
This is the **published version** of the bachelor thesis:

Prieto Hernando, Alejandro. *L'impacte del Reglament (UE) 2023/2854 (Data Act) en la contractació automatitzada : anàlisi jurídica dels Smart Contracts i el tractament autònom de dades*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Dret). 48 pàg.

This version is available at <https://ddd.uab.cat/record/331845>

under the terms of the  license.

UAB

Universitat Autònoma de Barcelona

Treball de final de grau

L'IMPACTE DEL REGLAMENT (UE) 2023/2854 (DATA ACT) EN LA CONTRACTACIÓ AUTOMATITZADA

**Anàlisi jurídica dels Smart Contracts i el tractament
autònom de dades**

Tutora: Glòria Ortega Puente

Curs: 2025/2026

Autor: Alejandro Prieto Hernando

10 de maig de 2026

*En agraïment a totes les decisions, persones, errors i encerts que m'han acompanyat
durant tota la carrera i fins a la finalització d'aquest treball.*

A la pluja de Dublín i el sol de Barcelona que han vist néixer i morir aquest treball.

*Un agraïment especial també a la meva tutora, la professora Glòria Ortega Puente, per
haver-me transmès amb excel·lència les bases del Dret Civil i per haver tutoritzat
aquest treball amb rigor, dedicació i una gran amabilitat.*

Aquest treball analitza la contractació mitjançant smart contracts com una realitat jurídica rellevant en el context de la transformació digital i de l'economia de les dades. A partir de l'estudi de la tecnologia blockchain, s'examina l'origen, el funcionament i les principals característiques tècniques dels smart contracts, així com la seva progressiva implantació en les relacions econòmiques i comercials. Posteriorment, s'aborda la seva qualificació jurídica dins del dret contractual, analitzant els requisits de validesa exigits per l'ordenament jurídic espanyol i europeu, amb especial atenció al consentiment, l'objecte i la causa. El treball identifica també els riscos associats a l'automatització de les obligacions contractuals i a la manca inicial d'un marc normatiu específic. En aquest context, s'analitza el marc regulador actual, amb especial referència al Reglament (UE) 2023/2854 (Data Act), que introdueix una definició legal del contracte intel·ligent i estableix requisits en matèria d'interoperabilitat, seguretat, control i mecanismes d'interrupció. A continuació s'aborda la proposta legislativa Òmnibus Digital i l'eventual reforma que proposa al Data Act. Finalment, s'avalua l'impacte d'aquesta regulació en la seguretat jurídica, la protecció de les parts contractuals i el foment d'una innovació tecnològica responsable dins del mercat digital europeu.

Paraules clau: smart contracts, blockchain, contractació automatitzada, Data Act, Omnibus Digital, dret digital, seguretat jurídica, mercat de dades.

Català

Aquest treball estudia la contractació mitjançant smart contracts com a fenomen jurídic emergent dins l'ordenament europeu. S'analitza la seva naturalesa tècnica i la seva qualificació com a contractes jurídicament vinculants, així com el marc normatiu vigent aplicable. L'estudi se centra en l'impacte del Reglament (UE) 2023/2854 (Data Act), especialment en els requisits d'interoperabilitat, seguretat i control previstos a l'article 36. Finalment, es valora el seu impacte en la seguretat jurídica i en l'activitat econòmica digital, tot apuntant que l'eventual aprovació del paquet Òmnibus Digital de la Unió Europea, que preveu la supressió d'aquest article, introdueix un nou element d'incertesa regulatòria en aquest àmbit.

Español

Este trabajo aborda la contratación mediante smart contracts como una realidad jurídica consolidada en el entorno digital europeo. Se analiza su naturaleza técnica y su encaje en el Derecho contractual, así como el marco regulador actualmente aplicable. El estudio se centra en el impacto del Reglamento (UE) 2023/2854 (Data Act), en particular en los requisitos de interoperabilidad, seguridad y control previstos en su artículo 36. Finalmente, se examina su incidencia en la seguridad jurídica y en la actividad económica digital, señalando que la eventual aprobación del paquete Ómnibus Digital de la Unión Europea, que prevé la supresión de dicho artículo, introduce un nuevo elemento de incertidumbre regulatoria en este ámbito.

English

This paper examines smart contract-based contracting as an established legal reality within the European digital environment. It analyses their technical characteristics, legal qualification and the current regulatory framework applicable to them. Particular attention is given to Regulation (EU) 2023/2854 (Data Act), especially the interoperability, security and control requirements set out in Article 36. The paper concludes by assessing their impact on legal certainty and the digital economy, noting that the potential adoption of the EU Digital Omnibus simplification package, which provides for the deletion of that article, adds a further layer of regulatory uncertainty to this area.

Abreviatura	Significat
UE	Unió Europea
CC	Codi Civil
LSSICE	Llei 34/2002, de serveis de la societat de la informació i de comerç electrònic
Data Act	Reglament (UE) 2023/2854 relatiu a les dades
MiCA	Markets in Crypto-Assets Regulation
DLT	Distributed Ledger Technology (tecnologia de registre distribuït)
IoT	Internet of Things (Internet de les coses)
B2B	Business to Business
B2G	Business to Government
DEEP	Dispositiu de Registre Electrònic Compartit
CC	Codi Civil espanyol
art.	Article
arts.	Articles
HB	House Bill
Reg. (UE)	Reglament de la Unió Europea
PIB	Producte Interior Brut
DGA	<i>Data Governance Act</i>
DOUE	Diari Oficial de la Unió Europea

Taula de contingut

1. Introducció	7
2. Context tecnològic: Blockchain i el naixement dels Smart Contracts	8
2.1. Origen i evolució del <i>blockchain</i> : de <i>Bitcoin</i> a <i>Ethereum</i>	8
2.2. Definició tècnica i jurídica del <i>Smart Contract</i>	10
2.2.1 Definició tècnica: El Smart Contract com a protocol informàtic.....	10
2.2.2 Definició jurídica: El Smart Legal Contract	13
○ L'objecte en els smart contracts	14
○ El consentiment en els smart contracts	15
2.3. Avantatges competitius en l'economia digital: eficiència, reducció de costos de transacció i automatització de processos.	18
3. Regulació dels contractes intel·ligents i dret comparat	19
3.1. La doctrina del Code is Law: la inmutabilitat enfront de la flexibilitat jurídica....	19
3.2. Vulnerabilitats i buits legals: la manca de mecanismes de resolució de conflictes en entorns descentralitzats.....	20
3.3. Panoràmica del dret comparat: on, des de quan i com es regulen	22
○ Estats Units	22
○ França	23
○ Rússia	23
3.4. El marc regulador espanyol i europeu	24
4. Marc normatiu i anàlisi jurídica del Reglament (UE) 2023/2854 (Data Act): Fonaments de l'accés just, interoperabilitat i el règim dels contractes intel·ligents ..	25
4.1. Marc normatiu del Reglament (UE) 2023/2854 (Data Act)	25
4.2. Fonaments i principis inspiradors del Reglament de Dades: l'accés just i la interoperabilitat.	27
4.3. Definició legal de contracte intel·ligent segons el Reglament.	29
5. La proposta de Reglament Òmnibus Digital i possible supressió de l'article 36 del Data Act.	33
6. Reflexions crítiques i conclusions	37
6.1. Compatibilitat del Reglament amb la natura descentralitzada de la Blockchain.	37
6.2. La seguretat jurídica com a motor de la innovació tecnològica.....	39
6.3. Balanç final: equilibri entre la protecció de l'usuari i la llibertat tecnològica. ..	40
7. Conclusions.....	41
8. Bibliografia i fonts documentals	42

1. Introducció

La transformació digital ha alterat de manera profunda la forma com es creen, s'executen i s'extingeixen les relacions jurídiques. En aquest nou escenari, el dret es veu interpel·lat per tecnologies que no només donen suport a l'activitat econòmica, sinó que intervenen directament en la formació i l'execució de les obligacions contractuals. Entre aquestes, la tecnologia blockchain i, en particular, els smart contracts, representen un dels canvis més disruptius en la manera d'entendre la contractació. Els smart contracts han deixat de ser una mera proposta teòrica o experimental per convertir-se en instruments utilitzats en sectors tan diversos com els serveis financers, l'internet de les coses, la gestió de dades o el comerç digital. La seva capacitat d'automatitzar l'execució de les prestacions contractuals planteja una promesa d'eficiència, seguretat i reducció de costos, però també genera interrogants jurídics de gran rellevància que afecten directament els fonaments del dret de contractes.

Aquest Treball Final de Grau neix de la inquietud per comprendre fins a quin punt aquestes noves formes de contractació poden encaixar dins dels esquemes jurídics tradicionals. Lluny d'assumir una ruptura absoluta amb el dret clàssic, el treball parteix de la premissa que els smart contracts constitueixen una nova expressió formal del contracte, que ha de ser analitzada a la llum dels principis generals de l'ordenament jurídic.

Un dels objectius centrals d'aquest estudi és analitzar la realitat jurídica dels smart contracts, diferenciant clarament la seva dimensió tècnica de la seva qualificació com a contractes jurídicament vinculants. En aquest sentit, s'examina si aquests mecanismes compleixen els requisits de validesa exigits pel dret espanyol i europeu, així com les particularitats que introdueixen en relació amb el consentiment, l'objecte i la causa.

Tanmateix, l'automatització contractual no està exempta de riscos. La rigidesa tècnica, la dificultat de modificació un cop desplegada i la gestió de situacions imprevistes evidencien la necessitat d'un marc normatiu que porti seguretat jurídica i garanteixi la protecció de les parts. És precisament en aquest context on adquireix especial rellevància la intervenció del legislador europeu.

El Reglament (UE) 2023/2854, conegut com a Data Act, suposa un punt d'inflexió en la regulació dels smart contracts utilitzats en entorns d'intercanvi de dades. Aquest treball pretén analitzar de manera crítica l'impacte d'aquesta norma, especialment pel que fa als requisits d'interoperabilitat, seguretat i control que introdueix, i valorar fins a quin punt aquests són compatibles amb la naturalesa tecnològica dels contractes intel·ligents.

En definitiva, l'objectiu d'aquest TFG és oferir una anàlisi jurídica rigorosa i reflexiva que permeti comprendre com el dret pot adaptar-se a la innovació tecnològica sense renunciar als seus principis essencials. El treball aspira a contribuir al debat sobre la necessitat d'equilibrar la llibertat tecnològica amb la seguretat jurídica, posant de manifest el paper del dret com a eina clau per ordenar i legitimar la transformació digital.

2. Context tecnològic: Blockchain i el naixement dels Smart Contracts

2.1. Origen i evolució del *blockchain*: de *Bitcoin* a *Ethereum*.

La tecnologia *blockchain* no és un invent espontani, sinó el resultat de dècades d'investigació en criptografia¹ que avui promet redefinir les regles del joc digital. Encara que molts la veuen com un concepte actual, desconegut o fins i tot amb certa desconfiança o escepticisme, la seva història és un relat fascinant de cerca d'integritat i llibertat que va començar molt abans de l'auge de les criptomonedes (Ballabriga Solanas, 2019).

Per comprendre aquesta tecnologia, ens hem de remuntar al 1991. Stuart Haber i W. Scott Stornetta es van obsessionar amb una idea: com poder confiar en que un document digital no ha estat alterat.

La seva solució va ser crear el sistema *blockchain* (*cadena de blocs*). Els propis autors van donar amb un recurs tecnològic que sostenia que "*Amb un esquema de signatura segura disponible, quan el servei de segellat de temps (TSS) rep el valor hash, hi afegeix la data i l'hora, i tot seguit signa aquest document compost i l'envia al client.*" (Haber & Stornetta, 1991, p.102).

Per explicar-ho de manera molt més senzilla: imagineu que cada document té una "empremta digital" única (el *hash*). Si canvies una sola coma del text, l'empremta canvia completament. En lloc de guardar aquestes empremtes en un calaix amb clau que només una persona controla, aquesta tecnologia les reparteix entre milers d'ordinadors alhora. Això vol dir que no cal confiar en una única empresa o govern; la confiança neix del fet que tothom té la mateixa llista i, si algú intenta fer trampa i modificar un document, la resta de la xarxa se n'adonarà immediatament perquè les empremtes ja no coincidiran. És, en essència, un llibre de registre que tothom vigila i que ningú pot esborrar. Aquesta fita científica va sembrar la llavor de la veritat digital, demostrant que podíem protegir la informació sense dependre de l'honestedat humana (Fetsyak, 2020).

¹ La criptografia és el conjunt de tècniques que serveixen per protegir la informació, transformant-la perquè només la puguin entendre les persones autoritzades. Permet garantir la confidencialitat, la integritat i la seguretat de les dades.

Tanmateix, la veritable explosió d'aquesta proposta va ocórrer l'any 2008 de la mà de l'enigmàtic Satoshi Nakamoto². No va ser fins a aquest moment, amb el llançament de *Bitcoin*, que la *blockchain* va passar de la teoria acadèmica a la pràctica. Creant, gràcies a aquesta tecnologia, la primera criptomoneda de la història. El fet revolucionari no va ser només crear una moneda, sinó eliminar d'un sol cop els intermediaris bancaris, permetent que el valor flueixi directament entre persones gràcies a una arquitectura descentralitzada i transparent (Nakamoto, 2008; Fetsyak, 2020).

Però l'evolució no es va aturar aquí. Va ser a l'any 2013 quan un jove programador anomenat Vitalik Buterin va fer un pas més enllà i va crear Ethereum³. La seva intenció era arribar a demostrar que la *blockchain* podia ser molt més que "diners". En introduir el llenguatge de programació Solidity, aquesta plataforma va convertir la cadena de blocs en un ordinador global capaç d'executar contractes intel·ligents (*smart contracts*) (Ballabriga Solanas, 2019). Aquests no són contractes avorrits en paper, sinó codis que es compleixen sols quan ocorre un esdeveniment, eliminant la necessitat d'advocats o jutges per a verificar que es respecti el que s'ha acordat (Fetsyak, 2020; Legerén-Molina, 2018).

Avui, aquesta tecnologia ha sigut capaç de transformar el nostre dia a dia. La veiem agilitzant pagaments internacionals en segons, rastrejant la ruta exacta dels aliments que consumim o protegint historials mèdics amb una seguretat sense precedents (Fetsyak, 2020). Des de la transparència en contractes públics fins a l'automatització d'assegurances, la *blockchain* ha deixat de ser una promesa per a convertir-se en la columna vertebral d'una nova economia digital més justa i eficient (Ballabriga Solanas, 2019).

² Satoshi Nakamoto és el pseudònim utilitzat per la persona o grup de persones que va crear Bitcoin l'any 2008, amb la publicació del *white paper* titulat *Bitcoin: A Peer-to-Peer Electronic Cash System*. Tot i que se li atribueix el desenvolupament inicial del protocol i de la primera cadena de blocs, la seva identitat real continua sent desconeguda. Després de participar activament en el projecte fins aproximadament el 2010, Nakamoto va desaparèixer de l'esfera pública, fet que ha donat lloc a nombroses especulacions sobre el seu origen, nacionalitat i motivacions, convertint-lo en una de les figures més enigmàtiques de la història de la tecnologia digital.

³ Ethereum és una plataforma *blockchain* pública creada l'any 2015, amb la finalitat d'ampliar les funcionalitats de Bitcoin més enllà dels pagaments digitals. A diferència d'aquest, Ethereum permet executar codi de manera descentralitzada mitjançant *smart contracts*, programes que s'executen automàticament quan es compleixen determinades condicions. Aquests contractes funcionen sobre la Ethereum Virtual Machine (EVM), que garanteix l'execució uniforme del codi a tota la xarxa sense necessitat d'una autoritat central. Ethereum utilitza l'ether (ETH) com a actiu propi per pagar les operacions (*gas*) i ha esdevingut una infraestructura clau per al desenvolupament d'aplicacions descentralitzades en àmbits com les finances, els actius digitals i l'automatització de relacions contractuals.

2.2. Definició tècnica i jurídica del *Smart Contract*

Els smart contracts són una innovació completament actual i que no hagués sigut possible sense tot al camí recorregut fins ara, en computació, criptografia, blockchain o sistemes de programació com Solidity⁴. Però tot i així, les seves arrels són molt anteriors. Hauríem de remuntar-nos al 1994 quan Nick Szabo va plantejar la possibilitat d'executar acords mitjançant codi informàtic per minimitzar la necessitat d'intermediaris (Szabo, 1994). Ara bé, dins d'aquest escenari de revolució conceptual i informàtica els *smart contracts* sorgeixen com una eina disruptiva que busca l'automatització plena de les obligacions contractuals mitjançant l'ús de codi informàtic (Fetsyak, 2020). Una eina que només va ser capaç de desenvolupar-se amb la irrupció i el perfeccionament de les tecnologies de registre distribuït (DLT)⁵, concretament de la blockchain, que la seva implementació pràctica ha esdevingut viable.



Imatge 1 - Esquema dels registres centralitzats vs distribuïts. Font: Anstey, S. M. (2023)

2.2.1 Definició tècnica: El Smart Contract com a protocol informàtic

Des d'una perspectiva purament informàtica, el smart contract es defineix com un protocol de transacció computat que executa els termes d'un acord (Szabo, 1994). Es tracta de seqüències d'instruccions redactades en llenguatge de programació que s'emmagatzemen i s'executen dins d'una xarxa blockchain (Legerén-Molina, 2018).

Per tant, podem definir els *smart contracts* com a seqüències de codi i dades que s'emmagatzemen en una adreça determinada de la *blockchain* (Tur Faúndez, 2018). Tanmateix, ja podem avançar que aquesta definició manca de naturalesa jurídica, atès que, en l'argot propi de la plataforma, qualsevol línia de codi desplegada a la *blockchain* pot ser qualificada com a *smart contract*.

⁴ Llenguatge de programació creat específicament per escriure contractes intel·ligents que s'executen sobre la blockchain d'Ethereum. Va ser desenvolupat amb l'objectiu de permetre la creació d'aplicacions descentralitzades i l'automatització de transaccions i processos digitals de manera segura i immutable. És àmpliament utilitzat en àmbits com les finances descentralitzades (DeFi), els tokens no fungibles (NFT) i els sistemes d'identitat digital.

⁵ Les tecnologies DLT (*Distributed Ledger Technology*) són sistemes digitals que permeten registrar i compartir dades de forma descentralitzada entre diversos participants. A diferència d'una base de dades tradicional gestionada per una sola entitat, la informació es replica i se sincronitza en múltiples punts de la xarxa, garantint que el registre sigui segur, transparent i molt difícil de modificar sense el consens del grup. La tecnologia *blockchain* n'és l'exemple més conegut.

Com s'analitzarà més endavant, la seva consideració com a contracte en sentit jurídic només serà possible quan el llenguatge de programació utilitzat compleixi els requisits que l'ordenament jurídic exigeix per a la vàlida formació dels contractes.

Alguns autors espanyols s'han pronunciat sobre la definició purament tècnica dels *smart contracts*. Puyol Montero (2016) els descriu com a protocols informàtics que faciliten, verifiquen i fan complir la negociació d'un contracte sense necessitat d'una clàusula contractual. D'una forma similar, Prenfeta Rodríguez (2016) els concep com a seqüències d'instruccions o indicacions destinades a ser utilitzades, directa o indirectament, en un sistema informàtic. Per la seva banda, Morell Ramos (2016) els defineix com l'ús de codi informàtic per articular, verificar i executar un acord entre parts.

La principal nota característica d'aquesta definició tècnica és l'automatització. El codi és capaç de llegir i reconèixer un supòsit de fet determinat i, de manera autònoma, aplicar-li una conseqüència jurídica preestablerta seguint una estructura *if-then-else* (Ballabriga Solanas, 2019). Aquesta configuració elimina la discrecionalitat humana en l'execució, convertint el programa en un instrument "obedient" que actua segons els paràmetres programats.

Smart contract tècnic: exemple pràctic

Imaginem el següent escenari: dos amics, en Xavier i en Luis, són apassionats del futbol i aquesta vegada tenen una aposta senzilla sobre el clàssic Barça vs. Reial Madrid.

Per evitar discussions, errors o la típica excusa de "me'n vaig oblidar de pagar-te", decideixen utilitzar un smart contract, un petit acord digital que funciona només quan es compleixen les regles.

En Xavier, confiat en la victòria del Barça, diposita la seva aposta al contracte. En Luis, segur que el Madrid guanyarà, fa el mateix. Tots dos saben que els seus diners estan segurs, ningú no els pot tocar ni amagar: el contracte és cert i només s'executarà sota certes condicions, i està dipositat a la blockchain, un lloc immutable i impossible d'enganyar.

El partit es juga. Gols, emocions, targetes... i finalment, el Barça guanya. Automàticament, gràcies al smart contract, els diners acumulats dels dos amics es transfereixen al guanyador, en aquest cas en Xavier. No cal que ningú truqui a l'altre, ni que signi papers, ni que es recordin de fer transferències; la regla estava clara des del principi, i el contracte la compleix al peu de la lletra.

Al final, el que semblava només una aposta es converteix en un exemple de com la tecnologia pot garantir justícia, transparència i confiança entre amics, tot mentre gaudeixen del joc i de l'emoció del clàssic. El smart contract no oblida, no discuteix, simplement executa el que s'ha promès.

Tot i l'autonomia d'execució i la naturalesa tancada de la *blockchain*, s'ha d'interpretar que els *smart contracts* tenen una "intel·ligència limitada" (Tur Faúndez, 2018). Per resoldre aquest aïllament, s'introdueix la figura dels oracles⁶.

En el supòsit de l'aposta entre en Xavier i en Luis, la figura de l'oracle és l'element que permet que el contracte conegui el resultat del partit sense dependre de la intervenció humana. Sense un oracle, el smart contract romandria en un estat d'espera permanent, ja que la *blockchain* no té capacitat per si sola de comprovar el resultat del clàssic de forma autònoma. En la pràctica, el contracte es programa per connectar-se a una font de dades externa oficial, com ara l'acta digital de la competició o un servei d'informació esportiva. Una vegada l'oracle transmet el resultat final del partit a la blockchain, el contracte valida la dada i executa la transferència de fons al guanyador.

Per tant, podem concloure que els *smart contracts* presenten una sèrie de característiques principals dins del sistema blockchain, les quals també condicionen el seu impacte jurídic. En primer lloc, destaquen per la descentralització, ja que la informació i el control no depenen de cap autoritat central ni govern, la qual cosa garanteix una gestió distribuïda i més resistent a manipulacions.

A més, aquests contractes ofereixen un elevat grau de seguretat, ja que la confiança es transfereix automàticament de les persones al codi matemàtic i al llenguatge de programació que els sustenta, minimitzant el risc d'errors o frauds. Aquesta seguretat va estretament lligada a la transparència, ja que qualsevol usuari pot auditar la informació emmagatzemada i comprovar-ne la correcta execució. Finalment, la immutabilitat és una altra característica clau: un cop registrada la informació, aquesta esdevé irreversible, cosa que assegura la integritat del registre.

Una vegada analitzada la naturalesa tècnica d'aquests contractes i les seves característiques, podem passar a examinar la seva vessant purament jurídica, on aquestes qualitats tècniques condicionen el règim legal i les implicacions normatives que poden derivar-se de la seva aplicació.

⁶ Són serveis de tercers que actuen de pont entre el món real i el protocol digital, enviant informació externa i verificable al contracte intel·ligent. L'oracle no és el contracte en si mateix, sinó la font de veritat que permet que la condició lògica programada (el supòsit de fet) es validi mitjançant dades reals, com ara preus de mercat, condicions meteorològiques o esdeveniments físics reals.

2.2.2 Definició jurídica: El Smart Legal Contract

Abans d'aprofundir en l'anàlisi, és molt rellevant assenyalar que la denominació *smart contract* és considerada per gran part de la doctrina com una imprecisió terminològica, ja que, molts autors defensen que en sentit estricte, no és ni intel·ligent ni constitueix un contracte de manera autònoma.

El jurista Carlos Tur Faúndez ja assenyala al seu llibre *Smart contracts. Análisis Jurídico (2018)* que aquest terme neix com un homenatge a la primigènia idea de codificació de Szabo i que no adquireixen per si mateixos la condició legal de contracte.

Respecte a la seva intel·ligència, l'autor adverteix que el codi no té capacitat de judici ni pot valorar conceptes indeterminats, essent un instrument merament executiu. Per tant, no es tant un contracte intel·ligent si no un contracte obedient.

Pel que fa a la seva naturalesa contractual, autors com Tur Faúndez i Fetsyak argumenten que l'ús del terme "contracte" en l'àmbit informàtic ha estat sovint informal, creant interpretacions equívokes en el món del dret. Es per aquest motiu, que des de la vessant del dret, la doctrina jurídica prefereix el terme "*smart legal contract*" per referir-se a aquells acords redactats en codi informàtic que tenen la voluntat de produir efectes jurídics vinculants (Fetsyak, 2020).

Aclarit aquest debat terminològic vull destacar que en el treball es farà servir el terme smart contract d'una forma genèrica per referir-se sempre als smart legal contracts. Ja que la naturalesa jurídica inherent a aquest estudi així ho requereix.

Però quins son els trets indispensables per a que la legislació espanyola considera aquest smart contracts com a textos legals vinculants? Ho analitzem a continuació.

○ Naturalesa contractual al ordenament jurídic espanyol

La següent pregunta que ens hem de realitzar per tal d'entendre de forma adequada als *smart contracts*. Es quan es podran considerar jurídicament parlant contractes. O el que encara és més important, ¿haurien de tenir la mateixa validesa i eficàcia que un contracte "tradicional"? És a dir, ¿estan sotmesos al principi d'obligatorietat dels contractes previst al article 1091 del Codi Civil⁷?

El primer punt de vista que cal analitzar és el formal. En aquest sentit, el fet de que es redactin total o parcialment en un llenguatge de codi informàtic no ha de suposar cap problema ni obstacle pel seu reconeixement legal. Doncs com es sabut, el article 1278 del Codi Civil⁸ reconeix la llibertat de forma dels contractes.

⁷ **art 1091 CC:** Las obligaciones que nacen de los contratos tienen fuerza de ley entre las partes contratantes, y deben cumplirse al tenor de los mismos.

⁸ **art 1278 CC:** Los contratos serán obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez.

Ara bé, independentment de la forma del contracte, aquest ha de complir una sèrie de requisits per a ser reconegut com a tal. En aquest sentit, tots els autors coincideixen de forma unànime en que la validesa legal a Espanya dels *smart contracts* depèn de si es, o no, capaç de reunir els requisits de l'article 1261 del Codi Civil⁹. Addicionalment, és important mencionar que a aquest tipus de contractes els hi es d'aplicació el article 23 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y el Comercio Electrónico¹⁰ (Legerén-Molina, 2018).

La literalitat del article 23.1 d'aquesta llei reafirma la tesi de que els *smart contracts* seran tractats amb la mateixa eficàcia i validesa que els contractes "tradicionals" sempre que concorrin consentiment, objecte i causa (Fetsyak, 2020). A la vegada, el article 23.2 LSSICE ens confirma que no es necessari cap acord previ de les parts respecte l'ús de mitjans electrònics per a que el contracte sigui vàlid.

- L'objecte en els smart contracts

La legislació exigeix un "objecte cert que sigui matèria del contracte". En aquest sentit, la doctrina majoritària coincideix en que l'objecte del contracte son les realitats con entitat material (física o jurídica) sobre la que recau el consentiment de les parts (De Pablo Contreras, 2016). Com a qualsevol contracte, aquest objecte haurà de ser determinat o determinable, lícit i no podrà recaure sobre coses que es trobin fora del comerç ni consistir en coses o serveis impossibles tal i com es disposa en els articles 1271, 1272 i 1273 del Codi Civil.

En aquest sentit és interessant puntualitzar l'avantatge del objecte cert quan es disposa en codi informàtic front el llenguatge natural, ja que els *smart contracts* no admeten cap classe d'ambigüitat (Fetysak, 2018).

⁹ **art 1261 CC:** No hay contrato sino cuando concurren los requisitos siguientes:

- 1.º Consentimiento de los contratantes.
- 2.º Objeto cierto que sea materia del contrato.
- 3.º Causa de la obligación que se establezca.

¹⁰ **art 23 LSSICE. Validez y eficacia de los contratos celebrados por vía electrónica.**

1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurren el consentimiento y los demás requisitos necesarios para su validez.

Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

2. Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

3. Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico.

4. No será de aplicación lo dispuesto en el presente Título a los contratos relativos al Derecho de familia y sucesiones.

Los contratos, negocios o actos jurídicos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica.

- La causa en els smart contracts

Per la seva part, el 1261 CC estableix com a requisit essencial del contracte la “causa de la obligació que s'estableixi” entenent que aquesta sigui la raó per la qual les parts han celebrat el contracte i que ha de ser: lícita (art 1275 CC), veraç (art 1276 CC) i existent (art 1277 CC).

En el particular cas dels *smart contracts* s'ha de tenir en consideració que la execució automàtica de les prestacions conforme als pactes de les parts forma part de la causa. I són les mateixes parts del contracte que han de ser conscients en tot moment de la naturalesa especial de l'execució de les prestacions (Lotz, 2018). En conseqüència, res no impedeix reconèixer l'existència d'una causa o raó antecedent en la qual es fonamenta el dret a exigir una conducta de prestació. Aquesta afirmació és especialment rellevant perquè descarta que el caràcter automatitzat de l'execució pugui alterar la causa de les obligacions que deriven del contracte.

És aquí on a diferència del contracte tradicional, el codi pot contenir l'acord entre les parts i que la seva autoexecució programada constitueix la forma natural i esperada de compliment de les prestacions. Sota aquest plantejament, la causa dels contractes intel·ligents no difereix de la dels contractes tradicionals: en els onerosos hi haurà una causa sinal·lagmàtica recíproca, en els gratuïts una causa de liberalitat, i en els remuneratoris, un servei o prestació anterior. El que canvia, en definitiva, no és l'element causal, sinó el mecanisme a través del qual les obligacions causalment justificades s'executen de forma efectiva i autònoma.

- El consentiment en els smart contracts

La perfecció del *smart contract* es produeix amb la concurrència de l'oferta i l'acceptació, així com de l'objecte i la causa del contracte, cosa que, en essència, comporta una externalització de la voluntat de les parts de quedar sotmeses a l'acord contractual.

Tanmateix, el consentiment és possiblement el requisit contractual que genera més debat doctrinal. En aquest sentit, Ballabriga Solanas sosté que cal parlar d'un consentiment “tridimensional”, que recau sobre el contingut del contracte, el mètode d'autoexecució i el suport de codi informàtic (Ballabriga Solanas, 2019). D'acord amb aquesta posició, l'autor argumenta que el consentiment va més enllà de la mera voluntat d'obligar-se i de les prestacions que s'han de dur a terme, ja que inclou també l'acceptació de l'autoexecució del contracte. Aquesta segona mostra de consentiment, recau sobre un consentiment “preconstituït” sobre la consumació automàtica.

En aquest sentit, sotmetre l'acord a aquesta peculiaritat pot interpretar-se com una renúncia al control de l'execució posterior, control que sí que existeix en la contractació tradicional. I per últim, la submissió del contracte a un codi informàtic implica un consentiment tàcit a prescindir de la intervenció humana tant en la redacció com en l'execució del contracte.

Aquesta triple vessant de consentiment està regulada en les mateixes disposicions generals del 1.261 i següents del CC. Tot i que, per tractar-se d'un contracte subscrit a través de dispositius automàtics, hi haurà consentiment en el moment en el que concorren la oferta, es manifesti l'acceptació (1.262.2CC i 54CCom¹¹).

Finalment, els *smart contracts* també requereixen d'una expressió tradicional del consentiment: la firma. En aquest sentit els *smart contracts* poden signar-se de forma convencional incloent la signatura natural al text i al *hash* o, per major seguretat, amb mètodes de signatura criptogràfica (Ballabriga Solanas, 2019). La regulació espanyola de aquesta metodologia de signatures electròniques està recollida a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza¹².

- **El moment de perfecció dels *smart contracts***

Determinar amb exactitud i rigor el moment exacte de la perfecció dels *smart contracts* és també una de les qüestions amb més rellevància jurídica, ja que d'aquesta interpretació es marcarà el moment en que neixen les obligacions vinculants entre les parts. A l'ordenament espanyol, el sistema de perfecció es regeix pel principi consensualista, segons el qual els contractes es perfeccionen pel mer consentiment manifestat pel concurs de l'oferta i de l'acceptació sobre la cosa i la causa (article 1258 del Codi Civil¹³). Sota aquesta premissa, la perfecció del contracte es produirà quan cada part del contracte realitzi els actes prèviament determinats i programats com a necessaris per a considerar l'existència del consentiment vàlidament emès. Aquestes actes seran suficients per a que el *smart contract* "dispari" el procés d'execució (Tur Faúndez, 2018).

La qual cosa implica que donat que l'acceptació s'articula mitjançant una acció tècnica com un *click* en una interfície o la signatura d'una transacció criptogràfica que s'envia a la xarxa, el moment de la perfecció es fixa en l'instant d'aquesta manifestació. Això és degut a que la recepció pel sistema de l'oferent es considera produïda de forma instantània o gairebé immediata (Obregón Siegmund, 2012).

¹¹ Major desenvolupament *ad infra*

¹² Aquesta norma sorgeix per adaptar l'ordenament jurídic espanyol al Reglament (UE) n.º 910/2014 (eIDAS), amb l'objectiu de garantir un marc normatiu homogeni en l'àmbit europeu per a la identificació i els serveis de confiança. La seva entrada en vigor va suposar la derogació de l'antiga Llei 59/2003 de signatura electrònica, que havia quedat desfasada davant la necessitat de reforçar la seguretat jurídica i l'eficàcia de les transaccions electròniques en el mercat interior.

¹³ **art 1258 CC:** Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan, no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley.

○ El lloc de perfecció dels *smart contracts*

Donada la pròpia idiosincràsia dels *smart contracts*, aquests es perfeccionen en un entorn digital, la qual cosa significa que ens trobem en un supòsit de contractació entre absents. En aquest sentit la legislació espanyola, tant en l'article 1262.2 del Codi Civil¹⁴ com en el 54 del Codi de Comerç estableixen que el contracte es pressuposarà celebrat en el lloc en el qual es va fer la oferta (Ballabriga Solanas, 2019).

No obstant, també hem de tenir en consideració l'article 29 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico¹⁵, on s'estableixen diferencien en funció de si el contracte es entre empresaris o si una de les parts té consideració de consumidor. En el primer cas, en defecte de pacte, el lloc del contracte serà l'establert pel prestador dels serveis.

Mentre que si una de les parts és un consumidor, el contracte s'entén perfeccionat al lloc en el consumidor tingui la seva residència habitual.

Per finalitzar, i un cop realitzat l'anàlisi de la rellevància jurídica dels *smart contracts*, és procedent aportar una definició acadèmicament vàlida que permeti referir-nos específicament a aquells que incorporen un veritable contingut jurídic. En aquest sentit, Tur Faúndez els defineix com "aquells contractes celebrats a través d'una pàgina web accessible per les parts, en què la seva forma està constituïda per una interfície d'usuari i un o diversos programes autoexecutables allotjats a la cadena de blocs, amb capacitat per interactuar recíprocament amb aquesta interfície".

Com ja em esmentat anteriorment, l'*smart contract* serà l'instrument creat per a l'execució automàtica i actuarà com un tercer inexorable que de produir-se el esdeveniment programat podrà (Tur Faúndez, 2018):

- Rebre fons del compte del deutor
- Transferir fons amb o sense interessos
- Retenir fons
- Rebre informació a temps real dels esdeveniments que afectin al contracte
- Iniciar-se, detenir-se, apagar-se, bloquejar-se o autodestruir-se

¹⁴ **art 1262.2 CC i 54 CCom:** Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.

¹⁵ **art 29 LSSICE:** Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual. Los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios.

2.3. Avantatges competitius en l'economia digital: eficiència, reducció de costos de transacció i automatització de processos.

Una vegada examinat tota la naturalesa tècnica i jurídica dels *smart contracts*, la següent pregunta que es pertinent pronunciar-se és perquè hauríem d'implementar aquesta tecnologia al dia a dia actual. Doncs bé, la implementació d'aquesta tecnologia ha ofert veritables beneficis estratègics a empreses i particulars. No només tecnològics si no també econòmics i de seguretat. D'aquestes avantatges hi ha tres particularment beneficioses.

- Eficiència

L'eficiència és un dels pilars fonamentals dels *smart contract*. A diferència dels contractes clàssics o tradicionals, l'automatització de la contractació i de l'execució permet una celeritat sense precedents. Ja que aquesta tecnologia permet que la eficàcia augmenti exponencialment quan els *smart contracts* s'apliquen a un gran volum de supòsits de fet similars. Aquesta immediatesa es tradueix en una eliminació de la càrrega administrativa. (Legerén-Molina 2018).

- Reducció de costos de transacció

Si per alguna cosa s'ha caracteritzat aquesta revolució tecnològica és per premiar la desintermediació. El fet que el codi sigui capaç d'autoexecutar-se elimina la dependència de tercers per verificar el compliment (Fetsyak, 2020). Aquest estalvi no es limita només a l'execució, sinó que abasta tot el cicle de vida contractual, des de la negociació fins a la perfecció. Cosa que òbviament permet abaratir molt tots els processos legals fins ara lligats a la contractació.

- Automatització de processos

Com ja hem vist, l'automatització permet que les relacions contractuals funcionin de manera autònoma basant-se en dades objectives. Ara, és un ordinador el que s'encarrega de llegir i reconèixer un supòsit de fet al qual li ha de programar una conseqüència jurídica d'automàtic compliment (Ballabriga Solanas, 2019).

3. Regulació dels contractes intel·ligents i dret comparat

3.1. La doctrina del *Code is Law*: la immutabilitat enfront de la flexibilitat jurídica.

L'expressió «*code is law*» fa referència a la tesi segons la qual el codi informàtic (és a dir, el conjunt d'instruccions tècniques que configuren el funcionament de les plataformes digitals i centrats en el cas d'estudi d'aquest treball; els *smart contracts*) exerceix una funció reguladora equiparable, i sovint superior, a la del dret positiu. La tesi que defensa aquest pensament sosté que a través del disseny tecnològic es determinen conductes possibles, es limiten opcions i s'imposen restriccions de manera automàtica, sense necessitat d'intervenció judicial ni administrativa. Aquest concepte té el seu origen al 1999 de la mà del jurista nord-americà Lawrence Lessig¹⁶.

Tanmateix, avui dia el concepte ha evolucionat cap a una realitat més palpable. On fins i tot, es defensa que el codi no només té efecte de llei, sinó que la pròpia llei es pot definir com a codi (De Filippi & Hassan, 2018). Això és un canvi de paradigma total que implica que les interaccions contractuals ja no depenen d'un sistema legal *ex-post* que intervé quan hi ha un incompliment, sinó d'un sistema *ex-ante* que fa impossible o extremadament costós el trencament del pactat.

Per a entendre millor aquestes implicacions alguns autors opten per esmentar el que metafòricament anomenen el “*Lex ex machina*” (Argelich Comelles, 2020). A diferència dels contractes electrònics tradicionals, que simplement informatitzen la formació de l'acord, els *smart contracts* automatitzen la fase d'execució, substituint la confiança en la contrapart i en la seva solvència per la confiança en un algoritme (Argelich Comelles, 2020). Aquesta substitució té conseqüències profundes per a la seguretat jurídica, ja que la immutabilitat del registre distribuït garanteix que les prestacions s'executin exactament tal com van ser programades, independentment de qualsevol canvi en les circumstàncies externes¹⁷.

No obstant això, aquesta immutabilitat entra en conflicte directe amb la necessària tasca interpretativa del Dret. El llenguatge jurídic és inherentment flexible i ambigu, dissenyat per permetre una aplicació equitativa en funció del context i dels fets de cada cas concret. En canvi, el codi informàtic és rígid i formalitzat, basat en una lògica booleana que no admet matisos. Com s'apunta en la literatura experta, és extremadament difícil transposar l'ambigüitat i la flexibilitat de les regles legals a un llenguatge que pugui ser interpretat per una màquina (De Filippi & Hassan, 2018).

¹⁶ Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books. És en aquesta obra on Lawrence Lessig introdueix per primera vegada el concepte “*code is law*”, defensant que l'arquitectura del codi informàtic regula el comportament tant com les lleis tradicionals.

¹⁷ L'exemple més pragmàtic per a entendre aquesta realitat es la d'una màquina expendedora. En definitiva, un *smart contract* funciona com una màquina expendedora digital: si l'usuari introdueix l'import exacte, el sistema lliura automàticament el producte, sense possibilitat de discrecionalitat ni d'incompliment. A diferència d'un contracte tradicional, no cal reclamar ni executar judicialment l'acord, perquè el codi mateix impedeix que el resultat sigui un altre que el prèviament programat.

Evidentment, aquesta anàlisi també ha de donar cabuda a la crítica. I és que els atributs que fan atractius els *smart contracts* poden esdevenir, alhora, una arma de doble tall, generadora de riscos significatius. En aquest sentit, nocions jurídiques fonamentals com la bona fe, la diligència deguda o la protecció dels drets dels consumidors difícilment poden ser encapsulades en una línia de codi (Argelich Comelles, 2020). Quan un contracte intel·ligent s'executa de manera automàtica i inflexible, sense atendre aquests estàndards de conducta, pot produir-se una asimetria negociadora que el propi sistema és incapaç de corregir.

Així, l'execució acrítica del codi pot desembocar en el que la doctrina ha qualificat com a *shadow contracting* o “contractació a l'ombra”: una pràctica que opera al marge dels mecanismes tradicionals de supervisió reguladora i que pot exposar els usuaris a situacions d'abús o indefensió (Argelich Comelles, 2020).

En síntesi, i tal com assenyala el mateix autor, prescindir completament de la intervenció humana pot constituir una utopia perillosa. Fins i tot en entorns altament robotitzats, la realitat contractual és tan rica i canviant que la programació difícilment pot anticipar totes les eventualitats (Argelich Comelles, 2020).

Ens trobem, doncs, davant d'un repte regulador sense precedents: estem realment immersos en una llacuna jurídica perillosa? Quines respostes està preparant el legislador per fer front a aquesta nova forma de contractació? Aquestes qüestions s'analitzen a continuació.

3.2. Vulnerabilitats i buits legals: la manca de mecanismes de resolució de conflictes en entorns descentralitzats.

No podem ignorar, que un dels principals atractius dels *smart contracts* rau en la seva capacitat per funcionar en entorns de no confiança. La qual cosa dins del argot cripto vol dir que les parts poden ser completament anònimes i no existir cap context social o legal compartit i tot i així, acudir a aquest tipus d'obligació (Eenmaa-Dimitrieva & Schmidt-Kessen, 2017). En aquests casos, la tecnologia mateixa actua com a mecanisme de governança, assegurant la cooperació a través de la impossibilitat tècnica de l'incompliment. No obstant això, aquesta mateixa descentralització genera buits legals significatius quan el codi falla o quan es produeixen situacions imprevistes.

A la manca de regulació i li hem de sumar una altra vulnerabilitat addicional: la tècnica. Els errors de programació (bugs) poden portar a l'execució de transferències no desitjades o al bloqueig perpetu de fons. Aquí el cas més paradigmàtic es l'atac a “The DAO” l'any 2016. Un atacant va aprofitar una vulnerabilitat en el codi per desviar milions de dòlars en Ether (l'actiu de la xarxa Ethereum). En aquell moment, la comunitat es va trobar davant d'un dilema moral i jurídic: si el codi és la llei, l'acció de l'atacant era legítima perquè el codi la permetia (Eenmaa-Dimitrieva & Schmidt-Kessen, 2017)¹⁸.

¹⁸ Aquest resulta un cas especialment interessant. Per a enriquir els coneixements d'aquest fet recomano la visualització d'aquest vídeo: CoinGecko. (2025, 11 d'abril). *Did Ethereum sell out? The controversial DAO hack explained* [Vídeo]. YouTube. https://www.youtube.com/watch?v=ae7ux_sM5OY

Ara, tot el entorn d'*Ethereum* es trobava en entredit. Ja que havien de resoldre una dicotomia molt complexa: alterar la *blockchain* i perdre el seu atribut essencial d'immutabilitat o permetre el *hackeig*. La decisió final (sotmesa a votació dels usuaris afectats) va ser realitzar una alteració de la cadena de blocs per revertir l'atac. Aquest fet va demostrar que la immutabilitat és, en realitat, relativa i que el sistema necessita mecanismes humans per corregir els resultats inadequats (Argelich Comelles, 2020).

La manca d'arbitratge judicial en aquests sistemes és una conseqüència directa de la seva naturalesa autoelegible. Com que les regles tècniques estan altament formalitzades i no deixen marge per a l'ambigüitat, s'elimina aparentment la necessitat d'arbitratge judicial (De Filippi & Hassan, 2018).

Adicionalment, la descentralització extrema dificulta la identificació dels responsables quan les coses van malament. En una plataforma pública on els nodes no estan identificats i la governança és difusa, es fa gairebé impossible exercir accions legals de responsabilitat civil (Argelich Comelles, 2020). Aquesta "anarquia contractual" deixa els usuaris més vulnerables sense una xarxa de seguretat jurídica efectiva.

Per fer front a aquestes vulnerabilitats, s'han proposat mecanismes de salvaguarda que busquen introduir certa flexibilitat en l'execució automatitzada:

1. **Sistemes de Multifirma (Multisig):** Requereixen la signatura de diverses parts, incloent-hi possiblement un àrbitre extern, abans que el contracte s'executi totalment (Eenmaa-Dimitrieva & Schmidt-Kessen, 2017)
2. **Oracles:** Entitats independents que certifiquen fets del món real perquè el contracte intel·ligent pugui actuar en conseqüència, actuant com a jutges de fets (Eenmaa-Dimitrieva & Schmidt-Kessen, 2017)
3. **Responsabilitat Objectiva:** S'apunta a la necessitat que les plataformes que predisposen contractes d'adhesió intel·ligents assumeixin una responsabilitat objectiva pels errors de programació (Argelich Comelles, 2020)

3.3. Panoràmica del dret comparat: on, des de quan i com es regulen

L'evolució del dret contractual afronta actualment un dels reptes més significatius de la seva història recent: el pas d'una voluntat expressada mitjançant llenguatge natural a una execució automatitzada basada en codi informàtic. Els *smart contracts* han deixat de ser una simple innovació tecnològica per convertir-se en una realitat amb conseqüències jurídiques de gran abast. La seva progressiva implantació obliga a replantejar categories clàssiques del dret de contractes, com ara la formació del consentiment, els mecanismes d'execució o el règim de responsabilitat derivat del seu incompliment.

La regulació dels contractes intel·ligents en l'àmbit internacional presenta, a dia d'avui, un panorama clarament heterogeni. Mentre que nombrosos estats han adoptat una actitud prudent, i han optat per romandre a l'espera dels avanços tecnològics, d'altres han optat per una intervenció normativa decidida. Aquests últims han estat pioners en la incorporació dels *smart contracts* als seus ordenaments jurídics amb l'objectiu d'afavorir la innovació tecnològica, atraure inversió i dotar d'un major grau de seguretat jurídica les transaccions basades en tecnologia *blockchain*. Aquí hi han alguns exemples:

- Estats Units

Als Estats Units, la regulació dels contractes intel·ligents s'ha desenvolupat principalment en l'àmbit estatal. En aquest context, el pioner ha sigut l'estat d'Arizona va ser el primer a adoptar una iniciativa normativa rellevant amb l'aprovació, el març de 2017, de la *House Bill 2417*. Aquesta llei va introduir modificacions als *Arizona Revised Statutes* amb la finalitat d'incorporar definicions específiques tant de la tecnologia *blockchain* com dels contractes intel·ligents. D'acord amb aquesta normativa, un contracte intel·ligent es defineix com un programa impulsat per esdeveniments, amb capacitat d'autoexecució, que opera mitjançant un llibre major distribuït, descentralitzat, compartit i replicat (Ballabriga Solanas, 2019).

La rellevància jurídica d'aquesta regulació recau, principalment, en el fet que prohibeix expressament negar l'eficàcia legal d'un contracte pel sol motiu d'incorporar termes executats mitjançant un *smart contract*. Així mateix, Arizona va establir un precedent significatiu en reconèixer que les signatures registrades a la *blockchain* tenen la consideració de signatures electròniques vàlides i que els registres emmagatzemats en aquests sistemes poden tenir valor probatori davant dels tribunals.

També destaca en la legislació mercantil estatunidenca, les esmenes a la Llei de Societats de Delaware signades el passat 2017. Des d'aquell moment, es permet la comptabilització, registre i transmissió de participacions socials a través de *blockchain*¹⁹.

És rellevant mencionar que altres estats s'han sumat a la legislació de la mateixa manera que ho va fer Arizona. Son els casos de Connecticut (Raised Bill nº 7310, 2019) Nebraska (Legislature Bill nº 695, 2018) i Illinois (House Bill nº 3575, 2019).

¹⁹ 149th General Assembly. (2017). *An Act To Amend Title 8 Of The Delaware Code Relating To The General Corporation Law*. LegiScan. Recuperat de <https://legiscan.com/DE/bill/SB69>

- França

Per la seva part, França ha optat per una aproximació més sectorial a la regulació de la tecnologia *blockchain*, centrant-se principalment en la seva aplicació dins del mercat de valors. Ja a l'abril de 2016, l'Ordenança núm. 2016-520 va autoritzar l'ús de la tecnologia de registre distribuït per a la subscripció i transmissió dels anomenats *bons de caisse*, permetent que aquestes operacions es duguessin a terme mitjançant *blockchain* (Ballabriga Solanas, 2019).

Aquest procés regulador va culminar amb l'Ordenança núm. 2017-1674, de desembre de 2017, que va ampliar aquest marc normatiu en permetre l'ús de dispositius de registre electrònic compartit (*dispositifs d'enregistrement électronique partagé*, DEEP) per a la transmissió de valors financers no admesos a cotització. D'aquesta manera, França es va convertir en el primer estat europeu a abordar de manera expressa la regulació de la tecnologia de la cadena de blocs i a dotar-la d'una definició legal pròpia (Ballabriga Solanas, 2019).

La rellevància d'aquesta regulació rau en el fet que reconeix a la inscripció efectuada mitjançant *blockchain* el mateix caràcter oposable davant de tercers que el que tradicionalment té la inscripció en registres convencionals, atribuint-li així funcions pròpies d'un títol de propietat.

- Rússia

La Federació de Rússia va dur a terme una reforma significativa del seu Codi Civil a l'octubre de 2019. L'article 309 es va modificar per permetre que les obligacions contractuals es compleixin mitjançant l'ús de tecnologies de la informació. Així, els acords poden establir que les obligacions s'executin automàticament en determinades circumstàncies, sense que sigui necessària una declaració de voluntat addicional per part de les parts en el moment de l'execució (Fetsyac, 2020) .

Aquesta innovació és especialment rellevant perquè reconeix legalment el que la doctrina russa denomina "transacció autoexecutable" (*self-executable deal*), en la qual el consentiment es presta de manera anticipada en el moment de la programació del contracte, i la seva execució posterior queda a càrrec d'un algorisme.

3.4. El marc regulador espanyol i europeu

A Espanya, a diferència dels exemples esmentats, no hi ha (de moment) una regulació que defineixi específicament els contractes intel·ligents. Tanmateix, això no vol dir que estiguin en un “buit legal”. La doctrina civilista espanyola ha defensat amb fermesa que la llibertat de forma consagrada en el nostre Codi Civil permet que, si reuneixen els requisits generals dels contractes, els *smart contracts* puguin considerar-se acords electrònics legalment vinculants (Ballabriga Solanas, 2019).

En aquest sentit, i recuperant l'anàlisi jurídic previ que s'ha exposat en aquest treball, els contractes intel·ligents a Espanya es regeixen per la Llei 34/2002 de serveis de la societat de la informació i de comerç electrònic (LSSICE). L'article 23 d'aquesta llei afirma que els contractes celebrats per via electrònica produeixen tots els efectes previstos per l'ordenament jurídic quan concorren el consentiment i els altres requisits per a la seva vàlidesa (Fetsyak, 2020). Per tant, un contracte intel·ligent a Espanya és plenament vàlid si hi ha oferta i acceptació, objecte i causa, seguint els requeriments de l'article 1261 del Codi Civil.

Però tot això està canviant a passos accelerats en els darrers anys. L'any 2024 ha estat decisiu per a la regulació europea d'aquests contractes. Parlem fonamentalment de dos reglaments europeus: reglament MiCA i el reglament Data Act. Sobre aquest darrer centrarem un anàlisi més existiu al següent apartat.

El Reglament MiCA²⁰ (*Markets in Crypto-Assets*), plenament aplicable des del desembre de 2024, estableix un marc normatiu harmonitzat a la Unió Europea per a l'emissió de criptoactius i per a l'activitat dels proveïdors de serveis relacionats amb aquests actius. Tot i que el seu objecte principal no són els contractes intel·ligents com a tals, el reglament incideix de manera indirecta en aquests mecanismes, atès que molts criptoactius es creen, gestionen i transfereixen mitjançant *smart contracts*. En aquest sentit, MiCA reforça exigències de transparència, governança i protecció de l'usuari que, en la pràctica, condicionen el disseny i el funcionament dels contractes intel·ligents que sustenten aquests actius.

D'altra banda, l'EU Data Act (Reglament (UE) 2023/2854), aplicable majoritàriament a partir de setembre de 2025, té una incidència molt més directa sobre els contractes intel·ligents utilitzats en entorns d'intercanvi de dades. Aquesta norma introdueix requisits específics per als *smart contracts* que donen suport a l'accés i la compartició de dades, especialment en contextos B2B i B2G. Entre altres obligacions, exigeix que aquests contractes incorporin mecanismes que permetin la seva interrupció o desactivació, així com garanties de seguretat, control i interoperabilitat. Amb això, el legislador europeu reconeix implícitament el paper jurídic dels contractes intel·ligents, però alhora limita la seva rigidesa tècnica per assegurar-ne la conformitat amb els principis generals del dret i la protecció dels interessos de les parts.

²⁰ Es tracta del reglament (UE) 2023/1114 del parlament europeu i que va entrar plenament en vigor el passat 30 de desembre del 2024

4. Marc normatiu i anàlisi jurídica del Reglament (UE) 2023/2854 (Data Act): Fonaments de l'accés just, interoperabilitat i el règim dels contractes intel·ligents

4.1. Marc normatiu del Reglament (UE) 2023/2854 (Data Act)

Com ja s'ha assenyalat, l'evolució de l'economia digital a la Unió Europea ha assolit una fita rellevant amb l'aprovació del Reglament (UE) 2023/2854 del Parlament Europeu i del Consell, de 13 de desembre de 2023, conegut com a Llei de Dades o *Data Act*. Tanmateix, aquesta norma no neix de manera aïllada ni espontània, sinó que constitueix la resposta lògica a anys de desenvolupament progressiu d'un ecosistema jurídic europeu orientat a la regulació digital²¹, emmarcat dins d'una estratègia clarament definida per la Comissió Europea a l'any 2020²².

L'objectiu d'aquest marc normatiu és posicionar Europa a l'avantguarda mundial en l'ús i la governança de les dades generades tant per empreses com per particulars en l'ús de productes i serveis digitals, especialment en un context marcat per l'expansió de tecnologies com la intel·ligència artificial, la *blockchain* i l'Internet de les Coses (IoT) (Lozano Hernández, 2024).

La Comissió Europea materialitza així l'objectiu de crear un mercat únic de dades que garanteixi la competitivitat global i la sobirania de les dades a Europa. Aquesta estratègia legislativa europea va acompanyada, alhora, d'una inversió de 2.000 milions d'euros en un projecte europeu d'alt impacte destinat a desenvolupar infraestructures de tractament de dades, eines d'intercanvi de dades, arquitectures i mecanismes de governança que afavoreixin un intercanvi de dades pròsper, així com a federar infraestructures al núvol eficients energèticament, fiables i amb els serveis associats.

Entre els principals beneficis que la Unió Europea pretén assolir amb aquesta estratègia destaquen la creació de nous productes i serveis, la reducció dels costos dels serveis públics i la millora de la sostenibilitat i de l'eficiència energètica (Comissió Europea, 2020).

²¹ Que inclou, per exemple, algunes normes ja aprovades, com el paquet de normes sobre serveis digitals, destinat a garantir-ne el caràcter obert i a reduir les conductes deslleials, i format pel Reglament de Serveis Digitals (Reglament (UE) núm. 2022/2065 del Parlament Europeu i del Consell, de 19 d'octubre de 2022, relatiu a un mercat únic de serveis digitals i pel qual es modifica la Directiva 2000/31/CE, DOUE, L277, de 27 d'octubre de 2022) i pel Reglament de Mercats Digitals (Reglament (UE) núm. 2022/1925 del Parlament Europeu i del Consell, de 14 de setembre de 2022, sobre mercats disputables i equitatius en el sector digital i pel qual es modifiquen les Directives (UE) 2019/1937 i (UE) 2020/1828, DOUE, L265, de 12 d'octubre de 2022).

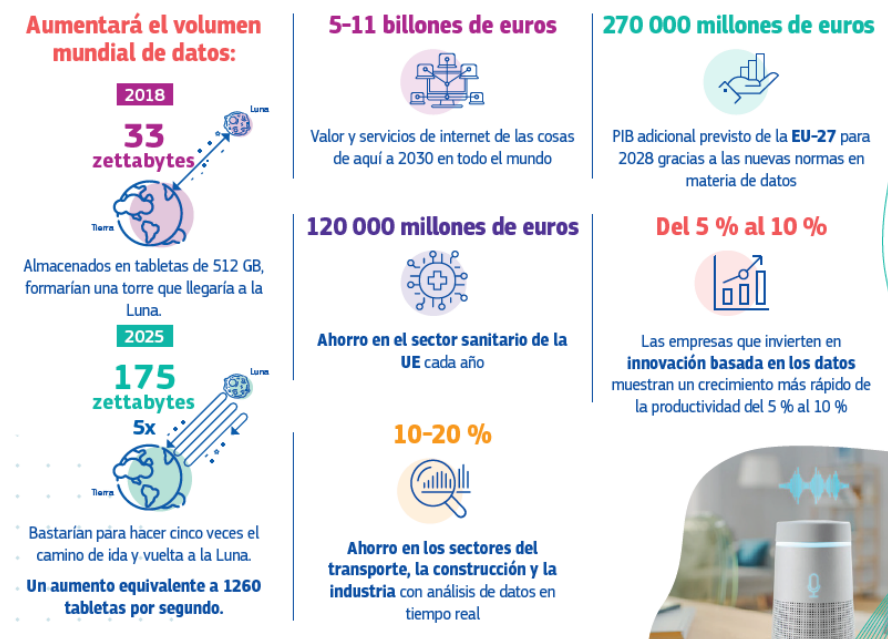
²² Per a més concreció en el marc normatiu i estratègic europeu consultin: <https://digital-strategy.ec.europa.eu/es/policies/strategy-data>

Amb tot aquest marc cronològic i estratègic en ment, s'ha de senyalar que el Reglament (UE) 2023/2854 (*Data Act*) constitueix el segon gran pilar de l'Estratègia Europea de Dades. Ja que anteriorment, es va impulsar l'aprovació de la Llei de Governança de Dades (DGA)²³. Mentre que la DGA es va centrar a crear els marcs institucionals, la *Data Act* intervé directament en la regulació de les obligacions materials, abordant el problema dels fabricants que exerceixen un control exclusiu de control sobre les dades (Kerber, 2023).

A aquestes alçades de l'anàlisi, sorgeix la següent pregunta: és realment necessària la regularització? Perquè hauria de ser tan important crear el mercat únic de dades? Doncs aquí tenim un recull de dades proporcionades pel *factsheet* de la Comissió Europea:

Potencial de crecimiento de la economía de los datos

Los datos constituyen la base de muchos **nuevos productos y servicios digitales**. El uso de objetos conectados (internet de las cosas) **genera cada vez más datos**.



Imatge 2 - La economia de dades (estimacions i dades de la UE). Font: Comissió Europea (2022)

Tal i com veiem a la infografia, l'economia de les dades presenta un enorme potencial de creixement econòmic, innovació i eficiència, amb un increment exponencial del volum mundial de dades i un impacte directe en sectors clau com la salut, el transport, la indústria i els serveis digitals. Aquest creixement es tradueix en nous productes i serveis, importants estalvis de costos i un augment significatiu de la productivitat empresarial, així com en un PIB addicional rellevant per a la Unió Europea.

²³ Reglament (UE) núm. 2022/868 del Parlament Europeu i del Consell, de 30 de maig de 2022, relatiu a la governança europea de les dades i pel qual es modifica el Reglament (UE) 2018/1724, DOUE, L152, de 3 de juny de 2022.

Davant d'aquest escenari, la UE legisla en matèria de dades per garantir un accés just i segur, fomentar la competència i la innovació, evitar pràctiques deslleials i assegurar la sobirania digital europea, tot establint un marc jurídic que permeti aprofitar aquest valor econòmic de manera sostenible, eficient i alineada amb l'interès públic.

L'anàlisi següent detalla la naturalesa normativa d'aquest Reglament, els pilars doctrinals que el sustenten i la regulació específica de les eines d'automatització contractual en l'entorn de les dades industrials i de consum.

4.2. Fonaments i principis inspiradors del Reglament de Dades: l'accés just i la interoperabilitat.

La iniciativa legislativa va correspondre formalment a la Comissió Europea, qui va presentar la proposta el 23 de febrer de 2022 sota la referència COM(2022)0068 (Comissió Europea, 2022).

Dins del Parlament Europeu, la Comissió d'Indústria, Investigació i Energia (ITRE) i el propi Parlament van designar al març de 2022 l'eurodiputada espanyola Pilar del Castillo Vera, del Grup del Partit Popular Europeu (PPE), com a ponent principal de la llei (Car, 2024). Posteriorment, el 14 de març de 2023, el Parlament Europeu va votar per primera vegada la proposta legislativa en sessió plenària, amb un suport majoritari: 500 vots a favor, 23 en contra i 110 abstencions.



Imatge 3 - Votació del Parlament Europeu sobre l'aprovació del Reglament (UE) 2023/2854 (Data Act). Sessió plenària del 14 de març de 2023. Font: Ganvam. (2023)

La llei neix des de la premissa de que la gran majoria de les dades generades per màquines i humans no s'utilitzen²⁴ o estan monopolitzades per unes poques empreses. De la qual cosa, suposa un fre a la innovació (Comissió Europea, 2022).

²⁴ Segons la defensa de la Sra Del Castillo Vera durant el debat plenari, s'estima que un 80%.

És precisament d'aquesta premissa que la UE centra els seus esforços legislatius en aconseguir un accés just de les dades. El Data Act busca corregir els desequilibris del mercat, especialment en el sector del IoT²⁵. Segons el preàmbul de la llei, aquest dret d'accés ha de ser la norma per defecte, permetent que els usuaris (ja siguin consumidors o empreses) tinguin el control real sobre les dades que "co-generen" en utilitzar un producte connectat (Reglament EU 2023/2854, 2023).

Tal i com hem vist anteriorment, la UE ha entès molt bé que les dades són un recurs valuós al qual i que fins ara està en mans de unes poques grans companyies. Tal com exposa la Comissió Europea, aquesta normativa pretén garantir que les dades generades per dispositius connectats puguin ser utilitzades de manera més oberta, equitativa i eficient. Un dels seus objectius principals és dotar de major força a usuaris i empreses, permetent-los accedir i compartir les dades que generen els dispositius que utilitzen. Això trenca dinàmiques de dependència amb fabricants o proveïdors dominants i fomenta la innovació, la competència i l'aparició de nous serveis digitals.

La norma també introdueix mecanismes per evitar clàusules contractuals abusives, especialment en relacions entre grans empreses i PIMES, reforçant així l'equilibri. Un altre aspecte rellevant és la possibilitat que, en situacions excepcionals d'interès públic, les administracions puguin sol·licitar dades al sector privat per gestionar emergències o crisis. D'aquesta manera, la llei combina competitivitat econòmica amb responsabilitat pública (Comissió Europea, 2025).

La votació definitiva i aprovació del Reglament va arribar el 9 de novembre de 2023 amb un resultat de 481 vots a favor, 31 en contra i 71 abstencions (Parlament Europeu, 2023). I va entrar en vigor el 11 de gener del 2024. La major part dels drets i obligacions previstos al Reglament de dades seran aplicables a partir del 12 de setembre de 2025, és a dir, 20 mesos després de la seva entrada en vigor. Tanmateix, algunes disposicions compten amb períodes transitoris més amplis: les relatives al disseny i la fabricació de productes s'aplicaran des del 12 de setembre de 2026, mentre que determinades normes sobre clàusules contractuals abusives ho faran a partir del 12 de setembre de 2027 (Bird & Bird, 2025).

²⁵ L'Internet de les Coses (IoT) (*Internet of Things*) és el conjunt de dispositius físics connectats a Internet que incorporen sensors, programari i capacitat de transmissió de dades, la qual cosa els permet recopilar, enviar i rebre informació sense intervenció humana directa. En l'àmbit quotidià, en són exemples els rellotges intel·ligents que monitoritzen l'activitat física, els assistents de veu com *Alexa* o *Google Home*, o els electrodomèstics connectats que poden gestionar-se des del telèfon mòbil.

4.3. Definició legal de contracte intel·ligent segons el Reglament.

El reglament defineix els contractes intel·ligents en el punt 39 de l'article 2 dedicat a definicions. Concretament ho fa amb el següent literal:

Art 2.39 Data Act: *“«contracte intel·ligent»: programa informàtic utilitzat per a l'execució automatitzada d'un acord o de part d'aquest, que utilitza una seqüència de registres electrònics de dades i en garanteix la integritat i l'exactitud de l'ordre cronològic”.*

Tot i que aquesta qüestió s'analitzarà amb més detall en apartats posteriors, resulta imprescindible examinar des d'ara les consideracions inicials del Reglament i l'esperit que informa la norma. Aquestes disposicions preliminars són determinants per entendre la configuració jurídica dels contractes intel·ligents i la lògica reguladora adoptada pel legislador europeu.

Si acudim al punt 104 de les consideracions inicials, ja veiem com el reglament imposa requisits essencials als contractes intel·ligents utilitzats per professionals en acords d'intercanvi de dades per garantir-ne la interoperabilitat i el control. Només obliga aquells que els desenvolupen per a tercers, no els usos interns, i adopta un enfocament tecnològicament neutre. Exigeix que puguin interrompre's o resoldre's amb base en el consentiment de les parts i aclareix que la seva automatització no desplaça el Dret Civil ni la normativa de protecció dels consumidors. A més, els que s'ajustin a normes harmonitzades d'acord amb el Reglament (UE) n° 1025/2012²⁶ gaudiran de presumpció de conformitat.

El punt 105 reforça aquesta arquitectura imposant una avaluació de conformitat i l'emissió d'una declaració UE de conformitat al proveïdor o al professional que els desplegui per a tercers. Aquest control s'integra en el sistema europeu d'acreditació previst al Reglament (CE) n° 765/2008 i a la Decisió n° 768/2008/CE, dotant aquests instruments tecnològics d'una disciplina jurídica clara.

El punt 106 amplia la mirada i aposta per un ecosistema europeu de dades cohesionat, animant els participants dels espais comuns europeus de dades a promoure eines interoperables d'intercanvi, inclosos els contractes intel·ligents, com a peça clau per a un mercat digital plenament integrat.

Pel que fa a l'àmbit subjectiu, el Reglament és clar, d'acord amb el seu article 1.3.g), la regulació afecta els participants en espais de dades, els proveïdors d'aplicacions que utilitzin contractes intel·ligents i totes aquelles persones físiques o jurídiques l'activitat comercial, empresarial o professional de les quals impliqui el desplegament de contractes intel·ligents per a tercers en el marc de l'execució d'un acord.

²⁶ El Reglament (UE) núm. 1025/2012 del Parlament Europeu i del Consell, de 25 d'octubre de 2012, regula la normalització europea, establint el marc jurídic per a l'elaboració de normes europees per part dels organismes de normalització i la seva relació amb les polítiques de la Unió. És vigent des de l'1 de gener de 2013.

4.4. L'Article 36.1 Data Act: Requisits essencials d'interoperabilitat i seguretat.

Mecanisme d'interrupció i terminació (*Kill Switch*): anàlisi del requeriment d'aturada segura

Una vegada analitzada la definició legal que el reglament atorga als *smart contracts*, considero essencial centrar ara l'anàlisi en el article 36. Aquest article pertany al Capítol VIII del reglament, dedicat a la interoperabilitat²⁷. Dins d'aquest marc legal, l'article 36 emergeix com una de les disposicions més disruptives, ja que estableix els requisits essencials per als *smart contracts* utilitzats en l'execució d'acords d'intercanvi de dades. Aquest article representa la primacia del dret sobre el codi, desafiant la immutabilitat del *blockchain* per garantir la seguretat jurídica.

L'objectiu del article és garantir que l'automatització no quedi fora del control legal. El reglament desglossa requisits fonamentals que s'han de complir per posar dades a disposició de la societat. El primer requisit exigeix que el contracte intel·ligent es dissenyi per oferir un grau de solidesa molt elevat amb el fi d'evitar errors funcionals i contrarestar intents de manipulació per tercers (Art. 36.1.a). El punt b) de l'Article 36.1 és el més controvertit, ja que exigeix un mecanisme que permeti posar fi a l'execució de transaccions, això es el que en l'argot es coneix com un *kill switch*²⁸ i que xoca frontalment amb la filosofia i l'esperit d'immutabilitat de les xarxes descentralitzades.

Ahora, el parlament europeu obliga a permetre l'arxiu de dades, tenir una continuïtat de les dades i que puguin ser auditables amb la finalitat de que el regulador revisi la seva legalitat (36.1.c). Finalment, l'article també exigeix un control d'accés al contracte i coherència en les condicions contractuals.

En resum, l'article 36.1 estableix quatre requisits essencials que els contractes intel·ligents emprats per a la transmissió de dades han de complir necessàriament: robustesa, possibilitat d'interrupció i terminació segures, arxiu de dades i continuïtat, i, finalment, control d'accessos. I des de un punt de vista estratègic, l'article 36 del Data Act actua com a pont entre les obligacions de compartició de dades que el Reglament imposa als titulars i les garanties que han d'acompanyar qualsevol cessió automatitzada.

Com ja es veu en l'article 5 del Reglament, que consagra el dret de l'usuari a exigir que el titular de les dades les posi a disposició d'un tercer sense cost addicional, i l'article 14, que permet als organismes públics accedir a dades privades en situacions de necessitat excepcional, troben en el règim dels contractes intel·ligents un dels seus principals mecanismes d'execució pràctica. Sense les garanties de l'article 36, ambdues disposicions perdrien bona part de la seva efectivitat real.

Tot i així, les veus més crítiques no veuen necessària la obligatorietat d'afegir el *kill switch* en aquest article. Com per exemple, la opinió de Thibault Schrepel que ha

²⁷ **Art 2. 40) del Reglament Data Act:** «interoperabilitat»: la capacitat de dos o més espais de dades o xarxes de comunicació, sistemes, productes connectats, aplicacions, serveis de tractament de dades o components per intercanviar i utilitzar dades amb la finalitat d'exercir les seves funcions;

²⁸ El «kill switch» (literalment, «interruptor d'emergència» o «interruptor d'aturada») és un mecanisme tècnic incorporat al codi d'un smart contract que permet interrompre, suspendre o finalitzar la seva execució automàtica de manera controlada. La seva funció és evitar l'execució de transaccions no desitjades, corregir errors funcionals o reaccionar davant vulnerabilitats de seguretat.

qüestionat que el precepte, tal com està redactat, inverteixi la lògica que hauria d'informar qualsevol règim d'alterabilitat raonable. En comptes d'instaurar el que l'autor anomena "immutabilitat pràctica" (on la immutabilitat roman com a principi i l'alterabilitat opera com a excepció justificada), el Reglament converteix l'alterabilitat en norma general. A més, Schrepel assenyala una llacuna procedimental que el text no resol: qui tindria legitimitat per a activar el mecanisme d'interrupció? El creador del contracte, les autoritats públiques o els tribunals? La norma guarda silenci sobre una qüestió que és, precisament, la que determina si el mecanisme és jurídicament operable (Schrepel, 2023).

Des de la pràctica professional, el bufet Osborne Clarke ha advertit que en un sistema plenament descentralitzat no hi hauria cap subjecte capaç d'operar el *kill switch*, i que en cadenes de blocs sense permisos complir el requisit podria resultar molt difícil o casi impossible. El Reglament, a més, no distingeix entre tipologies de xarxa ni estableix règims diferenciats segons el grau de descentralització, cosa que imposa la mateixa exigència amb independència de si la infraestructura permet o no permet una intervenció externa real (Osborne Clarke, 2023)²⁹.

4.4.1. Robustesa i control d'accessos: garanties contra la manipulació externa.

Entre els quatre requisits que l'article 36.1 imposa als contractes intel·ligents, a banda del esmentat *kill switch*, dos més poden presentar una especial transcendència des del punt de vista de la integritat i la seguretat jurídica: la robustesa i el control d'accessos. El Reglament exigeix que qualsevol contracte intel·ligent utilitzat en el marc de la compartició de dades tingui la capacitat d'evitar errors funcionals i de resistir la manipulació per part de tercers³⁰. Amb aquesta redacció, el requisit sembla raonable i fins i tot obvi. El problema és que la seva concreció pràctica resulta considerablement més complexa del que la redacció legal suggereix.

La robustesa d'un contracte intel·ligent no es pot reduir a una declaració d'intencions. Les vulnerabilitats associades a la tecnologia *blockchain* sobre la qual aquests instruments s'executen són reals i documentades. L'exemple paradigmàtic és l'atac contra *The DAO* del 2016 (que ja em mencionat breument *at supra* d'aquest treball), que va comprometre aproximadament un terç dels fons gestionats per aquesta organització autònoma descentralitzada i que només va poder ser parcialment resolt a través d'una

²⁹ Addicionalment, es recomana la lectura d'altres detractors a aquest requisit de la llei sobretot dins de la comunitat crypto. Com per exemple, aquest article del 2023 *EU Data Act smart contract 'kill switch' brings uncertainty* (<https://cointelegraph.com/features/eu-data-act-smart-contract-kill-switch-brings-uncertainty>)

O des de una vessant més tècnica que escapa a aquest anàlisis, el paper que Oshani Seneviratne elabora per al *Renssealer Polytechnic Institute Troy, New York, USA* anomenat: *The Feasibility of a Smart Contract "Kill Switch"* <https://arxiv.org/html/2407.10302v1>

³⁰ **Art 36.1.a) del Reglament Data Act:** a) *solidez y control de acceso, para garantizar que el contrato inteligente se haya diseñado de manera que ofrezca unos mecanismos de control de acceso y un grado de solidez muy elevado con el fin de evitar errores funcionales y contrarrestar los intentos de manipulación por terceros;*

polèmica modificació unilateral i controvertida del protocol de la xarxa que va invalidar les transaccions fraudulentes, però que va posar en qüestió la pròpia naturalesa de la immutabilitat que es predica d'aquestes arquitectures.

Un altre element que pot posar en risc la robustesa del *smart contract* és la dependència dels ja anomenats oracles. Si un oracle subministra dades errònies o és manipulats, el contracte intel·ligent executarà la seva lògica basant-se en una premissa falsa, el que trenca tota la seguretat del sistema. Sorprenentment, la *Data Act* no aborda de manera específica la responsabilitat dels proveïdors d'oracles, el que genera un buit preocupant en la cadena de confiança.

D'altra banda, el control d'accessos és vital per protegir no només la dada en si, sinó la governança de tot l'acord. El reglament exigeix mecanismes de control rigorosos tant a nivell de la pròpia aplicació com de l'estructura que la sustenta. Això implica que el contracte intel·ligent ha de ser capaç d'identificar de manera fefaent qui té dret a interactuar amb ell i sota quines condicions. En un entorn d'Internet de les Coses, on les dades poden incloure informació sensible sobre per exemple; rutes de transport, consum d'energia o telemetria industrial, un accés no autoritzat podria tenir conseqüències molt greus tant econòmicament com per a la privacitat.

Els productes i serveis connectats han de ser concebuts des del seu origen tècnic per permetre un accés segur i fàcil per a l'usuari, alhora que tanquen la porta a qualsevol explotació abusiva per part del fabricant o de tercers. No obstant això, aquesta transparència obligada sovint xoca amb la voluntat de les empreses de protegir els seus secrets empresarials. De fet, això ha estat una crítica recurrent ja que autors consideren que la passivitat de la UE estava provocant una desprotecció jurídica del consumidor i dels empresaris mentre a la vegada es desaprofitaven tot el valor de les dades generades (Lozano Hernández, 2024).

El legislador europeu sembla conscient del risc: per aquest motiu, l'article 36.5 habilita la Comissió a sol·licitar a organismes europeus de normalització que elaborin estàndards harmonitzats que satisfacin els requisits essencials del precepte. Tanmateix, la doctrina especialitzada ha qüestionat que la mera enumeració de requisits sense una especificació de com han d'assolir-se sigui suficient per a garantir el resultat perseguit.

La tensió entre el requisit de control d'accessos i la naturalesa pública de la cadena de blocs és, precisament, un dels punts on la proposta legislativa mostra una certa incongruència interna. Els contractes intel·ligents desplegats en xarxes de cadena de blocs públiques no poden garantir per si sols la confidencialitat de la informació que processen, llevat que s'implementin protocols criptogràfics addicionals la fiabilitat dels quals, és limitada i costosa. En el text de l'article 36 no resol aquesta ambigüitat, i la seva absència pot generar incertesa en els operadors que hagin de complir el Reglament.

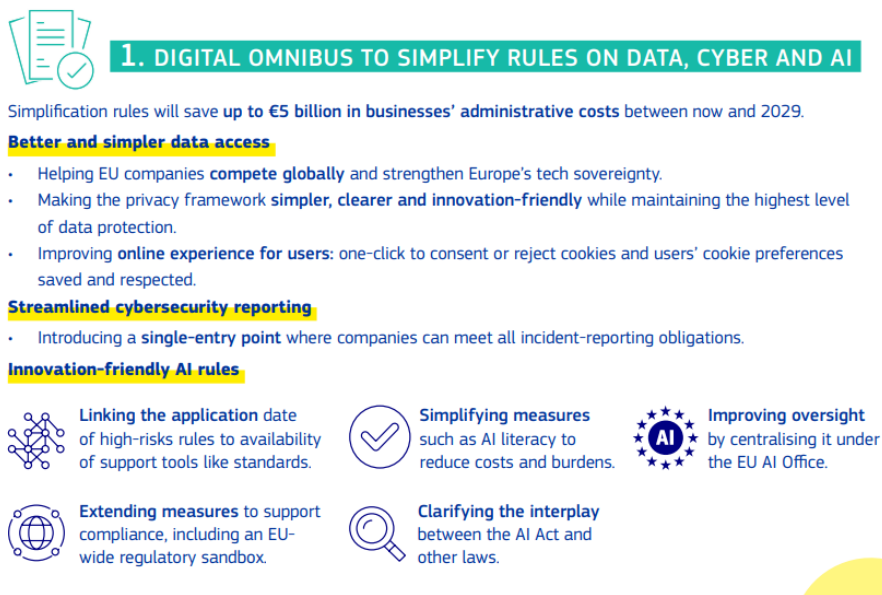
5. La proposta de Reglament Òmnibus Digital i possible supressió de l'article 36 del Data Act.

5.1. Context origen i naturalesa jurídica de la proposta

Aquest treball no pot ignorar els recents canvis legislatius que la UE està preparant, ja que poden canviar el paradigma que em analitzat fins ara. I és que el passat 19 de novembre de 2025, la Comissió Europea va publicar un paquet legislatiu molt ambiciós que pretén reconfigurar i corregir el recent dret digital europeu i entre les propostes hi ha alteracions al Data Act.

Estem parlant *Digital Omnibus Regulation Proposal*, la proposta de Reglament del Parlament Europeu i del Consell per la qual es modifiquen els Reglaments (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 i les Directives 2002/58/CE, (UE) 2022/2555 i (UE) 2022/2557 pel que fa a la simplificació del marc legislatiu digital. Constitueix en el primer intent d'optimitzar el conjunt normatiu acumulat al llarg de la darrera dècada en matèria de dades, ciberseguretat i més recentment intel·ligència artificial i a més, indirectament, els *smart contracts*.

La proposta neix de dos documents clau de l'agenda europea. L'Informe Draghi i l'informe Letta³¹. Tots dos assenyalen la sobrecàrrega regulatòria com un fre per a la competitivitat de l'economia digital europea davant dels Estats Units i Àsia. El seu diagnòstic era clar, la Unió Europea ha construït un marc normatiu molt sòlid, però amb un nivell de complexitat i fragmentació que pot acabar limitant la innovació. Tant es així, que la comissió europea estima que gràcies a aquesta proposta por estalviar més de 5 bilions d'euros en costos administratius a les empreses entre el 2025 i el 2029 (Comissió Europea, 2025).



Imatge 4 - Mesures del Digital Omnibus Regulation Proposal. Font: Comissió Europea. (2025)

³¹ D'una banda, Draghi, M. (2024) *The future of European competitiveness* analitza la pèrdua de competitivitat europea i assenyalava factors com la fragmentació del mercat, la baixa inversió en innovació i la complexitat reguladora. De l'altra, Letta, E. (2024) *Much more than a market* se centra en la necessitat de modernitzar el mercat únic i aprofundir en la integració per adaptar-lo als nous reptes globals.

En el moment de redactar aquest treball, la proposta es troba en la fase inicial del procediment legislatiu ordinari. Publicada per la Comissió el 19 de novembre de 2025, va ser remesa al Parlament Europeu a finals d'aquell mateix mes, que l'ha assignat a les comissions parlamentàries competents per a l'examen en primera lectura.

Segons les previsions, els membres del Parlament Europeu debatran la proposta i presentaran esmenes amb l'objectiu d'assolir un text definitiu a l'estiu de 2026 (Stevens & Bolton, 2026). Tot i que el calendari podria allargar-se en funció de la intensitat política del debat. Cal tenir present, en tot cas, que fins a l'aprovació i aplicabilitat efectiva del text modificatiu, el Data Act en la seva versió vigent continua sent plenament d'aplicació des del 12 de setembre de 2025.

5.1. La possible suspensió de l'article 36 i les seves conseqüències jurídiques

Amb la proposta del *Omnibus* i per tant, la modificació del Data Act, la Comissió Europea pretén simplificar i ordenar el marc normatiu de l'economia de les dades, actualment caracteritzat per una certa dispersió. En aquest sentit, es planteja integrar dins del mateix Data Act normes com el Data Governance Act i la Directiva de Dades Obertes, que quedarien derogades. Així, per exemple, les disposicions relatives als serveis d'intermediació de dades i a l'altruisme de dades (introduïdes pel Data Governance Act) passarien a incorporar-se com un nou capítol específic del Data Act (Garrigues, 2025).

La mesura del *Digital Omnibus* que presenta un interès més directe per al present treball és la proposta de supressió íntegra de l'article 36 del Data Act, relatiu als requisits essencials dels contractes intel·ligents en el context dels acords de compartició de dades. La supressió és total i sense substitució: no es proposa cap règim alternatiu, cap remissió a estàndards futurs de normalització, ni cap marc mínim de garanties per als operadors que facin ús d'aquestes tecnologies. Observem l'argumentació d'aquesta mesura en la consideració 16 de la proposta *Digital Omnibus*:

“Amb la finalitat de mitigar les incerteses jurídiques que podrien desincentivar els models de negoci innovadors, és necessari abordar les importants ambigüitats i càrregues de compliment associades a les disposicions relatives als contractes intel·ligents per a l'execució d'acords d'intercanvi de dades en virtut de l'article 36 del Reglament (UE) 2023/2854.

L'absència de normes harmonitzades i de definicions clares per a conceptes clau com «robustesa», «control d'accés» i «coherència amb les condicions de l'acord», juntament amb el requisit d'«un mecanisme que permeti [...] posar fi a l'operació o interrompre-la», potencialment incompatible amb arquitectures descentralitzades o públiques de cadena de blocs basades en llibres majors immutables, plantejava reptes per als innovadors des d'una perspectiva de costos i oportunitats.

A més, l'ambigüitat entorn de la realització d'una avaluació de conformitat d'acord amb l'article 36, apartat 2, d'aquest Reglament corre el risc d'imposar càrregues desproporcionades. Per tant, l'eliminació de l'article 36 del Reglament (UE) 2023/2854 fomentaria el desenvolupament i la introducció al mercat de nous models de negoci, afavoriria la innovació i reduiria els obstacles per a les tecnologies emergents.” (Comissió Europea, 2025)

Segons el raonament de la Comissió, la supressió pretén eliminar les ambigüitats de compliment i les incompatibilitats amb les arquitectures de cadena de blocs associades a les disposicions sobre contractes intel·ligents. Dit d'una altra manera: el legislador reconeix que la norma que va aprovar no pot ser complerta en la majoria dels supòsits pràctics als quals es pretenia aplicar.

Ara bé, des d'una perspectiva estrictament jurídica, la supressió de l'article 36 del Data Act té com a mínim tres conseqüències que mereixen una anàlisi detinguda. La primera és la desaparició del marc de seguretat mínima per als usuaris de contractes intel·ligents en el context del Data Act. Fins a l'entrada en vigor eventual de l'Òmnibus, l'article 36 constituïa l'única disposició de dret primari europeu que exigia que els contractes intel·ligents emprats per a la transmissió de dades respectessin criteris de robustesa, continuïtat, control d'accessos i possibilitat d'aturada d'emergència. La seva eliminació no substituïda implica que l'ús d'aquests instruments en el mercat interior de dades quedarà, de facto, sense un marc de garanties específic a escala supranacional, revertint als principis generals del dret contractual de cada Estat membre, amb la fragmentació normativa que això comporta.

La segona conseqüència és el que podríem denominar reconeixement tàcit de fracàs regulatori. Resulta revelador que la Comissió no hagi optat per reformular l'article 36 amb una redacció més tècnicament precisa o més adaptada a les diferents arquitectures de cadena de blocs, sinó per eliminar-lo sense residus. Organitzacions com la *European Crypto Initiative* (EUCI), que durant el procés legislatiu van advertir de la incompatibilitat del precepte amb les cadenes de blocs públiques, han valorat la decisió com un reconeixement que el plantejament original era defectuós (European Crypto Initiative, 2025). Dit en altres paraules, el legislador europeu suprimeix una disposició perquè és conscient que no pot ser complerta tal com estava redactada, en lloc d'esforçar-se a millorar-la. Si el problema era la manca d'estàndards harmonitzats, la solució hauria estat accelerar la seva elaboració (cosa per a la qual el propi article 36.5 ja habilitava la Comissió) i no abandonar el terreny regulatori.

La tercera conseqüència, potser la més preocupant des del punt de vista de la coherència del sistema, és la que afecta la posició dels operadors que, des del 12 de setembre de 2025, han invertit esforços i recursos per a adaptar els seus sistemes als requisits de l'article 36. Com han assenyalat els analistes de Kennedy's Law, la consolidació i derogació de disposicions existents genera qüestions de continuïtat legal i certesa jurídica que el Parlament Europeu probablement examinarà en profunditat (Kennedy's Law, 2026). Les empreses que han actuat de bona fe, invertint en l'adaptació als requisits ara eliminats, no obtindran cap reconeixement ni compensació per aquest esforç.

5.3. Implicacions, valoració i conclusió

La proposta del *Digital Omnibus*, i en particular la supressió de l'article 36, planteja una tensió de fons que va més enllà de la qüestió reguladora i que en la meua opinió, afecta a la seguretat jurídica.

L'Omnibus es presenta com una iniciativa que vol aconseguir una implementació clara, senzilla, més rendible i, sobretot, favorable a la innovació de les normes, preservant al mateix temps el nivell de protecció dels drets fonamentals (CMS Law, 2025). Però eliminar sense substitució l'únic precepte que fixava garanties mínimes per als *smart contracts* sembla més una aposta per desregularitzar i alleujar la carrega burocràtica que una simplificació o una mera ordenació jurídica.

El bufet Skadden, en la seva anàlisi de les primeres impressions sobre la proposta, ha subratllat que els canvis suggerits són prou significatius com per a recomanar a les empreses que revisin les propostes, segueixin la seva implementació i avaluin les oportunitats per a simplificar els seus programes de compliment (Skadden, 2025). Aquesta recomanació de prudència és simptomàtica d'una realitat latent, i es que, sembla bastant evident que el legislador europeu no pot seguir el ritme de la innovació i queda quan es proposa legislar ho fa sobre realitats tecnològiques que no comprèn del tot.

En definitiva, la proposta *Omnibus* és, al mateix temps, una resposta necessària a les limitacions del Data Act i un advertiment sobre els riscos de legislar sense la profunditat tècnica suficient. La supressió de l'article 36 no invalida l'anàlisi efectuada en els apartats precedents d'aquest treball. en la meua opinió, al contrari, la confirma i l'enriqueix mentre que alhora ajuda a comprendre les crítiques i limitacions que presenta. Personalment penso que l'exemple més paradigmàtic es com la Comissió Europea va imposar el *kill switch* que era jurídicament coherent però tècnicament inviable en una part significativa dels seus supòsits d'aplicació, i ara es veu obligat a reconèixer-ho per la via de la seva eliminació. Que aquesta eliminació es produeixi menys d'un any després de l'entrada en vigor del Reglament és com a poc, remarcable i força inusual. Però representa un "mal necessari" per a seguir legislant en un entorn d'accelerant innovació tecnològica.

6. Reflexions crítiques i conclusions

Al llarg d'aquest treball he tractat de construir, pas a pas, una anàlisi jurídica dels *smart contracts* que partia de les seves arrels tecnològiques en la criptografia de Haber i Stornetta allà a l'any 1991 i en la conceptualització pionera de Nick Szabo tres anys després. Un anàlisi que he decidit continuar amb l'examen de la primera regulació europea directament adreçada a aquest fenomen: l'article 36 del Reglament (UE) 2023/2854 (Data Act) i la seva eventual supressió a mans de la proposta del *Digital Omnibus*. Correspon ara, en aquest capítol de tancament, donar pas a una reflexió crítica de fons. Una reflexió que, penso necessària centrar en la compatibilitat real entre la lògica reguladora europea i la naturalesa tècnica dels *smart contracts*.

La meva conclusió gira al voltant d'una tensió central que ja s'ha vist present durant tot el treball: la tensió entre la immutabilitat i la descentralització que defineix la *blockchain*, i la necessitat del dret d'intervenir, corregir i garantir un bon ús d'aquesta tecnologia. Com va advertir Argelich Comelles (2020), *"les utopies no solen prosperar quan s'implementen. A un pla teòric, que un contracte funcioni sense dret pot resultar atractiu, perquè redueix temps i costos, però els abusos queden sense tractament legal."* El repte, en definitiva, és trobar el punt d'equilibri. Analitzaré, a continuació, si el legislador europeu l'ha sabut trobar.

6.1. Compatibilitat del Reglament amb la natura descentralitzada de la Blockchain.

En la meva opinió, la incompatibilitat estructural entre la naturalesa de la *blockchain* i les exigències del Data Act no és un problema superficial. Tal com s'ha posat de manifest en l'anàlisi de l'article 36, és una incompatibilitat que afecta el nucli conceptual de la tecnologia regulada. Per comprendre la profunditat del problema, convé recordar que la descentralització no és una característica optativa dels sistemes de registre distribuït, sinó la seva raó de ser principal. La mateixa raó per la qual Haber i Stornetta van concebre el sistema i per la qual Satoshi Nakamoto al 2008 el va materialitzar en una arquitectura operativa. Eliminar la descentralització per satisfer els requisits del Reglament no simplifica el sistema; el converteix en quelcom essencialment diferent.

El primer i més visible punt de fractura és, com ja s'ha examinat, el mecanisme d'interrupció de l'article 36.1.b), el *kill switch*. En essència en un sistema plenament descentralitzat no hi ha cap subjecte capaç d'operar el *kill switch*. Tot i que, paradoxalment, si que tenim un antecedent on va fer-se servir una mena d'interrupció. Parlo del *DAO hack* del 2016, que ja s'ha esmentat en aquest treball, que va demostrar que la intervenció d'emergència sí és possible, però al preu de vulnerar la immutabilitat que el sistema proclamava com a atribut essencial i després d'una votació comunitària que cap reglament havia previst ni regulat. Per tant, ja comptem amb un antecedent assimilable però en un context molt diferent i sobretot descentralitzat, lluny de qualsevol regulació.

Ara bé, la crítica de fons que m'agradaria recalcar és la de la redefinició del concepte de contracte intel·ligent. L'article 2.39 defineix el contracte intel·ligent de manera radicalment restrictiva: un "*programa informàtic utilitzat per a l'execució automatitzada*

d'un acord o de part d'aquest, que utilitza una seqüència de registres electrònics de dades i en garanteix la integritat i l'exactitud de l'ordre cronològic".

Aquesta definició, aparentment tècnica, amagaria una decisió de política legislativa de gran abast: el Reglament delimita el concepte en funció de l'ús en acords d'intercanvi de dades en contextos professionals, i deixa fora del seu àmbit la immensa majoria dels usos reals dels *smart contracts* en l'ecosistema blockchain com poden ser les finances descentralitzades (DeFi) o els tokens no fungibles (NFTs). Això pot generar el risc real de que l'ecosistema tecnològic esquivi intencionadament la definició reglamentària per no quedar subjecte als seus requisits.

En segon lloc, i en relació directa amb la compatibilitat tècnica, cal plantejar amb rigor el problema de l'oracle, que en la meua opinió constitueix el buit normatiu més preocupant del Reglament. Com s'ha exposat en la part tècnica d'aquest treball, els oracles són serveis de tercers que actuen de pont entre el món real i el protocol digital, enviant informació externa i verificable al contracte intel·ligent. Sense oracles, la majoria dels *smart contracts* de qualsevol complexitat mínima no podrien funcionar i aquesta matèria ha estat completament ignorada per la legislació europea.

Una tercera crítica que mereix atenció específica és la de la volatilitat de la criptomoneda com a medi de pagament en els smart contracts. Quan Szabo va concebre l'execució automatitzada d'obligacions contractuals, no podia anticipar que el vehicle d'execució de les prestacions dineràries seria un actiu amb una oscil·lació de valor que pot superar el 30% en un sol dia de mercat. La situació genera un problema jurídic afegit ja que en un contracte com l'exemple del Xavier i en Luis, si el guanyador de l'aposta havia d'obtenir 1 ETH i el valor d'aquest actiu ha caigut un 60% entre el moment de perfecció del contracte i el seu moment d'execució, ¿s'ha complert realment l'obligació? La resposta formal és afirmativa, perquè el codi s'ha executat tal com estava programat; la resposta des del principi d'equivalència de les prestacions és molt menys clara. La solució tècnicament més madura que l'ecosistema ha generat fins avui és la de les *stablecoins*, actius digitals dissenyats per mantenir una paritat fixa amb una moneda de referència, habitualment el dòlar nord-americà o l'euro.

Finalment, no és possible concloure l'anàlisi de la compatibilitat del Reglament amb la naturalesa de la *blockchain* sense referir-se al cost d'elaboració i execució dels smart contracts i al seu impacte mediambiental. El Reglament, augmenta inevitablement la complexitat dels contractes intel·ligents. Un *smart contract* tècnicament sofisticat, amb totes les salvaguardes que l'article 36 exigiria, pot resultar econòmicament inviable per a molts casos d'ús de valor moderat, comproment precisament el benefici d'eficiència i reducció de costos de transacció que s'identificaven com un dels principals atractius d'aquesta tecnologia.

Quant a l'impacte mediambiental, el debat és complex però no pot ser obviat. Els mecanismes de consens de prova de treball que sustenten algunes de les principals cadenes de blocs han estat objecte de crítiques fundades per la seva petjada de carboni. Forçar la implementació de *smart contracts* complexos sobre infraestructures energèticament intenses, per satisfer requisits normatius que el legislador podria no acabar exigint (com ha demostrat la proposta de supressió de l'article 36), genera un cost social i ambiental que hauria de tenir cabuda en qualsevol avaluació d'impacte regulatori.

6.2. La seguretat jurídica com a motor de la innovació tecnològica.

Un dels plantejament transversals d'aquest treball és la seguretat jurídica. Personalment, penso que la regulació no és l'enemic de la innovació tecnològica, sinó un requisit indispensable. Sense un marc normatiu clar, previsible i coherent, els operadors econòmics no poden calcular riscos, dissenyar productes ni invertir amb confiança. En aquest sentit, la intervenció legislativa europea en l'àmbit dels *smart contracts* era no només legítima, sinó necessària. El problema, però, no rau en el fet que la Unió Europea hagi decidit regular, sinó en la manera com ho ha fet.

El Data Act, en la seva configuració original, constitueix un exemple paradigmàtic d'allò que podríem denominar regulació amb bona intenció i fonament tècnic insuficient. L'article 36, en lloc de generar la certesa jurídica que es proclamava com a objectiu, ha acabat produint l'efecte contrari: incertesa, fragmentació interpretativa i una carrega de compliment que molts operadors no han sabut com satisfer. Des de el meu punt de vista, el legislador europeu ha redactat conceptes i legislat sobre un matèria que no acabada de conèixer al complet. Mentre que alhora ha imposat obligacions sense especificar-ne els mecanismes concrets d'implementació. El resultat és una norma que sembla precisa en la seva estructura formal però que resulta en gran mesura inaplicable en els seus supòsits pràctics més habituals.

A més, aquesta situació té un cost que no és només teòric. Les empreses que van adaptar de bona fe els seus sistemes als requisits de l'article 36 entre el setembre de 2025 i la proposta de l'*Omnibus* han invertit recursos en complir una obligació que el propi legislador ha reconegut com a defectuosa. Aquesta volatilitat normativa és, en si mateixa, una forma d'inseguretat jurídica molt greu.

Es per aquest motiu que en relació amb l'objectiu principal del meu treball, no es pot considerar confirmada la hipòtesi que el Reglament (UE) 2023/2854 (Data Act) reforça la seguretat jurídica i ordena adequadament l'ús dels smart contracts. Malgrat la seva finalitat protectora, la seva configuració ha generat incertesa aplicativa, fet que es veu confirmat per la necessitat de revisió reflectida en la proposta del Digital Omnibus. En aquest context, la norma no només no consolida un marc clar, sinó que, al meu entendre, ha contribuït a generar inseguretat jurídica i una certa desconfiança en el regulador.

Tot i que crec adient assenyalar que el repte regulatori és genuïnament difícil. La velocitat de la innovació tecnològica és, per definició, superior a la del cicle legislatiu ordinari, i cap parlament del món pot pretendre anticipar-se a cada nova configuració tècnica amb la precisió d'un enginyer de sistemes. Però precisament per això, el legislador hauria d'actuar tractant aproximar-se als nous fenòmens tecnològics amb el rigor analític que requereixen.

6.3. Balanç final: equilibri entre la protecció de l'usuari i la llibertat tecnològica.

Arribant a aquest últim punt del treball crec adient acabar amb una pregunta clara: s'ha assolit l'equilibri que es buscava? En el cas del Data Act i la seva relació amb els *smart contracts*, la resposta no pot ser altra que parcialment negativa, tot i que matisada. La Unió Europea ha encertat en identificar la necessitat d'intervenir. Ha fallat, en canvi, en la manera d'articular aquesta intervenció.

La protecció de l'usuari és un valor irrenunciable en qualsevol sistema jurídic que es pretengui just. En un entorn de contractació automatitzada, on el codi s'executa sense possibilitat d'intervenció humana posterior i on les parts sovint no disposen dels coneixements tècnics necessaris per comprendre plenament allò a què s'obliguen, la tutela normativa no és un luxe sinó una exigència.

Ara bé, protegir l'usuari no significa paralitzar la tecnologia. Quan una norma imposa obligacions que el mercat no pot complir, no protegeix ningú: desplaça l'activitat cap a jurisdiccions menys regulades i perjudica alhora els consumidors i els empresaris europeus que havien apostat per un entorn de compliment.

El dret digital europeu, en la seva ambiciosa construcció dels últims anys, corre el risc de caure en una paradoxa: voler ser el marc més protector del món i, precisament per excés de rigidesa, acabar sent el marc on menys innovació es produeix. Les dades de competitivitat que van motivar tant l'Informe Draghi com l'Informe Letta, i que han impulsat la proposta del *Digital Omnibus*, apunten exactament en aquesta direcció. Europa no es pot permetre el luxe de regular sense competitivitat, ni de competir sense regulació. Tots dos elements han de ser parts d'un mateix projecte, no forces oposades.

A més, m'agradaria finalitzar aquest treball amb una petita valoració final i perspectiva de futur per als *smart contracts*. Després d'haver estudiat amb certa profunditat aquesta matèria, puc concloure que la solució tecnològica i el marc teòric darrere dels *smart contracts* és simplement brillant i penso que a la llarga, revolucionaria. Es una redefinició del que poden ser les relacions contractuals tal i com a les coneixem i en un futur proper crec que seran una realitat molt comú en el ordenament jurídic personal i empresarial de moltes jurisdiccions.

La conclusió d'aquest treball no és, doncs, que no cal regular els *smart contracts*. És que cal fer-ho millor. Amb una comprensió tècnica més profunda dels fenòmens que es volen ordenar, amb mecanismes de consulta sectorial real i amb la voluntat de construir normes que siguin alhora protectores i operatives. La seguretat jurídica i la innovació tecnològica no s'exclouen: es necessiten. I el dret té aquí una responsabilitat que no pot delegar ni en el codi ni en el mercat.

7. Conclusions

Primera. Els *smarts contracts* no són per si sols contractes. Són seqüències de codi i dades que s'emmagatzemen a una determinada blockchain. No obstant, la majoria d'aquests neixen amb rellevància jurídica assimilable a un contracte electrònic.

Segona. Els *smart contracts* són vàlids a Espanya sense regulació específica si compleixen els requisits de l'art. 1261 CC i 23 LSSICE; la llibertat de forma (art. 1278 CC) impedeix negar l'eficàcia pel seu format en codi.

Tercera. Els *smarts contracts* tenen eficàcia probatòria plena gràcies a la pròpia idiosincràsia de la tecnologia blockchain (immutabilitat i registre de temps i identitat).

Quarta. El Data Act introdueix la primera regulació europea, però amb una definició restrictiva que pot excloure usos clau (DeFi, NFTs) i incentivar l'elusió normativa.

Cinquena. El *kill switch* (art. 36.1.b) és inviable en *blockchains* públiques descentralitzades, imposant obligacions tècnicament impossibles.

Sisena. La proposta *Digital Omnibus* (2025) de suprimir l'art. 36 evidencia el fracàs regulatori i genera inseguretat per a operadors que havien complert de bona fe.

Setena. El Data Act manté llacunes rellevants: oracles, control d'accés en xarxes públiques i volatilitat dels actius digitals.

Vuitena. La seguretat jurídica és condició per a la innovació; una regulació tècnicament deficient genera incertesa, sobrecostos i deslocalització.

8. Bibliografia i fonts documentals

Fonts acadèmiques

Anguiano Jiménez, J. M. (2023). *Smart Contract: ¿Contrato inteligente o programa informático? ¿Qué son –exactamente– los Smart Contracts? ¿Cuál es su naturaleza, filosofía y principios inspiradores?* Actualidad Civil, (6).

Argelich Comelles, J. (2020). *Smart contracts o code is law: Soluciones legales para la robotización contractual*. Atelier.

Ballabriga Solanas, T. (2019). *Régimen jurídico y problemática de los contratos inteligentes*. Revista de Derecho del Mercado de Valores, (25).

Bird & Bird. (2025). *Data Act tracker*. <https://www.twobirds.com/en/trending-topics/eu-data-act/data-act-tracker>

Casolari, F., Buttaboni, C., & Floridi, L. (2023). *The EU Data Act in Context: A legal assessment* [Esborrany de treball]. Department of Legal Studies, University of Bologna; Yale University Digital Ethics Center. <https://ssrn.com/abstract=4584781>

Casolari, F., Taddeo, M., Turillazzi, A., & Floridi, L. (2023). *How to improve smart contracts in the European Union Data Act*. Digital Society, 2(9), 1–6. <https://doi.org/10.1007/s44206-023-00038-2>

CoinGecko. (2025, 11 d'abril). *Did Ethereum sell out? The controversial DAO hack explained* [Vídeo]. YouTube. https://www.youtube.com/watch?v=ae7ux_sM5OY

Comissió Europea. (2025). *Data Act explained*. Shaping Europe's digital future. <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained>

Comissió Europea. (2025). *Digital Package (factsheet)*. <https://ec.europa.eu/commission/presscorner/api/files/attachment/881887/Factsheet%20Digital%20Package.pdf>

De Filippi, P., & Hassan, S. (2018). *Blockchain technology as a regulatory technology: From code is law to law is code*. First Monday, 23(10).

De Pablo Contreras, P. (2016). *Requisits del contracte*. A C. Martínez de Aguirre y Aldaz et al. (Eds.), *Curso de Derecho civil II. Derecho de obligaciones*. Edisofer.

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. J. (2017). *Regulation through code as a safeguard for implementing smart contracts in no-trust environments* (EUI Working Paper LAW 2017/13). European University Institute.

European Crypto Initiative (EUCI). (2025). *EU Data Act Article 36 and smart contracts: why deletion matters*. <https://eu.ci/data-act-article-36-smart-contracts-explained>

Fetsyak, T. (2020). *Contratos inteligentes: análisis jurídico desde el marco legal español*. REDUR. Revista Electrónica de Derecho de la Universidad de La Rioja, (18). <https://doi.org/10.18172/redur.4898>

Garrigues. (2025, 20 de noviembre). *Paquete Ómnibus Digital de la Comisión Europea: la regulación de la economía digital en la UE cambia de rumbo*. https://www.garrigues.com/es_ES/garrigues-digital/paquete-omnibus-digital-comision-europea-regulacion-economia-digital-ue-cambia

Haber, S., & Stornetta, W. S. (1991). *How to time-stamp a digital document*. Journal of Cryptology, 3(2).

Kennedy's Law. (2026, gener 26). *The 2025 European Commission EU Digital Omnibus Package: The Data Act*. <https://www.kennedyslaw.com/en/thought-leadership/article/2026>

Kerber, W. (2023). *Governance of IoT data: Why the EU Data Act will not fulfill its objectives*. GRUR International, 72(2), 120–135. <https://doi.org/10.1093/grurint/ikac107>

Legerén-Molina, A. (2018). *Los contratos inteligentes en España. La disciplina de los smart contracts*. Revista de Derecho Civil, 5(2).

Lozano Hernández, J. (2024). *La Data Act: ¿un nuevo motor económico para Europa?* REDI: Revista Española de Derecho Internacional, 76(2), 281–293. <https://doi.org/10.36151/REDI.76.2.15>

Lotz, C. M. (2018, 11 de setembre). *Smart contract: ¿Contratos verdaderamente inteligentes?* Rödl & Partner.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. <https://bitcoin.org/bitcoin.pdf>

Obregón Siegmund, G. (2012). *La perfección del contrato en Internet según el ordenamiento jurídico español. Especial referencia al caso de las páginas web*. Revista Chilena de Derecho y Ciencia Política, 3(2). <https://dialnet.unirioja.es/descarga/articulo/4095022.pdf>

Parlament Europeu. (2023, 9 de novembre). *Data Act (2022/0047(COD)) – Document summary*. Legislative Observatory (OEIL). <https://oeil.europarl.europa.eu/oeil/en/document-summary?id=1765341>

Prenafeta Rodriguez, J. (2016). *Smart Contracts: aproximación al concepto y problemática legal básica*. Diario la Ley.

Puyol, J. (2016). *¿Qué son los “smart contracts” o contratos digitales?* Confilegal.

Morell Ramos, J. (2016). *Como crear un smart contract con términos y condiciones*. Legaltech.

Skadden, Arps, Slate, Meagher & Flom LLP. (2025, novembre). *Commission proposes significant changes to EU digital rules: first impressions*. <https://www.skadden.com/insights/publications/2025/11>

Tur Faúndez, C. E. (2018). *Smart contracts: Análisis jurídico*. Editorial Reus.

Car, P. (2024, 15 de desembre). *Data Act – A Europe Fit for the Digital Age*. Members' Research Service, Parlament Europeu. <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act>

Llistat normatiu

Arizona House of Representatives. (2017). House Bill 2417: An act amending section 44-7003, Arizona revised statutes; amending Title 44, Chapter 26, Arizona revised statutes, by adding article 5; relating to electronic transactions. <https://legiscan.com/AZ/text/HB2417/2017>

Comissió Europea. (2020). Una estratègia europea de dades (COM(2020) 66 final). <https://eur-lex.europa.eu>

Comissió Europea. (2022). Proposta de Reglament del Parlament Europeu i del Consell sobre normes harmonitzades per a un accés just a les dades i la seva utilització (Reglament Data Act), COM/2022/68 final. EUR-Lex. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0068>

Comissió Europea. (2022). Proposta de Reglament del Parlament Europeu i del Consell sobre normes harmonitzades per a un accés just a les dades i la seva utilització (Reglament Data Act), COM/2022/68 final.

Comissió Europea. (2025). Proposta de Reglament del Parlament Europeu i del Consell pel qual es modifiquen els Reglaments (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 i les Directives 2002/58/CE, (UE) 2022/2555 i (UE) 2022/2557 pel que fa a la simplificació del marc legislatiu digital (Digital Omnibus).

Connecticut General Assembly. (2019). Raised Bill No. 7310: An act authorizing the use of smart contracts. <https://www.cga.ct.gov/2019/TOB/h/pdf/2019HB-07310-R00-HB.PDF>

DE SB69 | 149th General Assembly. (2017). An Act To Amend Title 8 Of The Delaware Code Relating To The General Corporation Law. LegiScan. <https://legiscan.com/DE/bill/SB69/2017>

Govern d'Espanya. (1885). Reial Decret de 22 d'agost de 1885 pel qual es publica el Codi de Comerç.

Govern d'Espanya. (1889). Reial Decret de 24 de juliol de 1889 pel qual es publica el Codi Civil.

Govern d'Espanya. (2002). Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

Govern d'Espanya. (2003). Llei 59/2003, de 19 de desembre, de signatura electrònica.

Govern d'Espanya. (2020). Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

Illinois General Assembly. (2019). House Bill 3575: Blockchain Technology Act (2019–2020).

<http://ilga.gov/legislation/fulltext.asp?DocName=10100HB3575&GA=101&SessionId=108&DocTypeId=HB&LegID=120249&DocNum=3575&GAID=15&Session>
=

Nebraska Legislature. (2018). Legislative Bill 695: Authorize and define smart contracts. <https://legiscan.com/NE/text/LB695/2017>

Parlament Europeu i Consell de la Unió Europea. (2000). Directiva 2000/31/CE del Parlament Europeu i del Consell, de 8 de juny de 2000, relativa a determinats aspectes jurídics dels serveis de la societat de la informació, en particular el comerç electrònic en el mercat interior.

Parlament Europeu i Consell de la Unió Europea. (2002). Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques.

Parlament Europeu i Consell de la Unió Europea. (2008). Decisió núm. 768/2008/CE del Parlament Europeu i del Consell, de 9 de juliol de 2008, sobre un marc comú per a la comercialització dels productes.

Parlament Europeu i Consell de la Unió Europea. (2008). Reglament (CE) núm. 765/2008 del Parlament Europeu i del Consell, de 9 de juliol de 2008, pel qual s'estableixen els requisits d'acreditació i vigilància del mercat relatius a la comercialització dels productes.

Parlament Europeu i Consell de la Unió Europea. (2012). Reglament (UE) núm. 1025/2012 del Parlament Europeu i del Consell, de 25 d'octubre de 2012, sobre la normalització europea.

Parlament Europeu i Consell de la Unió Europea. (2014). Reglament (UE) núm. 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior (eIDAS).

Parlament Europeu i Consell de la Unió Europea. (2016). Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (RGPD).

Parlament Europeu i Consell de la Unió Europea. (2018). Reglament (UE) 2018/1724 del Parlament Europeu i del Consell, de 2 d'octubre de 2018, relatiu a la creació d'una passarel·la digital única d'accés a informació, procediments i serveis d'assistència i resolució de problemes.

Parlament Europeu i Consell de la Unió Europea. (2018). Reglament (UE) 2018/1725 del Parlament Europeu i del Consell, de 23 d'octubre de 2018, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les institucions, òrgans i organismes de la Unió.

Parlament Europeu i Consell de la Unió Europea. (2019). Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, de 23 d'octubre de 2019, relativa a la protecció de les persones que informin sobre infraccions del Dret de la Unió.

Parlament Europeu i Consell de la Unió Europea. (2020). Directiva (UE) 2020/1828 del Parlament Europeu i del Consell, de 25 de novembre de 2020, relativa a les accions de representació per a la protecció dels interessos col·lectius dels consumidors.

Parlament Europeu i Consell de la Unió Europea. (2022). Directiva (UE) 2022/2555 del Parlament Europeu i del Consell, de 14 de desembre de 2022, relativa a les mesures destinades a garantir un nivell elevat comú de ciberseguretat a tota la Unió (NIS2).

Parlament Europeu i Consell de la Unió Europea. (2022). Directiva (UE) 2022/2557 del Parlament Europeu i del Consell, de 14 de desembre de 2022, relativa a la resiliència de les entitats crítiques.

Parlament Europeu i Consell de la Unió Europea. (2022). Reglament (UE) 2022/1925 del Parlament Europeu i del Consell, de 14 de setembre de 2022, sobre mercats disputables i equitatius en el sector digital (Digital Markets Act).

Parlament Europeu i Consell de la Unió Europea. (2022). Reglament (UE) 2022/2065 del Parlament Europeu i del Consell, de 19 d'octubre de 2022, relatiu a un mercat únic de serveis digitals (Digital Services Act).

Parlament Europeu i Consell de la Unió Europea. (2022). Reglament (UE) 2022/868 del Parlament Europeu i del Consell, de 30 de maig de 2022, relatiu a la governança europea de les dades (Data Governance Act).

Parlament Europeu i Consell de la Unió Europea. (2023). Reglament (UE) 2023/1114 del Parlament Europeu i del Consell, de 31 de maig de 2023, relatiu als mercats de criptoactius (MiCA).

Parlament Europeu i Consell de la Unió Europea. (2023). Reglament (UE) 2023/2854 del Parlament Europeu i del Consell, de 13 de desembre de 2023, sobre normes harmonitzades per a un accés just a les dades i la seva utilització (Data Act).

Imatges

Imatge 1- Anstey, S. M. (2023, 7 d'agost). *Distributed ledger technology (incl. blockchain) use cases - digital assets, AI, and beyond*. Kilpatrick Townsend & Stockton LLP. <https://ktslaw.com/en/insights/alert/2023/8/%7BD4E20141-59D9-442A-B277-7E4D26E5FDF7%7D?pdf=1>

Imatge 2 - Comissió Europea. (2022, 14 de febrer). *Data Act — Factsheet*. Shaping Europe's digital future. <https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet>

Imatge 3 - Ganvam. (2023, 15 de març). *Parlament Europeu aprova la futura Data Act*. Ganvam. <https://ganvam.es/el-parlamento-europeo-aprueba-la-futura-data-act-los-fabricantes-tendran-que-compartir-los-datos/>

Imatge 4 - Comissió Europea. (2025, 19 de novembre). *Digital package — Factsheet*. Simpler EU digital rules and new digital wallets to save billions. <https://ec.europa.eu/commission/presscorner/api/files/attachment/881887/Factsheet%20Digital%20Package.pdf>