

Web3 Legal approach

Following the first static version of the World Wide Web, and web 2.0 where users became content creators, some experts anticipate that we are at the dawn of web3, a new version of the web where some of its elements will be owned by developers and users, and managed by tokens. This Briefing includes a multidisciplinary analysis of the impact that web3 will have on companies through phenomena such as cryptocurrencies, NFTs and DAOs.



Web3: Legal Approach

1. Introduction

In the technology sector, every period of major economic expansion has been brought about by the commercialisation of some technology that led to the opening of a new market. In the 1970s and 1980s, mainframe technology, by which computers first entered companies, led to the development of a new hardware and software industry around these systems. In the 1990s, it was home computing and the popularisation of personal computers that led to the opening of new companies offering products and services to consumers. In the first decade of this century, the popularisation of the internet and the World Wide Web led to the birth of a new digital economy, where companies offered services in an environment based on abundance. In the 2010s, it was mobile technology that brought a new economic revolution and, at a time of stabilisation in the sale of mobile devices and services, the industry is eager to find the next technology that will bring the birth of new products and services.

Among these technologies is the metaverse, the virtual, immersive and decentralised universe which, according to most experts, will be a full reality in five to ten years. However, another technology, the blockchain, is already in place. This is enabling the birth of new services, such as cryptocurrencies, DAOs (Decentralised Autonomous Organisations) and NFTs (Non-Fungible Tokens), as

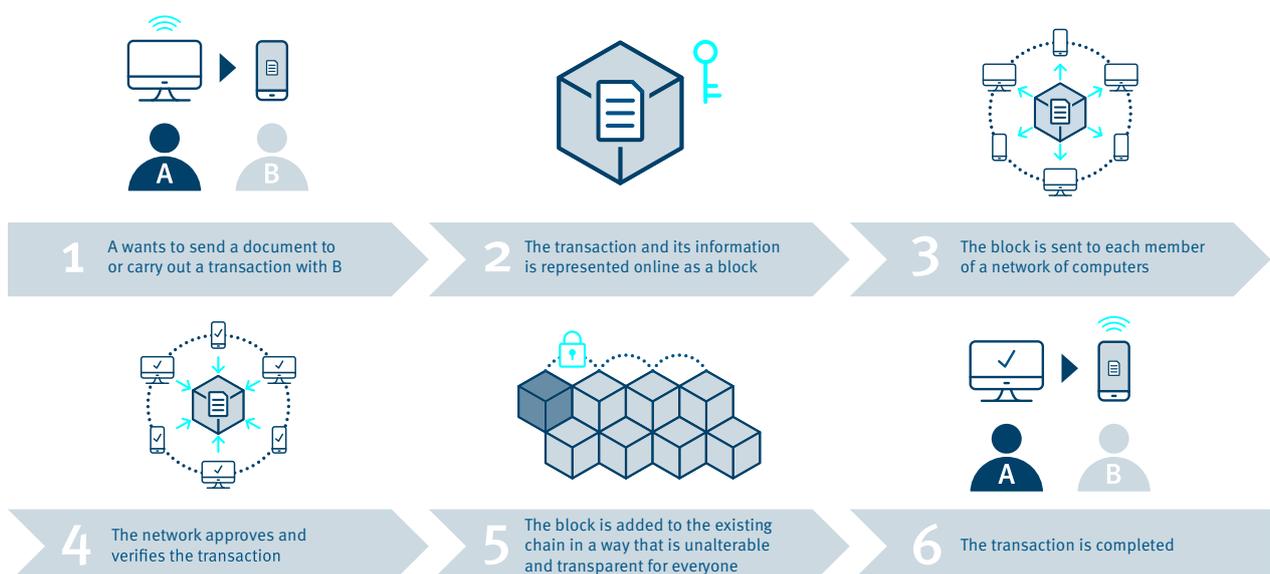
well as the *tokenisation* of a wide range of assets (from communities to real estate). The blockchain is a relatively mature but complex technology, conceptualised in 2008 by a person or group of people operating under the name of Satoshi Nakamoto. It allows the creation of a decentralised data structure with information grouped in blocks and metadata relating to the previous block in order to trace the information securely through cryptographic calculations.

It seemed that blockchain technology would revolutionise, in the very short term, the world of business, finance and decentralised payments. With the benefit of hindsight, we can see that its implementation has not been as widespread as envisaged a decade ago, mainly due to its complexity (and, on occasions, energy consumption), although success stories and projects are gradually emerging in which its use is no longer merely experimental.

With web3, the user will have a certain perception of ownership over data and information

As a result of such business initiatives, in recent years, rather than blockchain, the concept of web3 has been invoked as an evolution of web 1.0 (the static internet, where users were mere readers) and web 2.0 (the omnichannel internet, in which internet users were also content producers, mainly through social platforms). Web3 aims to further disseminate information on the internet using blockchain

How blockchain technology works



technology, so that it is not hosted and dependent on certain operators (hosts, marketplaces, social networks, etc.), but so that the user has access to such data at all times and will have a certain perception of *ownership* over it. The web3 model promises to further decentralise the internet, in which both information and decentralised apps (dApps) will be distributed across thousands of nodes, rather than concentrated on specific platforms. These open source-based platforms will issue access tokens to perform a type of function over a peer-to-peer network.

In this way, web3 leverages the architecture of the internet to increase its decentralising powers with the promise that users will have more control over their data and digital assets. However, web3 does not dispense entirely with intermediaries, who are still present, albeit in different roles. This is mainly in the form of marketplaces for digital assets or the management and custody of wallets where users store their NFTs.

As in previous stages of the current technological revolution, with each new technology or technological approach, voices arise demanding a change in regulation or lamenting the inadequacy of the legal system in the face of this new reality. On the contrary, this new approach should be implemented while respecting the existing regulations, albeit with certain adjustments, and after careful analysis.

In this briefing we will outline certain legal issues relating to web3 according to the services that are emerging and the legislative changes that are already taking place.

2. Crypto-assets:



Within this technological expansionism, crypto-assets have emerged strongly in recent years. These are intangible virtual assets, but have a value given by the market. These include cryptocurrencies, with Bitcoin being the virtual currency of reference since its creation in 2009. However, cryptocurrencies such as Bitcoin and Ether are not the only type of crypto-asset in existence, as others have been developed in recent years, such as real estate tokens¹ and NFTs, as mentioned in the previous section.

These intangible digital assets are unique and based on cryptography. However, crypto-assets can be placed into two broad categories: cryptocurrencies on one hand, and tokens, which can be fungible or non-fungible, on the other.

Within the universe of cryptocurrencies, the virtual wallet where users store their crypto-assets plays a fundamental role, a necessary tool to make them available given the decentralised nature of Bitcoin and the rest of the digital currencies. From a functional point of view, wallets allow you to check your balance, store cryptocurrencies, trade, or view transactions that have been carried out. Despite their nomenclature (and inevitable comparison with physical wallets), these wallets actually store cryptographic keys, both public and private, on which the blockchain relies to generate and operate crypto-assets.

Until 2024, crypto-assets will not be regulated throughout the European Union, thanks to the MiCA Regulation

All these technological advances have led to a regulatory response from European institutions and national regulators. On this point, the most relevant regulation, which has yet to be approved, is the MiCA Regulation².

This Regulation pursues several objectives, including the following:

- Ensuring secure access to crypto-assets for investors.
- Contributing to access to innovative investment.
- Monitoring fraud and the prevention of money laundering and terrorist financing.
- Establishing uniform legislation to replace existing national legislation in each EU country.

In addition, one of the most important points is that this regulation will mean that crypto-asset service providers³ must comply with transparency requirements in relation to the information they provide, their operation and internal governance, as well as requirements on asset pooling (for stablecoins⁴), consumer protection and rules to prevent market abuse.

The MiCA Regulation will enter into force 20 days after its approval, but it will not be applicable for 18 months, so we will have to wait until at least 2024 to see its real implications for the European crypto-asset market. Therefore, there is currently a lack of regulation in the European market, which is of concern to European authorities and regulators due to the strong presence of these assets among retail investors.

¹ In 2021, Reental.co, a Spanish fintech dedicated to real estate tokenisation, managed to sell a house in Seville with tokens thanks to 57 investors from 4 different countries. The total purchase cost of the property was €69,194 and the return that Reental.co achieved was 10%.

² Proposal for a Regulation of the European Parliament and of the Council on crypto-asset markets and amending Directive (EU) 2019/1937.

³ The MiCA Regulation defines them as "a person whose trade or business consists of the professional provision of one or more crypto-asset services to third parties".

⁴ Stablecoins or stable cryptocurrencies are tokens associated with the value of a fiat currency (such as the euro), material goods (such as gold), another cryptocurrencies (such as Bitcoin) or that try to avoid the volatility of these crypto-assets through algorithms.

However, the European Union has already taken a small step towards regulating crypto-asset service providers. With the adoption of the Fifth Money Laundering Directive⁵, providers of services for the exchange of virtual currencies for fiat currencies and providers of custody services for electronic wallets became regulated entities as regards money laundering and terrorist financing.

Spain transposed the Fifth Money Laundering Directive in 2021 and, since then, the activities of these providers in Spain have been subject to Spanish regulations on money laundering and terrorist financing, as mentioned in section 6 below.

Concerning national regulations on crypto-assets, the only regulation approved so far is the Circular of the National Securities Market Commission (“CNMV”) on advertising⁶. In summary, this Circular regulates the following:

The main rules, principles and criteria that apply to the advertising of crypto-assets when they are presented as an investment.

The CNMV's supervisory powers in this area, which include, among others, the power to order the cessation or rectification of advertising messages on crypto-assets and the power to penalise possible infringements.

The obligation for obliged entities to keep a register with information and documentation relating to advertising campaigns that are in progress or have been carried out in the last two years.

The requirement to notify the CNMV in advance of mass advertising campaigns, i.e. those aimed at more than 100,000 people.

A requirement that advertising for crypto-assets must provide sufficiently clear information on the risks associated with this type of investment product.

These regulations, together with the amendment of the Spanish money laundering regulations, are the only existing legal mechanisms that attempt to regulate the Spanish crypto-assets market. Compliance with anti-money laundering regulations and CNMV supervision of crypto-asset advertising are the first building blocks for the future regulatory regime of this market with an increasing presence of retail investors. Furthermore, the CNMV, the Bank of Spain and the Directorate-General of Insurance and Pension Funds (in line with the European authorities) have

in recent years issued warnings to investors on the risks to consumers posed by this asset class, stressing that they are not suitable as an investment or as a means of payment or exchange for most retail investors.

Finally, a brief mention should be made of the *Digital Euro project*. The emergence of cryptocurrencies coupled with a gradual decline in the use of cash in favour of payment methods such as cards and the emergence of new technological solutions have attracted the attention of the world's major central banks. In this context, the European Central Bank (“ECB”), after a preliminary phase of analysing and studying the requirements and risks, decided in 2020 to start the research phase on the implementation of a digital euro, as a complement to the current cash system, but in a more secure, digital form, and guaranteed by the ECB⁷. Although the project is at an early stage, according to the ECB, the emergence of a digital euro would enable the use of a commission-free and technologically robust alternative to physical money. In addition, the digital euro would add confidence to unregulated payment solutions, encourage a higher degree of digitisation and prevent the use of foreign digital currencies (such as the yuan or the digital dollar, both of which are currently under development).

A future digital euro would also reduce fraud levels and allow a reduction in the costs of issuing and circulating cash for the ECB (cost of issuance, risk of counterfeit banknotes, etc.). However, this research phase will last until October 2023, after which the ECB will assess the appropriateness of its implementation. Therefore, any potential implementation will not happen in the short term.



3. NFTs

3.1. NFTs as objects capable of ownership

The main differentiating element of NFTs⁸ compared to traditional digital files (e.g. JPG, mp4, etc.) is their potential uniqueness, based on a transaction log. In other words, NFTs give their owner⁹ the certainty that the object represented has unique, non-replicable and indivisible qualities. Therefore, the very nature of NFTs (hybrid assets that combine the representation of a physical or virtual object with a sequence of data stored in a blockchain network that can be traded thanks to orders supplied by smart contracts¹⁰) has meant that, unlike digital assets that predated web3, their value, as well as interest in their possession and ownership, is increasing. A new economy

⁵ Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU.

⁶ Spanish Circular 1/2022 of 10 January of the Spanish National Securities Market Commission on the advertising of crypto-assets as an investment.

⁷ The report is available in English at the following [link](#) (last accessed on 11 July 2022).

⁸ Despite the diversity of NFTs (e.g. NFTs linked to rights or services), in this analysis we will focus on content NFTs (i.e. digital art, avatars, video game elements, collectibles, etc.).

⁹ Understood as one who has the right to enjoy and dispose of a thing, with no limitations other than those established by law (article 348 of the Civil Code).

¹⁰ Despite its name, a smart contract is not a smart contract, but a computer programme deployed on a blockchain, usually Ethereum.

has emerged thanks to online platforms dedicated to the trading of NFTs, such as OpenSea¹¹, and the possibility of linking a digital asset to a holder. As a result, users' problems and doubts about what exactly they are buying and what they own are becoming more and more frequent.

Upon acquiring an NFT, the user's perception is that they *own* it and can store it in a software (or digital) wallet such as MetaMask, in centralised or decentralised hosting systems and in hardware wallets. However, as will be discussed below, what is actually stored in some of the ways mentioned above is the address of the *smart contract* that signals the location of the NFT. Thus, the concept of *ownership* rests on the metadata stored on the blockchain. This is similar to a company's securities, which are recorded in a ledger, but, in the case of NFTs, it is stored on the underlying digital asset.

As mentioned above, an NFT is made up of two distinguishable elements that function as a whole in the market. Firstly, an NFT has an underlying digital asset (a JPG, mp3, GIF, etc. file) that corresponds, as we will explain below, to the *corpus mechanicum* (incorporeal, in this case) of the work or subject-matter represented (an image, audiovisual recording, 3D work, etc.). Secondly, an NFT has the *hash* and other metadata that identifies the underlying digital asset and gives it, thanks to the technology, its unique character.

In an NFT there are two elements: the entry on a blockchain and the underlying digital file, which is what can be owned

This means that when an NFT is acquired, a record is created through a smart contract that identifies the location of the NFT on the blockchain and links it to a digital wallet owned by the acquirer of the NFT. However, except in particular cases such as the Autoglyphs collection¹², the metadata and underlying digital asset of which are stored on the same blockchain network, it is usual that, due to the size of the underlying digital assets and the cost of such storage, they are not stored on the blockchain itself along with their metadata. In effect, most commonly, only the web address (of the location where the full information of the NFT and the underlying digital asset is stored) is recorded on the blockchain, which means that NFTs, at least as far as the underlying digital file is concerned, are not as decentralised, or as indestructible¹³.

It is common for the underlying digital file to be hosted on the InterPlanetary File System¹⁴ ("IPFS"), as in the case of OpenSea, and for the NFT to be stored on numerous devices. Thus, contrary to what is commonly thought, the entire NFT is not on a blockchain and therefore, as mentioned above, it could be manipulated or removed. If the underlying digital asset is hosted in a centralised hosting system, access to the asset may be cut off, the image may be replaced, or the link may simply be non-functional. In contrast, using a decentralised storage system such as IPFS provides greater security, but not absolute certainty that some server will have the underlying digital file, guaranteeing its availability and ownership. This should be known to the acquirer of the NFT, as *ownership* of the NFT could be frustrated by such technical limitations.

Moreover, even in this case, the content of the underlying digital file may change or disappear, as happened with the "Raccoon Secret Society"¹⁵ collection hosted on the IPFS, a project whose smart contract stated "*the function serBaseUri allows the owner to remove all the metadata, arts, etc. at any time*" or, in other words, it gives the creator and owner of the NFTs the power to completely modify the underlying digital files at will. In other words, the final ownership of an NFT will depend on not only the technical characteristics of the NFT, but also the terms of its smart contract, which may be a traditional ownership or a licence to use and enjoy the underlying digital asset.

Despite the above reality, at present, case law and judgments regarding the possibility of treating NFTs as objects capable of ownership are scarce and, as we shall see, do not go into assessing the nature of NFTs. In our view, to the extent that they do so, it is with little precision. The High Court of England and Wales¹⁶ has already ruled on the recognition of NFTs (without going into detail on their composition) as assets eligible for ownership. For its part, the Spanish Directorate-General of Taxation, in response to consultation Vo486-22, has considered that the transfer of NFTs does not necessarily involve the transfer of the digital file itself (which contains an image or video), but of the digital certificate of authenticity that represents the NFTs. This means completely disassociating the content from the *hash* (the cryptographic function that acts as a "cadastral reference" of the digital asset that is to be made unique, in order to transfer its *ownership* by means of a smart contract, through a blockchain network) and other metadata that identifies it, all of which are inextricably linked to it.

11 OpenSea provides a peer-to-peer service that allows its users to discover and interact directly with each other and with the NFTs available on public blockchain networks.

12 Autoglyphs are the first on-chain generative art on the Ethereum blockchain. They are a completely autonomous mechanism for the creation and ownership of a work of art.

13 For example, if we look at the NFT contract "Sneaky Vampire #4903" hosted on Etherscan, we can see in the "tokenURL" section that, unlike the NFT metadata located on the blockchain, the actual location of the underlying

digital asset (from the image) is at the web address https://ipfs.io/ipfs/fybeibuzedpaeds5w2a23m6cnwlaakvqvz3ywx4pl2m3i4iigynqdvuy/4903_no_bg.png a web address that may not be available or have copies available on any of the servers around the world to which this peer-to-peer network makes calls, frustrating any exercise of ownership over the asset.

14 A peer-to-peer network for the storage of file data on computing devices.

15 The article is available at the following [link](#) (last accessed on 11 July 2022).

16 More information at the following [link](#) (last accessed on 11 July 2022).

Thus, the Directorate-General of Taxation considers that there are *two digital assets with their own identity, i.e., firstly, the underlying digital file* (video, image, graphic, etc.) *and, secondly, the "non-fungible token" or NFT that would represent the digital property of the underlying digital file*, the object of the transfer being the NFT itself and not the video or image, as will be explained in the section on intellectual property rights. In other words, the Directorate-General of Taxation considers that in the trade of NFTs, it is primarily the metadata, which serves to identify and certify their authenticity, that is transferred, and not the visual or audio content linked to them. This would be analogous to arguing that in the transfer of a real estate property the actual transfer is the cadastral reference which is registered in the name of the new owner, but not the real estate property itself. Or, in accounting terms, the transfer is the transfer of ownership of the accounting entry and not of the property itself, which is the object of the economic transaction. In any case, NFTs must be treated as hybrid and complex assets, the nature of which makes it impossible to separate the representation of the digital file from the hash and other metadata that functionally identify it. Thus, what is actually transferred and *owned* is the underlying digital file, the other elements that accompany it being merely functional or "registry" elements and, therefore, not capable of being owned in their own right independently of the asset they identify and represent, as the Directorate-General of Taxation intends to establish.

With all of the above, we can conclude that NFTs in Spain are assets capable of being owned and that they exist in the market as an asset subject to ownership, with said ownership resting on the physical or virtual object represented by the NFT and whose other functional and inseparable elements will guarantee that it is unique, non-replicable, indivisible and that, in conjunction with a blockchain network and using smart contracts, it corresponds to a specific owner. However, owners of NFTs should be aware that such ownership does not authorise them to reproduce, distribute, communicate to the public or transform their NFT when it consists of protected works or other subject-matter, unless they have been authorised or, where applicable, assigned the rights to do so by the owner of the rights to such works or subject-matter. Also, depending on the specific smart contracts of each NFT, owners who have acquired a non-fungible token may find that the use and enjoyment of the token is altered or even that they are no more than mere licensees of its exploitation, to a greater or lesser extent.

17 In particular, Book Four of Royal Decree-law 24/2021, of 2 November, on the transposition of European Union directives in the areas of covered bonds, cross-border distribution of collective investment undertakings, open data and re-use of public sector information, the exercise of copyright and related rights applicable to certain online transmissions and to radio and television broadcasts, temporary exemptions for certain imports and supplies, for consumers and for the promotion of clean and energy-efficient road transport vehicles. This Royal Decree-law transposes Directive (EU) 2019/789 of the European Parliament and of the Council of 17 April 2019

3.2. Intellectual Property Rights

As we have explained, the blockchain technology on which an NFT is based makes it possible to associate a graphic, audio or audiovisual element with the cryptographic key, which, due to its uniqueness, can achieve a significant market price. Although, at this early stage, the behaviour of operators in the NFT market does not always follow a specific pattern, the value of the NFT is generally determined, as in the traditional art market, by the work or subject-matter included in the NFT (which in most cases will be copyrightable), by its author and by the number of copies published, all based on the non-fungible nature of the token.

The proven resilience of classic intellectual property laws shows that even web3 does not escape the laws in force regarding the regulation of all types of works and subject-matter in the context of NFTs. Therefore, it should be understood that in Spain, Royal Legislative Decree 1/1996, of 12 April, which approves the revised text of the Intellectual Property Law, standardising, clarifying and harmonising the current legal provisions on the subject ("TRLPI"), according to the scope of application provided in its Fourth Book, as well as any related material rule¹⁷ and, by extension, all European law on intellectual property, is fully applicable to web3.

The application of blockchain-based technology facilitates the recording of all types of transactions of works and performances, especially when using NFTs as a non-fungible (i.e. unique) representation of any form of works or performances. It should be noted that an NFT is not the work or other subject-matter itself, but a way of representing it digitally¹⁸, which, in a certain way, is a continuation of the classical duality between *corpus mysticum* and *corpus mechanicum*, as a difference between intellectual work and a physical medium, and that now this would be more of a digital file containing the protected work or other subject-matter, associated with a token ID and the address of the smart contract (i.e. the blockchain record), both potential objects of legal business in the form of NFTs.

Acquisition of an NFT does not imply ownership of the underlying intellectual property rights

In other words, in exactly the same way that, for example, in the art market we must differentiate the ownership of the physical object (canvas, piece of marble, etc.) where

providing rules on the exercise of copyright and related rights applicable to certain online transmissions by broadcasters and to retransmissions of radio and television programmes, and amending Directive 93/83/EEC, and Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC. However, the legislature has chosen not to include the entire content of the reform in the TRLPI.

18 See Guadamuz, Andrés. *The treachery of images: non-fungible tokens and copyright*. Journal of Intellectual Property Law & Practice, 2021, Vol. 00.

an intellectual work (a pictorial work, sculpture, etc.) is embodied, with NFTs, we must distinguish, on one hand, the cryptographic key that a user has in their wallet and which refers to a smart contract deployed on a blockchain that guarantees the integrity of transactions and, on the other, the graphic or audiovisual element incorporated into it. As established in article 56 of the TRLPI, the ownership of the physical object or digital file and its transfer to a third party does not imply a transfer of the intellectual property rights inherent in it, which will continue to be held by the author or owner and which, in principle¹⁹, will only be transferred to the new holder of the tokenID if there is a written agreement (article 45 TRLPI).

The fact that the intellectual property rights inherent in an NFT are not assigned to the new holder of the NFT means that several NFTs can be generated for the same work or subject-matter. It would therefore be wrong to conclude, as some people have suggested²⁰, that the acquisition of an NFT automatically implies the holding of a licence or assignment of intellectual property rights over the work or subject-matter contained therein, which must be articulated through other channels, or included unequivocally in the metadata of the NFT.

However, this is independent of the resale right or *droit de suite*, which is directly linked to the resale of works on the secondary market, regulated in Spain in article 24 TRLPI. The possible creation of the resale right linked to the sale of an NFT, considered as incorporeal property, will be determined by the concurrence of a *copy* of works of art subject to this right, such as, among others, paintings, engravings or sculptures, provided that they are embodied in some kind of medium. In this respect, Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art states that "the subject-matter of the resale right is the physical work, namely the medium in which the protected work is incorporated"²¹.

Earlier we stated that, in civil terms, there can be a property right over an NFT thanks to the broad concept of *thing* in the Civil Code; however, there are no pronouncements on whether the concept of *copy* associated with the resale right can also be interpreted in such expansive terms, although the mention of the *medium* may lead us to conclude, *a priori*, that it cannot. Therefore, if there is an identification between the NFT as the *thing* that is the subject of the transaction, then the resale right can be understood to arise under the same conditions as it does in a transaction for a physical work. Conversely, where the NFT is a mere

representation of a work, it can be understood that there would be no resale right, as the *medium* requirement unequivocally required by the law is not met.

In any case, the reality of the market is that, thanks to the great potential of blockchain technology, the issuers of NFTs (presumably the authors of the physical work linked to it) usually stipulate said remuneration rights on future transfers of it through the smart contract for the NFT, automatically charging a percentage or lump sum for each resale or any other legal transaction on the cryptographic key associated with the tokenised work or subject-matter. The characteristics and functionalities of a smart contract therefore make it possible to contractually establish a sort of *para-resale right*, by programming this remuneration right into the software that will allow the transfer of the NFT in question.

3.3. Trade marks and industrial designs

The rise in the use of blockchain and, in particular, of NFTs, is also a cause for reflection on the behaviour and scope of the protection of industrial property rights (essentially trade marks and industrial designs). There are still no specific legislative precedents or case law that raise this issue in Spain, and there is currently no limitation in the Trade Marks Act²² or the Industrial Designs Act²³ that prevents the same protection being provided to a trade mark or design when the infringing use takes place in a virtual environment through an NFT.

It is well known that the registration of a trade mark confers on its owner an exclusive right over it, as well as a right to exclude, which allows them to prevent any third party from using an identical or similar sign in the course of business to identify identical or similar goods or services for which the trade mark is registered. However, this exclusive right held by the owner is not absolute, and one of its limits can be found in article 37 of the Trade Marks Act. The doctrine and case law have been accepting certain uses of a registered trade mark without the consent of the owner when it is used without a distinctive purpose with respect to the goods and services in which it is incorporated and in accordance with honest practices in industrial or commercial matters, provided that it does not generate a risk of confusion and/or association with the registered trade mark for the consumer.

If we look at the interpretation of the courts in numerous decisions concerning the infringing use of trade marks in classic digital environments, *a priori*, there is no doubt

19 We say in principle because the Spanish courts have considered some cases in which, in the absence of a written agreement, an implicit assignment of intellectual property rights had taken place.

20 Spice DAO confused the rights to the work with the rights to the medium holding it when it bought a copy of *Jodorowsky's Dune* for three million dollars to turn it into NFT, publish it and produce a series inspired by the book. Mistakenly, they acquired the book as a physical object, but not the

work. See <https://www.esquire.com/entertainment/books/a38815538/dune-crypto-nft-sale-mistake-explained/> (last accessed on 11 July 2022).

21 Recital (2) of Directive 2001/84/EC.

22 Act 17/2001, of 7 December, on Trade Marks.

23 Act 20/2003, of 7 July, on the Legal Protection of Industrial Designs.

that the owner holds the same rights and has the same protection mechanisms for the product in both its physical and virtual format. There is no indication that this position will change when the infringing use is by means of an NFT.

In fact, in other countries, courts are already addressing this issue, and are assessing the existence of infringement on the basis of the conventional criteria. In the US, the well-known fashion brand Hermès International filed a trade mark infringement lawsuit against artist Mason Rothschild for marketing NFTs inspired by the iconic *Birkin* bags. The judge has recently rejected the defendant's motion -which was based on the well-known *Rogers* case- on the basis that it is also necessary to assess whether the use of the trade mark creates confusion in the consumer in relation to the business origin of the product represented by an NFT²⁴.

On the other hand, in relation to the industrial design, the holder has an exclusive right to use it and to prohibit its use by third parties who do not have consent, with use being understood as, among other acts, the marketing or use of a product incorporating the design. The issue here is whether the concept of use extends to the NFT product, or whether the virtual representation of a registered design does not *per se* imply an infringement of the right holder's rights.

Again, without prejudice to the current lack of specific precedents outlining the scope of an industrial design right when the infringing use is by means of an NFT, the numerous rulings on this matter in relation to other digital platforms enable us to answer this question. Notably, in the *Activision Blizzard* case, although the infringement claim was ultimately dismissed, the judge analysed the infringement of an industrial design through a video game, so it can be implicitly understood that the infringement can occur both through its use in a physical and virtual product, given that what is protected is the design itself²⁵.

Trade mark and industrial design law is also fully applicable to NFTs

Therefore, the legal challenges are not so much in determining the scope of protection of trade marks and industrial designs when they are used by means of an NFT -which does not seem to be more problematic- but rather in the way in which the protection mechanisms provided for in the regulations operate when the infringing product is an NFT.

Firstly, doubts arise in relation to actions seeking an injunction and a destruction order against an infringing NFT. As we know, blockchain technology allows transfers to be made in a distributed and immutable manner, which, by its very nature, prevents use being discontinued or it being destroyed - since it is impossible to make it disappear. This issue is currently being raised in the US, where Nike is seeking the destruction of an infringing NFT that an online retail platform used to market popular virtual trainers²⁶. Faced with this legal -and technological- challenge, experts are considering the possibility of sending NFTs to a burned wallet in order to prevent them from being subject to further transfers.

The same question arises in relation to the possibility of applying for and enforcing an interim injunction aimed at preventing the continuation -or the commencement- of the infringement for the duration of the proceedings. One of the measures *par excellence* requested in these types of proceedings is the pretrial attachment of infringing products, a measure that is materially impossible to carry out in relation to an NFT because of its nature. In this regard, the High Court of England and Wales has recently granted an interim injunction ordering the "freezing" of the offending NFTs so that they cannot be transferred for the duration of the main proceedings, which could certainly be a solution.

Finally, because of the nature and characteristics of blockchain technology, we are also faced with a difficulty in determining standing to be sued, i.e. to whom the infringement action or injunction should be addressed when it is not known who the holder of the NFT is. A few days ago, the Supreme Court of the State of New York, faced with the impossibility of identifying the natural or legal persons involved in a fraud case, approved the notification of an interim measure by means of a "service token" (an *Ethereum-based token*) sent to the address of the anonymous user behind the NFT, which may provide an answer to the problem of identifying the infringer²⁷.

While we can begin to respond to many of the legal issues involved in defending industrial property rights against infringing use through a NFT, we will have to wait for our courts to develop solid precedents in this area.

24 Hermès International and Hermes of Paris, Inc., v. Mason Rothschild, United States District Court, S.D. New York. The defendant filed a motion to dismiss the claim on the basis of the well-known *Rogers Test*, under which the use of a registered trade mark without the owner's consent does not constitute infringement when it is artistically relevant and does not explicitly mislead the consumer. In this regard, the defendant argued that the trade mark was being used through an artistic work that virtually represented the original product; however, the Court considered that, even if the NFT was considered artistically relevant, it is necessary to assess whether it

generated confusion in the consumer in relation to the business origin of the product. For this reason, it rejected the motion and the case is ongoing.

25 United States District Court, E.D. Arkansas, Western Division. Feb 21, 2014, 140 F. Supp. 3d 795 (E.D. Ark. 2014) P.S. Products Inc. v. Activision Blizzard Inc.

26 Nike, Inc., v. StockX, LLC., United States District Court, S.D. New York.

27 LCX A.G., v. John Doe nos. 1-25, Supreme Court of the State of New York.

4. DAOs and Web3



A **DAO** (Decentralised Autonomous Organisation) is a virtual entity governed by smart contracts, constructed using a sequence of instructions written in a programming language²⁸, which are responsible for establishing the organisational rules²⁹, with the capacity to autonomously implement the guidelines or decisions that the members (token holders) have decided that the organisation should implement, and where decision-making takes place in a decentralised manner and is recorded on the blockchain.

These organisations, which are born outside of any corporate regulations, (i) are managed by their members, who form part of them through governance tokens and exercise authority democratically; (ii) provide decentralisation; and (iii) are characterised by transparency³⁰.

In a broad sense, this is a governance structure (such as a public limited company or a cooperative) in which a group of people can make decisions that are coordinated, implemented and recorded on the blockchain³¹. Whereas traditional companies require a series of intermediaries or enforcers, DAOs are a new form of organisation that aim to be freer and more autonomous. Ultimately, the goal of a DAO is to function without human hierarchical management.

There are numerous examples of DAOs formed in relation to web3 activities, virtual reality and the metaverse³², as well as NFTs. For example, a DAO in which token holders vote or have a say in the creation of an NFT, which is automatically executed by a creation algorithm.

DAOs currently do not have legal personality, which adds to their complexity

With these ideas in mind, it is an entity that shakes up and dynamises company law, and one that arises outside any legal system, which raises a number of practical questions.

Firstly, at the moment, there is no legislation granting it legal personality, with the difficulties that this entails³³, without prejudice to the fact that it can be understood to have the capacity to act, insofar as it assumes obligations in legal transactions. From a Spanish civil law perspective, the possibility has been raised of including this type of organisation within the scope of the type of partnership

under article 1665 of the Civil Code (“CC”), on the basis that *affectio societatis* exists, or within the scope of jointly owned entities, as ERCILLA points out. In this case, the liability, according to the majority legal opinion, would be subsidiary with respect to the company or the jointly owned entity, but not limited.

The questions concerning the liability of its members and whether this can be limited, as would be the case for a limited liability company, relate to its legal personality or lack thereof, as well as to its capacity to act. In light of the above, at present, we cannot speak of the existence of limited liability.

As an additional issue, if we were to consider DAOs as cyber entities³⁴ with the capacity to act with relative autonomy from the human actors involved, we must take into consideration the provisions of the European Parliament’s resolution of 16 February 2017, with recommendations to the Commission on civil law rules on robotics. This would be particularly relevant in the area of liability, where it is worth considering *robot fault*, by which the imposition of liability could be isolated, in which case token holders would not be at fault. However, there is also a basis for arguing the existence of a kind of *culpa in educando*.

Finally, the international nature of the DAO phenomenon does not adequately fit in with national laws and their territorial scope, which also raises problems of applicable law and jurisdiction. Therefore, in the corporate sphere, a kind of international law (or standard) of a specific nature, a *lex mercatoria*, is called for. Finally, an alternative that could go some way to resolving private international law issues would be to submit these issues to arbitration, and there are currently specific institutions such as the Blockchain Arbitration Society.

5. web3 data and cybersecurity



From a data protection perspective, web3 has certain advantages over traditional internet networks as a result of its distributed and decentralised nature. However, this decentralised and shared nature also brings with it significant challenges or issues when it comes to analysing the legal implications of this new network in terms of privacy and security.

28 ERCILLA, J., “Aproximación Jurídica a las Organizaciones Autónomas Descentralizadas (DAOs)” in *Revista Aranzadi de Derecho y Nuevas Tecnologías*, no. 51/2019, [BIB 2020/9477].

29 CALLEJO, G., “ConstitutionDAO: el ejemplo de cómo las DAO transformarán las industrias de la web3”, in *Observatorio Blockchain*, 19.11.2021, available via the following [link](#) (last accessed on 11 July 2022).

30 MONTROYA GAGO, B., “Organizaciones descentralizadas: ¿qué es una DAO y cuál es su papel dentro de la web3?”, in *Blog ThinkBig*, May 2022, Organizaciones descentralizadas: qué es una DAO y su papel en la web3 ([blogthinkbig.com](#)) (last accessed on 11 July 2022).

31 GUO, C., “DAOs and web3 Governance: The Promise, Implications and 32 Challenges Ahead”, in *ANTLER*, 01.03.2022, available at the following [link](#) (last accessed on 11 July 2022).

32 ROOSE, K., “¿Qué es la web3?”, in *The New York Times* (La guía cripto para despistados), available at the following [link](#) (last accessed on 11 July 2022).

33 OULEGO ERROZ, J.R., “DAO: Naturaleza e implicaciones jurídicas”, in *A Definitivas*, 10.12.2021, available at the following [link](#) (last accessed on 11 July 2022).

34 ZAPATA SEVILLA, J., “Inteligencia artificial y responsabilidad civil: el caso de las organizaciones descentralizadas autónomas”, Universidad de Málaga, 28.10.2019.

As opposed to the traditional Web 2.0, based on storage in centralised databases owned by different service providers and controlled by multiple agents acting as independent data controllers, web3 can provide greater privacy and security guarantees to data subjects in two ways: (i) in relation to the control of the data; and (ii) in relation to the access or display of the data.

In terms of data control, users will, *a priori*, be able to operate with a single set of credentials that will allow them to navigate and communicate with third parties without the need to make use of centralised services, controlled by professional intermediaries. In other words, in order to use web3, users will not be obliged to create multiple user accounts or provide personal data of a disparate nature to the different service providers that are part of the web as a *sine qua non* for using the web. In this way, data subjects will be able to prevent the dissemination of their personal data and have more control over how it is used. In terms of access, the fact that personal data is stored in a hierarchical manner limits the processing of personal data by third parties, who cannot indiscriminately access the previous records in which users' personal information is stored.

With web3, it is not always easy to identify the roles of those who process personal data

In addition, the distributed and decentralised nature of web3 also entails an improvement in the cybersecurity of this network. The rationale of peer-to-peer networks inevitably leads to the distribution of risk in the event of hacking, as a potential attacker would have to target all the nodes that are part of the decentralised network itself. This seems unlikely in an open and massively used ecosystem such as the web3 environment. Consequently, it is clear that web3 can also help to ensure the integrity and availability³⁵ of personal data and information, thereby reducing the number of security breaches to which data subjects' personal data may be exposed.

However, despite the above advantages for users' privacy, the immutability of blockchain networks, which prevents the modification or deletion of information stored on blockchains, clashes directly with certain rights recognised by data protection regulations in favour of data subjects. In particular, the impossibility of altering the blockchain prevents the exercise of the rights of rectification or erasure, based precisely on the modification or deletion of the personal data processed. This issue is inextricably linked to the principles of accuracy and time limits for conservation, which establish the obligation to take all reasonable steps

to ensure that personal data can be updated, erased or rectified.

Finally, to the extent that the servers are distributed and do not have a reference intermediary to determine the purposes and means of the data processing, the operation of web3 entails an additional challenge, based on the identification of the data controller and, consequently, of the processor - if there can or should be one. Thus, in those cases in which a transaction carried out within web3 involves the communication of personal data, the traditional model of data controller and data processor will be difficult to implement as the identification of users or the processing activities to be carried out on behalf of third parties will be more complex.

6. Money laundering on web3



Web3 is emerging as a new paradigm of web use. There are still many unknowns in this new environment for users who wish to conduct business in a decentralised manner and without intermediaries through the use of blockchain technology. These characteristics - which make it easier for users to remain anonymous and more difficult to trace transactions - are precisely those which, in our opinion, will be the focus of the legislature's interest in trying to control this type of activity in the coming years.

This inevitably leads us to think about the possibility that web3 could be used for money laundering or to finance illicit activities if there are no control measures to prevent this. These measures include establishing adequate traceability of transactions and identifying those involved in them. All of this is intended to adequately protect the interests at stake: on one hand, those of consumers and users and, on the other hand, those of the financial system as a whole.

This is already the case with some uses of blockchain technology to allow transactions to be carried out. This is the case with crypto-assets, which have already led to a recent reform of the Money Laundering Prevention Act to include providers of virtual currency exchange services for fiat currency and electronic wallet custody services³⁶ in the list of obliged parties. And the trendy but as yet unregulated NFTs, which have already been the subject of a US Treasury Department warning³⁷ because of their ease of use as a platform for money laundering, appear to be following in their footsteps.

³⁵ In this regard, the Spanish Data Protection Agency has shown that distributed information storage techniques, such as blockchain, can be used to ensure data availability. The article is available at the following [link](#) (last accessed on 11 July 2022).

³⁶ See art. 2.1 z) of Law 10/2010, of 28 April.

³⁷ See US Treasury Department, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art", 2022, pp. 26-27. Available at: <https://home.treasury.gov/news/press-releases/jy0588>.

The Money Laundering Prevention Act already covers certain web3 operators

On the basis of the above considerations, in our view, the difficulty that the authorities will face in relation to web3 lies in the absence of centralised organisations to manage the transactions that take place within it. In other words, on whom can the obligations provided for in the prevention of money laundering regulations be imposed in order to prevent the commission of unlawful acts? It seems logical that, following the crypto model, such obligations would rest on those virtual service providers that make such an exchange possible.

If, as it seems, cryptos are the currency for exchanging goods and services on web3, the problem could already be covered by the obligations already imposed on virtual service providers in this area. If, on the contrary, other types of mechanisms are used that allow these transactions to take place, we believe that the legal solution will be to identify new potential participants who can assume the obligations provided in the anti-money laundering legislation to avoid these risks.

7. Tax aspects of web3



Discussions around the taxation of the different components of web3 began in 2013, with the nascent spread of bitcoin. At the time, the analysis by countries generally revolved around whether cryptocurrencies should qualify as a foreign currency or as a non-monetary asset. Initially, countries such as Switzerland, Italy and Malta took the position that cryptocurrencies should be treated as a foreign currency, arguing that their main function was to serve as a means of payment. However, the general stance of countries gradually shifted towards treating cryptocurrencies as an asset³⁸.

In the particular case of Spain, the Directorate-General of Taxation, the body responsible for interpreting tax regulations by issuing rulings and answering taxpayers' queries, is issuing more and more pronouncements on cryptocurrencies, although these refer to the issues specifically raised by taxpayers in each case and in relation to each tax on a standalone basis. Broadly speaking, it can be concluded from these replies that cryptocurrencies are considered currencies (means of payment) for indirect taxation purposes (Value Added Tax or Stamp Duty), and assets likely to produce income or profits subject to taxation for direct taxation purposes (Personal Income Tax or Corporation Tax).

The Directorate-General of Taxation has already analysed the nature of NFTs in a binding consultation

In relation to NFTs, the Directorate-General of Taxation issued its first ruling on 10 March 2022 (the aforementioned binding reply to consultation Vo486-22), analysing their nature for Value Added Tax purposes. In particular, also noting the lack of interpretations by the Court of Justice in Luxembourg, it considered that NFTs do not share the characteristics of cryptocurrencies as they are neither currencies nor fungible goods. Nor does it seem appropriate to characterise the sale of NFTs as a 'supply of goods', given that, in the case of that consultation, the underlying asset involved in the sale of the NFT was not an existing tangible asset, but was also of a digital nature (the digital certificate of authenticity representing the NFT itself was sold, without any physical delivery of the NFT or the associated digital file itself taking place). Thus, it concluded that the digital art services that took the form of the sale of the NFT in that case qualified as electronically supplied services for indirect taxation purposes.

Apart from the apparent clarity regarding the taxation of cryptocurrencies, there are no clear regulations regarding the rest of the other components that make up web3. Notably, there are general doubts regarding the tax treatment of the rights attached to smart contracts. For example, in countries where income is subject to specific taxation depending on whether it derives from the exchange of "securities", it is unclear whether the public offering of investment through an unregulated smart contract should be considered a financial investment or a private activity.

However, the most relevant issue surrounding web3 taxation is not the classification of income, but the means for tax authorities to obtain information on taxpayers' transactions, and to verify and, where appropriate, settle tax debts. Let's consider Web 2.0, where large intermediaries (e.g. Amazon and Uber), duly registered with the relevant tax authorities, have significant KYC obligations to register and provide regular information on transactions between users of their platforms, and even to withhold taxes. This will be much more difficult in the case of web3, where the decentralisation and automation of transactions, carried out on the blockchain through smart contracts, means that there is no longer an established and auditable intermediary on which to impose these tax obligations (both material - payment - and formal - provision of information).

More importantly, web3 presents great opportunities for its participants to avoid having to use the traditional financial system to conduct their transactions. Digital wallets on

³⁸ Notably, in 2014, the US Internal Revenue Service (IRS) determined that cryptocurrencies should be classified as a personal asset for tax purposes, which broadly speaking generates taxable income when exchanged for traditional (fiat) currencies, goods, services or other cryptocurrencies,

as well as when new cryptocurrencies are received, such as in the case of hard forks, play-to-win, airdrops and through mining. Generally speaking, this has been the position adopted by the tax administrations of the major economies.

the decentralised web3, unlike traditional bank accounts, are not tied to a particular person. As such, peer-to-peer transactions carried out through decentralised platforms, such as financial transactions on DeFi platforms or capital transactions on DAO platforms, are virtually anonymous, making it difficult to audit the use of resources in the purchase of virtual assets or rights through these platforms.

In Spain, the tax administration has been devoting significant efforts to controlling the holding and operation of cryptocurrencies for at least three years, including these issues in its *Annual Tax and Customs Control Plans* and issuing massive requests for information to financial institutions, management companies and taxpayers themselves. The Directorate-General of Taxation has also reiterated the obligation to include this type of asset in declarations such as the declaration on assets and rights located abroad (form 720 -or perhaps the new form 721-) or the Wealth Tax return. In fact, the recent Law 11/2021 of 9 July on measures to prevent and combat tax fraud, which has yet to be implemented, has introduced two new reporting obligations aimed at operators managing cryptocurrencies and exchanges in certain circumstances.

At the same time, various international bodies are working on a multilateral solution. Notably, the OECD has dedicated the first quarter of 2022 to open discussions with industry stakeholders to find a solution, which will then be adopted by member countries. While there is no agreed upon position to date, indirect taxes on the consumption of goods or services with digital assets, as well as entry/exit taxes that are triggered when the crypto-asset is bought/sold in exchange for traditional fiat currencies, have been put forward as possible solutions. The OECD task force is expected to deliver a report with initial recommendations at the G20 meeting in Indonesia in October 2022.

In any case, one thing seems clear to us: new functionalities and new services will gradually appear which, in the context of taxes, will have to be classified and integrated into rules that have not always been designed with these technological advances in mind.

8. Impact of web3 on the insurance sector



8.1. Advantages and challenges

As a starting point, we must refer to the complexity and breadth of the insurance sector to understand the impact of web3. The insurance industry does not only consist of

insurance companies, but also of entities dedicated to operating in the insurance mediation channel, where we find insurance distributors (insurance agents, brokers or bancassurance operators, whose regulation can be found in arts. 134 et seq. of Royal Decree-law 3/2020 of 4 February³⁹); different persons or companies that support intermediaries in the distribution function (external collaborators, teleoperators, comparators, etc.); as well as support or management companies that help in the processing of claims. At the same time, there are different distribution channels through which the aforementioned persons and entities can market insurance policies, among which, of course, electronic contracting via the Internet plays a key role.

Therefore, the parties involved in the insurance distribution process are currently adapting to the advantages offered by web3 to optimise and facilitate their respective tasks thanks to the tools that this technology makes available to them, allowing them to gain a competitive advantage over their competitors by offering automated advice through blockchain-structured algorithms.

Two of the most relevant points to highlight from web3 in the insurance sector are the following:

- (i) The conclusion of insurance contracts via web3 relies primarily on the collection of personal data from policyholders, insured persons, beneficiaries and injured third parties. This is because the automation of this data creates an efficient process that is in the best interests of both insurers and policyholders. However, the intensity with which this data may be processed requires special attention to be paid to the requirements that art. 99 of Law 20/2015, of 14 July, on the regulation, supervision and solvency of insurance and reinsurance entities ("LOSSEAR") imposes on insurance sector entities in this regard.
- (ii) The objectification of the data collected allows for greater effectiveness in the fight against insurance fraud. This is because insurers and distributors have a more accurate understanding of the reality of the risks insured. Therefore, the proliferation of web-based contracts is an opportunity to prevent, deter, identify, report and remedy fraudulent conduct relating to insurance in a more efficient way, in accordance with the literal wording of art. 100 LOSSEAR.

Another essential factor in understanding the impact of web3 on the insurance sector is the phenomenon of digitalisation that is increasingly affecting financial markets. All companies involved in the insurance industry

³⁹ Royal Decree-law 3/2020 of 4 February on urgent measures transposing into Spanish law various European Union directives in the area of public procurement in certain sectors; private insurance; pension plans and funds; taxation and tax litigation.

are investing resources and efforts in moving away from paper to electronic underwriting, marketing and processing of all documentation relating to the contracting of an insurance policy.

Insurers wishing to use web3 tools must do so in compliance with LOSSEAR obligations

In this regard, among the tools that web3 gives insurance companies is the option of providing completely automated advice to policyholders, without the involvement of human beings. This is the case with smart insurance policies, which are part of smart contracts, as their use allows the creation of insurance policies using parametric values that serve to pay the insured subject an immediate indemnity if the guaranteed risk is deemed to have occurred, through the analysis of automated objective values. An example is an intelligent insurance policy that includes coverage against the occurrence of certain weather conditions and which, when it identifies through big data that these conditions have occurred, pays the agreed compensation to the insured. This allows for transparent and accessible contracts for policyholders, as well as efficient and effective contracts for insurers and distributors.

However, we must remember that this form of automated and decentralised advice does not escape the regulation applicable to insurance contracts in general. In this respect, the following issues are worth highlighting from a regulatory perspective:

- (i) Smart insurance policies are legal transactions of a commercial nature that serve as a source of rights and obligations for the contracting parties. They must therefore meet the essential requirements for the validity of commercial contracts (art. 1261 et seq. of the Civil Code and arts. 50 et seq. of the Commercial Code). For example, to have a validly concluded intelligent insurance policy, it is equally necessary to have the following elements: the valid consent of the policyholder and the insurer; an insured risk as the basis of the contract⁴⁰; and, as an object of the contract, the policyholder's interest in protecting himself against the eventual occurrence of the risk to the insured element, with which he has an economic link⁴¹.
- (ii) Smart insurance policies must also comply with the requirements that Spanish law imposes specifically on insurance contracts. For example, clauses

limiting the rights of the insured must be specially highlighted and specifically accepted in writing by the policyholder⁴² (art. 3 of Law 50/1980 of 8 October 1980 on the insurance contract, "LCS"); the policy, or, at a minimum, the provisional coverage document, must be delivered to the policyholder (art. 5 LCS); or the policy must necessarily refer to certain elements, such as the nature of the risk covered or the amount of the premium (art. 8 LCS). The policy, despite being eminently digital and structured through decentralised blockchains, must be stored in a durable medium that allows its content to be preserved and easily accessed, without making changes or modifications to it, as established in the First Additional Provision of the LCS.

- (iii) Art. 96 LOSSEAR enshrines the general duty to inform the policyholder. This provides that, before concluding an insurance policy, the insurer must inform the policyholder in writing of various matters, such as the Member State and the authority responsible for supervising the activity of the insurer.
- (iv) Similarly, arts. 122 to 127 of Royal Decree 1060/2015, of 20 November, on the regulation, supervision and solvency of insurance and reinsurance companies, implement art. 96 LOSSEAR. These provisions specify certain obligations to be observed by insurers in certain situations, such as in the conclusion of life, death and health insurance, or insurance offered under the right of establishment or the freedom to provide services.

8.2. Securing against new risks inherent to web3

Meanwhile, we continue to find that the insurance industry is adapting by designing and offering insurance products to cover any new risks that may arise as a result of the various technological advances.

Thus, with the rise of web3, we expect to see an increase in fully automated and decentralised trading coupled with an increase in the buying and selling of digital assets configured through blockchain technology, such as NFTs or cryptocurrencies. These elements, which are intangible assets, are subject to very specific risks from a financial point of view (for example, the risk relating to aggressive and unpredictable fluctuations in the value of cryptocurrencies); technical (connection failures, errors in the transfer of funds and data from one blockchain to

⁴⁰ The doctrine defines risk as an event or occurrence capable of generating damage or need, against which the policyholder intends to protect himself through the conclusion of an insurance contract. On this point, see BATALLER GRAU, J., LATORRE CHINER, N., OLAVARRÍA IGLESIA, J., *Derecho de los seguros privados*, Madrid: Marcial Pons, 2007, p. 174.

⁴¹ GARRIGUES. "El interés en el derecho" in *Temas de derecho vivo*, Madrid: Tecnos, 1978, pp. 233-235. In this text, the author refers exclusively to property and damage insurance. However, the reasoning can be extended to all types and branches of insurance, since in all of them risk and interest are

manifested as cause and object respectively, in accordance with art. 1261 CC.

⁴² On this point, the Supreme Court has held that, in order to comply with the provisions of art. 3 LCS, the limiting clauses must observe certain requirements. Some of these requirements are to be written in "bold" type or to respect the requirement of the double signature of the policyholder in the insurance contract in general and, jointly, in the particular conditions that shape them (Judgments of the Supreme Court No. 402/2015, of 14 July [R] 2015\4129) and No. 76/2017, of 9 February [R] 2017\424).

another that affect the conclusion of a smart contract, etc.); or operational (such as a human failure in programming or digital contracting), among many others.

The traditional insurance market currently provides answers to some of the above risks. For example, a property damage insurance policy may include special theft cover that would include as a risk the unlawful removal of digital assets, under arts. 50 and 53 LCS. Similarly, there is secondary case law that applies other types of insurance to similar cases of damage to virtual archives, such as the Judgment of the Court of Appeal of Asturias (7th Section) no. 360/2019, of 25 October [JUR 2020\34631]. In that decision, the Court heard a policy that included a guarantee covering damage caused

by "acts of vandalism or malicious acts", and held that this cover was applicable to a cyber-attack that affected various data and computer files, considering that this guarantee was not limited only to acts of a physical nature.

However, there is no doubt that web3 brings us into a scenario with different insurance opportunities and opportunities to take advantage of the new technology in the insurance sector, so it is to be expected that different traditional insurance companies and *insurtechs* will continue to design new specific products for their risks and develop new business models that allow them to optimise the use of web3.

CONTACTS



Andy Ramos Gil de la Haza
Partner, Intellectual Property
and Technology
aramos@perezllorca.com
T: +34 91 423 20 72



Eduardo Castillo
Partner, Intellectual Property
and Technology
ecastillo@perezllorca.com
T: +34 91 423 66 57



Pedro Fernández
Partner, Corporate/M&A
pfernandez@perezllorca.com
T: +34 91 423 70 41



Josefina García Pedroviejo
Partner, Financial Services and
Investment Funds
jgarciapedroviejo@perezllorca.com
T: +34 91 389 01 09



Joaquín Ruíz Echaui
Partner, Insurance and Reinsurance
jruiz-echaui@perezllorca.com
T: +34 91 432 51 58



Juan Palomino
Partner, White Collar Crime
and Investigations
jpalomino@perezllorca.com
T: +34 91 423 20 87



José Suárez
Partner, Tax
jsuarez@perezllorca.com
T: +34 91 423 67 41

AUTHORS

Iván Bejarano, Diego de la Vega, María de Arcos, Pedro Fernández, Rafael Fernández, Enrique Hernández, Josefina García Pedroviejo, Isabel Iglesias Feal, Fernando Luján, Alicia Maddio, Álvaro Martínez Crespo, Guillermo Meilán, Inés Molina, Raquel Pérez Gargallo, Andy Ramos Gil de la Haza, Marta Rodríguez Castillo, José Suárez

www.perezllorca.com | Madrid | Barcelona | London | New York | Brussels

The information contained in this Information Briefing is of a general nature and does not constitute legal advice. This document was prepared on 21 July 2022 and Pérez-Llorca does not undertake any commitment whatsoever to update or review its content.