain permite, en principio, sinergias más seguras y transparentes, garantizando un registro claro y accesible de las actividades laborales, proporcionando tanto a empleadores como a empleados un nivel de confianza fundamentado en datos verificables y más objetivos. De este modo, la maquinaria no solo complementa, sino que, en cierta medida, sustituye la necesidad de confianza basada únicamente en lo humano, configurando un nuevo paradigma en las dinámicas laborales.

Partiendo de estas premisas, nos encontramos con una nueva tecnología que redefine las estructuras tradicionales de gestión laboral. Así las cosas, resulta necesario centrarnos ahora en incluir algunas nociones básicas sobre el blockchain para, con posterioridad, valorar su impacto en la gestión laboral.

El blockchain significa textualmente cadena de bloques y “es un sistema con el cual se pueden hacer transacciones seguras entre personas en todo el mundo sin necesidad de intermediarios, es un tipo de inteligencia artificial basada en las tecnologías de libro mayor distribuido, que parten de una estructura de datos compartida, de naturaleza descentralizada y que no se puede modificar, por la que se gestionan las transacciones y se transmiten a varios nodos³ de una red en la que se valida la transacción”⁴. Por consiguiente, esta tecnología ofrece la posibilidad de eliminar obstáculos y facilitar procesos en los cuales se pueden realizar transacciones de manera más fluida, verificando la autenticidad de los datos almacenados en el sistema.

Esta tecnología crea una cadena digital de registros con enlaces encadenados para formar un registro inmutable, único e irrepetible. Un aspecto destacable de esta tecnología, la cual la hace única con relación a otros sistemas, es que esta base de datos no permite borrar o modificar la información que ahí se contiene, sino que sólo posibilita escritura bajo consenso. “En este sentido, la tecnología blockchain propone un nuevo modelo en que la autenticidad no la verifica un tercero, sino la red de nodos que participan en cadena de bloques. De ahí que ninguna transferencia de valor se efectúe por medio de un intermediario, sino a través de un consenso, permitiendo almacenar la información en todo momento de manera transparente”⁵. Así las cosas, la forma de archivo y la seguridad que proporciona técnicamente el blockchain permite comprobar si el documento generado ha sido alterado en algún momento posterior al registro⁶.

3. “Para poder comunicarse entre sí a través de una blockchain, todos los ordenadores involucrados deben funcionar bajo el mismo software o protocolo. Las computadoras se encuentran conectadas en la red”. Por otro lado, nos encontramos con los nodos regulares, que son “los encargados de replicar la blockchain, aceptando los bloques generados por los validadores y ejecutando las transacciones incluidas en los mismos. Estos nodos son los que inyectan transacciones en la red, a partir de fuentes externas al blockchain”, visto en: Bartolomeo, Alejandro; Machin Urbay, Gustavo: “Introducción a la tecnología blockchain: su impacto en las ciencias económicas”, 2020, p. 3. Disponible para su consulta en: https://bdigital.uncuyo.edu.ar/objetos_digitales/15304/14.-introduccinalatecnologia.pdf (Consultado el 30 de abril de 2025).

4. Herrero Jiménez, Marcial: “Gobierno corporativo e inteligencia artificial”, op. cit., p. 103.

5. Bartolomeo, Alejandro; Machin Urbay, Gustavo: “Introducción a la tecnología blockchain: su impacto en las ciencias económicas”, op. cit. p. 3.

6. Díaz Díaz, Efrén; Moreno Cea, Fernando: “Las aplicaciones del Blockchain a las actividades de las fundaciones y a sus relaciones con la Administración Pública”, *Anuario de derecho de fundaciones*, núm. 1, 2017, p. 25.



Introduciéndonos un poco más en el funcionamiento de esta tecnología, debemos mencionar que el blockchain –la cual originalmente se había diseñado para facilitar las transacciones de criptomonedas–, contiene una serie de datos relevantes almacenados en bloques. Cada bloque incluye un componente crítico conocido como *hash*⁷, que es esencial para mantener la integridad de la cadena. El hash es una función criptográfica que toma un conjunto de datos (como las transacciones dentro de un bloque) y produce una cadena de caracteres alfanuméricos que actúa como una huella digital única⁸. Este código no solo representa el contenido del bloque, sino que también se vincula al hash del bloque anterior, creando así un encadenamiento seguro de bloques.

Este proceso de encadenamiento es fundamental para la resistencia de la tecnología blockchain, lo cual dota al sistema de una gran seguridad porque si alguien intentara modificar la información en uno de los bloques, el hash correspondiente cambiaría, alterando también el hash de todos los bloques siguientes, dificultando enormemente cualquier intento de fraude o manipulación. Y es que, en el caso de que se realizara esto, se requiere modificar no solo un bloque, sino toda la cadena de bloques, siendo algo ciertamente detectable de forma inmediata en la red.

El uso de esta lógica de hash y encadenamiento establece un nivel de seguridad sin precedentes y, del mismo modo, también promueve la transparencia y la confianza entre las partes involucradas, permitiendo así, por ejemplo, en la gestión laboral, un registro inmutable de todos los procesos vinculados a los empleados, desde contratos de trabajo hasta evaluaciones de desempeño, asegurando que toda la información sea verificada y accesible sin posibilidad de alteración. Podemos decir por tanto que “el blockchain se autoprotege gracias a su propia estructura, su propia arquitectura”⁹.

Por otra parte, uno de los aspectos más destacados de esta tecnología es su capacidad para garantizar la privacidad de los datos. Mientras que la desmaterialización de la información puede suscitar inquietudes sobre la exposición indebida de datos sensibles, el blockchain permite establecer controles que aseguran que la identificación de los individuos se mantenga confidencial. Esto se logra a través de técnicas de encriptación que permiten a los usuarios acceder a la información sin revelar su identidad pública. Es decir, eso significa que, “si se cambia el número del bloque, la información automáticamente cambia el hash. Se puede imaginar como una pieza de puzzle. Según la información tendrá una determinada forma. Si alguien cambia la información, la forma también cambiará por lo que dejará de encajar y la cadena quedará invalidada. No es que haya una única base de datos, sino que cada usuario

7. “Algoritmo matemático que transforma cualquier bloque de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud”, en Bartolomeo, Alejandro; Machin Urbay, Gustavo: “Introducción a la tecnología blockchain: su impacto en las ciencias económicas”, op. cit. p. 3.

8. Díaz Díaz, Efrén; Moreno Cea, Fernando: “Las aplicaciones del Blockchain a las actividades de las fundaciones y a sus relaciones con la Administración Pública”, op. cit. p. 26.

9. Díaz Díaz, Efrén; Moreno Cea, Fernando: “Las aplicaciones del Blockchain a las actividades de las fundaciones y a sus relaciones con la Administración Pública”, *Anuario de derecho de fundaciones*, núm. 1, p. 29.

de Blockchain tiene una «copia» de ella¹⁰. Sin embargo, la implementación del blockchain en el ámbito laboral, aunque puede ser algo interesante y eficiente para algunas cuestiones en concreto, a su vez, es crucial analizar no solo sus beneficios, sino también los desafíos que pueden derivarse de su uso.

De tal manera, podemos decir que las características básicas¹¹ de esta tecnología son:

1. Almacenamiento seguro e «inmutable»: la información se transmite y se almacena de manera extremadamente segura, asegurando la identidad de los usuarios mediante el uso de claves criptográficas y firmas digitales. Una de las características más destacadas es que la información no puede ser modificada una vez registrada; cualquier cambio requiere la creación de un nuevo registro. Por lo tanto, todos los datos quedan disponibles públicamente y son accesibles para cualquier participante de la red.
2. Descentralizado: la estructura es inherentemente descentralizada, lo que significa que no se basa en un servidor o autoridad central. Esto establece un sistema de confianza sin la necesidad de intermediarios. Debido a su diseño descentralizado, se minimiza igualmente la posibilidad de fraude –aunque por supuesto pudieran también existir–. En particular, todos los nodos mantienen una copia del estado más reciente y pueden validar la información almacenada, lo que facilita la detección de cualquier intento de manipulación. Además, jurídicamente, asegura la trazabilidad de todas las transacciones realizadas, ofreciendo así una alta resistencia frente a ataques cibernéticos y prácticas fraudulentas.
3. La «cadena de bloques»: los datos se agrupan en bloques que contienen múltiples transacciones. Cada bloque está interconectado con el bloque que le precede. Esta interrelación es asegurada mediante técnicas criptográficas, y la cadena incluye toda la información y modificaciones desde su creación original. Este sistema también se conoce como “libro mayor distribuido”.
4. Trazabilidad y auditoría¹²: el blockchain proporciona un registro meticuloso y minucioso de todos los cambios realizados sobre los datos. La información está replicada en todos los nodos, lo que significa que cada uno posee un histórico completo de modificaciones. Esta capacidad resulta extremadamente útil para llevar a cabo auditorías, ya que permite verificar cualquier actividad desde el inicio del blockchain. La trazabilidad se garantiza a través de la interconexión de los bloques, por lo que los auditores pueden ser integrantes de la red blockchain y tener acceso constante y actualizado a la totalidad de los datos.

-
10. Díaz Díaz, Efrén; Moreno Cea, Fernando: “Las aplicaciones del Blockchain a las actividades de las fundaciones y a sus relaciones con la Administración Pública”, op. cit. p. 27.
 11. Díaz Díaz, Efrén; Moreno Cea, Fernando: “Las aplicaciones del Blockchain a las actividades de las fundaciones y a sus relaciones con la Administración Pública”, op. cit. p. 32-35.
 12. Díaz Díaz, Efrén; Moreno Cea, Fernando: “Las aplicaciones del Blockchain a las actividades de las fundaciones y a sus relaciones con la Administración Pública”, op. cit. p. 34.

En la actualidad, a título ilustrativo, se pueden mencionar algunas innovaciones vinculadas a la blockchain. En un primer término se destacan las remesas de dinero de un país a otro, ya que este tipo de operatoria está sujeta a cargos elevados por parte de las compañías que las realizan –por ejemplo, Western Union–. Sin embargo, en el caso del bitcoin (u otra criptomoneda) y blockchain se puede solucionar esto a un costo marginal muy pequeño, lo cual resulta ciertamente interesante. En segundo lugar, se tiende a utilizar cada vez más esta tecnología para el registro de personas, esto es, para identificarlas y hacerles llegar servicios, educación o salud. Y es que, en este caso, tenemos un registro inviolable que dificulta, en principio, posibles falsificaciones o extravíos –el caso del documento a papel–. En tercer lugar, debemos destacar los conocidos contratos inteligentes (smart contracts), los cuales, aunque profundizaremos en ella más adelante, es menester hacer referencia a algunas cuestiones. En este sentido, el “blockchain funciona como un “oráculo”, dando lugar a cierta acción o respuesta si se cumplen ciertas y determinadas condiciones. Es una especie de contrato autoejecutable, condicionado a un conjunto de especificaciones, que disparan un evento o compensación en caso de que se produzcan, sin la intervención de las partes contratantes o las instituciones relacionadas al contrato. Un ejemplo específico podría ser el cobro automático de una indemnización por haber sufrido un accidente, que estaba asegurado con un smart contract”¹³.

Dicho lo cual, parece no haber duda de que nos encontramos ante tecnología vanguardista de última generación¹⁴ pero que, a su vez, resulta esencial establecer mecanismos que respeten la privacidad y los derechos de las personas trabajadoras, asegurando que la transparencia y la seguridad no comprometan la confidencialidad de la información personal y, sobre todo, que, a pesar de su uso, se integren los principios de seguridad y transparencia mediante su estructura de hash y cadena, y se presente como una herramienta prometedora para optimizar algunas cuestiones relacionadas con la gestión laboral, pero, del mismo modo, garantizando su orientación hacia el elemento humano, salvaguardando los derechos más básicos de las personas trabajadoras.

162

II. MARCO NORMATIVO

El fenómeno de la protección de la privacidad de los datos personales constituye una de las principales preocupaciones en el ámbito digital contemporáneo, con una presencia constante en foros internacionales, nacionales, y en los debates de políticas públicas.

La problemática radica, de un lado, en la vulnerabilidad de los datos ante accesos no autorizados y, de otro, en la dificultad de certificar de manera fiable la identidad¹⁵ de las personas en entornos digitales. Y es que la existencia de numerosos “silos” de

13. Bartolomeo, Alejandro; Machin Urbay Gustavo: “Introducción a la tecnología blockchain: su impacto en las ciencias económicas”, op. cit. p.5.

14. Díaz Díaz, Efrén; Moreno Cea, Fernando: “Las aplicaciones del Blockchain a las actividades de las fundaciones y a sus relaciones con la Administración Pública”, *Anuario de derecho de fundaciones*, núm. 1, p. 29.

15. Colle, Raymond: “La identidad digital en la internet futura con blockchain”, *INCOM*, 2018, p. 4

datos, en los que cada organización mantiene una base interna aislada, ha provocado que los usuarios tengan que gestionar múltiples perfiles, con contraseñas y credenciales distintas en innumerables plataformas, generando fricciones y riesgos de filtraciones involuntarias que atentan directamente con la privacidad. De hecho, hasta ahora, son escasos los usuarios que tienen su propia identidad digital consolidada. Sin lugar a duda, esta dispersión de la información, además de limitar el control del usuario sobre sus datos, fomenta prácticas de intercambio y uso inadecuado de la información ocasionando importantes desafíos para el legislador nacional e internacional.

Ante estas preocupaciones y dificultades, el blockchain, que se presenta como una tecnología descentralizada y segura, parece tener una potencial solución al ofrecer un sistema de identidad digital algo más consolidada a lo que estábamos acostumbrados, difícilmente falsable y verificable. Sin embargo, la adopción generalizada de un sistema estándar de identidad digital basada en blockchain aún enfrenta desafíos técnicos y normativos sustanciales.

Actualmente, numerosos proyectos, tanto gubernamentales como del sector privado, participan en la experimentación y desarrollo de soluciones de identidad digital a través del blockchain¹⁶. Entre ellos, algunos promovidos por Naciones Unidas y diversas agencias internacionales, que buscan avanzar hacia un esquema de identidad digital autogestionada por el propio ciudadano, respetando principios de soberanía y protección de datos.

Así las cosas, podemos observar que una de las principales preocupaciones relacionadas con esta tecnología es los problemas que pudiera presentarse con relación a la no protección jurídica de los derechos más básicos de los ciudadanos, como es en este caso la privacidad o protección de datos personales. Hoy en día, aunque aún resulta difícil encontrar un concepto que satisfaga todas sus acepciones y complejidades que trae aparejada relacionado con la privacidad, debemos mencionar que es concebida como un derecho inherente a toda persona humana¹⁷.

El marco normativo europeo, en particular el Reglamento General de Protección de Datos (RGPD), ha establecido un paradigma de protección de datos basado en principios de privacidad que exigen que las organizaciones aseguren la protección de los datos personales, siendo esta una prioridad en todas las fases de cualquier proyecto¹⁸, incluyendo aquellos ligados a tecnologías disruptivas como la inteligencia artificial o el blockchain. En particular, la normativa establece que el tratamiento de datos debe ser lícito, leal y transparente, con obligaciones de minimización, limitación del tiempo y seguridad en la gestión.

Así las cosas, como se ha venido citando con anterioridad, desde una perspectiva jurídica la naturaleza descentralizada del blockchain plantea conflictos evidentes con el RGPD, en particular respecto al principio de responsabilidad, la inmutabilidad de los datos y el derecho de rectificación y supresión (derecho al olvido).

16. Colle, Raymond: "La identidad digital en la internet futura con blockchain", *op. cit. ibidem*, p. 4

17. Grigera del Campillo, Santiago: "Privacidad y Blockchain", *Revista Blockchain inteligencia artificial*, núm. 2, 2021, p. 14.

18. Grigera del Campillo, Santiago: "Privacidad y Blockchain", *op. cit.* p. 19.

La regulación europea señala que los datos personales encriptados en blockchain siguen siendo datos personales, en virtud del artículo 4 (1) del RGPD, ya que la encriptación no convierte los datos en anónimos de forma absoluta. Es por ello por lo que muchos autores¹⁹ han afirmado que consideran que hay una incompatibilidad total entre esta tecnología y el RGPD, ya que, aunque los datos estén encriptados, siguen siendo datos personales. En este sentido, uno de los argumentos principales es que, en la práctica, la cadena de bloques impide la eliminación física de datos, contraviniendo el artículo 17 del RGPD, que reconoce el derecho al olvido.

Ello plantea un sinfín de preguntas relacionadas con este carácter inmutable de los datos y es que, por ejemplo, si los datos en la cadena son inalterables, ¿cómo cumplir con los derechos de los titulares frente a la posibilidad de solicitar la rectificación o supresión? He aquí uno de los principales problemas que nos encontramos en la actualidad entre esta tecnología y la normativa comunitaria y nacional.

Ante esta problemática, la solución propuesta por algunos expertos y organismos de protección de datos consiste en limitar el uso del blockchain a redes privadas o permisos, donde la participación y el control estén restringidos y que en ellas los responsables del tratamiento puedan ejercer un control más preciso sobre quién participa y cómo se gestionan los datos. Esta solución, “encajada con pinzas”, al menos, permite definir quiénes son los responsables y también los encargados del tratamiento.

Sin embargo, esta inmutabilidad inherente a la estructura del blockchain, en la que, una vez registrado un dato, no puede ser modificado ni eliminado, entra en conflicto directo con el derecho de rectificación y el derecho al olvido, previstos en los artículos 16 y 17 del RGPD. “Este conflicto surge ante la característica propia de transparencia, que si bien resulta positiva para evitar actos fraudulentos, manipulación, falsificación o para la generación de confianza y seguridad, podemos analizarlo como algo negativo si las partes, por ejemplo, buscan la confidencialidad de la existencia del contrato o la privacidad de sus cláusulas –aun con la existencia de cláusulas de confidencialidad– (...). Mantener la confidencialidad requeriría la restricción de los accesos a la información o, por lo menos, intentar garantizar el anonimato de la información relevante mediante técnicas de encriptación, por ejemplo. En cualquier caso, siempre existirá un cierto nivel de tensión e incertidumbre al utilizar plataformas abiertas, dada la incertidumbre y las potenciales vulnerabilidades a las que se los usuarios se exponen”²⁰.

Por el momento, no parece existir una posición unánime para conciliar ambas aunque resulta recomendable que, al menos, los datos personales sensibles no residan en la cadena de bloques en forma definitiva, sino que se utilicen referencias hash u otros metadatos enlazados a datos almacenados en soportes tradicionales donde sí sean eliminables o modificables.

Asimismo, la existencia de “derechos de control” del usuario, como la portabilidad, la rectificación o la supresión, debe ser preservada. Por ello, otros enfoques

19. Flores, María Emiliana: “Smart contracts y protección de datos personales”, *PAPELES del Centro de Investigaciones de la Facultad de Ciencias Jurídicas y Sociales de la UNL*, vol. 5, núm. 26, 2023, p. 17.

20. Flores, María Emiliana: “Smart contracts y protección de datos personales”, op. cit. p. 4

persiguen que los datos se “desprendan” de la inmutabilidad del blockchain mediante técnicas de encriptación reversible, en las cuales la clave de desencriptación pueda ser destruida o modificada por el interesado, logrando así la satisfacción de los derechos en términos prácticos y jurídicos. Sin embargo, en la práctica, esto reviste de cierta complejidad.

Esta problemática también se mantiene en el ámbito laboral con, por ejemplo, los conocidos contratos inteligentes o smart contracts. En este caso, la distribución equitativa de responsabilidades y la delimitación de quién ejerce la condición de responsable o encargado del tratamiento en un sistema automatizado requiere de una cierta delimitación atendiendo a quién controla los datos y quién los procesa.

La tendencia actual es operar en redes blockchain restrictivas o en plataformas privadas controladas por entidades que asumen dicha responsabilidad, facilitando así el cumplimiento del marco legal; sin embargo, es cierto que existe cierta problemática con relación a la identificación de actores.

Así las cosas, podemos observar que, aunque por el momento nos encontramos con dificultades a nivel normativo en esta tecnología, las instituciones europeas y nacionales están trabajando en caminos de conciliación entre las capacidades tecnológicas del blockchain y la protección de datos. Diversos grupos de trabajo²¹, incluyendo la Comisión Europea y la Agencia Española de Protección de Datos, han iniciado estudios y recomendaciones que apuntan hacia modelos híbridos y soluciones tecnológicas como la encriptación selectiva, los derechos de control y las redes autorizadas; sin embargo, aún nos queda mucho por recorrer y por garantizar. Eso sí, al menos por el momento, la tendencia apunta hacia la creación de plataformas blockchain autorizadas, con capacidades específicas para garantizar la adecuada gestión de datos, respetando los derechos de los titulares y facilitando la responsabilidad en tratamientos automatizados.

Por su parte, el Reglamento Europeo de Inteligencia Artificial, de 13 de junio de 2024, clasifica los sistemas de IA según su nivel de riesgo (inaceptable, alto, limitado o mínimo), y establece obligaciones proporcionales a cada categoría. Por consiguiente, es necesario en estos casos que las empresas evalúen los riesgos de sus sistemas y cumplan con los requisitos correspondientes. En este caso, si bien el Reglamento de la IA no menciona directamente el blockchain, su combinación con la IA podría generar sistemas de alto riesgo que requerirían un análisis cuidadoso bajo las disposiciones de la normativa referenciada. A título ilustrativo, si nos encontramos con un sistema de gestión laboral basado en blockchain que utilice IA para la toma de decisiones automatizadas sobre la contratación o evaluación de personal, estaría sujeto a los requisitos del Reglamento de la IA (art. 6).

En particular, el Reglamento de IA pretende que las empresas que utilicen este tipo de tecnología, de un lado, evalúen los riesgos de sus sistemas, incluyendo la identificación y mitigación de posibles sesgos y discriminaciones; y, del mismo modo, implementen medidas de transparencia y explicabilidad para que los usuarios puedan comprender cómo funciona esta tecnología y la razón por la que se toman decisiones.

21. Flores, María Emiliana: “Smart contracts y protección de datos personales”, *op. cit.*, p. 17.

Principalmente la norma resalta la importancia de establecer mecanismos de supervisión humana para garantizar que las decisiones automatizadas sean justas y responsables. Por consiguiente, aunque el Reglamento de IA no cite textualmente nada sobre el blockchain, para el estudio de este campo debe ser tenida muy en cuenta.

Por otro lado, el Libro Blanco de la Comisión Europea sobre inteligencia artificial, presentado en 2020 –el cual no tiene carácter normativo, pero marca las directrices adoptadas por la UE en políticas públicas relativas a la innovación y desarrollo de la IA–, plantea la creación de un “ecosistema de confianza” que implique seguridad, ética y respeto por los derechos fundamentales²². La estrategia europea busca promover una IA centrada en el ser humano, responsable y ética, que respete derechos como privacidad, no discriminación y protección de datos personales. Se desprende de este texto su orientación antropocentrista, esto es, la relevancia del elemento humano por encima del factor tecnológico, donde no se pierda la confianza depositada en las personas, aun utilizando este tipo de herramientas tecnológicas como es, en su caso, el blockchain.

Finalmente, es necesario apuntar algunas ideas relacionadas con la Ley orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). En particular, es cierto que la normativa no aporta referencias expresas a la tecnología del blockchain; sin embargo, podemos destacar algunos preceptos que se encuentran directamente relacionados y son perfectamente aplicables.

En un primer término, el art. 5 de la LOPDGDD menciona una serie de principios básicos relacionados con la licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación e integridad y confidencialidad. En este caso, parece que la tecnología blockchain permite la aplicabilidad de estos principios básicos aun teniendo presente las dificultades planteadas con anterioridad relacionadas con la limitación del plazo de conservación, puesto que los datos almacenados en la tecnología, en principio, tienen el carácter de ser inmutables y permanentes.

Con relación a esto, también nos encontramos con ciertos desafíos de esta tecnología en la garantía de los derechos ARCO (acceso, rectificación o supresión) de los datos personales –los cuales se relacionan con los arts. 15-18 del RGPD–, principalmente los derivados del derecho al olvido. Por lo tanto, parece que también de esta normativa se desprende, de un lado, la importancia en establecer mecanismos para anonimizar o seudonimizar los datos, procedimientos para su rectificación y supresión en caso necesario; y, de otro, contratos claros para definir roles y obligaciones de cada parte involucrada en el tratamiento de datos en blockchain.

III. BLOCKCHAIN Y GESTIÓN LABORAL

La tecnología blockchain está transformando los paradigmas operativos de las organizaciones, ofreciendo un modelo de gestión de datos, en principio, más eficiente y

22. Herrero Jiménez, Marcial: “Gobierno corporativo e inteligencia artificial”, AA.VV.: *La privacidad en el metaverso, la inteligencia artificial y big data: Protección de datos y derecho al honor* / Acedo Penco, Ángel (coord.), Dykinson, 2023, p. 106

seguro con relación a otros métodos. La implementación de esta tecnología por parte de las empresas resulta cada vez más próxima, principalmente en el ámbito de los recursos humanos de entre otros escenarios. En este contexto, cuando valoramos verdaderamente que la gestión de datos personales de las personas trabajadoras demanda un alto grado de responsabilidad y precisión, una tecnología como esta parece ser ciertamente segura para potenciar estas características.

En particular, de entre las ventajas que ofrece esta tecnología, se destacan una gestión más eficaz de los flujos de trabajo y la optimización de los procesos internos²³. Cada actividad puede registrarse en un bloque y añadirse a la cadena de bloques, incorporando información que facilita la trazabilidad y supervisión. Por lo tanto, por ejemplo, las empresas pueden gestionar con mayor facilidad los horarios de los empleados y realizar un seguimiento detallado de sus actividades. "Además de gestionar los horarios de los empleados, la tecnología blockchain también puede ayudar a las empresas a optimizar el flujo de trabajo. A través de blockchain, es fácil hacer un seguimiento del proceso de producción, adquisición de piezas y ventas"²⁴. Por consiguiente, se revela como una herramienta útil para optimizar la producción, la adquisición de materiales y las ventas, lo cual contribuye a la reducción de costos, al permitir un acceso ágil a la información sin necesidad de verificaciones múltiples y ajustes.

En el ámbito de la gestión laboral puede resultar un acierto para ciertas acciones, puesto que esta información almacenada en la tecnología no puede ser alterada ni falsificada, ya que cada transacción requiere la confirmación unánime de los participantes. Esto previene la suplantación de identidad, la falsificación y el fraude. Sin lugar a duda, en el caso de que se efectúen contratos inteligentes o se emplee este tipo de tecnología para almacenar cierta información, los datos pueden ser encriptados y almacenados de forma segura, garantizando su inmutabilidad²⁵ en el caso de que así se pretenda.

Así las cosas, teniendo presente las ventajas y desafíos que el uso de esta tecnología ocasiona en el ámbito laboral, podemos destacar que de una manera cada vez más habitual se emplea para automatizar procesos contractuales, garantizando el cumplimiento de las obligaciones y la transparencia en las relaciones laborales; facilitar el registro inmutable de la jornada laboral de los empleados; o, por ejemplo, para agilizar la gestión y el pago de nóminas, reduciendo errores y costos administrativos, a la vez que garantiza la transparencia y la seguridad en las transacciones. Por consiguiente, aun sabiendo que su desempeño se está desplegando cada vez con más habitualidad por parte de las empresas, es necesario reiterar en la idea de que su

23. Cruz Manzo, Jessica; Ortuño Barba, Luis Carlos; Villafuerte Palavicini, Faustino Sergio; Araoz Baltazar, Iván; Quintanilla Montalvo, Marifer: "De la cadena de bloques al talento humano: innovaciones disruptivas en recursos humanos", *Ciencia Latina Revista Científica Multidisciplinar*, Vol. 8, núm. 5, 2024, p. 9111

24. Cruz Manzo, Jessica; Ortuño Barba, Luis Carlos; Villafuerte Palavicini, Faustino Sergio; Araoz Baltazar, Iván; Quintanilla Montalvo, Marifer: "De la cadena de bloques al talento humano: innovaciones disruptivas en recursos humanos", op. cit. ibidem.

25. Cruz Manzo, Jessica; Ortuño Barba, Luis Carlos; Villafuerte Palavicini, Faustino Sergio; Araoz Baltazar, Iván; Quintanilla Montalvo, Marifer: "De la cadena de bloques al talento humano: innovaciones disruptivas en recursos humanos", op. cit. ibidem.



implementación se efectúe con cautela, evaluando cuidadosamente los riesgos asociados a la privacidad y la protección de datos personales.

A. Smart Code Contract

Tradicionalmente, un contrato se ha definido como un “negocio jurídico bilateral, dirigido a crear, modificar o extinguir relaciones obligatorias o a constituir relaciones de otra índole (reales o familiares)”²⁶. Bajo esta concepción, es evidente que el concepto de contrato puede abarcar una variedad de modalidades y formas en las que se articula o canaliza dicho negocio jurídico. “Con esa idea presente, se comprende que bajo tal concepto podemos albergar, a su vez, modalidades o formas dispares en que se vertebre o canalice semejante negocio jurídico. En pacífica conexión con esta concepción, cabe la realización de contratos sirviéndonos de vías electrónicas, dado que el grado de desarrollo tecnológico con el que contamos actualmente, con un acceso sencillo y virtualmente universal, lo permite e, incluso, lo facilita resueltamente”²⁷.

En este contexto, es necesario puntualizar que en la actualidad existen dos contratos inteligentes. De un lado, los denominados smart code contracts, y, por otro, los smart legal contracts. “Ambas clases son códigos informáticos. La principal diferencia entre ellos es que los primeros son almacenados en la cadena de bloques, mientras que los segundos no. Nosotros nos centramos aquí en el análisis de los smart code contracts”²⁸.

En consonancia con esta idea, la celebración de contratos a través de medios electrónicos se ha vuelto una práctica común, facilitada por el avance hacia lo tecnológico. A pesar de ello, esta forma de contratación exige la implementación de controles, garantías, previsiones y cautelas legales²⁹. En contraposición a un contrato tradicional, que describe los términos de una relación en un documento físico, un smart contract lo hace a través de un programa informático, lo cual puede plantear ciertos desafíos que el sector legal no puede permanecer ajeno³⁰. La utilización de este tipo de contratos inteligentes pretende “reducir significativamente la carga de trabajo asociada a la recuperación y transmisión segura de documentación”³¹; y, del mismo modo, también el coste de la comprobación y verificación de antecedentes.

168

26. Sánchez Álvarez, Eduardo; García Pacios, Adrián: “Tecnología blockchain y contratación electrónica: puntos críticos de integración de los denominados Smart contracts en nuestro sistema de derecho contractual”, *Revista CE-FLegal*, núm. 246, 2021, p. 75.

27. Sánchez Álvarez, Eduardo; García Pacios, Adrián: “Tecnología blockchain y contratación electrónica: puntos críticos de integración de los denominados Smart contracts en nuestro sistema de derecho contractual”, *Revista CE-FLegal*, núm. 246, p. 75.

28. Sánchez Álvarez, Eduardo; García Pacios, Adrián: “Tecnología blockchain y contratación electrónica: puntos críticos de integración de los denominados Smart contracts en nuestro sistema de derecho contractual”, op. cit. p. 88.

29. Sánchez Álvarez, Eduardo; García Pacios, Adrián: “Tecnología blockchain y contratación electrónica: puntos críticos de integración de los denominados Smart contracts en nuestro sistema de derecho contractual”, op. cit. ibidem.

30. Flores M. E., (2023), “Smart contracts y protección de datos personales”, op. cit., p. 2

31. Cruz Manzo, Jessica; Ortuño Barba, Luis Carlos; Villafuerte Palavicini, Faustino Sergio; Araoz Baltazar, Iván; Quintanilla Montalvo, Marifer: “De la cadena de bloques al talento humano: innovaciones disruptivas en recursos humanos”, op. cit. p. 9112.



Centrándonos en el funcionamiento de estos contratos inteligentes, podemos decir que, en primer lugar, se incorpora a la red blockchain donde los términos del acuerdo se codifican dentro de la cadena de bloques. Esto permite que todos los usuarios confirmen que el evento desencadenante del pago (por ejemplo, la fecha) se ha producido y que el contrato se cumple. En este sentido, los términos del acuerdo se ejecutan entre las partes sin necesidad de intermediación, resultando ser una idea básica que puede aplicarse a configuraciones más complejas.

Por consiguiente, estos contratos son idóneos para cualquier transacción que requiera un acuerdo registrado entre partes –como la contratación de productos financieros o de seguros, los depósitos en garantía y las operaciones de compraventa de instrumentos financieros en los mercados bursátiles, de préstamos sindicados, etc.-. Así las cosas, al trasladar estos principios al ámbito de la gestión laboral, los smart contracts presentan un enorme potencial para el aseguramiento en el cumplimiento de las obligaciones contractuales y la transparencia en las relaciones laborales en la automatización de la ejecución de contratos de trabajo. Del mismo modo, sirven para garantizar la seguridad y la trazabilidad de las transacciones en gestionar el pago de salarios y prestaciones.

En particular en el ámbito de estos contratos se utiliza una “condición”, es decir, “este término hace referencia a las circunstancias externas de las que se hace depender el smart contract y cuyo advenimiento produce su autoejecución. Si esta condición no se cumple, no se ejecuta el contrato”³². Esta figura se conoce con la llamada fórmula *if-then-else*. Básicamente consiste en verificar que si ocurre la condición pactada por las partes (if), se ejecuta en sus justos términos (then). Por el contrario, en el caso de que no se produzca la circunstancia prevista (if not), entonces ocurre otra cosa diferente (else). Teniendo presente por ende esta configuración, los nodos comprueban que la condición se ha producido y, en su caso, ejecutan el contrato directamente.

Un aspecto destacable es que los nodos deben cotejar que la circunstancia realmente se haya cumplido para realizar esta ejecución. Esto se efectúa a través de una herramienta informática conocida como “el oráculo”, la cual comprueba los datos del mundo real de los que se hace depender la ejecución del contrato inteligente. “Pongamos un ejemplo: imaginemos que esta fórmula de los contratos inteligentes se utiliza en el ámbito de las apuestas de pago en partidos de fútbol. La ejecución de ese contrato se está haciendo depender de un elemento externo que no conocemos en el momento de perfección de aquél, el resultado del partido. Una vez que el partido ha finalizado, para conocer el resultado de este, los nodos le preguntan al oráculo (por ejemplo, la página web de la Federación Española de Fútbol). Si el apostante acierta (es decir, si se cumple la condición), el contrato se autoejecuta y recibe la cantidad de dinero que le corresponda”³³. Para la correcta configuración del oráculo

32. Sánchez Álvarez, Eduardo; García Pachos, Adrián: “Tecnología blockchain y contratación electrónica: puntos críticos de integración de los denominados Smart contracts en nuestro sistema de derecho contractual”, op. cit. p. 89.

33. Sánchez Álvarez, Eduardo; García Pachos, Adrián: “Tecnología blockchain y contratación electrónica: puntos críticos de integración de los denominados Smart contracts en nuestro sistema de derecho contractual”, op. cit. p. 89.



se deben evitar conceptos jurídicos indeterminados, estas son condiciones que no sean objetivas o puedan ser objeto de interpretación –en este caso, por ejemplo, podríamos señalar principios como la diligencia de un buen padre de familia, actuar conforme a la buena fe, entre otros-.

Es cierto que esta autonomía de las decisiones en la ejecución de estos contratos puede resultar contrario al RGPD o a nuestra normativa interna, las cuales insisten en la importancia de que exista una supervisión humana. “Sin embargo, la versatilidad de la tecnología Blockchain permitirá que dichos contratos inteligentes puedan ser configurados y adaptados para cumplir con la exigencia de la intervención humana”³⁴.

Una cuestión controvertida en el ámbito de los smart contracts es la admisibilidad de la firma electrónica como mecanismo de autenticación y validez jurídica. Esto es, los usuarios se identifican con un número de referencia, lo que implica en relación de causalidad directa que no conocemos su veraz identidad. En particular, “el RGPD impone obligaciones y responsabilidades a los diferentes actores involucrados en el tratamiento de datos personales, lo que hace necesario identificar la posición jurídica de cada uno de ellos. Sin embargo, esto puede resultar complicado en la tecnología Blockchain, donde cada actor de la red tiene acceso a los datos personales y resulta difícil determinar quién es el responsable y el encargado del tratamiento. Esta cuestión no es pacífica y se encuentra en debate entre las autoridades de protección de datos y los grupos de trabajo especializados en Europa. Una posible solución es operar en una red Blockchain privada, en la que los propietarios deciden quién puede participar en la misma y se puede identificar mejor el rol de cada actor en la protección de datos”³⁵.

En este sentido, es preciso señalar que la firma electrónica, en virtud del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, debe cumplir una serie de requisitos esenciales tales como: a) Permitir identificar al firmante y detectar cualquier cambio ulterior de los datos firmados; b) estar basada en un certificado reconocido; c) ser generada mediante un dispositivo seguro de creación de firma.

El primero de estos requisitos plantea un desafío particular en el contexto de la tecnología blockchain. Como se ha mencionado, una característica fundamental de la blockchain –y, por ende, de los smart contracts que la utilizan como base– es que los usuarios se identifican mediante un número de referencia, lo que implica que la identidad real del firmante permanece desconocida. En consecuencia, la exigencia de identificación del firmante podría entrar en conflicto con uno de los principios básicos de la cadena de bloques. Como solución, en el supuesto de que se opte por admitir la firma electrónica en los smart contracts, es imperativo señalar que dicha firma tendrá el mismo valor probatorio que una firma manuscrita³⁶, con las consecuencias legales que ello implica.

34. Flores, María Emilia: “Smart contracts y protección de datos personales”, op. cit. p. 4

35. Flores, María Emilia: “Smart contracts y protección de datos personales”, op. cit. ibidem.

36. Sánchez Álvarez, Eduardo; García Pacios, Adrián: “Tecnología blockchain y contratación electrónica: puntos críticos de integración de los denominados Smart contracts en nuestro sistema de derecho contractual”, op. cit. p. 89.

Finalmente, debemos mencionar –aunque no reiterarnos en esta idea la cual ha sido abordado en el capítulo referente al marco normativo– que también en los contratos inteligentes nos encontramos con dificultades relacionadas con el ejercicio de derechos, rectificación o supresión de datos personales. Y es que, más allá de establecer posibles soluciones, el derecho de supresión y el de rectificación plantean dudas en cuanto a su aplicación en la tecnología Blockchain que es por naturaleza inmutable³⁷.

B. Registro horario

Las empresas tienen la obligación legal de registrar la jornada laboral efectuada por las personas trabajadoras. Y, aunque esta obligación ha sido objeto de controversia por parte de la jurisprudencia y doctrina, es necesario mencionar algunos apuntes previos al registro horario a través del blockchain.

La Sentencia de la Audiencia Nacional, núm. 207/2015, de 4 de diciembre de 2015 (Rec. n.º 301/2015)³⁸, mantuvo que el registro de jornada que debía realizarse era un requisito esencial para el control de los excesos de jornada en los que podían incurrir las personas trabajadoras, es decir, el control debía efectuarse exclusivamente para contabilizar las horas extraordinarias realizadas. Sin embargo, el Tribunal obligó a la empresa a realizar un registro de jornada ordinario y diario por entender que dicho registro es un requisito “sine qua non” para demostrar las horas extraordinarias realizadas³⁹.

Posteriormente, el Tribunal Supremo, mediante la STS Núm. 246/2017 de 23 de marzo de 2017⁴⁰, casó y anuló la anterior resolución por entender que según la legislación no existía la obligación de realizar un registro de jornada laboral ordinario, por lo que los tribunales no podían actuar como legisladores imponiendo a una empresa la obligación genérica de establecer un sistema de control horario.

En este contexto, la Audiencia Nacional, en desacuerdo con tal resolución, planteó una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea (TJUE) para que se pronunciase acerca de la obligatoriedad de implantar la obligación de establecer un registro de jornada laboral. A este respecto, mediante la STJUE asunto C-55/18 de 14 de mayo de 2019⁴¹, se confirmó que los Estados miembros de la Unión deben exigir a las empresas la obligación de establecer un sistema fiable, objetivo y accesible que compute la jornada laboral diaria efectuada por cada persona trabajadora contratada, y se enuncia que cada Estado podrá definir los criterios concretos que podrán exigirse en la implantación de estos sistemas.

37. Flores, María Emilia: “Smart contracts y protección de datos personales”, op. cit. p. 4

38. Se puede acceder al contenido de la sentencia en el siguiente enlace: https://www.laboral-social.com/sites/laboral-social.com/files/NSJ052983_0.pdf (Consultado el 1 de mayo de 2025)

39. Martínez Boada, Javier: “Blockchain como sistema para cumplir con la obligación de control y registro de la jornada laboral de los trabajadores”, *Revista de internet, derecho y política*, núm. 41, 2024, p. 4.

40. Se puede acceder al contenido de la sentencia en el siguiente enlace: <https://vlex.es/vid/677346465> (Consultado el 1 de mayo de 2025).

41. Se puede acceder al contenido de la sentencia en el siguiente enlace: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=214043&pageIndex=0&doclang=ES> (Consultado el 1 de mayo de 2025)



En respuesta a esta situación, se promulgó el Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, a fin de regular la obligación de registro de la jornada laboral. En su Capítulo III, se estipula la obligación empresarial de garantizar un registro diario que refleje el inicio y fin de la jornada laboral, con la finalidad de conservar los registros horarios durante cuatro años y ponerlos a disposición de las personas trabajadoras, sus representantes y la Inspección de Trabajo. Esta normativa encuentra ahora su reflejo en el art. 34 del Estatuto de los Trabajadores, la cual, si bien clarifica la obligación del registro diario, no especifica el sistema o soporte a utilizar⁴², abriendo la puerta a sistemas informáticos y digitales⁴³.

En principio, parece que el blockchain se presenta como una opción para que las personas trabajadoras registren su jornada laboral real sin estimaciones. La SAN Núm. 00022/2022 de 15 febrero⁴⁴ refuerza esta idea al rechazar registros de tiempos estimados, mientras que la cadena de bloques permitiría almacenar y presentar información horaria a las autoridades competentes. Sin embargo, es importante señalar que la mera existencia de aplicaciones digitales convencionales plantea interrogantes sobre el valor añadido real del blockchain. Y es que, aunque aparentemente no introduce novedades disruptivas, la tecnología blockchain podría abordar, aunque con limitaciones, problemas persistentes de falsificación de registros por parte de empresarios y personas trabajadoras, garantizando una mayor fidelidad en el cumplimiento normativo.

Aunque no es lo habitual, el blockchain, en teoría, permitiría a las personas trabajadoras registrar sus entradas, pausas y salidas de forma inmutable, eliminando la posibilidad de manipulación. Las modificaciones requerirían un nuevo bloque con los datos actualizados, manteniendo el registro original para su análisis. Es decir, la solución blockchain a utilizar para registrar la jornada de las personas trabajadoras será el sistema privado en el que el encargado de gestionar la cadena otorgue acceso a los nodos que estime oportuno –en este caso, a las personas trabajadoras–, y se les aporte la capacidad de validar transacciones, es decir, fichar, bajo un sistema blockchain en el que solo los nodos autorizados (personas trabajadoras) puedan crear el bloque en el que se establezca su fichaje exacto de entrada y salida⁴⁵.

De tal manera que esta tecnología presenta un paradigma en el que la gestión del registro de jornada recae directamente en la persona trabajadora, requiriéndose de un cierto nivel de confianza y buena fe. Sin embargo, es necesario igualmente mencionar que esta circunstancia no asegura una situación de mayor seguridad y veracidad, puesto que quedaría en manos de las personas trabajadoras únicamente el registro

42. En este sentido es necesario clarificar que, al menos, la Agencia Española de Protección de Datos (AEPD) ha limitado el uso de sistemas biométricos, como el fichaje con huella dactilar o por reconocimiento facial. Se puede consultar la Guía publicada por la AEPD a través del siguiente enlace: <https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf> (Consultado el 1 de mayo de 2025)

43. Martínez Boada, Javier: "Blockchain como sistema para cumplir con la obligación de control y registro de la jornada laboral de los trabajadores", op. cit. ibidem.

44. AN (Sala de lo Social, Sección 1^a) Sentencia núm. 22/2022 de 15 febrero AS\2022\49.

45. Martínez Boada, Javier: "Blockchain como sistema para cumplir con la obligación de control y registro de la jornada laboral de los trabajadores", op. cit. p. 5.



de sus entradas y salidas, pudiendo efectuar acciones fraudulentas a las previamente pactadas con la empresa y percibiendo una remuneración por el mismo.

Este punto, a mi parecer, merece una especial reflexión puesto que, si bien el registro de la jornada laboral a través de blockchain ofrece una supuesta transparencia y seguridad, es crucial analizar las implicaciones en esa confianza depositada hacia las personas trabajadoras en la gestión del registro horario. Y es que la posibilidad de requerir la introducción de un nuevo bloque para modificar un registro previo, manteniendo así la trazabilidad de la información, representa un cambio de paradigma significativo.

Tradicionalmente, el control de la jornada laboral ha recaído en el empleador, quien, en teoría, vela por el cumplimiento normativo y la veracidad de los registros o, al menos, así debiera ser considerado. Sin embargo, transferir esta responsabilidad por completo a la persona trabajadora plantea interrogantes sobre la necesidad de que la relación que une a ambas partes (persona trabajadora y empresa) implique una mayor confianza y buena fe. Es cierto que la persona trabajadora podría registrar sus entradas, pausas y salidas de forma autónoma, sin la injerencia del empleador; pero, en este sentido cabría preguntarse: ¿qué ocurre si la persona trabajadora de forma colusoria con la empresa registra entradas y salidas fraudulentas a cambio de una remuneración adicional? ¿Cómo se garantiza que los registros reflejen la realidad del tiempo trabajado y no un simple acuerdo entre las partes?

Esta perspectiva crítica no busca deslegitimar el potencial del blockchain, puesto que estas mismas preguntas se pudieran plantear con otros métodos de registro de jornada-, sino más bien destacar la importancia de un análisis ponderado de sus implicaciones. La confianza y la buena fe, aunque deseables, no son suficientes para garantizar la integridad del sistema, sino que más allá de la reciprocidad de las partes, es necesario establecer mecanismos de control adicionales que permitan verificar la veracidad de los registros y detectar posibles fraudes.

En este sentido, la tecnología blockchain no elimina la necesidad de supervisión, sino que traslada la responsabilidad de la gestión del registro, en principio, a la persona trabajadora. De hecho, esto podría generar situaciones de vulnerabilidad en las que la persona trabajadora se sienta presionado a falsear los datos o a no registrar adecuadamente su jornada laboral.

Por lo tanto, desde una perspectiva personal, la implementación del blockchain en el registro de jornada laboral debe ir acompañada de medidas de seguridad y de una supervisión adecuada para garantizar que los registros sean precisos, confiables y transparentes. Así, a nuestro parecer, la tecnología, por sí sola, no es una solución mágica, sino que su eficacia depende de cómo se implemente y utilice.

Dentro del blockchain van a almacenarse datos de carácter personal que se encuentran amparados por las legislaciones garantes y protectoras de los datos de las personas. Así las cosas, antes de implantar este sistema deberá cumplirse con las disposiciones relativas a la protección de datos⁴⁶. Sin embargo, en este sentido debemos

46. Martínez Boada, Javier: "Blockchain como sistema para cumplir con la obligación de control y registro de la jornada laboral de los trabajadores", op. cit. p. 7

preguntarnos: ¿es realmente necesario un sistema tan complejo para una tarea relativamente sencilla? ¿No existen soluciones más ágiles y económicas para garantizar la transparencia del registro de jornada? A pesar de estas interrogantes, la tecnología blockchain se presenta como una alternativa interesante para cumplir con la legislación vigente en materia de registro de jornada.

IV. CONCLUSIONES: ¿ESTÁ EL BLOCKCHAIN ORIENTADO EN MATERIA DE DESCARBONIZACIÓN?: PRINCIPALES RETOS EN EL MUNDO DEL TRABAJO Y VACÍOS DE JUSTICIA

La implementación de la tecnología blockchain en la gestión laboral, si bien ofrece ventajas en seguridad y transparencia, plantea interrogantes sobre su idoneidad en el contexto de la descarbonización, la equidad y la justicia en las relaciones laborales.

En este sentido, resulta innegable mencionar previamente que la implementación efectiva del blockchain exige un profundo conocimiento técnico y una inversión significativa. La compatibilidad con los sistemas de gestión laboral existentes puede ser compleja, y la preocupación por la privacidad y el consumo energético son factores limitantes. Y es que las redes blockchain, especialmente aquellas que emplean algoritmos de prueba de trabajo, requieren un considerable consumo de energía⁴⁷, lo cual contraviene con los objetivos de descarbonización. Por lo tanto, a nuestro parecer, aunque sea una tecnología muy interesante, quizá verdaderamente no sea un sistema justificable que, en su diseño, contribuya a la crisis climática en favor de una mayor transparencia y seguridad laboral.

Son pocos los estudios que relacionan el blockchain con la descarbonización, pero, a mi parecer, es un aspecto crucial que merece ser estudiado con mayor detenimiento. En este sentido, la interrogante planteada sobre la justificación de un sistema que contribuye a la crisis climática en aras de una mayor transparencia y seguridad laboral requiere un análisis multifacético y profundamente crítico. La cuestión central radica en ponderar si los beneficios derivados de una mejora en la transparencia y la seguridad laboral son suficientes para compensar los costos ambientales inherentes al despliegue de la tecnología blockchain, cuyo consumo energético es innegable.

En primer lugar, es imperativo reconocer la magnitud de la crisis climática como un desafío global apremiante. La necesidad de reducir las emisiones de carbono y promover prácticas sostenibles es un imperativo ético y legal que trasciende los intereses particulares de cualquier sector o industria. En este contexto, la adopción de tecnologías que contribuyen al calentamiento global debe ser objeto de un escrutinio riguroso. Por otro lado, la transparencia y la seguridad en el ámbito laboral son valores fundamentales que contribuyen a la justicia social y al bienestar de las personas trabajadoras. De hecho, son consideradas garante de derechos.

47. Cruz Manzo, Jessica; Ortuño Barba, Luis Carlos; Villafuerte Palavicini, Faustino Sergio; Araoz Baltazar, Iván; Quintanilla Montalvo, Marifer: "De la cadena de bloques al talento humano: innovaciones disruptivas en recursos humanos", op. cit. p. 9113.



Un sistema que garantice la integridad de los registros de jornada, la trazabilidad de las transacciones salariales y la protección de los derechos laborales podría generar beneficios significativos en términos de confianza, equidad y cumplimiento normativo. Sin embargo, es preciso evaluar si estos beneficios son exclusivos del blockchain o si existen alternativas menos intensivas en energía que puedan lograr objetivos similares.

A mi parecer, aunque en este estudio hemos puesto de manifiesto una realidad existente que, pese a sus desafíos a nivel normativo, resulta ser una alternativa interesante, es fundamental considerar la existencia de tecnologías alternativas, o la posibilidad de desarrollar versiones más eficientes del blockchain, que minimicen el consumo energético sin comprometer la seguridad y la transparencia. Es decir, la cuestión radica en adoptar un enfoque basado en la proporcionalidad y la necesidad.

Desde una perspectiva crítica, es posible argumentar que la implementación de un sistema blockchain intensivo en energía en el ámbito laboral podría ser una decisión miope, que sacrifica el bienestar colectivo a largo plazo en aras de beneficios individuales a corto plazo. Por consiguiente, debemos abogar por garantizar un principio rector en la toma de decisiones tecnológicas, que busquen soluciones que armonicen los objetivos de transparencia, seguridad y justicia social con la necesidad urgente de mitigar el cambio climático.

Para ello, centrándonos en esta tecnología, es crucial analizar los retos y vacíos que puede generar en relación con la socialidad, la reciprocidad y la institucionalidad, dimensiones clave de la justicia relacional según el profesor Márquez Prieto⁴⁸.

Por un lado, con relación a la socialidad, apreciamos que la adopción de blockchain en el ámbito laboral puede generar resistencia cultural. De hecho, centrándonos en la relación jurídica de la persona trabajadora y la empresa, podrían mostrarse reticentes a adoptar una nueva tecnología por desconocimiento o escepticismo. Por lo tanto, debiéramos cuestionarnos o, al menos, considerar, si la implementación del blockchain respeta los valores de grupo y la cultura organizacional.

En un principio, parece que la gestión de la resistencia y la promoción de una cultura de confianza y aceptación hacia la tecnología blockchain en el entorno laboral requieren un enfoque estratégico y sensible que considere las dinámicas sociales que subyacen a la adopción de nuevas tecnologías. Así las cosas, la gestión de la resistencia y la promoción de una cultura de confianza y aceptación hacia la tecnología blockchain en el entorno laboral exigen un enfoque integral que considere los aspectos técnicos, sociales, éticos y legales.

En segundo lugar, es necesario mencionar la reciprocidad y es que, aunque parece que esta tecnología garantiza la transparencia y seguridad, aún quedan muchos interrogantes relacionados al comportamiento recíproco de las partes. Se requiere que

48. Márquez Prieto, Antonio: "La relación laboral como relación social (justicia relacional y socialidad común)", *Revista de Trabajo y Seguridad Social*, CEF, núm. 382, 2015, pp. 13-42; Márquez Prieto, Antonio: "Una investigación en equipo sobre justicia relacional y principio de fraternidad", AA.VV.: *Justicia relacional y principio de fraternidad* / coord. por Márquez Prieto, Antonio, 2023, pp. 17-30; Márquez Prieto, Antonio: "Relación jurídica y social: la justicia y el otro", en AA.VV.: *Estudios jurídicos interdisciplinares sobre justicia relacional y servicios de interés general: Teoría del cuidado, alteridad y relaciones laborales* / coord. por Márquez Prieto, Antonio; Rueda Monroy, José Antonio; Vol. 1, 2023, pp. 225-242.

las personas trabajadoras tengan la capacidad y los recursos para comprender y participar activamente en el sistema blockchain, y más si cabe si esta tecnología puede generar una asimetría de poder, siendo fundamental garantizar una implementación justa y equitativa en el entorno laboral. Para ello, se requiere que las empresas se encuentren orientadas hacia lo justo y muestren esa especial concienciación.

La reciprocidad la podemos analizar teniendo presente si las empresas ofrecen, por ejemplo, programas de formación diseñados específicamente para las necesidades y el nivel de conocimiento de las personas trabajadoras. Esta formación debe abarcar tanto los aspectos técnicos del blockchain como sus implicaciones prácticas en el ámbito laboral. A ello se suma la dotación por la parte empresarial de materiales de apoyo accesibles y fáciles de entender, como manuales, tutoriales y guías prácticas. De igual manera, las empresas deberán garantizar los recursos necesarios (como ordenadores, dispositivos móviles, acceso a Internet y soporte técnico) en el caso de que empleen este tipo de tecnología.

De igual manera, considero esencial que las empresas prioricen la usabilidad y la accesibilidad en el diseño de la interfaz de usuario, es decir, creando un sistema fácil de entender y utilizar, incluso para aquellas personas trabajadoras con poca experiencia en tecnología; e, incluso, que tenga en cuenta las opiniones o sugerencias de las personas trabajadoras para que esta tecnología sea fácil de usar, intuitiva y adaptada a sus necesidades.

Y, de la misma manera, que se garantice la transparencia en el funcionamiento del sistema blockchain, incluyendo la información sobre los datos que se almacenan, cómo se utilizan y quién tiene acceso a ellos. Para ello es fundamental el establecimiento de mecanismos de rendición de cuentas para asegurar que los responsables del sistema blockchain sean responsables de sus acciones y decisiones.

En esta misma línea es necesario que se fomente el diálogo social y la negociación colectiva para abordar las implicaciones laborales del blockchain, en el que se puedan adoptar acuerdos colectivos que reflejen el diseño e implementación del sistema blockchain. Para poder ser garantes de estos derechos, sería interesante valorar la posibilidad de diseñar un sistema de flexible y adaptable a las necesidades cambiantes de la organización, el cual permita adaptar el sistema en caso de ser necesario, garantizando que las decisiones se tomen de forma participativa.

Finalmente, con relación a la institucionalidad, han sido muchas las cuestiones planteadas a lo largo del estudio acerca de los desafíos que esta tecnología presenta en el ámbito normativo, especialmente relacionadas con la protección de datos personales y la privacidad. Por consiguiente, a pesar del auge y el potencial transformador del blockchain en la gestión laboral, la falta de un marco legal específico y adaptado a esta tecnología genera incertidumbre y dificulta su adopción generalizada.

Así, aunque se han venido planteando algunas posibles soluciones, la realidad de las cosas muestra que aún existen ciertos vacíos de justicia. En primer lugar, tras analizar la normativa referenciada en el estudio, se ha observado que, si bien el RGPD y la LOPDGDD establecen principios generales sobre la protección de datos personales, no existe una definición legal específica del blockchain ni de sus diferentes tipos. Esto dificulta la aplicación



de la normativa vigente a esta tecnología, generando incertidumbre sobre la responsabilidad de los diferentes actores involucrados en el tratamiento de datos.

De igual manera, en un sistema blockchain descentralizado resulta complejo determinar quién es el responsable del tratamiento de los datos personales. En este sentido, pensar que el creador de la cadena de bloques es el responsable puede ser un error porque, como regla general, el creador de la cadena de bloques no suele ser considerado el responsable del tratamiento, a menos que también participe activamente en la gestión y el control de los datos personales que se almacenan en ella. De igual modo, los nodos que validan las transacciones tampoco suelen ser considerados responsables del tratamiento, ya que su función es meramente técnica y se limita a verificar la integridad de las transacciones, salvo que tengan acceso a datos personales y los utilicen para fines propios. En este caso sí podrían ser considerados corresponsables del tratamiento.

En el caso, por ejemplo, que el empleador utilice el sistema blockchain para registrar la jornada laboral, entonces parece que será considerado el responsable del tratamiento, puesto que es quien decide la finalidad y los medios del tratamiento de los datos personales de sus empleados, y quien ejerce el control efectivo sobre los mismos. En consecuencia, le corresponde garantizar el cumplimiento de la normativa de protección de datos, incluyendo la obtención del consentimiento, la información a los interesados, la seguridad de los datos y la garantía de los derechos ARCO. Aunque, como hemos referenciado anteriormente, el almacenamiento los datos de los empleados en una cadena de bloques puede dar lugar a problemas de privacidad, ya que son inmutables una vez registrados.

Por consiguiente, esta inmutabilidad del blockchain entra en conflicto directo con el derecho al olvido (supresión) y el derecho de rectificación reconocidos en el RGPD y la LOPDGDD. Por ende, aunque parecen existir técnicas alternativas más orientadas al cumplimiento normativo –como la anonimización, el cifrado y la utilización de hashes–, su efectividad no es absoluta y plantea interrogantes sobre la posibilidad de revertir el proceso y acceder a la información original, ocasionando ciertos vacíos de justicia.

De igual modo, otro de los aspectos a tener presente –aunque no nos hayamos detenido en exceso a lo largo del estudio–, es la posibilidad de que utilizando este tipo de tecnología, las personas trabajadoras se encuentren más expuestas a la filtración de sus datos por posibles ataques informáticos. En este sentido, “algunos de estos fallos de seguridad, que desde la perspectiva técnica escapan de nuestro alcance, coinciden con la posibilidad de que los nodos que supervisan la blockchain sean corruptos, si bien se precisaría para que el sistema dejase de ser seguro que un porcentaje elevado de nodos supervisores fueran corruptibles, lo que en términos de probabilidades es ínfimo. Por otra parte, podría fallar la seguridad a través de un ataque de “denegación de servicio”, por el que se inutilicen parte de estos nodos supervisores, en la búsqueda de favorecer a los nodos corruptos”⁴⁹. Es decir, la utilización de este

49. De Íscar de Rojas, Paula: “La aplicación de la tecnología blockchain en los órganos sociales de las sociedades cooperativas”, *REVESCO* (148), 2024, p. 9

tipo de tecnología también implica una cierta exposición a cuestiones relacionadas con la ciberseguridad. Así, el hecho de que nos encontramos ante una tecnología ciertamente segura en su configuración, los riesgos en ciberseguridad coexisten con las ventajas, requiriéndose mejoras, actualizaciones y, sobre todo, ser probada.

Dicho lo cual, y para concluir el estudio, debemos mencionar que el blockchain se considera una tecnología emergente en su configuración, novedosa, y que plantea un escenario muy interesante con relación a su efectividad y automatización en las transacciones que se realicen. Sin embargo, aún no se mantiene ciertamente alineada con los principios básicos de nuestra normativa internacional y nacional en materia de protección de datos, lo cual ocasiona una evidente inseguridad jurídica en su implantación por parte de las empresas. Estas reflexiones ayudan a comprender que los vacíos de justicia de esta tecnología, al menos por el momento, son ciertamente evidentes. A ello se suma su escasa orientación hacia la descarbonización, no siendo considerada una práctica sostenible por el momento en la materia analizada.

Así las cosas, aunque se considera una alternativa interesante que merece ser estudiada por parte de la doctrina laboralista, la prudencia en su implantación debe ser tenida muy en cuenta, teniendo presente los riesgos y, sobre todo, los desafíos que presenta para el derecho del trabajo como garante de los derechos más básicos de las personas trabajadoras.

Bibliografía

178

- Bartolomeo, Alejandro; Machin Urbay, Gustavo: "Introducción a la tecnología blockchain: su impacto en las ciencias económicas", *Biblioteca Digital UNCUYO*, 2020, p. 3. Disponible para su consulta en: https://bdigital.uncuyo.edu.ar/objetos_digitales/15304/14.-introduccinatecnologia.pdf (Consultado el 30 de abril de 2025).
- Colle, Raymond: "La identidad digital en la internet futura con blockchain", *INCOM*, 2018.
- Cruz Manzo, Jessica; Ortúñoz Barba, Luis Carlos; Villafuerte Palavicini, Faustino Sergio; Araoz Baltazar, Iván; Quintanilla Montalvo, Marifer: "De la cadena de bloques al talento humano: innovaciones disruptivas en recursos humanos", *Ciencia Latina Revista Científica Multidisciplinar*, vol. 8, núm. 5, 2024. https://doi.org/10.37811/cl_rcm.v8i5.14300
- De Íscar de Rojas, Paula: "La aplicación de la tecnología blockchain en los órganos sociales de las sociedades cooperativas", *REVESCO* (148), 2024. <https://doi.org/10.5209/reve.99737>
- Díaz Díaz, Efrén; Moreno Cea, Fernando: "Las aplicaciones del Blockchain a las actividades de las fundaciones y a sus relaciones con la Administración Pública", *Anuario de derecho de fundaciones*, núm. 1, 2017.
- Flores, María Emiliana: "Smart contracts y protección de datos personales", *PAPELES del Centro de Investigaciones de la Facultad de Ciencias Jurídicas y Sociales de la UNL*, vol. 5, núm. 26, 2023. <https://doi.org/10.5209/reve.99737>
- Grigera del Campillo, Santiago: "Privacidad y Blockchain", *Revista Blockchain inteligencia artificial*, núm. 2, 2021. [https://doi.org/10.22529/rbia.2021\(2\)02](https://doi.org/10.22529/rbia.2021(2)02)
- Herrero Jiménez, Marcial: "Gobierno corporativo e inteligencia artificial", *AA.W.: La privacidad en el metaverso, la inteligencia artificial y big data: Protección de datos y derecho al honor / Acedo Penco, Ángel (coord.)*, Dykinson, 2023. <https://doi.org/10.2307/jj.1866788.8>
- Márquez Prieto, Antonio: "La relación laboral como relación social (justicia relacional y socialidad común)", *Revista de Trabajo y Seguridad Social, CEF*, núm. 382, 2015. <https://doi.org/10.51302/rtrs.2015.2522>





Márquez Prieto, Antonio: "Relación jurídica y social: la justicia y el otro", en AA.VV.: *Estudios jurídicos interdisciplinares sobre justicia relacional y servicios de interés general: Teoría del cuidado, alteridad y relaciones laborales* / Márquez Prieto, Antonio (coord.); Rueda Monroy, José Antonio (coord.); vol. 1, 2023.

Márquez Prieto, Antonio: "Una investigación en equipo sobre justicia relacional y principio de fraternidad", AA.VV.: *Justicia relacional y principio de fraternidad* / Márquez Prieto, Antonio (coord.), 2023.

Martínez Boada, Javier: "Blockchain como sistema para cumplir con la obligación de control y registro de la jornada laboral de los trabajadores", *Revista de internet, derecho y política*, núm. 41, 2024. <https://doi.org/10.7238/idp.v0i41.430846>

Sánchez Álvarez, Eduardo; García Pacios, Adrián: "Tecnología blockchain y contratación electrónica: puntos críticos de integración de los denominados Smart contracts en nuestro sistema de derecho contractual", *Revista CEFLegal*, núm. 246, 2021. <https://doi.org/10.51302/ceflegal.2021.9385>