GUÍA GRATUITA PARA EMPRESAS TECNOLÓGICAS

CÓMO ADAPTAR PROYECTOS BLOCKCHAIN AL RGPD

HOLA, SOMOS LARA Y LEYRE, CO-FUNDADORAS DE EDJ XTECH LAW SCHOOL.

Leyre, CEO y experta en transformación digital con más de 15 años de experiencia. Desde 2008 a 2017 trabajé en marketing digital en agencias como Havas, Ogilvy UK o Mediacom UK para marcas como IBM o Procter & Gamble. Desde el 2017, me he dedicado a la disrupción tecnológica de industrias como la banca y los seguros. Fui la Responsable de Originación Digital en EVO Banco durante la transición de la entidad hacia un banco digital y participando en el diseño del onboarding digital de la Cuenta Inteligente y el lanzamiento de la primera hipoteca 100% digital en España.

Posteriormente, asumí el rol de responsable de adquisición digital y web en Liberty Mutual en Europa.

Más recientemente, ocupé el cargo de Chief Growth Officer en Asistensi, la primera insurtech especializada en capitalizar el mercado de las remesas, ofreciendo seguros de salud adaptados a migrantes.

A nivel académico, tengo dos títulos universitarios: uno en Publicidad y Relaciones Públicas y otro en Derecho, y varios masters, postgrados y cursos de especialización en e-commerce, analítica web, growth hacking, big data & data science, ciberinteligencia, ciberseguridad y protección de datos.

"Autoras libro abogados innovadores: el manual definitivo para sobrevivir a la era digital."

Lara, COO y abogada con una sólida experiencia de 15 años en el asesoramiento integral en asuntos de tecnologías exponenciales y protección de datos. He ejercido como abogada en un despacho de primer nivel de 2008-2014 llevando asuntos a nivel nacional e internacional y, con posterioridad, he desempeñando puestos en la función pública, como Capitán Auditor Asesora jurídica en la Armada Española y en la Jurisdicción militar hasta 2023.

Además, he sido profesora de opositores al Cuerpo Jurídico Militar desde 2016, profesora de Derecho en la Escuela de Intendencia de la Armada entre 2018-2021 y tutora de una tesina sobre ciberseguridad en el Master de Derecho Militar de la EMEJ-Universidad de Alcalá en 2022.

Siempre he estado en constante formación, contando con varios Master, cursos y especializaciones, destacando entre mis estudios el Máster de Derecho y Negocio Marítimo en ICADE (2008), el Máster oficial de Derecho Militar de la UCAM (2017) y el Diploma jurídico de especialización del Ministerio de Defensa (2021), habiendo realizado la tesina sobre "Las implicaciones para la seguridad de los buques autónomos".

Índice

Como institución educativa, tenemos la responsabilidad de fomentar el buen uso de las tecnologías exponenciales, incluyendo el blockchain y el mayor aprovechamiento para la evolución social.

El impacto de la blockchain 04

Retos legales y blockchain 05

¿Por qué es importante la protección de datos en la empresa? 06

¿Cómo cumplir el GDPR en nuestro proyecto de blockchain? 07

¿Y si no nos adaptamos al GDPR? 12

El blockchain generará un impacto de 40 mil millones de dólares en 2025.

Aunque con la llegada de las herramientas de inteligencia artificial, otras tecnologías como el blockchain parecían estar quedando en el olvido de la sociedad, la realidad es que la inversión en esta tecnología exponencial no ha dejado de aumentar año tras año.

Según el informe publicado por MarketsandMarkets en 2022 se prevé que el mercado global de la tecnología blockchain alcance casi los 40 mil millones de dólares en este próximo 2025 [1] con una tasa de crecimiento del 47% en Europa y del 45% en Latinoamérica.

Solamente en España, para 2030, se espera que la tecnología blockchain genere un impacto en el PIB de 20 mil millones. [2]

Y respecto a los sectores que más uso realizan de la blockchain, destaca por antonomasia el sector financiero, en gran parte, por el aumento de las inversiones en criptomonedas. Aunque esta no es ni mucho menos su única funcionalidad. Así, para 2025, IDC prevé que el 20% de los préstamos al consumo ya se transfiera en una moneda digital del banco central.

Aunque el sector logístico se encuentra también a la cabeza de su implementación, esperándose que en 2025 se firmen grandes alianzas con empresas logísticas y de IoT.

RETOS LEGALES Y BLOCKCHAIN

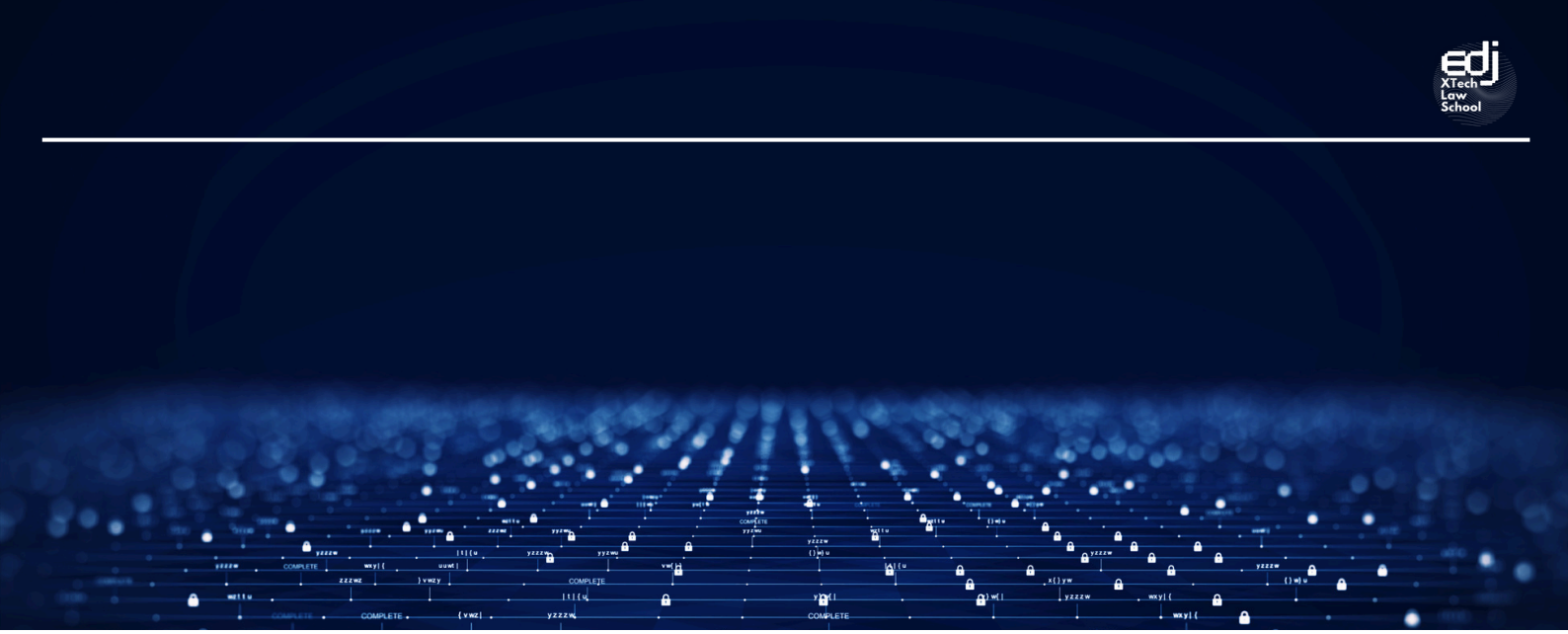
¿QUÉ RETOS PRINCIPALES PLANTEA LA BLOCKCHAIN?

Según el informe 'Blockchain: riesgos, recompensas y regulación', elaborado por la firma de abogados Bird & Bird, el blockchain plantea diversos retos tanto en lo relativo a la gobernanza de la blockchain y la identidad de los sujetos intervinientes [3]. Además de otras controversias en aspectos clave de la la propiedad intelectual, la protección de datos o la resolución contractual.

1. **Protección de datos personales:** Las características inherentes a la tecnología, como la descentralización y la inmutabilidad, generan interrogantes sobre la identificación del responsable del tratamiento, la forma en la que los interesados podrán ejercer derechos, la ubicación de la información y las implicaciones de las transferencias internacionales. En esta guía nos centraremos en resolver estos retos.

2. **Propiedad Intelectual:** Su aplicación en diversos sectores demanda desarrollos adicionales y su integración en los sistemas informáticos específicos de los usuarios; lo que tendrá consecuencias significativas en lo que respecta a la titularidad y explotación de dichos desarrollos.

3. **Ámbito contractual:** Surgen numerosas preguntas respecto a la resolución de conflictos relacionados con las transacciones registradas en la cadena de bloques. ¿Cómo se procederá a la anulación de una transacción? Además, la regulación de los smart contracts utilizados para validar transacciones presenta grandes desafíos jurídicos, especialmente, en cuanto a la traducción al lenguaje informático de todas las posibilidades e interpretaciones que actualmente permiten los contratos tradicionales.



¿POR QUÉ ES IMPORTANTE LA PROTECCIÓN DE DATOS EN LAS EMPRESAS?

La protección de datos: una obligación empresarial

En un escenario de ataques diarios a las empresas, la seguridad de la información es un elemento indispensable.

Todas las empresas, sin importar su tamaño, deben cumplir con las normativas de protección de datos.

La protección de datos es un derecho fundamental de los ciudadanos del EEE. El RGPD protege los derechos y libertades fundamentales de las personas físicas, en particular, su derecho a la protección de los datos personales. Por lo tanto, las empresas deben velar por el respeto a dichos derechos y cumplir con las obligaciones señaladas en el Reglamento General de Protección de Datos.

Ventajas del RGPD para las empresas

Además de ser una responsabilidad, seguir el RGPD presenta claras ventajas para las organizaciones:

- Reducción del riesgo de sanciones.
- Mayor fidelización de clientes.
- Mejora de la reputación.
- Optimización de procesos internos.
- Facilidades para la expansión internacional.
- Promoción de la innovación en ciberseguridad.
- Mejora en la toma de decisiones gracias al análisis de datos.
- Acceso a nuevos mercados con menor dificultad.

Las empresas que se adapten al RGPD obtendrán ventajas competitivas que las prepararán mejor para posicionarse en el mercado global.

¿CÓMO CUMPLIR EL GDPR EN NUESTRO PROYECTO BLOCKAHIN?

El conflicto en materia de protección de datos surge debido a la colisión entre la naturaleza de esta tecnología y la regulación actual de protección de datos. Desde 2016, está en vigor el Reglamento (UE) 2016/679 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos (en adelante, RGPD). Este reglamento fue incorporado a nuestro ordenamiento jurídico a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD).

Esta normativa se presenta como una auténtica carta de derechos en materia de protección de datos en el entorno digital. Sin embargo, el desafío radica en que esta nueva tecnología no parece encajar plenamente con todas sus disposiciones.

Pero existen soluciones.

1. La identificación del responsable

Conforme al artículo 27 del RGPD, es necesario designar un responsable del tratamiento de datos. Sin embargo, la naturaleza descentralizada de la blockchain plantea un conflicto con este precepto.

Si tenemos una red descentralizada, y en el caso de las blockchain privadas no hay un autoridad pública controlando, determinar al responsable del tratamiento es una tarea que exige revisión.

BLOCKCHAIN PRIVADA

Por lo general, una blockchain privada será controlada por un grupo limitado de creadores que establecen las normas. En estos casos, podemos seguir unos criterios de referencia para la determinación del responsable.

1. Se fija el criterio de la existencia de corresponsabilidad, entre personas que decidan realizar conjuntamente un tratamiento de datos.
2. La creación de persona jurídica en representación de los participantes.
3. La designación de uno de los participantes como responsable del tratamiento.

Este tipo de blockchain privada suelen ser internas de una empresa, por ejemplo. En este caso, el responsable del tratamiento sería la empresa, o podría haber una corresponsabilidad entre ella o usuarios de la misma.

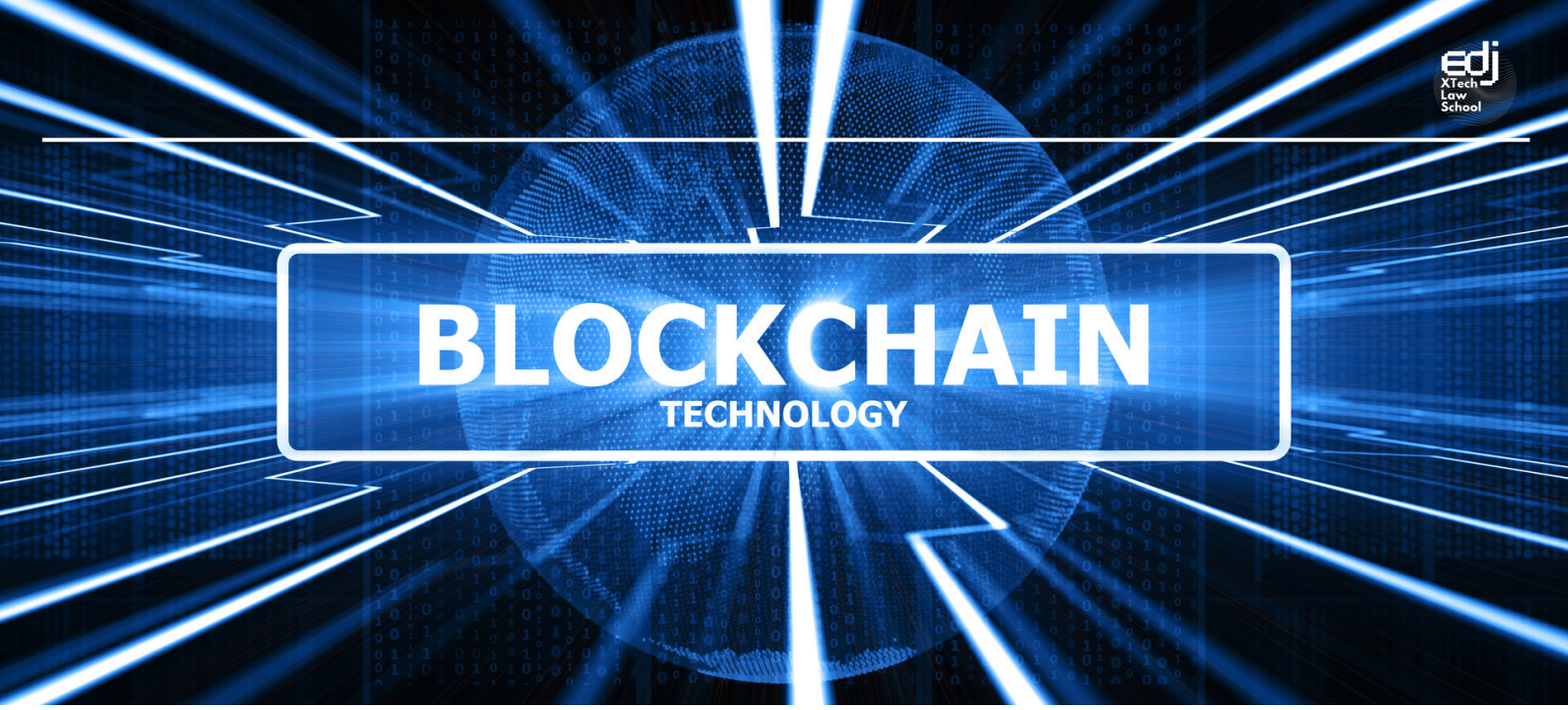
BLOCKCHAIN PÚBLICA

La blockchain pública es aquella que todos pueden usar y unirse al proceso de validación también está abierto a todos. Por ejemplo, Etherum. En estos casos, ¿quién podría ser considerado responsable? En la teoría se debate si podrían ser:

1. Los usuarios que envían transacciones a la cadena vía un nodo, siempre que sea una persona física y el tratamiento de datos personales esté relacionado con una actividad profesional o comercial.
2. Los participantes de la persona jurídica que envían transacciones a la cadena.
3. El interesado pudiera ser responsable de sus propios datos.

LA RECOMENDACIÓN

La realidad práctica es que este tipo de blockchain plantean mucho conflicto para superar este criterio del RGPD. Es por ello, que si tienes un proyecto basado en tecnología blockchain, la recomendación legal será o bien, que se utilice una blockchain privada o bien, que no se incorpore ningún dato de carácter personal a la blockchain pública. En otro caso, habrá que analizar el riesgo para el tratamiento antes de definir su compatibilidad.



2. Derechos de los interesados

La inmutabilidad de la información del blockchain, confronta con el derecho a la supresión de los datos -más conocido popularmente como el derecho al olvido-; y el principio de conservación de datos por no más tiempo del necesario.

El principio de conservación de datos se recoge en el artículo 5 del RGPD que dispone que: "*Los datos personales serán [...] mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.*"

Por su parte, el artículo 17 del RGPD recoge el derecho de supresión en los siguientes términos: *"El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:*

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, o el artículo 9 (relativo a los datos de categoría especial).

LA RECOMENDACIÓN

Ante la complejidad para compatibilizar estos derechos con la tecnología blockchain, las opciones para los proyectos de blockchain sería simplementa no aportar datos a la tecnología y archivarlos en una base externa. Es decir, proteger la información con hash con salt en blockchain y base externa.

3. Transferencias internacionales de datos

Dado que el blockchain funciona el registro de información en una cadena de nodos, que están en distintos países, el establecimiento de un nodo en países fuera de la Unión, puede suponer una transferencia internacional de datos.

El tratamiento transfronterizo se define en el artículo 4 del RGPD como:

1. El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

2. El tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

En otras palabras, una transferencia de datos internacional de datos consiste en la cesión o comunicación de datos por parte de responsables o encargados del tratamiento ubicados en España a otro responsable o encargado del tratamiento situados fuera del EEE.

¿Cómo lo resolvemos?

Existen varias opciones:

1.País con decisión de adecuación

2.Transferencias con garantías adecuadas

3.Adopción de normas corporativas vinculantes

4.Consentimiento expreso del interesado

LA RECOMENDACIÓN

En primer lugar será siempre evitar que haya datos personales en la blockchain. No obstante, existen otras opciones, aunque la solución dependerá de las necesidades de cada proyecto:

1. Transferencias basadas en una decisión de adecuación: Es decir, el tercer país al que se enviarán los datos está aceptado como destinatario adecuado por la Comisión Europea. Son países seguros: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón, Reino Unido, Corea del Sur y EE. UU.

2. Transferencias mediante garantías adecuadas: En este caso, se emplean cláusulas contractuales tipo elaboradas por la Comisión Europea -recogidas en la Directiva 2021/914-, códigos de conducta o códigos tipo.

3. Adopción de normas corporativas vinculantes: Son normas establecidas para las transferencias de datos entre compañías de un mismo grupo de empresas.

4. Consentimiento expreso del usuario: Este consentimiento debe ser expreso e informado debidamente de los riesgos que la transferencia implicará.

2.

¿Y SI NO NOS ADAPTAMOS AL GDPR?

El principio de responsabilidad proactiva que exige el RGPD implica que el responsable de los tratamientos (es decir, la empresa) debe demostrar una actitud activa hacia la protección de datos en el desarrollo de su actividad. Pero, además, incumplir la obligatoriedad de ciertas disposiciones como los términos que debe contener tu web, no realizar un EIPD o no tener DPO cuando sea preciso, tiene diversas consecuencias relevantes para tu startup.

1. Consecuencias legales: En incumplimiento del RGPD puede dar lugar a una infracción mismo conforme a las disposiciones 35 y 36 del RGDP, generando responsabilidad para el responsable o encargado del tratamiento.

2. Consecuencias económicas: Así por ejemplo, no realizar una EIPD obligatoria o no tener Delegado de Protección de Datos son infracciones , que pueden suponer sanción administrativa de hasta 10 millones de euros o del 2 % del volumen de negocios total anual.

3. Consecuencias reputacionales: Lo anterior puede generar, además, desconfianza en tus clientes respecto a la protección que realiza tu startup sobre los datos personales y dañar tu imagen de marca.

1ª CONSULTA JURÍDICA TECNOLÓGICA GRATIS

En EDJ entendemos la convergencia entre la tecnología y el derecho, y los 15 años de experiencia de nuestras CEO y COO en el asesoramiento en transformación digital y en el asesoramiento integral en proyectos de índole tecnológica, nos avalan para ofrecer el mejor asesoramiento.

Nuestra oferta de consultoría y plataforma educativa nos permite abarcar las necesidades legales completas de las empresas en su crecimiento tecnológico, asesorando y formando cuando es necesario a su personal.

Además, formar parte del ecosistema emprendedor de innovación de Madrid nos permite estar en contacto con las necesidades legales reales de las startups.

Entra en nuestra web y reserva tu cita GRATIS

www.edjxtechlawschool.com

DATA SOURCES

[1] Sáez, J. (s.f.) ¿Qué es blockchain y cómo funciona? IEBS.https://www.iebschool.com/blog/blockchain-cadena-bloques-revoluciona-sector-financiero-finanzas/#:~:text=Y%20es%20que%20seg%C3%BAn%20el,a%C3%B1o%20tras%20a%C3%B1o%20hasta%202025.

[2] EFE (2021, Abr. 11) El blockchain generará un impacto de 20 mil millones en España en 2030. Cinco días. https://cincodias.elpais.com/cincodias/2021/04/10/companias/1618078216_033474.html

[3] Cáceres, I (2019, oct. 25) Principales retos en la aplicación del blockchain. Confilegal. https://confilegal.com/20191025-los-principales-retos-en-la-regulacion-del-blockchain-explicados/

GRACIAS

Gracias por haber tomado el tiempo de leer esta guía sobre adaptación de proyectos blockchain al GDPR Esperamos que esta guía te haya proporcionado una visión sólida de las claves básicas a tener en consideración para la adaptación de protección de datos, así como de su trascendencia jurídica para tu empresa.

Te animamos a continuar explorando y profundizando en este tema, ya que las las sanciones de datos son cada vez más frecuentes y es fundamental estar preparados para enfrentar los desafíos que surgen en el mundo digital.

ADAPTACIÓN DE PROYECTOS BLOCKCHAIN AL GDPR

EDJ XTECH LAW SCHOOL

@EDJuristas
contacto@eficienciadigitalparajuristas.com
www.eficienciadigitalparajuristas.com