


The Regulation of Money Laundering and Corporate Criminal Responsibility in Spain: compliance as a key for Virtual Asset Service Providers

La regulación de blanqueo de capitales y la responsabilidad penal de la persona jurídica en España: compliance como clave para los proveedores de servicio con activos virtuales

Ayelén Anzola¹

Universidad de Salamanca, Salamanca, España


anzola@usal.es


 <https://orcid.org/0000-0001-7416-6108>

Marina Oliveira Teixeira dos Santos²

Universidad de Salamanca, Salamanca, España

marinaoliveira.737@gmail.com

 <http://lattes.cnpq.br/5631870315520284>

 <http://orcid.org/0000-0002-3276-2590>

-
- ¹ Professora investigadora na *Universidad Nacional del Nordeste*, Argentina. Doutoranda na *Universidad de Salamanca*. Bolsista do programa para estudantes latino-americanos USAL-Santander. Investigadora em formação no *Centro de Investigación para la Gobernanza Global* (CIGG) da *Universidad de Salamanca*. Mestre em Estratégias Anticorrupção e Políticas de Integridade pela Universidade de Salamanca y Mestre em Direito Administrativo pela Universidade Austral de Argentina.
- ² Doutoranda na *Universidad de Salamanca*. Contratada *predoctoral* financiada com cargo à convocatória de *contratos predoctorales* USAL 2021, cofinanciada pelo Banco Santander. Investigadora em formação no *Centro de Investigación para la Gobernanza Global* (CIGG) da *Universidad de Salamanca*. Mestre em ciências-jurídico criminais pela Universidade de Coimbra. Graduada em Direito pela Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo. Advogada OAB/SP. Membro do Projeto de Pesquisa I+D “*Configuración y efectos de los sistemas de Gestión del riesgo legal*” do Ministério de Ciência e Inovação espanhol, com a referência PID2019-107743RB-I00.

ABSTRACT: Initiating with the conceptualization of who are Virtual Asset Service Providers (hence forward: exchangers), especially the ones who work with virtual exchangeable assets, this paper aims to study the high risk their activities suppose on increasing money laundering and what are Spain's legal framework on money laundering and if they can be enforced on exchangers, based not only on the national legislation but also on the European Union's existing directives on the subject. Moreover, it will be analysed the role of compliance as a practical procedure tool to prevent money laundering in exchangers activities and how the current legislation in Spain already promotes that, as the current criminal law extinguishes responsibility of legal persons who demonstrate an effective compliance program if they fulfil all requisites. Hence, this paper will be able to make a comprehensive study on exchangers, who they are and what are their activities as regulated in Spain's legal framework. Therefore, is going to answer the investigation's main question regarding the role of compliance to deter money laundering in this focus group.

KEYWORDS: Virtual Asset Service Providers; Exchangers; Money laundering; Spain; Compliance.

RESUMEN: *A partir de la conceptualización de los Proveedores de Servicios de Activos Virtuales (en adelante: exchangers), especialmente de aquellos que trabajan con activos virtuales intercambiables, este trabajo pretende estudiar el alto riesgo que sus actividades suponen en el incremento del blanqueo de capitales, cuál es el marco legal español sobre el blanqueo de capitales y si éste se puede aplicar a los exchangers. Para ello, la investigación se ha basado no sólo en la legislación nacional sino también en las directivas de la Unión Europea existentes en la materia. Además, se analizará el papel del compliance (o cumplimiento normativo) como herramienta de procedimiento práctico para prevenir el blanqueo de capitales en las actividades de los exchangers destacando los mecanismos mediante los cuales la legislación actual en España ya lo promueve, puesto que el derecho penal vigente extingue la responsabilidad de las personas jurídicas que demuestren un programa de compliance efectivo si cumplen todos los requisitos impuestos por ley. De este modo, este trabajo pretende realizar un estudio exhaustivo sobre los exchangers, determinando quiénes son y cuáles son sus actividades reguladas en el marco legal español. En resumen, intentará responder a la pregunta principal de la investigación sobre el papel del compliance para prevenir el blanqueo de capitales en este sector.*

PALABRAS CLAVE: *Provedores de Servicios con Activos Virtuales; Casas de Cambio; Blanqueo de Capitales; España; Programas de cumplimiento normativo.*

SUMMARY: Introduction and Methodology; 1. Who are the virtual asset service providers? The European Union and Spain's restrictive approach. 2. Money laundering regulatory framework regarding virtual asset service providers; 3. Compliance as an effective solution; 3.1. Comments on the corporate compliance culture applied to virtual asset service providers; 3.2. Criminal benefits of a compliance program; Conclusions; Bibliography and References.

INTRODUCTION AND METHODOLOGY

Virtual Asset Service Providers, also known as exchangers, are the ones who make transactions with virtual assets and offer certain services to clients. Specifically, in this paper, it will be analysed the activities perpetuated by Virtual Asset Service Providers who deal with virtual exchangeable assets, which includes, for instance, individuals and enterprises who provide exchange services online, by doing online transactions and trading virtual assets that may be or will be converted to real coin for a client.

It is an important and ever-growing activity in contemporary's globalized world, that affects not only specific shareholders from these enterprises, as well as all stakeholders, governments and society included, as consumers and possibly victims of grand money laundering offences perpetuated within this structure.

This activity is a natural evolution of the regular exchange service provided in physical stores for people who needed to trade coins. With the consolidation of the internet and the technological era, they transformed themselves – or were substituted by new ones – in order to become virtual asset service providers.

With the natural chain formed by the online exchange and trade of assets on the internet, new risks began to appear, adding to the already existing ones, related to the high possibility of money laundering.

This paper aims to answer the following questions: is the ruling provided in Spain's context the best on preventing money laundering in virtual asset service providers who deal with virtual exchangeable assets? Is compliance a practical and efficient tool that should be enforced on these exchangers in order to prevent money laundering? How does the current legal framework that exists in Spain already promotes the existence of effective compliance programs?

Therefore, the hypothesis states a presumed relationship between three dependent variables: a) the risk of money laundering in virtual exchangers activities; b) the adequacy or insufficiency of traditional anti-money laundering measures; and c) compliance as a solution.

Based on the whole outline previously traced, the focus group will be Spain's virtual asset service providers who work with virtual exchangeable assets that are subject to Spain's jurisdiction. Moreover, relying on compliance and corporate governance concepts, the existing and current legislation from Spain and the European Union will be analysed – this one in accordance with the Financial Action Task Force's (FATF) recommendations on anti-money laundering measures, and basing on the existing Spanish model of criminal responsibility for legal persons, in order to constitute a global view on how virtual asset service providers that deal with virtual exchangeable assets are currently regulated.

It will be conducted a bibliographical and legislative investigation to answer this paper's question. We will focus on Spain's regulation on money laundering; the existing normative that makes a legal person criminal liable, and the specific associated risks related to virtual asset service providers activities. In addition, this paper's methodology is based on the analysis of legislation and doctrine aiming to corroborate the hypothesis through the deductive method.

1. WHO ARE THE VIRTUAL ASSET SERVICE PROVIDERS? THE EUROPEAN UNION AND SPAIN'S RESTRICTIVE APPROACH

From the point of view of money laundering regulation, Virtual Asset Service Providers-related activities have been considered especially risky. In this regard, it has been seen that the sophistication, complexity, and professionalism employed for money laundering techniques have led

the perpetrators of such crimes to adopt new mechanisms in which the laundering procedure could be carried forward quicker and more opaquely³. To do this, they have used cyberspace, thus generating the migration from the traditional crime of money laundering to this new scope⁴.

Cyberspace is the electronic medium of the digital networks used for storing, communicating, and modifying information. This definition includes the Internet and information systems that support business, infrastructure, and services. This new space of interaction presents defining characteristics such as: the transnationality, time alteration, network neutrality⁵, anonymity, dynamism, and change⁶. The consolidation of cyberspace, at the same time as it has been favoured by the interconnection between people, has allowed the emergence of a new market and new digital goods. To make possible the operations in this new area, it was necessary to digitally represent the goods or assets that are the object of these transactions. This is how the token was born, and with it, what was later called the tokenization of economy, referring to the revolution that has caused this phenomenon.

The token is the digital representation of value that may or may not be linked to an underlying asset. It consists of an alphanumeric code that uses the blockchain as a backup technology for its activity. The Blockchain is a type of distributed ledger technology that works as a decentralized registry. It was created by Satoshi Nakamoto, an anonymous

³ BLANCO CORDERO, Isidoro. *El delito de blanqueo de capitales*. Cizur Menor: Aranzadi, 2002, p. 51. SAVONA, Ernesto; ADAMOLI, Sabrina; ZOFFI, Paola. Organised crime across the borders. Preliminary results. *HEUNI Papers*, v. 6, p. 24, p.1-53, 1995. Available at <<https://www.heuni.fi/en/index/publications/heunipapers.html>>. Accessed 24 nov. 2020; FABIÁN CAPARRÓS, Eduardo. *El delito de blanqueo de capitales*. Madrid: Colex, 1998, p. 233.

⁴ MIRÓ LLINARES, Fernando. La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista electrónica de ciencia penal y criminología*, v. 7, n. 13, p. 1-55, 2012. MIRÓ LLINARES, Fernando. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Barcelona: Marcial Pons, 2012, p. 47-84.

⁵ ÉCIJA BERNAL, Álvaro. *Ciberespacio, Dark Web y Ciberpolicía*. *Diario La Ley*, v. 2 (Sección Ciberderecho), p. 1-5, 2017.

⁶ López Torres, Jonathan. *Ciberespacio & ciberseguridad. Elementos esenciales*. Valencia: Tirant lo Blanch, 2020, p. 29.

author whose goal was to create a new alternative, decentralized, secure and private means of payment.⁷ To do so, he based his work on two older technological tools: a. cryptography, as an alternative source of trust; and b. peer-to-peer networks, that are the mechanism through which information is stored, distributed, or decentralized in the nodes⁸.

In this regard, the technological support of virtual assets has an important role to play amidst the analysis of anti-money laundering measures effectiveness on these specific assets. While in traditional financial systems, trust is centralized or guaranteed by a central bank or regulators to avoid double payment or money authenticity problems, with tokens, trust is cryptographically guaranteed through two mechanisms: data mining or complex mathematical problem solving and, secondly, consensus mechanisms through which it is possible to validate the operation or check which algorithm has been solved according to the protocols that regulate the virtual asset. The distributed trust has led to the disappearance of the central authorities as necessary intermediaries, involved in traditional payment mechanisms. Somehow it has been replaced by cryptographic trust.

Despite the previous affirmations about the decentralized and distributed trust – and the consequent absence of a central authority’s control- it needs to be underlined that it doesn’t mean that there are no intermediaries on virtual asset’s operations. Its main characteristic is that virtual assets only need the nodes⁹ and the customers to operate.

⁷ GARCÍA MEXÍA, Pablo. Del ciberderecho al criptoderecho. In: GARCÍA MEXÍA, Pablo (org.). *Criptoderecho. La Regulación de Blockchain*. Madrid: Wolters Kluwer, 2018, p.78.

⁸ GARCÍA MEXÍA, Pablo; ARANDA BRIONES, Beatriz; ALCAIDE SOLER, Francisco; BAENA ZAPATERO, Rafael; CODES CALATRAVA, Alfonso; GARCÍA ESPINAR, Eduardo; MENÉNDEZ ARIAS, María José; et al. *Criptoderecho. La Regulación de Blockchain*. Madrid: Wolters Kluwer, 2018, p. 78-79 and 363-410; LIN, luon-Chang; LIAO, Tzu-Chun. A survey of blockchain security issues and challenges. *International Journal of Network Security*, v. 19, n.5, p. 653-659, 2017.

⁹ “En la tecnología Blockchain se utilizan un conjunto de protocolos y técnicas criptográficas gracias a los cuales los datos de la aplicación y los registros de operación se constituyen como una cadena de bloques de información unidos entre sí de forma descentralizada y pública, almacenándose en unos equipos interconectados a través de una red de ordenadores distribuidos, los nodos, para

On the other hand, in traditional systems, its own centralized structure needs the customers, the financial institutions, the central bank or a central authority -that controls double payment or authenticity problems- to operate.

It should be underscored that the disappearance of these intermediaries on virtual assets has caused a deterrence problem of law. Because in the field of virtual assets there is an anti-money laundering regulation, but the subjects to whom these norms are imposed no longer are necessarily present on virtual transactions. In this disintermediation scheme, we can find the virtual asset service providers, who are not needed to make a transaction with the virtual assets, but could appear under certain circumstances offering specific products to the customers. The exchangers or virtual asset service providers are individuals or enterprises that provide many services related to virtual assets. These services may involve the creation of wallets and the management of its public and private keys¹⁰, virtual asset storage, ease of exchange operations, and several other services¹¹.

The FATF's¹² recommendations follow a broad approach towards Virtual Asset Service Provider's definition. According to the recent guide published in 2019, a Virtual Asset Service Provider is:

evitar cualquier punto central de fallo." (MORALES BARROSO, José. "¿Qué es Blockchain?". In: GARCÍA MEXÍA, Pablo (org.). *Criptoderecho. La regulación de Blockchain*. España: Wolters Kluger, 2018, p. 43).

¹⁰ ANZOLA, Ayelén. La ejecución de las resoluciones de decomiso de Activos Virtuales en España. *Revista General de Derecho Procesal*, v. 57, p. 9, 2022.

¹¹ GUAITA MARTINEZ, José Manuel; CARRACEDO GARNATEO, Patricia; ISIDRO NUÑEZ, Francisco. *Las criptomonedas: Digitalización del dinero 2.0*. Cizur Menor: Aranzadi, 2019, p. 63.

¹² FATF (or GAFI) is the financial Action Task Force, also known by its French name, *Group d'action financière*. It is an inter-governmental body that sets international standards to prevent money laundering and terrorist financing by establishing recommendations or standards that must be implemented by members fully and effectively. As not complying with FATF's recommendation leads to warnings and being held accountable. However, it needs to be stated that FATF's recommendations are soft law in its nature, as they do not state an obligation (FATF, Financial Action Task Force. Available at <www.fatf-gafi.org/about>. Accessed 22 nov. 2020).

(...)any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- i. Exchange between virtual assets and fiat currencies;
- ii. Exchange between one or more forms of virtual assets;
- iii. Transfer of virtual assets;
- iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets and
- v. Participation in and provision of financial services related to an issuer's offer and/or sale of virtual assets.¹³

More specifically, regarding money laundering, the Directive 2018/843¹⁴ 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 purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU- have already included virtual asset service providers as obligated subjects. For instance, article 2 includes as obligated entities: providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers. In this sense, this regulation includes definitions according to the FATF's recommendation mentioned above, section i. and iv.:

(...) virtual currencies means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically [and] custodian wallet provider means an entity that provides

¹³ FINANCIAL ACTION TASK FORCE, FATF. *Guidance for a risk-based approach. Virtual assets and virtual asset service providers*. Paris: FATF, 2019, p.13.

¹⁴ Also known as the fifth anti-money laundering Directive.

services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies¹⁵.

Despite the progress achieved by this regulation, it needs to be pointed out that this norm has a limited view compared to FATF's recommendation. Besides that, there are many other activities not included such as the exchange of a virtual asset to another virtual asset¹⁶, or the participation in and provision of financial services related to an issuer's offer and sale.

Spain has already transposed the Directive UE 2018/849 into national law through the Royal Decree-Law 07/2021¹⁷. However, and as it is still going to be more specifically treated along this article, this transposition is almost an exact text transcription of the European Regulation, which means that Spain has followed the restrictive European Union's guideline on the subject.

Finally, it should be noted that there is still uncertainty regarding the Virtual Assets regulation that affects the legal qualification of virtual asset service providers. Although virtual assets can be compared to currencies or securities, in Spain they do not have this legal qualification. As it is expressly stated in Law 10/2010, virtual assets are not legally considered as currency or money as it is a means of exchange. Therefore, despite the very high turnover of values within the VASPS, they are not legally considered as financial entities and the payment services rules or similar do not apply to them. However, there is legal certainty concerning the fact that the virtual asset service providers are obligated subjects by

¹⁵ EUROPEAN UNION. Directive (EU) 2018/849 of the European Parliament and of the Council of 30 May 2018. Available at <<https://eur-lex.europa.eu/eli/dir/2018/849/oj>>. Accessed 23 oct 2020.

¹⁶ Although if we make a broad interpretation of Directive EU 2018/849, Article 2, we could conclude that "transferring virtual assets" also covers the exchange of virtual assets. However, in our opinion, this activity should have been specifically stated.

¹⁷ SPAIN. *Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores*. Available at <<https://www.boe.es/buscar/doc.php?id=BOE-A-2021-6872>>. Accessed 16 sep. 2022.

Law 10/2010 and that their inclusion in this legal framework enforce them to comply with the obligations it imposes.

2. MONEY LAUNDERING REGULATORY FRAMEWORK REGARDING VIRTUAL ASSET SERVICE PROVIDERS

Money laundering can be perceived as the act of “concealing the origins of money linked to crime or otherwise attempting to diminishing the connection between property and some criminal undertaking”¹⁸. It became a worldwide problem, and the construction of international norms began in the end of the 80’s with an agreement of states to penalize money laundering, even though initially limited to the scope of illegal drugs¹⁹. The importance to deter money laundering in a global way grew and with it appeared the most important Conventions that tried to deal with it in an international approach: International Convention for the Suppression of the Financing of Terrorism, 1999; Convention Against Transnational Organized Crime, 2000; Convention Against Corruption, 2003. Moreover, it is with a non-state actor, the Financial Action Task Force (FATF) that the formation of national and regional regulation begins to be shaped. As stated by Gallant, “most states equate the voice of the FATF with the authoritative voice of international law”²⁰. The European Union is part of the narrated context and has anti-money laundering measures as one of its priorities: in the last twenty years there have been numerous initiatives in this area, among which we would like to highlight the following three money laundering directives, from 1991, 2001 and 2005.

Therefore, money laundering is the process that consists in the integration of criminal assets into the legal economic system as if they were

¹⁸ GALLANT, Michelle. Money Laundering consequences. Recovering wealth, piercing secrecy, disrupting tax havens and distorting international law. *Journal of Money Laundering Control*, v. 17, n. 3, p. 302, 2014.

¹⁹ As can be perceived by the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances from 1988.

²⁰ Gallant, Michelle. Money Laundering consequences: Recovering wealth, piercing secrecy, disrupting tax havens and distorting international law. *Journal of Money Laundering Control*, v. 17, n. 3, p. 302, 2014.

obtained lawfully²¹. Moreover, criminal conducts categorized as money laundering by Spain's Penal Code consist on the acquisition, possession, use, conversion, transmission or on the performance of any other action aiming to cover up the illicit origin of the goods, implying dynamic conducts.

From an international law's point of view, Spain has acceded to several hard law international agreements, such as: The United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, adopted in Vienna on 19 December 1988; The United Nations Convention against Transnational Organized Crime, adopted in Palermo on 15 November 2000; The United Nations Convention against Corruption, adopted in Mérida on 31 October 2003; Council of Europe's Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, adopted in Strasbourg on 08 November 1990; Council of Europe Convention on the Prevention of Terrorism, adopted in Warsaw on 16 May 2005.

Regarding European Community Law, currently are in effect the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and its amending Directive (EU) 2018/849 of the European Parliament and of the Council of 30 May 2018, which has been transposed in Spain by Royal Decree 7/2021; and the Directive 2018/1673 of the European Parliament and of the Council of 23 October 2018, on combating money laundering by criminal law, that in Spain led to the adoption of LO 06/2021 amending Organic Law 10/1995, of 23 November, Penal Code.

Hence, in Spain coexist two different legal frameworks with different functions on money laundering regulation. Aiming to prevent criminal conduct, administrative law sets a frame through Law 10/2010. Its main proposal is to enforce compliance measures on certain subjects, while also establishing administrative bodies to control their activities. Secondly, money laundering is treated by criminal law on articles 301 and following of Spain's Penal Code. Despite that, there are cases of more severe penalties under certain circumstances, and it is a crime that can be committed by any natural or legal person.

²¹ BLANCO CORDERO, Isidoro. *El delito de blanqueo de capitales*. Cizur Menor: Aranzadi, 2002, p. 93.

Regarding the criminal and administrative systems mentioned before, it needs to be pointed out that while administrative sanctioning procedures can be directed against both human and legal persons, the criminal system only allows the punishment of legal persons under the cases explicitly set by law on article 31 bis and following of Spain's Penal Code.

In this context, it should be noted that Spain's money laundering crime can be assigned to enterprises due to the stipulated on article 302, 2, of its Penal Code, according to which an enterprise or company, legally constituted as a legal person²², can be criminally liable by a money laundering offense and penalized with a criminal fine from two to five years, if the crime committed by the natural person provides a prison term of more than five years and, in other cases, a penal fine from six months to two years. They can also be penalized with its dissolution, suspension for less than five years, enclosure of certain premises, prohibition of practicing certain activities, disqualification for contracting and receiving economic help from the government and judicial intervention for a maximum of five years, in the cases and according to the rules stipulated on art. 66 bis²³. In line with Spain's regulation, it is important to say that all enterprises defined as a legal person can be criminally prosecuted, including state's mercantile societies, except the State, its public administrations, and other entities stated on article 31 *quinquies*²⁴.

Due to the activities developed by virtual asset service providers, which involve the exchange of virtual assets to fiat currencies, the European Union has remarked the need to reinforce these subjects to the current anti-money laundering regulations. This was set in line with the FATF's interpretative note on the 15th recommendation regarding new

²² "Legal person" as the terminology used in FAFT's recommendation. In Spain the term used is "persona jurídica". GRUPO DE ACCIÓN FINANCIERA - FATF/GAFI. *Guidance for a risk-based approach. Virtual assets and virtual asset service providers*. Paris: FATF, 2019, p.13.

²³ Related to its necessity to prevent money laundering, social and economic consequences to its employees and the position occupied in the company by de individuals who did not comply with its control duties.

²⁴ Spain's Penal Code, art.31 (SPAIN. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Available at < <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>>. Accessed 15 sep 2022).

technologies²⁵, and has been widely accepted in the Spanish legal system. Accordingly, the most part of the issues derived from this recommendation are already part of its national law, including the following:

Table 1: Comparison between FATF’s interpretative note to the 15th recommendation and of Spain’s National Law.

FATF interpretative note to the 15th recommendation

- Countries should consider virtual assets as “property,” “proceeds,” “funds,” “funds or other assets,” or other “corresponding value”.

Countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of virtual asset service providers. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. - Countries should require virtual asset service providers to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.

Spain’s National Law

There is still no certainty about virtual asset’s legal status. However, as it has stated by Law 10/2010, virtual currencies are accepted as a means of exchange. It is considered by some legal doctrine as digital movable property²⁶.

In accordance with this, the Directive UE 2018/843 has stated some risks and measures to prevent them²⁷. For instance, the pseudo anonymity²⁸ of the users or clients can be solved by the implementation of remote mechanisms based on real identification. Anonymity is closely related to red flags because it allows virtual asset service providers to develop other measures related to anti-money laundering legislation, such as “know your client” or “Customer Due Diligence”. The lack of knowledge about the client’s real identity forces virtual asset service providers to operate blindly, placing them in a dangerous position in the face of money laundering among other crimes.

²⁵ GRUPO DE ACCIÓN FINANCIERA - FATF/GAFI. *Guidance for a risk-based approach. Virtual assets and virtual asset service providers*. Paris: FATF, 2019, p. 27.

²⁶ VELASCO NÚÑEZ, Eloy. *Aspectos jurídicos penales vinculados al blockchain y las criptomonedas: delito fiscal, blanqueo de capitales, robo, estafa*. Madrid: Servicio de formación continua – Consejo general de Poder Judicial, 2019, p. 6.

²⁷ In line with FATF 2020 guideline (FATF/GAFI. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*. Paris: FATF, 2020).

²⁸ NAVARRO CARDOSO, Fernando. *Criptomonedas (en especial, bitcoin) y blanqueo de dinero*. *Revista electrónica de ciencia penal y criminología*, n. 21,

The Directive mentioned above, also obligates virtual asset service providers to identify suspicious activity. However, this ruling clearly states that the anonymity of virtual assets will prevent a complete assessment of risky activities and therefore, the service of the national Financial Intelligence Units “should be able to associate virtual currency address to the identity of the owner of the virtual currency”. Furthermore, it stipulates an assessment of the risks of money laundering to be conducted by the Commission and by each Member-State, that shall have its own authority designated to that end.²⁹

p. 19, p. 1-45, 2019. Available at <<http://criminet.ugr.es/recpc>>. Accessed 20 nov 2020.

²⁹ Besides risks related to Virtual Asset Service Provider’s activities, there are some specific risks regarding the use of virtual assets, such as its anonymity in the blockchain, the distributed and decentralized ledger technology, transnationality, or currency convertibility. LIN, Iuon-Chang; LIAO, Tzu-Chun. A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, v.19, n. 5, p.653-659, 2017; PÉREZ LÓPEZ, Xesus. Las criptomonedas: consideraciones generales y empleo de las criptomonedas con fines de blanqueo. In: FERNÁNDEZ BERMEJO, Daniel (org.). *Blanqueo de Capitales y TIC: Marco Jurídico Nacional y Europeo, Modus Operandi y Criptomonedas. Ciberlaundry. Informe de situación*. Cizur Menor: Aranzadi, 2019, p. 71-140; PASCUA MATEO, Fabio. Criptomonedas. In: GARCÍA MEXÍA, Pablo (ed). *Criptoderecho. La Regulación de Blockchain*. Madrid: Wolters Kluwer, 2018, p. 363-410; NAVARRO CARDOSO, Fernando. Criptomonedas (en especial, bitc oin) y blanqueo de dinero. *Revista electr onica de ciencia penal y criminolog a*, n. 21, p. 25, p.1-45, 2019. Available at <<http://criminet.ugr.es/recpc>>. Accessed 20 nov. 2020; GUAITA MARTINEZ, Jos  Manuel; CAR-RACEDO GARNATEO, Patricia; ISIDRO NU EZ, Francisco. *Las criptomonedas: Digitalizaci n del dinero 2.0*. Cizur Menor: Aranzadi, 2019, p. 63; GRUPO DE ACCI N FINANCIERA, FATF. *Directrices para un enfoque basado en riesgo: Monedas virtuales*. Paris: FATE, 2015.

- Virtual asset service providers should be required to be licensed or registered. At a minimum, virtual asset service providers should be required to be licensed or registered in the jurisdiction where they are created. In cases where the virtual asset service

Accordingly, the second additional provision of the Real Decree 7/2021³⁰ requires virtual asset service providers to enroll in a registry set up for this purpose within the Bank of Spain, established that any legal or natural person of any nationality offering or supplying the

³⁰ By the transposition of Directive 2018/843 facilitated by the Real Decree 7/2021, that amends Law 10/2010 by adding on, as previously mentioned, not only including exchangers that deal with virtual assets, but also distributing the responsibility of regulating and supervising money laundering to a national authority specifically designated. (Available at <<https://www.boe.es/buscar/act.php?id=BOE-A-2021-6872>>. Accessed 16 sep 2022). This obligation has been established in accordance to Article 47 of the Directive (UE) 2018/843. In its original version: “*Disposición adicional segunda: Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos. 1. Las personas físicas o jurídicas que, cualquiera que sea su nacionalidad, ofrezcan o provean en España servicios de los descritos en los apartados 6 y 7 del artículo 1 de la ley, deberán estar inscritas en el registro constituido al efecto en el Banco de España. 2. Se inscribirán asimismo en el registro: a) las personas físicas que presten estos servicios, cuando la base, la dirección o la gestión de estas actividades radique en España, con independencia de la ubicación de los destinatarios del servicio. b) Las personas jurídicas establecidas en España que presten estos servicios, con independencia de la ubicación de los destinatarios. 3. La inscripción en el registro estará condicionada a la existencia de procedimientos y órganos adecuados de prevención previstos en esta ley y al cumplimiento de los requisitos de honorabilidad comercial y profesional en los términos del artículo 30 del Real Decreto 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. El incumplimiento de los requisitos de honorabilidad determinará la pérdida de la inscripción en el registro. 4. El Banco de España será competente para supervisar el cumplimiento de la obligación de registro y de las condiciones de honorabilidad exigidas para el acceso y mantenimiento de la inscripción. 5. La prestación de los servicios descritos en el apartado 1 sin contar con el preceptivo registro tendrá la consideración de infracción muy grave, pudiendo ser considerada como grave si la actividad se hubiera desarrollado de forma meramente ocasional o aislada, y será sancionada por el Banco de España de conformidad con lo dispuesto en las normas en materia de sanciones, de procedimiento y las relativas al régimen de publicidad que forman parte del título IV de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito”.*

providers are natural persons, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require virtual asset service providers that offer products or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a virtual asset service provider. Countries should take action to identify natural or legal persons that carry out Virtual Asset Service Provider activities without the requisite license or registration, and apply appropriate sanctions.

- Virtual asset service providers should be subject to effective systems for monitoring and ensuring compliance with national anti-money laundering requirements. They should also be supervised or monitored by a competent authority which should conduct risk-based supervision or monitoring. It excludes the possibility of self-regulation. Supervisors should have adequate powers to supervise or monitor and ensure compliance by

following services³¹ in Spain must be enrolled in the registry set up for this purpose at the Bank of Spain:

- Exchange of virtual currency into fiat currency.
- Cryptographic key safekeeping or custody services on behalf of its customers for the holding, storage and transfer of virtual currencies.

To sum up, registration of natural persons providing these services is also mandatory when they settle their activity, the address or administration in Spain, regardless the location of the customers receiving the service. The same rule applies to legal persons that provide these services and are established in Spain.

Since the inclusion of the vaspas to the law 10/2010, they are subject to the administrative bodies for the prevention on money laundering. Specifically, they are subject to the commission for the prevention of money laundering; to the secretary of the commission; and to the SEPBLAC, which is the FIU of Spain.

³¹ Law 10/2010, April 28, for the prevention of money laundering and terrorist financing, art. 1.6 y 1.7. (SPAIN. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Available at < <https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737>>. Access 16 sep 2022).

virtual asset service providers with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the virtual asset service providers' license or registration, where applicable.

- Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with the virtual asset service providers that fail to comply with anti-money laundering requirements, in line with Recommendation 35. Sanctions should be applicable not only to the virtual asset service providers, but also to their directors and senior management.

- Finally, it strengthens international cooperation. In particular, it provides that supervisors must share information "rapidly, constructively and effectively" with their foreign counterparts regardless of the supervisor's nature or status and differences in virtual asset service provider's nomenclature or status.

As it was analyzed before, in Spain coexist two different legal frameworks aiming to prevent and punish money laundering. It is also important to mention that according article 31 bis and 301 and following of its Penal Code, this legal framework applies to both legal and natural persons. It also needs to be underscored that Law 10/2010 established compliance programs applied to virtual assets service providers according to articles 26, 26 bis and following.

Among other provisions in this area, it is important to highlight that the Directive EU 2018/849 provides the establishment of a central registry for data consultation and several times mentions the cooperation and the sharing of information between the member states's FIUs.

Note: The table shows a comparative summary between the FATF's interpretative note to the 15th recommendation and Spain's National Law.

In conclusion, we have seen that most of the FATF recommendations are based on the fundamentals of compliance. This is an approach that

Spain has also adopted through Law 10/2010 by requiring obliged parties to adopt a prevention program (art. 26), an anonymous whistleblower channel (art. 26 bis) or the figure of a compliance officer (26 ter.), among others.

3. COMPLIANCE AS AN EFFECTIVE SOLUTION

3.1. COMMENTS ON THE CORPORATE COMPLIANCE CULTURE APPLIED TO VIRTUAL ASSET SERVICE PROVIDERS

The idea of compliance as corporate governance emerges from the realization that the State's formal instances of control cannot monitor and directly regulate every enterprise, company, and private initiative³². Therefore, the concept of compliance surfaces inside the notion of a (good) corporate governance, as a necessary support for its maintenance and sustainability. Compliance derives³³ from the verb “comply”, which means to act according to an order, set of rules, or requests and, specifically in compliance's case, to observe what is demanded by the legal system or even by rulings that do not have a legal nature but must be followed, such as ethical and moral guidelines³⁴.

From this description, Adan Nieto Martín's comment on the cloudy nature of the term “compliance” gains strength. He points out that compliance is one of the most inexpressive terms, as by itself means act according to the legality. However, it becomes something complex by the time it is verified how it behaves inside a company, as somewhat more

³² Miranda Rodrigues explains that the lack of supervision related to neoliberal politics could not prevent a number of financial scandals, whereas the proposals of self-regulation based on corporate governance and compliance constituted a way out of the eminent crisis (MIRANDA RODRIGUES, Anabela. *Direito penal económico – fundamento e sentido da aplicação das penas de prisão e de multa. Revista do Ministério Público*, v. 151, p. 12, p.11-34, 2017).

³³ Cambridge Dictionary. Available at <www.dictionary.cambridge.org>. Accessed 22 nov. 2020.

³⁴ ENGELHART, Marc. The nature and Basic Problems of compliance Regimes. *Max-Planck-Institut für ausländisches und internationales Strafrecht*, p. 2, 2018. Available at <https://pure.mpg.de/rest/items/item_2643714_7/component/file_3007899/content>. Accessed 22 nov. 2020.

than just plain legal conformity³⁵. Although it is not easy to establish a common pattern of compliance programs for all companies, as each and every one of them will have its own peculiarity that might lead to different risks, it is possible to draw some basic objectives that can be applied in general³⁶. Therefore, Cigüela Sola³⁷ and Sieber³⁸ both propose that a compliance program must define the enterprise's values and objectives that must be respected, based on its risk and on the demands of the public sphere and by creating training programs for its own employees about the prevention mechanisms implemented. Moreover, in general, compliance programs determines that the company: names someone responsible for the risk assessment, known as the compliance officers; establishes an effective documentation system and rules of conduct; institutionalizes a specialized organ, a lot of times named "compliance department", that contains information, material and it is autonomous enough so as to manage and watch out the compliance programs as well as train employees, delegate functions and facilitate a periodic control by external controllers, as by specialized auditory companies. Within this compliance program, it is convenient the creation of information systems

³⁵ NIETO MARTÍN, Adán. Problemas Fundamentales del Compliance y el Derecho Penal. In: KUHLEN, Lothar; MONTIEL, Juan; ORTIZ, Iñigo. (org.). *Compliance y teoría del derecho Penal*. Madrid: Marcial Pons, 2013, p.21-50, p.23.

³⁶ Since 1950 there are several rulings and initiatives that try to elaborate the best "compliance" actions, even though it hasn't always been called "compliance". From rulings elaborated by ISO and UNE, there is a complex system that each company must apply to its own scenario with the realization that apart from all the specifics determinations, the two most important elements is the transparency with which the company elaborates its own ruling and the existence of verification by external auditors (RODRÍGUEZ-LOPEZ, Fernando; SÁNCHEZ-MACÍAS, José Ignacio. Normalización y certificación en compliance, de la autoregulación al valor social. In: In: RODRÍGUEZ-GARCÍA, Nicolás; RODRÍGUEZ-LOPEZ, Fernando (org.). *Compliance y Responsabilidad de las Personas Jurídicas*. Valencia: Tirant lo Blanch, 2021, p.461-494, p.490).

³⁷ CIGÜELA SOLA, Javier. *La culpabilidad colectiva en el derecho penal: crítica y propuesta de una responsabilidad estructural de la empresa*. Madrid: Marcial Pons, 2015, p. 343-344.

³⁸ SIEBER, Ulrich. Programas de compliance en el derecho penal de la empresa. Una nueva concepción para controlar la criminalidad económica. In: ARROYO ZAPATERO, Luis; NIETO MARTÍN, Adán (org.). *El derecho penal económico en la era compliance*. Valencia: Tirant lo Blanch, 2013, p.63-110, p. 75.

thought for discovery and clearing of crimes, in which the anonymous reporting is permitted and even stimulated and the infractions that do not constitute crime are proportionally punished internally by disciplinary measures. To sum up, compliance within a company must mean: a change of culture that incorporates the anti-corruption ideal, more transparency and ethic, trainings, integrity throughout the enterprise's chain, multiple regulations, internal control and external audits and a disclosure culture³⁹.

The arise of a corporate compliance culture might have started, as adverted by Laufer, in the Foreign Corrupt Practices Act from 1977 and several of the reforms made in the end of the 1970's in the United States of America that planted corporate governance⁴⁰. This structure of corporate governance is the one that has been implemented by Spain's regulation on exchangers regarding the prevention of money laundering⁴¹.

It is thanks to the establishment of rulings and orders that exchangers that worked in Spain, with fiat currencies were obligated to constitute a structure similar to a "corporate compliance", based on the constitution of an internal organ responsible for the assessment of risk, training of employees, communication with the authorities and prevention of crime, in this case, money laundering.

³⁹ CIGÜELA SOLA, Javier. *La culpabilidad colectiva en el derecho penal: crítica y propuesta de una responsabilidad estructural de la empresa*. Madrid: Marcial Pons, 2015, p.343-344.

⁴⁰ LAUFER, William. *Corporate bodies and guilty minds. The failure of corporate criminal liability*. Chicago: The University of Chicago Press, 2006, p.30.

⁴¹ It must be noticed that corporate compliance also gains strength by the carrot and stick strategy that aims to recompense good practices (by the means of corporate compliance) with the penal sanctioning of enterprises, located specially in Europe. By the menace of penal sanctions to enterprises (whereas in a hetero-responsibility model or a self-responsibility one) and the legal possibility to not penalize enterprises that demonstrate the existence of an effective compliance program within its structure, companies are stimulated to implement and maintain a real compliance program (NIETO MARTÍN, Adán. Problemas Fundamentales del Compliance y el Derecho Penal. In: KUHLEN, Lothar; MONTIEL, Juan; ORTIZ, Iñigo. (org.). *Compliance y teoría del derecho Penal*. Madrid: Marcial Pons, 2013, p.21-50, p.15-21. CIGÜELA SOLA, Javier. *La culpabilidad colectiva en el derecho penal: crítica y propuesta de una responsabilidad estructural de la empresa*. Madrid: Marcial Pons, 2015, p.349-350).

In Spain there were already some rulings regarding the formation and procedure of exchangers since 1998⁴². However, it is only by 2006 that Spain commences to regulate exchangers specifically with the intent of preventing money laundering, precisely with Order EHA/2619/2006, issued by the Ministry of Economy and Treasury⁴³. This order is structured around the increment on exchangers activities in Spain due to the increase of alien residents and tourism. Moreover, it does not overrule the 1993 ruling for exchangers, but it compliments it by focusing on preventing money laundering. It is applied to all people and enterprises which provide exchange services whereas as a principal activity or not⁴⁴.

The EHA/2619/2006's Order establishes the obligation for the exchangers to implement an intern procedure and organization focused on control and communication to detect, prevent, and deter money exchange activities that might be related to money laundering⁴⁵. Such structure must be implemented in an organized and homogenous way throughout the exchanger's network and has to establish by writing, as

⁴² For instance: (i) SPAIN, Ley nº19/1993, of December 28th, about some preventive measures on money laundering; *Real Decreto 2660/1998* about the Exchange of foreign currencies in open to face establishments; (ii) the Ministry of Economics order regarding the regulation of certain aspects of the legal regimen of exchangers and its agents from 2000 or (iii) the circular provided by the Bank of Spain nº6 from 2001 that regulated exchanger's owner's activities.

⁴³ It is necessary to point out that a Ministry Order in Spain has the same validity as a ruling, which means it should be enforced and above are only laws and the Constitution (GOBIERNO DE ESPAÑA. *Las fuentes del Derecho*, 2018. Available at <www.administracion.gob.es>. Accessed 20 nov. 2020).

⁴⁴ Law nº19, 1993, art.2 (SPAIN. Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales. Available at <<https://www.boe.es/buscar/doc.php?id=BOE-A-1993-30991>>. Accessed 16 sep 2022).

⁴⁵ The ruling focuses on identifying its clients, by requesting its documents and applying additional measures when each client's operation surpasses the amount of 3000€ with transfers and 6000€ with money exchange in a trimester. It also states, although dates back only over fourteen years, that the primary identification of the client, even though he has a private code, must be an on-site identification. All client's personal documents, as well as all its forms and transfer's tickets (which must be signed by the client and the exchanger's employee), must be kept by the exchangers for a period of six years.

a minimum, its client's admission policy, with a description of who is considered a high risk client and the measures to prevent it; a structured procedure to identify and renovate client's identification; a list of operations that are susceptible to money laundering; a description of the intern information traffic, with precise instructions to personal and employees on how to act in case of a suspect operation; a procedure to detect suspect and unusual activity and a description of the informatic application implemented and the criteria or parameters of such capture; a structured procedure to analyse suspect or unusual activity that is concentered in a written form; a detailed description of this control organ that includes its functioning, composition, competence and frequency; and the identity of the person responsible to communicate operations to Spain's *Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias*, which is Spain's UIF (in Spanish meaning: *Unidad de Inteligencia Financiera*). Finally, the ruling establishes some criteria to measure the efficacy of each exchanger's internal control organism, based on its capacity to automatically prevent the execution of transactions when a client personal data is missing, to automatically select risky operations and to periodically communicate with the state agency devoted to the prevention of money laundering.

Complementing these rulings, Spain's commission on money laundering's prevention and monetary infractions (*Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias*) issued an exemplary and undated catalog of money exchange operations that might be risky. It's a list that should be accounted by the exchangers by the time they are developing their "compliance" structure in the in the model proposed by EHA/2619/2006's order, so that each exchanger can evaluate its own clients, operations and elaborate its own personalized list of potential risky clients and operations. In general, the risk level of someone will be measured by its own personal profile and its typical operation traffic or activity, in function of its previous operations. Besides that, the presence of any of the intervenients in a Tax Haven or in risk territories constitutes an additional factor that increases the operation's or behaviour's risk⁴⁶.

⁴⁶ Some of the concrete elements that this catalog lists as risky are: existent of doubt regarding a client's identity or data; clients that present different

As we stated above, this structure applies to exchange of currency. The main problem is that, according to Directive (UE) 2018/843 and the Royal Decree 7/2021, virtual assets do not have the legal status of currency. This means that the compliance structure established by Order EHA/2619/2006 does not apply to the virtual asset service providers.

Looking back on 2010, Spain had reformed its Law 10/2010 from April 28th, about preventing money laundering and terrorism financing. It had had the intuit of renovating the orders regarding the prevention of money laundering firstly regulated by Law n°19/1993, with more comprehensive legal provisions that, as said in its preface, “might be considered overly regulatory”. It obligated every person who practiced professionally an exchangers activity and therefore stipulated measures regarding: (i) the identification of its clients, (ii) the need to act following the due diligence within their service and in its partners; (iii) the possibility of operating by electronic or telematic means when the client is identified by an electronic firm or its first operation provides from a bank account in Spain or Europe; (iv) the realization of a previous

documents in each operation or alter last name's order; clients that are from or reside in countries that are considered dangerous by Spain's Ministerio de Economía y Hacienda for money laundering or its drugs production; clients that might be directed by others; clients that seem to be in doubt, nervous or that consult information when asked about the data needed on the transfer's recipiente (element of risk that might only be accessed on face-to-face transfers); client that uses recipient's names that are clearly fake or invented, as names of famous singers and actors; clients that have criminal or policy background; operations made by associations or foundations constituted in Spain whose members are mostly foreigners; clients who consistently and repeatedly transfer values below the amount of 3.000€; clients that make several transfers to different people that are members of the same family, but not its own; clients that try to mix real and counterfeit coin; clients that begin to exchange “big amount” coins to “small” ones when then usually do not use cash; clients that intend to make the transaction by handing in money that is too dirty, wet or present an estrange odor; clients than send out transfers from a country different than its nationality; clients that systematically transfer during the high point hour of the exchangers so that it goes unnoticed; transfers that do not relate to any legitimate contract, service or product; exchanger's employees that show a way of living that its superior than its own salary or that shows a change in its behavior; exchanger's employees whose clients are all different and do not build up a “loyal” clientele; exchanger's employees that make a number of operations greater than the usual number of operations done by its other employees.

exam concerning every fact or operation that might be related to money laundering or terrorism funding and inform Spain's authority (*Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias*) when in these operations are seen an indication or certainty regarding money laundering or terrorism funding. Besides these examples, Law 10/2010 established several other obligations on communication with Spain's authority, the need to keep client data and information and the constitution of an organism responsible for this internal control in a similar way to EHA/2619/2006's Order.

Although it would have been preferable to add the exchange of virtual currencies as an evolution of the activity, it is important to highlight that the measures established by Law 10/2010, which are mandatory for virtual asset service providers, provide a framework to implement specific programs in order to prevent money laundering. For instance, It has been stated that:

“(...) regulated entities must adopt appropriate written policies and procedures for due diligence, reporting, record keeping, internal control, risk assessment and management, compliance assurance and communication to prevent and deter transactions related to money laundering or terrorist financing. In brief, it is the obligation to set up a specific compliance program or to integrate this obligation within the broader criminal compliance program. The content of this program must include a specific money laundering prevention policy.”⁴⁷

⁴⁷ This is a self-translation from its original version: “(...) se establece la obligación de aprobar por escrito políticas y procedimientos adecuados en materia de diligencia debida, información, conservación de documentos, control interno, evaluación y gestión de riesgos, garantía del cumplimiento de las disposiciones pertinentes y comunicación, con objeto de prevenir e impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo. Se trata en definitiva de la obligación de constituir un compliance específico o integrar dicha obligación dentro del compliance más amplio penal. En el contenido de dicho programa debe incorporarse una política específica de prevención del blanqueo de dinero.” (FERNÁNDEZ TERUELO, Javier. El compliance y las políticas y procedimientos del art. 26 de la Ley 10/2010, modificado por el RDL 11/2018: Su Integración en el modelo de compliance penal corporativo (art. 31 bis y ss. CP). In: ABEL SOUTO, Miguel; LORENZO SALGADO, José Manuel; SÁNCHEZ STEWART, Nielson (org.). *VII congreso sobre prevención y represión del blanqueo de dinero*. Valencia, Tirant lo Blanch, 2020, p. 424) .

In this regard, it needs to be pointed out that allowing the implementation of compliance programs already in use, adapting them to new risks, promotes a better response to crime prevention while reducing compliance costs.

3.2. CRIMINAL BENEFITS OF A COMPLIANCE PROGRAM

The UNE 19601 standard “aims to reduce an organization’s exposure to criminal risk and promote a culture of crime prevention”.

“This standard establishes the requirements of a management system to: prevent criminal acts that may be committed by legal entities and that give rise to criminal liability; promote a culture of prevention and compliance and demonstrate the commitment of the organisation’s leaders to the same, establishing suitable surveillance and control measures to prevent crime and significantly reduce the risk of crimes being committed, improve management, help to reduce the criminal risk, and give a greater guarantee of safety and trust to governing bodies, shareholders and investors, among other stakeholders.”⁴⁸

As stated before, in Spain currently there is an autoresponsibility model of criminal liability of legal persons regulated on article 31 bis and following of the Penal Code. Therefore, there is an automatic and direct attribution of criminal responsibility to legal persons basing on the analysis of its internal structure⁴⁹.

Specifically, the existence of a formal and effective compliance program inside a legal person that may be investigated for the commission

⁴⁸ AENOR. *Crime prevention certification for organisations in accordance with UNE 19601*, 2021. Available at <<https://www.en.aenor.com/certificacion/compliance-y-buen-gobierno/gestion-prevencion-delitos#:~:text=Under%20standard%2019601%2C%20it%20aims,give%20rise%20to%20criminal%20liability>> .Accessed 23 jun. 2022.

⁴⁹ CLEMENTE, Ismael; ÁLVAREZ, Manuel. ¿Sirve de algo un programa de compliance penal? ¿Y qué forma le doy? Responsabilidad penal de la persona jurídica en la LO 5/2010: incertidumbres y llamado por la seguridad jurídica. *Actualidad Jurídica Uría Menéndez*, v. 28, p.12, p. 26-46, 2011.

of money laundering may exempt or attenuate the criminal punishment, regardless of the commission of such crime in the means of this enterprise.

In order to exempt completely a legal person of a crime, there are two possible scenarios. The first one refers to crimes perpetrated by directives, legal representatives or anyone who has authorization to act on behalf of the legal person or has faculties of organization or control. In this case, the company will be exempted of criminal responsibility if, on its criminal trial, can prove not only the existence of an effective crime prevention program, but also the verification of a compliance officer with duties of supervision of functioning and compliance of the prevention model implemented and that the offender has skipped a whole series of these control mechanisms in a fraudulent manner. The second scenario alludes to crimes committed by anyone, inside the company structure, that is submitted to the authority of the people referred to in the first scenario. In this circumstance the company would only have to prove⁵⁰ on trial that, previously of the commission of the crime, a model of organization and management that proves adequate to prevent criminal offences or reduce significantly the risk of its commission was effectively implemented (article 31 bis, 3 and 4, Penal Code).

In any of these two scenarios, when the company is not able to prove all the circumstances listed above, an attenuation of the punishment imposed may also be granted. Moreover, such attenuation can be conceived when the legal person, after the commission of the crime and through its legal representatives, establishes, prior to the commencement of the oral trial, effective measures to prevent and detect crimes that may be

⁵⁰ On both questions, Spain's jurisprudence has already decided on the sense that it is the company that will sustain the burden of proof (SSTS 639/2016, de 14 de julio) and in this matter Antonio del Moral García states that the company will have the obligation to firstly allege the existence of a compliance program and, if there are doubts regarding its efficacy or the fulfillment of every requisite as seen above, the tribunal should decide basing itself on the most favorable decision towards the company, respecting both *in dubio pro reo* principle and the presumption of innocence principle (MORAL GARCÍA, Antonio. Responsabilidad penal de las personas jurídicas y presunción de Inocencia. In: RODRÍGUEZ-GARCÍA, Nicolás; RODRÍGUEZ-LOPEZ, Fernando (org.). *Compliance y Responsabilidad de las Personas Jurídicas*. Valencia: Tirant lo Blanch, 2021, p.31-70, p.65).

committed in the future with the means or by the legal person (article 31 quarter d), Penal Code).

Moreover, these compliances programs, in order to exempt or attenuate the punishment imposed, have to be effective in a particular manner, regulated by the same article 31 bis, 5. This means it not only has to be effective generally, but also it has to (i) identify in which activities can be committed the crimes that should be prevented; (ii) establish protocols and procedures that specify the process of formation of the will of the legal person and the adoption and the execution of decisions; (iii) have adequate financial resource management models than can prevent the commission of crimes; (iv) impose the obligation to report possible risks and non-compliance actions to the person or body in charge; (v) establish a disciplinary system capable of imposing sanctions and (vi) have a periodic verification of the compliance model and occasional updates when relevant breaches of its provisions are revealed or when there are changes in the organization, its control structure or in the activity carried out.

This pattern is in line with Spain's regulation in what concerns exchangers, as previously studied. Therefore, regarding these exchangers, if already in compliance with Spain's regulation, they would also have sufficient juridic armor to prove, in a trial for money laundering, either committed by its directives or subordinates, the existence of an implemented compliance program effective enough to exempt or attenuate the company's criminal liability.

This means that compliance is not only a practical solution to prevent money laundering in Spain within the activity of Virtual Active Service Providers, but also a realistic and juridically enforceable institution that, if money laundering has already been perpetuated, may exempt completely or attenuate criminal responsibility for those exchangers who are legal persons.

However, as we have also studied previously, Spain's regulation on exchangers do not apply and are not enforceable to those who deal with virtual assets because they are not legally conceived as money. Which means these specific exchangers will not have the previous obligation to implement compliance procedures according to the Order EHA/2619/2006. However, they must comply with the procedures

established by Law 10/2010. Despite the fact that the objective scope of this law only concerns money laundering, it is important to integrate the measures established in this law into criminal compliance.

We are aware that the main difference between the compliance program established by law 10/2010 and the Spanish criminal code lies in the fact that the former is mandatory while the latter is voluntary or self-imposed in order to avoid the criminal liability of a legal person. Even so, their integration will favor the prevention of money laundering along with other particularly risky crimes related to the activities carried out by the virtual asset service providers which, in what concerns legal persons, may involve the exemption or mitigation of the punishment. To conclude, in addition to the several benefits on the implementation of the compliance programs mentioned above, we must highlight that the measures established by Law 10/2010 are particularly valuable to assess the effectiveness of the compliance programs within the virtual asset service providers, fact that must be considered by the Spanish courts when judging the effectiveness of those compliance programs in order to grant criminal benefits in the case of legal persons.

CONCLUSIONS

1) Virtual asset service providers, as defined by the FATF, are any legal of natural person who exchange between virtual assets and fiat currencies or one or more forms of virtual assets, who transfer virtual assets, who provide services of safekeeping or administration of virtual assets or who participate or provide financial services related to the offer or sale of virtual assets. Despite the FATF broad approach, the Directive UE 2018/849 of the European Parliament and of the Council of 30 May 2018, transposed into national Spanish Law through the Royal Decree-Law 07/2021 following its guideline, has a limited view. In fact, there are many other activities not included such as the exchange of a virtual asset to another virtual asset, or the participation in and provision of financial services related to an issuer's offer and sale.

2) As it was pointed out by FATF Guideline published in June 2019, the activities involving virtual asset service providers generate a high risk of money laundering, which is a worldwide problem relating the conceal of

the origins of money linked to some crime – or all criminality, depending on the stipulated by the national legislation. Virtual asset service providers are based on a new, complex, sophisticated, and professional system that is no longer subject to the traditional one based on the necessary presence of intermediaries in a centralized structure, as they only need the nodes and the customers to operate. Hence, this disintermediation scheme has generated a deterrence problem of law regarding the high possibility of money laundering within its operation.

3) In Spain coexist two different legal frameworks with different functions on anti-money laundering regulation. Aiming to prevent criminal conduct, administrative law sets a frame mainly through Law 10/2010. Its main proposal is to enforce compliance measures on certain subjects, while also establishing administrative bodies to control their activities. Secondly, money laundering is treated by criminal law on articles 301 and following of Spain's Penal Code. Despite that, there are cases of more severe penalties under certain circumstances, and it is a crime that can be committed by any natural or legal person. In this context, it should be noted that Spain's money laundering crime can be assigned to Virtual Asset Service Providers due to the stipulated on article 302, 2, of its Penal Code, according to which an enterprise or company, legally constituted as a legal person, can be criminally liable by a money laundering offense and penalized. In accordance, all enterprises defined as a legal person can be criminally prosecuted, including state's mercantile societies, except the State, its public administrations, and other entities stated on article 31 quinquies of its Penal Code.

4) Regarding the anti-money laundering legal framework, it should be pointed out that in the last 5 years several regulations have been approved, changed or dismissed and the perspective for the next year is that both the European Union and Spain will keep on changing and improving these matters. This means, by one hand, more adaptable instruments should be implemented in order to keep up with all the changes that may come. By another hand, it also implies that every conclusion this article has come to may also change or require future revision depending on the implication of every new normative that may surge.

5) Due to the money laundering risk presented by the exchangers and to avoid possible criminal liability, the existence of a formal and effective compliance program inside a legal person that may be investigated

for the commission of money laundering may exempt or attenuate criminal punishment, regardless of the commission of such crime in the means of this enterprise. Also, as we previously said in this study, the notion of corporate compliance appears from the state's lack of capability of controlling and monitoring every legal or natural person. And, specifically regarding this research, means a series of structures implemented in any company to assess risks, prevent crime or other infractions, and create a firm culture based on ethics and compliance. Therefore, another benefit of implementing compliance programs is that it solves the deterrence deficiency encountered within virtual asset service provider's system.

6) Based on the investigation conducted it is possible to answer this paper question to know if the ruling provided in Spain's context is the finest to prevent money laundering in this focus group and what would be the best scenario regarding the prevention of money laundering in virtual asset service providers who trade with virtual exchangeable assets. The answer is that, besides legal provisions on the matter, it is necessary to implement practical tools to ensure enforcement. In this scenario, the adjustment of the legal provisions of compliance programs to these new structures seems to be the key. As we said before, not in terms of self-regulation but in terms of risk assessment.

7) In conclusion, this paper aims to point at corporate compliance as a necessary means towards money laundering's prevention within virtual asset service providers who deal with convertible virtual assets. Spain's legislation has been strong on creating a compliance structure on exchangers, but it needs an update to reflect current virtual activities. All of the above, in order to extended, in the near future, the legal horizon set by the European Union with the purposes of strengthening the legal market and fighting against crime.

BIBLIOGRAPHY AND REFERENCES

AENOR. Crime prevention certification for organisations in accordance with UNE 19601, 2021. Available at <<https://www.en.aenor.com/certificacion/compliance-y-buen-gobierno/gestion-prevencion-delitos#:~:text=Under%20standard%2019601%2C%20it%20aims,give%20rise%20to%20criminal%20liability>> .Accessed 23 jun. 2022.

ANZOLA, Ayelén. La ejecución de las resoluciones de decomiso de Activos Virtuales en España. *Revista General de Derecho Procesal*, v. 57, p. 1-25, 2022.

BLANCO CORDERO, Isidoro. *El delito de blanqueo de capitales*. Cizur Menor: Aranzadi, 2002.

Cambridge Dictionary. Available at <www.dictionary.cambridge.org>. Accessed 22 nov. 2020.

CIGÜELA SOLA, Javier. *La culpabilidad colectiva en el derecho penal: crítica y propuesta de una responsabilidad estructural de la empresa*. Madrid: Marcial Pons, 2015.

CLEMENTE, Ismael; ÁLVAREZ, Manuel. ¿Sirve de algo un programa de compliance penal? ¿Y qué forma le doy? Responsabilidad penal de la persona jurídica en la LO 5/2010: incertidumbres y llamado por la seguridad jurídica. *Actualidad Jurídica Uría Menéndez*, v. 28, p. 26-46, 2011.

ÉCIJA BERNAL, Álvaro. Ciberespacio, Dark Web y Ciberpolicía. *Diario La Ley*, v. 2 (Sección Ciberderecho), p. 1-5, 2017.

ENGELHART, Marc. The nature and Basic Problems of compliance Regimes. *Max-Planck-Institut für ausländisches und internationales Strafrecht*, p.2, 2018. Available at <https://pure.mpg.de/rest/items/item_2643714_7/component/file_3007899/content>. Accessed 22 nov. 2020.

EUROPEAN UNION. *Directive (EU) 2018/849 of the European Parliament and of the Council of 30 May 2018*. Available at <<https://eur-lex.europa.eu/eli/dir/2018/849/oj>>. Accessed 23 oct 2020.

FABIÁN CAPARRÓS, Eduardo. *El delito de blanqueo de capitales*. Madrid: Colex, 1998.

FATF, *Financial Action Task Force*. Available at <www.fatf-gafi.org/about>. Accessed 22 nov. 2020.

FATF/GAFI. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*. Paris: FATF, 2020.

FERNÁNDEZ TERUELO, Javier. El compliance y las políticas y procedimientos del art. 26 de la Ley 10/2010, modificado por el RDL 11/2018: Su Integración en el modelo de compliance penal corporativo (art. 31 bis y ss. CP). In: ABEL SOUTO, Miguel; LORENZO SALGADO, José Manuel; SÁNCHEZ STEWART, Nielson (org.). *VII congreso sobre prevención y represión del blanqueo de dinero*. Valencia, Tirant lo Blanch, 2020, p. 424.

FINANCIAL ACTION TASK FORCE, FATF. *Guidance for a risk-based approach. Virtual assets and virtual asset service providers*. Paris: FATF, 2019.

GALLANT, Michelle. Money Laundering consequences. Recovering wealth, piercing secrecy, disrupting tax havens and distorting international law. *Journal of Money Laundering Control*, v. 17, n. 3, p. 302, 2014. <https://doi.org/10.1108/JMLC-12-2013-0048>

GARCÍA MEXÍA, Pablo; ARANDA BRIONES, Beatriz; ALCAIDE SOLER, Francisco; BAENA ZAPATERO, Rafael; CODES CALATRAVA, Alfonso; GARCÍA ESPINAR, Eduardo; MENÉNDEZ ARIAS, María José; et.al. *Criptoderecho. La Regulación de Blockchain*. Madrid: Wolters Kluwer, 2018.

GARCÍA MEXÍA, Pablo. Del ciberderecho al criptoderecho. In: GARCÍA MEXÍA, Pablo (org.). *Criptoderecho. La Regulación de Blockchain*. Madrid: Wolters Kluwer, 2018.

GOBIERNO DE ESPAÑA. *Las fuentes del Derecho*, 2018. Available at <www.administracion.gob.es>. Accessed 20 nov. 2020.

GRUPO DE ACCIÓN FINANCIERA, FATF. *Directrices para un enfoque basado en riesgo: Monedas virtuales*. Paris: FATF, 2015.

GUAITA MARTINEZ, José Manuel; CARRACEDO GARNATEO, Patricia; ISIDRO NUÑEZ, Francisco. *Las criptomonedas: Digitalización del dinero 2.0*. Cizur Menor: Aranzadi, 2019.

LAUFER, William. *Corporate bodies and guilty minds. The failure of corporate criminal liability*. Chicago: The University of Chicago Press, 2006.

LIN, Iuon-Chang; LIAO, Tzu-Chun. A survey of blockchain security issues and challenges. *International Journal of Network Security*, v. 19, n.5, p. 653-659, 2017, [https://doi.org/10.6633/IJNS.201709.19\(5\).01](https://doi.org/10.6633/IJNS.201709.19(5).01)

MIRANDA RODRIGUES, Anabela. Direito penal económico – fundamento e sentido da aplicação das penas de prisão e de multa. *Revista do Ministério Público*, v. 151, p. 11-34, 2017.

MIRÓ LLINARES, Fernando. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Barcelona: Marcial Pons, 2012.

MIRÓ LLINARES, Fernando. La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista electrónica de ciencia penal y criminología*, v. 7, n. 13, p. 1-55, 2012.

MORALES BARROSO, José. “¿Qué es Blockchain?”. In: GARCÍA MEXÍA, Pablo (org.). *Criptoderecho. La regulación de Blockchain*. España: Wolters Kluger, 2018, p.39-74.

MORAL GARCÍA, Antonio. Responsabilidad penal de las personas jurídicas y presunción de Inocencia. In: RODRÍGUEZ-GARCÍA, Nicolás; RODRÍGUEZ-LOPEZ, Fernando (org.). *Compliance y Responsabilidad de las Personas Jurídicas*. Valencia: Tirant lo Blanch, 2021, p.31-70, p.65.

NAVARRO CARDOSO, Fernando. Criptomonedas (en especial, bitcóin) y blanqueo de dinero. *Revista electrónica de ciencia penal y criminología*, n. 21, p. 1-45, 2019. Available at <<http://criminnet.ugr.es/recpc>>. Accessed 20 nov 2020.

NIETO MARTÍN, Adán. Problemas Fundamentales del Compliance y el Derecho Penal. In: KUHLEN, Lothar; MONTIEL, Juan; ORTIZ, Iñigo (org.). *Compliance y teoría del derecho Penal*. Madrid: Marcial Pons, 2013, p.21-50.

PASCUA MATEO, Fabio. Criptomonedas. In: GARCÍA MEXÍA, Pablo (ed). *Criptoderecho. La Regulación de Blockchain*. Madrid: Wolters Kluwer, 2018, p. 363-410.

PÉREZ LÓPEZ, Xesus. Las criptomonedas: consideraciones generales y empleo de las criptomonedas con fines de blanqueo. In: FERNÁNDEZ BERMEJO, Daniel (org.). *Blanqueo de Capitales y TIC: Marco Jurídico Nacional y Europeo, Modus Operandi y Criptomonedas. Cyberlaundry. Informe de situación*. Cizur Menor: Aranzadi, 2019.

RODRÍGUEZ-LOPEZ, Fernando; SÁNCHEZ-MACÍAS, José Ignacio. Normalización y certificación en compliance, de la autoregulación al valor social. In: RODRÍGUEZ-GARCÍA, Nicolás; RODRÍGUEZ-LOPEZ, Fernando (org.). *Compliance y Responsabilidad de las Personas Jurídicas*. Valencia: Tirant lo Blanch, 2021, p.461-494.

SAVONA, Ernesto; ADAMOLI, Sabrina; ZOFFI, Paola. Organised crime across the borders. Preliminary results. *HEUNI Papers*, v. 6, 1995, p. 1-53. Available at <<https://www.heuni.fi/en/index/publications/heunipapers.html>>. Accessed 24 nov. 2020.

SIEBER, Ulrich. Programas de compliance en el derecho penal de la empresa. Una nueva concepción para controlar la criminalidad económica. In: ARROYO ZAPATERO, Luis; NIETO MARTÍN, Adán (org.). *El derecho penal económico en la era compliance*. Valencia: Tirant lo Blanch, 2013, p.63-110.

SPAIN. *Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo*. Available at < <https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737>>. Access 16 sep 2022.

SPAIN. *Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales*. Available at < <https://www.boe.es/buscar/doc.php?id=BOE-A-1993-30991>>. Accessed 16 sep 2022.

SPAIN. *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*. Available at < <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>>. Accessed 15 sep 2022.

SPAIN. *Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores*. Available at < <https://www.boe.es/buscar/doc.php?id=BOE-A-2021-6872>>. Accessed 16 sep. 2022.

SPAIN. Ministerio de Economía y Hacienda, *Real Decreto 2660/1998*, nº28816, BOE nº299, 15 dic 1998.

SPAIN. *Circular nº6/2001 del Banco de España de 29 de octubre, nº21296*, BOE nº41723, 15 nov 2001.

SPAIN. Ministerio de Economía y Hacienda. *Orden EHA/2619/2006*, de 28 de julio. BOE nº190, nº14513, 10 aug 2006.

SPAIN. Ministerio de Economía. *Orden de 16 de noviembre de 2000*, nº21340, BOE nº283, 25 nov 2000.

UNITED NATIONS. *The United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, 1998.

VELASCO NÚÑEZ, Eloy. *Aspectos jurídicos penales vinculados al blockchain y las criptomonedas: delito fiscal, blanqueo de capitales, robo, estafa*. Madrid: Servicio de formación continua – Consejo general de Poder Judicial, 2019.

Authorship information

Ayelén Anzola. Doutoranda na Universidad de Salamanca. Bolsista do programa para estudantes latino-americanos USAL-Santander. Investigadora em formação no Centro de Investigación para la Gobernanza Global (CIGG) da Universidad de Salamanca. Professora investigadora na Universidad Nacional del Nordeste, Argentina. Mestre em Estratégias Anticorrupção e Políticas de Integridade pela Universidade de Salamanca y Mestre em Direito administrativo pela Universidade Austral de Argentina. anzola@usal.es

Marina Oliveira Teixeira dos Santos. Doutoranda em “Estado de Derecho y Gobernanza Global” pela Universidad de Salamanca. Mestre em ciências jurídico-criminais na Universidade de Coimbra. Bacharel em Direito pela Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo. marinaoliveira.737@gmail.com

Additional information and author's declarations (scientific integrity)

Acknowledgement: To the *Centro de Investigación para la Gobernanza Global* of the University of Salamanca and the scholarship program for Latin American doctoral students of the University of Salamanca and Santander. Ayelén Anzola was funded by the program for Latin American doctoral students of the University of Salamanca. Marina Oliveira Teixeira dos Santos was funded with a position in the call for „*contratos predoctorales*” USAL 2021, co-funded by Banco Santander. To the Spanish Ministry of Science and Innovation I+D research project PID2019-107743RB-I00 on „*Configuración y efectos de los sistemas de gestión del riesgo legal*”.

Conflict of interest declaration: the authors confirm that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

- *Ayelén Anzola:* conceptualization, methodology, data curation, investigation, writing – original draft, validation, writing – review and editing, final version approval.
- *Marina Oliveira Teixeira dos Santos:* conceptualization, methodology, data curation (partial), investigation, writing – original draft, writing – review and editing, final version approval.

Declaration of originality: the authors assure that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; they also attest that there is no third party plagiarism or self-plagiarism.

Editorial process dates

(<https://revista.ibraspp.com.br/RBDPP/about>)

- Submission: 24/06/2022
- Desk review and plagiarism check: 30/06/2022
- Review 1: 04/07/2022
- Review 2: 06/07/2022
- Review 3: 10/07/2022
- Preliminary editorial decision: 04/09/2022
- Correction round return 1: 20/09/2022
- Preliminary editorial decision 2: 22/09/2022
- Correction round return 2: 29/09/2022
- Final editorial decision: 12/10/2022

Editorial team

- Editor-in-chief: 1 (VGV)
- Reviewers: 3

HOW TO CITE (ABNT BRAZIL):

ANZOLA, Ayelén; SANTOS, Marina Oliveira T. The Regulation of Money Laundering and Corporate Criminal Responsibility in Spain: compliance as a key for Virtual Asset Service Providers. *Revista Brasileira de Direito Processual Penal*, vol. 8, n. 3, p. 1335-1370, set./dez. 2022. <https://doi.org/10.22197/rbdpp.v8i3.730>



License Creative Commons Attribution 4.0 International.