Boletim do Tempo Presente - ISSN 1981-3384

The cybersquatting of NFTs: The Rise of Civil Liability

Maria Renata K. Gois Cruz[I]
Alexandre Dimitri[II]
Maria Amália de Oliveira Arruda Camara[III]

Abstract: Non-fungible tokens (NFT) are at the driving center of exponential profit monetization and opening opportunities on the internet, especially in the gamified or augmented reality field, and the metaverse. Under that narrative of decentralization, sustainable development, and cyber fraud-free space, this article aims to bring new paths looking forward to minimizing illegal acts. These cyber frauds are highly seen in cybersquatting crimes, even when blockchain is used. It also can be seen in public or private digital environments, when cybercriminals attempt to control operations, earn fees, and collect data of the parties involved, waiting for a moment to extort the target. The NFT system is an "excellent tool" for criminals because most people know about its volatility and others don't know how to buy these items online, turning them an easy spot to fall in some of the crackers' links. The mysterious digital difficulties of life in a cyber world impact the relations between the subjects of intellectual property and their rights. Without a doubt faced with the dilemmas of digitization in the sphere of civil liability, cybersquatting is a cyber crime4 that demands attention and lacks reflections that prove capable of understanding its causes, its authors, and its mode of operation to protect and repair its victims. It can be said that the digital environment operates under the possibility of someone copying it, making it cheaper and repeating the process endlessly. It is believed that, after twenty years, via non-fungible tokens (NFT) one of its oldest problems can be solved: respect for intellectual property. And that's because this technological disruption promises to make it impossible to copy everything that is or will be created in this virtual universe. (FAIRFIELD, 2021)[IV]. The very personal right to own digital assets and no longer just subscribe to streaming. File services in the cloud become viable with NFT technology, too. The way people own digital things on the internet will never be the same again. Regulatory progress is confronted by the new possibilities and risks arising from how people will become owners, will invest, publish, and trade their own or third-party digital assets. (FAIRFIELD, 2021). Therefore, the objective of the article is to analyze how to combat abuses of domain registration on the internet and illegalities in intellectual property rights via cybersquatting of NFT. For that, the descriptive-analytical method and the bibliographic, documentary, and jurisprudential techniques are applied. Considering the proposal of the article, we decided to structure it into three parts. In the first one, we approach what cybersquatting is and its illegal framework. In the second, we emphasize its relationship with the violation of intellectual property rights and the result in civil liability. And third, we focus on legal solutions to this problem. Explaining what cybersquatting is, classifying it as a crime, identifying the causal link between the illicit and the damage and the elements of the civil liability of this fraud to digital intellectual property rights are essential to aim legal solutions.

Keywords: NFT. Metaverse. Cybersquatting. European Union. Civil liability.

THE CYBERSQUATTING OF NFTS: THE RISE OF CIVIL LIABILITY

CRUZ, M. R. K. G.
DIMITRI, A.
CAMARA, M. A. O. A.

1. INTRODUCTION

In 2021, a new digital trend, at the height of the Covid-19 pandemic promises to bring prosperity and liberation to world artists: digital certification on blockchain owned by a unique tokenized intellectual creation. A year later, the best example of this NFT craze is the purchase by famous personalities of 'The Bored Ape' a collectible digital asset[V]. It is about the digital monetization of culture: anything digital can become unique, certified via blockchain, and displayed to others for the satisfaction of its owner ego.

In this craze for NFTs, digital art, photos and videos stand out for the amounts of money involved in the acquisitions. It is possible to glimpse it by Neymar and Eminen's new acquisition: the NFT sold by 'The Bored Ape'. This new trend of tokenized art has its first purely digital work of art created by Beeple[VI] offered by a large auction house: Christie's, on March 11th, 2021. But as in every market where profit margins are remarkably high, there is always an opportunity to practice fraud. So, inside the NFT universe of gamified metaverse or augmented reality metaverse, the great villain is cybersquatting.

As shown above, this article aims to analyze how to combat abuses of domain registration on the internet and illegalities in intellectual property rights via cybersquatting of NFT.

In this perspective, the descriptive-analytical method and the bibliographic, documentary, and jurisprudential techniques will be applied. The terms 'cybersquatting' and 'non-fungible token' were searched on Google Scholar, SciElo, and Routledge at Taylor & Francis online. We decided to eliminate publications older than 2013 and those that were not linked to the topic. The sample resulted in 11 studies to tackle this problem: how does cyber fraud from NFT cybersquatting give rise to civil liability in the European Union?

Considering the proposal of the article, we decided to structure it into three parts. In the first one, we approach what cybersquatting is and its illegal framework. In the second, we emphasize its relationship with the violation of intellectual property rights and the resulting civil liability. And third, we focus on legal solutions to this problem.

2. EXPLAINING WHAT CYBERSQUATTING IS AND ITS ILLEGAL CONTEXT

2.1 Cybersquatting approach

Humanity is involved in the fatality of dogmas, laws, things, and the human heart: the mysterious difficulty of life is born of these needs[VII] (HUGO, 2009).

The mysterious digital difficulties of life in a cyber world impact the relations between the subjects of intellectual property and their rights. Without a doubt faced with the dilemmas of digitization in the sphere of civil liability, cybersquatting is a cybercrime[VIII] that demands attention and lacks reflections that prove capable of understanding its causes, its authors, and its mode of operation to protect and repair its victims.

This is what Boldt[IX] (2021) refers to as the key theme of the future: give viable responses to the challenges of digitalization in the legal-criminal field. As observed by Jaishankar (2007)[X] it is necessary to think of a cyber criminology focused on analyzing the causes of cybersquatting, its criminals' personalities, their ways of acting, and the means to prevent it.

It can be said that the digital environment operates under the possibility of someone copying it, making it cheaper and repeating the process endlessly. It is believed that, after twenty years, via non-fungible tokens (NFT) one of its oldest problems can be solved: respect for intellectual property. And that's because this technological disruption promises to make it impossible to copy everything that is or will be created in this virtual universe11. (FAIRFIELD, 2021).

The very personal right to own digital assets and no longer just subscribe to streaming. File services in the cloud become viable with NFT technology, too. The way people own digital things on the internet will never be the same again. Regulatory progress is confronted by the new possibilities and risks arising from how people will become owners, will invest, publish and trade their own or third-party digital assets. (FAIRFIELD, 2021).

Considering that current financial capitalism cannot survive without the internet, the NFT is a revolutionary technological tool of a new era, which includes extraordinary productivity gains and agglomeration of wealth, as intended by the bourgeoisie born with the industrial revolution. It is defended by Resende (2021)[XI] that the viability of representative democracies is at breaking point due to the strength that economic theory has at the service of financial capitalism, in the elite of technocracy and public policymakers.

As Dias (2022) declares that in the world of crypto assets almost ninety percent of all existing crypto assets are in the wallet of five or six people. Although the digital currency has been advertised as a tool of decentralization, it is possible to argue that it represents more concentration of wealth. So, at an open (run by a DAO)[XII] or centralized (only one company is in charge of managing all the aspects related to this metaverse, i.e. the economic activity among users or the data generated by them) metaverse, NFT has a distinct purpose to optimize the profits of financial capitalists and its counterpart: cybercriminals.

2.2 Cybersquatting legal arrangement

Still on this topic, since we have explained what cybersquatting is, the second specific objective must be addressed: detailing the framework of cybersquatting illegality. To begin with, Barlow (1996)[XIII] has already said that cyberspace would not submit to any jurisdiction.

According to Clough, none of the terms used for cybercrimes are perfect, because they suffer one or more deficiencies, not reaching the perfect meaning of the whole category of this crime. For example, the term 'cybercrime' could focus only on crimes made ON the internet, crimes of high technology would include delicts made involving advanced and recent technology, such as nanotechnology or bioengineer. Therefore, this lack of a pattern turns into more difficult to analyze each case. (BARRETO, A. KUFA, K. 2021)[XIV]

It should be noted what Huff [XV](2021) says: cybersquatting is substantially a form of extortion. It is claimed that in the United States of America the jurisprudence of the Eleventh Circuit was consolidated in this regard. So undoubtedly, the statistics compiled in the 2020 FBI report confirm cybersquatting in third place at digital crimes rank and identity theft in fifth place.

Thus, it cannot be thoughtfully argued, as did Barlow back in 199617, that victims of transnational cybercrimes such as extortion or identity theft would not have access to jurisdiction capable of enforcing reparation and prevention of their rights. In America for example on November 29, 1999, the Anticybersquatting Consumer Protection Act (ACPA) was signed into law. It provides that a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark'. But requires, under the 15 U.S. Code § 1125(d), that the domain name was 'registered before, on, or after the date of the enactment of this Act. It also yields that damages can be awarded for violations of the ACPA, if the registration, trafficking, or use of a domain name occurs after the date of the enactment of this law.18

As Huff (2021, p. 3) claims when he reflects on the element of bad faith intent on civil liability at cyberpiracy prevention involving registration, trafficking (sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration), or use of a domain name, '[c]ourts have relied on this provision to infer bad faith intent via factors beyond those suggested in the statute [ACPA]'.

In the view of Isenberg (2022) the NFT is a unique digital asset that exists in the digital environment linked to a blockchain technology capable of certifying its entire chain of ownership, timing, and pricing. It is noteworthy that the first case examined, in May 2021, by the Uniform Domain-Name Dispute Resolution (UDPR), implemented in 1999 by the Internet Corporation for Assigned Names and Numbers (ICANN), of litigation for irregular registration of domains on the internet involved: nftmorganstanley.com. Filed by Morgan Stanley against Joseph Masci, under Forum Claim No. 1940938, the dispute was judged in favor of the complainant because the disputed domain name causes confusion in consumers for not falling within the Morgan Stanley trademark usage policy, as well as the accused incurs in the offer of services and goods with a lack of good faith when offering third-party links in the conflicting domain that remunerate per click of deceived consumers.

1. IDENTIFYING CAUSAL LINKS OF CYBERSQUATTING VERSUS DAMAGES AND ITS ELEMENTS OF CIVIL LIABILITY

3.1 Towards the causal link between cybersquatting and damage

The enormous number of cybercrimes originating from the sales of NFT is higher daily. It is profoundly important to keep in mind that these transactions are not, in general, by the law. The jurisdiction has not kept up with the rapid evolution of the technological world. Therefore, cyber awareness and cyber education are essential.

Although it is sold to the young ones so that they can 'earn money' rapidly, in the majority of cases they lose everything. However, losing money is a 'lucky card' in this field, because, if you make a

wrong transaction, you can be hacked and lose not only your NFTs but also all your accounts, including banking ones.

Astonishing as it may sound, digital goods which people will come to use, dispose and entitle via NFT are not mere licenses governed by smart contracts, blockchain, and AI. In a different manner, they are the exercise of civil rights overpriced digital things. And it comes to our notice which one of the normative rules would be applied to solve conflicts of this nature, for example, whether arbitration in the Cayman Islands or the Uniform Commercial Code (UCC) of The United States of America, supporting Fairfield 20(2021) the prevalence of the latter.

Notwithstanding, immersive digital environments and augmented reality via the superposition of elements in people's non-virtual daily lives are being developed, promoted, and advertised by large corporations. As Dias21 (2022) explains, the NFT lives in the gamified or augmented reality metaverse, which is nothing more than the capacity to certificate ownership of only digital assets. It is also advertised by Dias (2022) that this certification may have similarities to a pyramid scheme as NFT´s smart contracts foresee that there will be chain remuneration on future sales, profiting original and previous buyers.

OpenSea has a 'bug' in their system, which helps malicious people to scam buyers. This scheme works in this manner: the scammer sends to a famous person- such as Neymar, or Eminem, the fake NFT. A person doesn’t need to agree with the 'donation'. After that, the buyer checks the history of the 'hypothetical store' and sees that it has been sold to a famous person, and he concludes that this store is a serious one, and he can buy it. Later, the 'store' sends the NFT for him; but a fake one, which only lasts some minutes, and after, it goes away. Then, the buyer understands that he has fallen into a scam, notwithstanding the fact is: it is too late, he cannot have his money back, the transaction was made using bitcoin, and he cannot accionate justice. It is highly important to be aware that there are a large number of people who invest in this field and lose more than a thousand dollars in those transactions.

There are other bugs in the OpenSea[XVI] platform, the bigger NFT store of nowadays. Has been published Engadget[XVII] an article explaining another type of fraud, the typosquatting[XVIII]. Hackers are buying an NFT which has a price of 99 ETH25 for 0,01 ETH. The bug in this site is creating an enormous breach for the occurrence of this crime because they buy it intentionally thinking of gaining a high-profit tax.

3.2 Civil liability essentials from cybersquatting NFTs

For Sérgio Vieira26 (BRANCO, JUNIOR, S. 2007), the development of NFT helps to verify if the version is an original or a copy. However, there is a huge gap/lack of laws, which would regulate cyberspace. The NFT is a tool to protect the art; this new protection has a double nature *a) patrimonial; and b) law of personality.*

Nevertheless, it is relevant to say that cybercriminals most commonly use domain parking, ransoming domain names, affiliate marketing, hit stealing, and various scams for their monetization practices. And according to the most recent, 2020, Internet Crime Report of the FBI, digital frauds

have resulted in about US$ 13.3 Billion in total losses in a universe of 2,211,396 complaints over the last five years27 (FBI, 2020).

In this sense, it is worth noting the teaching of Bhusari and Rampure (2022, p. 2283): When the domain names are registered with the mala fide intention to be sold to existing business and/or to conduct business in their name by misinterpretation, such practice is recognized as 'Cybersquatting'.

The European IPR helpdesk (2017) conceptualizes cybersquatting as a practice of making abusive registrations of domain names already registered as domain names in one or more top-level extensions or as trademarks or trade names. It is highly important to remember that this practice not only originated with the advances of the internet after the 2010s but has also, this was expressed since the 1980s, with the Minitel. In Journalism History, there is an article that shows the beginning of this crime 'Even the practice of cybersquatting had a precursor in Minitel. Instead of URLs, Minitel users access various sites through shortcodes, which combine numbers and a handful of letters. Some clever individuals seized opportunities and registered certain short codes, mimicking or copying the names of famous businesses and politicians. (Arcenaux, Noah, 2018)

And as a species of internet fraud known as cybersquatting, there are four more common conflicts between the domain of internet address names and intellectual property rights: typosquatting, identity theft, name jacking and reverse cybersquatting. About typosquatting, well defined by Gilwit (2003) and conceptualized by Bhusari and Rampure (2022, p. 2290) is the registering of domain names:

which are similar but not the same as the popular or well-known trademarks, by intentionally making a typographical error in the domain name that is to be registered. These errors are generic and there are chances that many of the users would type incorrectly and then would be directed to the cybersquatters' website. This kind of squatting is something where the squatters would have to bet upon the errors made by the people at large while typing a specific domain name.

In addition to typosquatting, it is worth mentioning that another sort of cybersquatting is the theft of the virtual identity that has been registered by trademarks online but not renewed periodically. Cybercriminals patrol these digital opportunities to gain dominance over the online domains of brands whose digital governance is not mindful of expiring intellectual property registration deadlines. Furthermore, whether this fraud is targeted at celebrities or ordinary people on social media or not, this criminal scheme is known as name jacking. Coupled with that, reverse cybersquatting occurs when the criminal agent seeks for himself the domain of a third-party trademark registered on the internet. Cybersquatters use pressure via social engineering to carry out all these goals.

1. LEGAL SOLUTION FOR CYBERSQUATTING

After all the Hail of NFTs as the solution for digital conundrums, reality knocks on the door and shows that it can be used as a detour.

The Bored Ape Yacht Club creator released a teaser website for an upcoming collaboration with crypto game developer Animoca Brands Thursday night, but many users are hesitant to sign up. The reason is that to register an Ethereum wallet, users must undergo full know-your-customer verification. The requirements include providing a passport, national ID, or driving license, along with a slew of personal details, including family name, date of birth, and proof of address. (CRAIG, TIMOTHY, CryptoBriefing, 2022)[XIX]

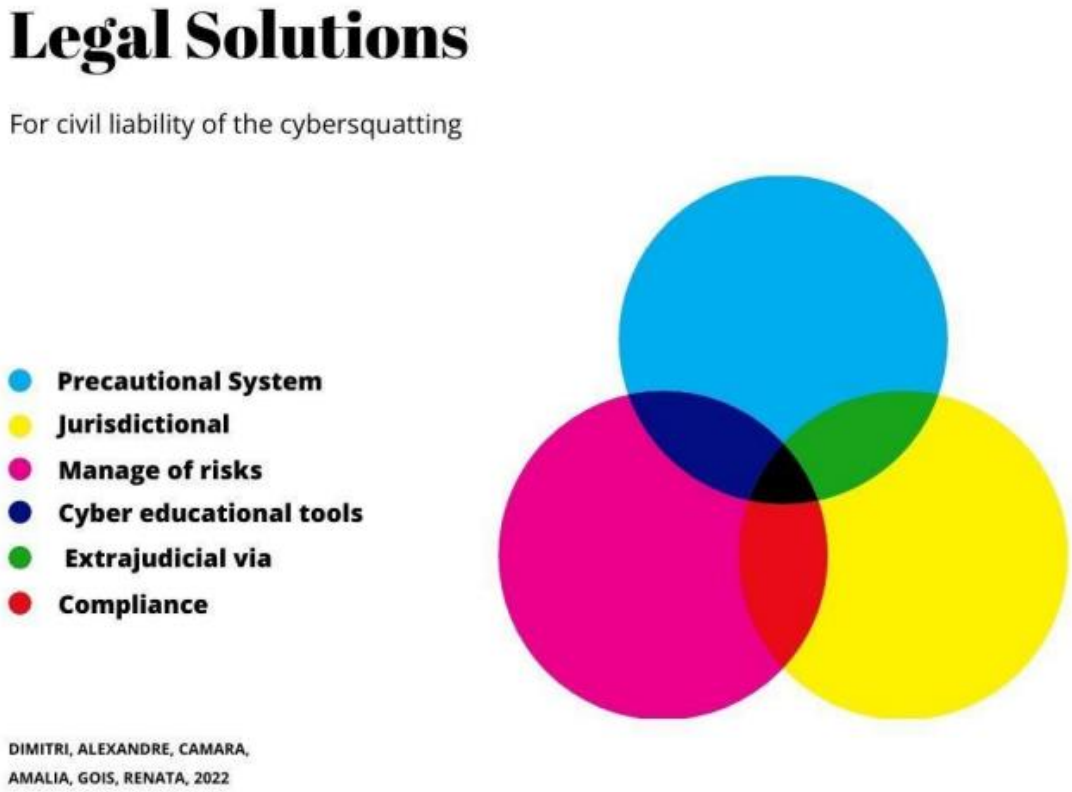
These requirements including personal information may be handy in cases of joinders. Notwithstanding, it is widely known that creating a fake ID, is no longer as difficult as it was one day. After the digital banks were created it was highly diffused the bank accounts, including the fake ones. It is not hard to read in a newspaper that someone used IDs from dead people to create these accounts, and in other cases, they change personal information to invent a new identity or a new person. Therefore, this is not the best detour.

Even though this new compliance is presented as a precaution, it is highly important to think about the juridical solutions for joinders. The main problem in cybercrimes, nowadays, is to know exactly where and for whom it was made. However, using an NFT turns out to be clear. Besides that, another complication derived from the internet civil liability is: how to execute in a jurisdictional via. This study came up with a new idea, which intends to be handy: the Digital use of a Notice of Dishonor.

To generate this Digital Notice of Dishonor, this article came up with a solution: The procedure is simple, when you buy an NFT with your cryptocurrency it is done by a blockchain service. Therefore, it automatically generates a smart contract, and there will be a serial number in this transaction. While this smart contract is made, the system will also create a clause of Direct court enforcement of debt instruments, which would allow a nottery's protest, which would be used in case of non-fulfillment of the obligations. When the buyer has this Direct Court Enforcement in their hands, he will be able to execute the contract, being able to go in a judicial via too.

Getting NFT sales out of hand is tremendously easy. For this reason, not only preventive compliance is enough, but you shall have excellent CIA criteria[XX] and also, plans to risk management. Consequently, compliance is fundamental to managing and attenuating the risks involved in those transactions. Likewise, a cyber educational act will be extremely convenient, to educate and create a social awareness of what crimes can be caused by those sales. The preventive aspect which was shared by 'The Bored Ape' is just the beginning of this consciousness.

In conclusion, the legal solutions, in your view, can be divided into 3 main parts: precautional (using cyber educational tools), jurisdictional (which would be divided into 2, a) extrajudicial via, b) judicial via, and the management of risks (using compliance).



1. CONCLUSIONS

In conclusion, cybersquatting is an illegal act that is enormously increasing in a short period, due to the exponential development of technology and the open diffusion of NFTs.

This crime enhances the problems around digital law and the lack of regulations in this field. Also, it verifies the gap in efficient legally friendly detours that could be used to minimize the bureaucratic solutions that are done in legal processes.

European IPR HelpDesk (2017) conceives this practice as being maleficent and reminds us that it is not a new illegal act, but has been used since the 1980s with the Minitel. Therefore, it is highly important to find another legal way that could be more rapid and more efficient, in exchange for minimizing this old fashion crime.

The application of the graphic in figure 1 is tremendously important to build strong compliance in any area. Not only the jurisdictional via is effective, but also procedures not based on joinders may be able to solve faster and better for both parties.

Using the Digital Notice of Dishonor the user gains time, and the procedure is simpler and more objective. It can be implemented in the Smart Contract, passing safety for the buyer and the seller.

It is widely known that NFTs platforms, such as OpenSea, have bugs in their system which leads maleficent people to make harm. Although NFTs are sold as being safe and secure, in real life many of them are used as tools for cybercrime, or maybe, physical crimes, as people can sell digital assets for any price, and does not imply taxes on them. Also, there are a lot of bugs on those platforms that create giant breaches for the occurrence of illegal civil acts.

In conclusion, cybersquatting in NFTs is not an easy task to solve, and it can not be surpassed by only following one criterion. It needs to have good compliance, follow the CIA criteria, and keep in mind routes of detours, such as the Digital Notice of Dishonor and time management.

Notas

[I] Law student at the University of Pernambuco, Member of the research group Smart Cities, Teachers assistant in the discipline of anthropology, member of the Penal Commission of OAB/PE

[II] Lawyer, Mastering in Law at CERS college.

[III] Doctor in Law. Doctor in Social Politics. Professor at the University of Pernambuco. Professor of post-graduation at CERS College.

[IV] As defined by the Federal Bureau of Investigation (FBI), cybercrime represents a malicious cyber activity that threatens the public's safety and national and economic security. Available at: https://www.fbi.gov/investigate/cyber Accessed on: 13 Feb 2022

[V] A limited NFTs collection where the token doubles as your membership to a swamp club for apes. The club is open! Ape in with us. Available at: https://boredapeyachtclub.com/#/ Accessed on: 13 Feb. 2022

[VI] Beeple is Mike Winkelmann, a graphic designer from Charleston, SC, USA who does a variety of digital artwork including short films, Creative Commons VJ loops, everyday and VR/AR work. After he began releasing a set of widely used Creative Commons VJ loops he has worked on concert visuals for Justin Bieber, One Direction, Katy Perry, Nicki Minaj, Eminem, Zedd, deadmau5, and many more. One of the originators of the current 'everyday' movement in 3D graphics, he has been creating a picture every day from start to finish and posting it online for over ten years without missing a single day. Available at: https://www.beeple-crap.com/about. Accessed on: 23 Feb 2022.

[VII] HUGO, Victor. Sea workers. Translation by Machado de Assis. Belo Horizonte, MG: Itatiaia, 2009

[VIII] As defined by the Federal Bureau of Investigation (FBI), cybercrime represents a malicious cyber activity that threatens the public's safety and national and economic security. Available at: https://www.fbi.gov/investigate/cyber Accessed on: 13 Feb 2022

[IX] BOLDT, Raphael. Anocratic criminal procedure? The resignification of criminal justice in the platform society. Brazilian Journal of Criminal Sciences. vol. 183. year 29. p. 227-246. São Paulo: Ed. RT, September 2021

[X] JAISHANKAR, Karuppannan. Establishing a theory of cybercrime. International Journal of Cyber Criminology, 1(2), 2007, p. 7-9. See also: JAHANKHANI, Hamid. Cyber Criminology. London: Springer, 2018 11 FAIRFIELD, Joshua, Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property (6 Apr 2021). Indiana Law Journal, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3821102

[XI] RESENDE, André Lara. The ideological straitjacket. Valor Econômico, Me & Weekend, Article, 11 Feb 2022, p. 9.

[XII] Decentralized Autonomous Organization is an autonomous organization regulated through a set of rules embedded in computer programs, technically known as smart contracts.

[XIII] BARLOW, JOHN PERRY. 'A Declaration of the Independence of Cyberspace (Electronic Frontier Foundation, 8 Feb 1996) <www.eff.org/cyberspace-independence> accessed 22 February 2022.

[XIV] BARRETO, Alesandro; KUFA, Karina. Cibercrimes e seus Reflexos no Direito Brasileiro. Editora Juspodium, 2021.

[XV] 16 CHRIS A. Huff. (2021): License and registration: how both property and contract legal frameworks fall short on interpreting domain name registration under the US Anticybersquatting Act, Information & Communications Technology Law, DOI: 10.1080/13600834.2021.1892019.

[XVI] OpenSea is an open marketplace for NFTs.

[XVII] Engadget is a blog and webpage focused on gadgets and electronics. DENT, STEVE. OpenSea faces $1 million lawsuit over stolen Bored Ape NFTs. https://www.engadget.com/open-sea-facing-1-million-lawsuit-over- stolen-bored-app-nft-133044623.html

[XVIII] Typosquatting is when 'such persons with mala fide intention might sell the registered domain name to their competitor or the owner himself at an exorbitant price; this act of persons shall be recognized as Cybersquatting.' (BHUSARI, Radhika V; RAMPURE, Karan R. 2022)

[XIX] CRAIG, TIMOTHY, CryptoBriefing, 2022 https://cryptobriefing.com/bored-ape-yacht-club-slammed-for- new-KYC-restricted-project/

[XX] CIA Criteria is a model to guide and enhance information security in organizations, which is known for being: Confidentiality, Integrity, and Availability.

References

BARLOW, JOHN PERRY. 'A Declaration of the Independence of Cyberspace (Electronic Frontier Foundation, 8 Feb 1996) <www.eff.org/cyberspace-independence> accessed 22

February 2022.

BARRETO, Alesandro; KUFA, Karina. Cibercrimes e seus Reflexos no Direito Brasileiro. Editora Juspodium, 2021.

BHUSARI, Radhika V; RAMPURE, Karan R. Cybersquatting: A threat to the globalizing world. Indian Journal of Law and Legal Research, v. 3, no. 2, 15 Jan. 2022. Available at: https://doi-ds.org/doilink/01.2022-68535724/IJLLR/V3/I2/A221. Accessed on: 14 Feb. 2022.

BOLDT, Raphael. Anocratic criminal procedure? The resignification of criminal justice in the platform society. Brazilian Journal of Criminal Sciences. vol. 183. year 29. p. 227-246. São Paulo: Ed. RT, September 2021

CBN Magazine. Understand what NFT is. Interviewer: Petria Chaves. Interviewee: Álvaro Machado Dias. RadioCBN, 29 Jan 2022. Podcast. Available at: https://www.youtube.com/watch?v=eg9XZhBvJVI. Accessed on: 13 Feb 2022.

CHRIS A. Huff. (2021): License and registration: how both property and contract legal frameworks fall short on interpreting domain name registration under the US Anticybersquatting Act, Information & Communications Technology Law, DOI: 10.1080/13600834.2021.1892019.

EUROPEAN IPR HELPDESK, Luxembourg, 2017. Available at: https://www.ipoi.gov.ie/en/commercialise-your-ip/tools-for-business/domain-name-and-cybersquatting.pdf. Accessed on: 15 Feb 2022

FAIRFIELD, Joshua, Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property (6 Apr 2021). Indiana Law Journal, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3821102

FEDERAL BUREAU OF INVESTIGATION (FBI), Internet Crime Complaint Center. 2020. Internet Crime Report, Accessed 21 Feb 2022.

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

JAISHANKAR, Karuppannan. Establishing a theory of cybercrime. International Journal of Cyber Criminology, 1(2), 2007, p. 7-9. See also: JAHANKHANI, Hamid. Cyber Criminology. London: Springer, 2018

BRANCO JUNIOR, Sérgio Vieira. Direitos autorais na Internet e o uso de obras alheias. Rio de Janeiro: Lumen Juris, 2007, p. 3. Disponível em: https://itsrio.org/wp-content/uploads/2017/01/Direitos-autorais-nainternet.pdf. Last visited 07 Apr 2022.

CRAIG, TIMOTHY, CryptoBriefing, 2022 https://cryptobriefing.com/bored-ape-yacht-club-slammed-for-new-KYC-restricted-project/

DARA B. GILWIT, The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How to Prevent Public Deception and Trademark Infringement, 11 Washington University Journal of Law & Policy (2003).