Co-funded by the
Erasmus+ Programme
of the European Union

Jean Monnet Network on EU Law Enforcement
Working Paper Series

Establishing principles for the use of artificial intelligence against cryptolaundering in European bank law

Théo Antunes

Abstract

As the establishment of the crypto market allows more inclusive conduits for the everyone to access the financial market; it also allows new pathways for criminals to launder money originating from their criminal activities. Traditional means of Anti-Money laundering (AML) show limits when assessing this new threat, for both financial public and private institutions. As per the saying "*fighting fire with fire*", the use of artificial intelligence by financial institutions becomes inevitable for adapting to the cryptolaundering threat.

Artificial intelligence has the capacity to detect pattern that qualifies as money laundering: whether during the phase of placing, the phase of layering and during the phase of integration of criminal money in the financial system. Not only the quantitative aspect, but the intrinsic features of artificial intelligence can detect and adapt to new trends of money laundering where cryptolaundering currently thrives. Artificial intelligence represents a new mean for adapting to this new trend of laundering. However, the nature of such technology brings challenges for its operability under European law. Challenges focusing on the reliability, the use, and the remedies against the artificial intelligence output arise in the context of the prevention of cryptolaundering. Principles of use must be erected in order to answer such challenges. Thus, this article will identify at what extent artificial intelligence can be used to detect and identify cryptolaundering under the European banking legal framework. It will identify the operating principles that underpin a compatible use with the overall European framework. This paper will thus focus on the following question: at what extent can artificial intelligence be used for identifying instances of cryptolaundering under European bank law?

In order to answer such question, one needs to establish the context for artificial intelligence use against cryptolaundering (I). Secondly, the extent under which cryptolaundering is committed under European bank law (II). Thirdly, to identify the uses of artificial intelligence in this context (III). This will allow to pinpoint the principles for a compatible use under European bank law (IV).

Keywords:

Robotic decision; EU Law; Ethical Charter; New Digital Humanism

Establishing principles for the use of artificial intelligence against cryptolaundering in European bank law

-

Théo Antunes

As the establishment of the crypto market allows more inclusive conduits for the everyone to access the financial market; it also allows new pathways for criminals to launder money originating from their criminal activities. Traditional means of Anti-Money laundering (AML) show limits when assessing this new threat, for both financial public and private institutions. As per the saying "*fighting fire with fire*", the use of artificial intelligence by financial institutions becomes inevitable for adapting to the cryptolaundering threat.

Artificial intelligence has the capacity to detect pattern that qualifies as money laundering: whether during the phase of placing, the phase of layering and during the phase of integration of criminal money in the financial system. Not only the quantitative aspect, but the intrinsic features of artificial intelligence can detect and adapt to new trends of money laundering where cryptolaundering currently thrives. Artificial intelligence represents a new mean for adapting to this new trend of laundering. However, the nature of such technology brings challenges for its operability under European law. Challenges focusing on the reliability, the use, and the remedies against the artificial intelligence output arise in the context of the prevention of cryptolaundering. Principles of use must be erected in order to answer such challenges. Thus, this article will identify at what extent artificial intelligence can be used to detect and identify cryptolaundering under the European banking legal framework. It will identify the operating principles that underpin a compatible use with the overall European framework. This paper will thus focus on the following question: at what extent can artificial intelligence be used for identifying instances of cryptolaundering under European bank law?

In order to answer such question, one needs to establish the context for artificial intelligence use against cryptolaundering (I). Secondly, the extent under which cryptolaundering is committed under European bank law (II). Thirdly, to identify the uses of artificial intelligence in this context (III). This will allow to pinpoint the principles for a compatible use under European bank law (IV).

Keywords:

Cryptolaundering, Money laundering, artificial intelligence, banking law, financial law, AML, Fintech, compliance

I. Artificial intelligence as an answer to the cryptolaundering challenge

"Cryptocurrency, with its decentralized and digital nature, may provide a solution to this issue by advancing financial inclusion. Cryptocurrencies can be stored and transferred digitally and do not require physical banking infrastructure. This enables individuals living in remote or underserved areas to access and use cryptocurrency without the need for a traditional bank branch, providing an alternative solution for those who may not have access to traditional banking or prefer to maintain their privacy."[1]. This light side of the crypto market also shares a darker side. Cryptocurrencies also represent a pathway for criminals to launder money earned from their criminal activity. Such criminal profit can

[1] John Wingate, the role of cryptocurrency in advancing financial inclusion, published on February 10 2023, available at: https://cointelegraph.com/innovation-circle/the-role-of-cryptocurrency-in-advancing-financial-inclusion [Accessed on 3rd March 2023].

be earned through both physically or in the cyber-realm. Hence, as its name suggests, cryptolaundering is the act of using cryptocurrencies to commit money laundering[2].

Cryptolaundering represents a new challenge for the European AML framework and credit institutions. The European Union (EU) became aware of such challenge by expending the *rationae materiae* and *personae* scope of money laundering to some actors of the crypto market in the fifth Anti Money laundering directive (AMLD)[3]. If the scope is adapted, it does not address the means for detecting cryptolaundering. However, one can assume that the means for preventing money laundering need to reach a certain degree of effectiveness for credit institutions to fulfil their AML obligations. Artificial intelligence has grown to be such an effective tool for the financial market.

Artificial intelligence is a relevant new mean for AML frameworks as it can detect patterns of money laundering by monitoring transactions and screening clients. Furthermore, the very nature of artificial intelligence underlies a new policy in the prevention of cryptolaundering. When applied for detecting criminal activities, it is not in the nature of artificial intelligence to give certainties, it rather gives **a probability of a criminal activity**[4]. Artificial intelligence thus represents a step for a risk-based approach of prevention of criminal behaviours[5]. The AML framework is already based on the obligation by credit institutions to report "*suspicious transactions*"[6], on the risk of commission of money laundering. It does not require for such transactions to constitute money laundering, but rather a risk that it does. The very nature of artificial intelligence thus fits in such approach.

In this context, artificial intelligence would present an output for a probable suspicious transaction. The use of artificial intelligence for preventing cryptolaundering could thus lead to a framework based on the "ultra-risk", focusing on probabilities rather than certainties. This approach further entails the necessity for principles to be erected and enforced in the prevention of AML. They aim at giving artificial intelligence a legitimacy in the fight against cryptolaundering while retaining its effectiveness. They also aim at preventing arbitrariness and providing legal certainty for both users and persons impacted by the technology. Such use of artificial intelligence would impact the rights of targeted persons, both from a financial and human rights perspective. Such impact and such ultra-risk feature further entail the necessity for establishing a framework for its use. Properly framed, artificial intelligence represents a milestone in the fight against cryptolaundering.

II. Assessing cryptolaundering under European bank law

The European Union has taken several steps to prevent cryptolaundering. However, before assessing such framework (B), one needs to clarify the methodology of cryptolaundering to identify both the legal and technological challenges it represents (A).

---

[2] Loren Jolly, 'Les cryptomonnaies perçues comme la nouvelle menace légitimant un droit pénal de contrôle : l'exemple du dispositif anti-blanchiment', (2022) in la réglementation des cryptomonnaies, l'émergence d'un droit en réseau dans une société globalisée, 1st edition, Bruylant edition, p142

[3] European Parliament and Council Directive (EU) 2018/843 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 [2018] OJ L156, article 1, 1(c) and article 1, 2(d);.

[4] Sonia M. Gipson Rankin, 'Technological Tethereds: Potential Impact of Untrustworthy Artificial Intelligence in Criminal Justice Risk Assessment Instruments', (2021), 78, 2 Washington and Lee Law review, 647 651; Geoffrey Barnes 'Focusing Police Resources: Algorithmic Forecasting in Durham', paper presented to the 9th International Conference on Evidence-Based Policing, Cambridge, United Kingdom, 16th July 2016

[5] Marion Oswald, Jamie Grace, Sheena Urwin & Geoffrey C. Barnes, 'Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, (2018), 27, Information & Communications Technology Law, 223, 228

[6] European Parliament and Council, Directive 2015/849 terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015], OJL 141, (35), article 15, article 33, article 46.

A. Determining the methodology of cryptolaundering

The first part of cryptolaundering requires the placing criminal profits in the crypto market. It is achieved by exchanging fiat currency to virtual currency[7]. It requires a virtual asset service provider (VASP) platform to provide exchanges between fiat currency to crypto currency and vice versa. The integration part of money laundering is eased by the financial inclusion rooted within the functioning of cryptocurrency[8]. A simple wiring using a crypto exchange application is sufficient. It is challenging thus for it occurs quasi-instantaneously[9].

The second step of the money laundering is the layering of transactions to hide the illicit origins of the funds. Such phase poses challenges by the mere nature of the cryptocurrency relying on the blockchain technology. Blockchain is part of the family of decentralized ledgers; *"When a transaction occurs**, a block is added to the ledger**, forming a **sequential chain with previous transactions**, thus the name blockchain. **Each block contains data from the previous block**, […] **without reliance on any central authority***[10]". Every transaction is crypted by the blockchain and pseudonymise it. It is not possible to manually assess who is part of the transaction. This pseudonymity of transactions is intrinsically carved in the blockchain technology and already provides a certain extent of hiding without further transactions needed[11]. Nevertheless, the practice of cryptolaundering reveals a supplementary phase in the layering of illicit funds. Cryptocurrencies can be either changed in fiat currencies or be converted to other cryptocurrencies[12]. In this aspect, the layering of illicit fund can be done through multiple transactions between cryptocurrency exchange platforms; this leads to further lose tracks of the origin of the funds.

The last phase that concludes the money laundering process is the integration in the mainstream financial circuit. This can be achieved by exchanging cryptocurrencies back into fiat currency, by integrating them in the mainstream economic activity through other vehicles (investments, bonds…) or by buying licit goods with it[13]. With such a degree of anonymity and interconnection of cryptocurrencies, the cryptolaundering process is challenging for credit institutions to detect.

B. The European framework for cryptolaundering

The process of cryptolaundering is challenging because of its advanced technology base, its universality, and its rapidity. The existence of a universality of entry and exit points in the mainstream financial circuit shakes the traditional approach, where such points were credit institutions. This led the EU to focus its approach on gatekeepers (1). Nevertheless, such framework does not address the entirety of legal challenges of cryptolaundering (2).

[7] Europol, Cryptocurrencies: tracing the evolution of criminal finances, (2021) European Union Agency for Law Enforcement Cooperation Europol spotlight, p11.
[8] Daniel Holman and Barbara Stettner, 'Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches', Allen & Overy, LLP, 26, 32
[9] Gaspare Jucan Sicignano, 'Money Laundering using Cryptocurrency: The Case of Bitcoin!' , (2021), 7, 2, Athens Journal of Law 253, 259
[10] Laura E. Jehl, Blockchain Primer, (2018), Bloomberg Law, The Bureau of National Affairs, 1, 3.
[11] Er. Puneet Er. Deepika and Er. Rajdeep Kaur, 'Cryptocurrency: trends, perspectives, and challenges', (2017), 4, International Journal of Trends in Research and Development, 4.
[12] Fan Fang, Carmine Ventre, Michail Basio, Hoiliong Kong, Leslie Kanthan, David Martinez-Rego, Fan Wu, and Lingbo Li, Cryptocurrency Trading: A Comprehensive Survey, (2021), Financial innovation, volume 8, n°13, pp 1-30, p3.
[13] Chad Albrecht and Kristopher McKay Duffin, Steven Hawkins and Victor Manuel Morales Rocha, The use of cryptocurrencies in the money laundering process, (2019), 22 2, Journal of Money Laundering control, 210, 211

1. The legal challenges of cryptolaundering

Cryptolaundering represents major legal challenges for AML, especially considering two of its features.

Firstly, the most prominent feature of cryptolaundering is its capacity shroud the identity of the persons involved in the transactions. This feature is mainly built on the blockchain technology and allows for the transactions to occur without necessarily unveil the identity of the sender and the recipient[14]. Anonymity allows criminals to launder their money in a more effectively way[15]. It stands against the very nature of the AML framework. The European banking framework relies on many KYC and CDD obligations for credit institutions requiring transparency. To fulfil these obligations, credit institutions monito, at some extent, transactions occurring in the services they provide to effectively assess whether money laundering is committed on their watch[16]. The lack of transparency, carved in the use of cryptolaundering, might impair and limit the effectiveness of such obligation[17]. This brings the challenge of the extent for banks to fulfil their obligations where not all the parameters are known. It is challenging for banks to detect whether a transaction qualifies as cryptolaundering or whether funds licit transfer of fund from a cryptocurrency platform[18]. Without such transparency it is challenging to assess the licit quality of transactions. The necessity to unveil anonymity to assess whether one's is committing cryptolaundering is imperative to maintain the effectiveness of their measures and the integrity of the preventive framework both at the financial institutions and financial authority's level.

Secondly the decentralized nature of cryptocurrencies presents a challenge. Whereas in the traditional fiat currency system, credit institutions play an intermediary role in the exchange of funds, cryptocurrency can rely on intermediaries (VASP) or on a peer-to-peer approach; directly connecting two persons without intermediaries that could assess the legality of the transaction[19]. Cryptolaundering can also occur using intermediaries such as custodian wallet provider, that are defined as "*natural or legal persons that provide private cryptographic key safeguarding services on behalf of their clients,* ***for the holding, storing and transferring virtual currencies*** *in a manner similar to that of the custody of traditional financial funds or assets* "[20]. They are nexuses that allow users to access crypto funds and allow them to make transactions through a private key[21]. In this perspective, they act as "credit institutions" for cryptocurrencies, thus representing a core node for cryptolaundering.

Such challenges brought the necessity to adapt the AMLD in order to prevent cryptolaundering to occur within credit institutions and VASP.

---

[14] World Bank Group, Cryptocurrencies and Blockchain, (2018), Office of the Chief Economist, Europe, and Central Asia Economic Update, 32.

[15] European Parliament and Council Directive (EU) 2018/843 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 [2018] OJ L156 (9); Simon Butler, 'Criminal use of cryptocurrencies – a great new threat or is cash still king?' (2019), 4 3 , Journal of cyber policy, 1 11

[16] European Parliament and Council Directive (EU) 2018/843 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 [2018] OJ L156, Article 13, 1, (d)

[17] Ethem Ilbiz and Christian Kaunert, 'Sharing Economy for Tackling Crypto-Laundering: The Europol Associated 'Global Conference on Criminal Finances and Cryptocurrencies'' (2022), Sustainability MPDI, 1 7.

[18] Financial action task force, Virtual Currencies Key Definitions and Potential AML/CFT Risks, published in June 2014, FATF report, pp1-17, p9.

[19] Mahmoud Mostafa, 'Bitcoin's Blockchain Peer-to-Peer Network Security Attacks and Countermeasures', 13 7 Indian journal of science and technology (2020), 767 772-773.

[20] European Central Bank, Opinion of the European Central Bank of 18 December 2020 on the application of money laundering and terrorist financing requirements to virtual currency service providers, CON/2020/35, 1

[21] Joint Money Laundering Steering Group, Prevention of money laundering/ combating terrorist financing (2020), Guidance for the UK financial sector part II: Sectorial guidance, 254.

2. The preventive approach focused on the "Gatekeepers".

The fifth AMLD introduced virtual currencies as part of its material scope[22]. It also encompasses some actors providing virtual currency services: "*providers engaged in exchange services between virtual currencies and fiat currencies*" and "*custodian wallet providers*"[23]. The European AML framework does not encompass all the actors of the crypto market. It focuses on the "*gatekeepers*", meaning VASP that can transfer and receive funds to and from credit institutions[24]. As such, it does not extend to VASP providing services of exchange between virtual currencies with other virtual currencies and non-custodian wallet providers[25]. This choice of not addressing all the actors of the crypto market is carved in the logic of the EU to only address the gatekeepers of cryptocurrencies, despite calls for extending the European AML framework to all the actors involved in cryptocurrencies[26]. Hence, if the directive encompasses custodian wallet provider, it fails to encompass non-custodian wallet providers who are more likely to contribute in the cryptolaundering especially in the layering phase[27].. Indeed, these non-custodian wallet providers promote the fact that their activities are not under AML/KYC obligations and list it as an advantage to use their services[28]. The AMLD thus focuses on the placing and integration phases.

Under the fifth AML directive, gatekeepers must fulfil know your clients (KYC) and client's due diligence (CDD) obligations. Hence, they must identify any clients who would establish a business relationship with them[29] and report any suspicious conduct or activity that would qualify as money laundering[30]. They also have the obligation to monitor suspicious transactions that are occurring on their services to ensure they do not constitute cryptolaundering[31]. The spirit of the AMLD is to adapt all previous obligations to VASP without establishing new ones.

The challenge is not focused on the substantial obligations, but the means to fulfil them[32]. Such listing presents a current answer to identify suspicious crypto transaction, however the mean to reach such identification is not addressed.

---

[22] European Parliament and Council Directive (EU) 2018/843 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 [2018] OJ L156, article 1, (2), (d), (18).
[23] Ibid, article 1 (c) (g) and article 1, (2), (d), (19).
[24] European Central Bank, Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures, published in May 2019, ECB Crypto-Assets Task Force, 4.
[25] European Banking Authority, Report with advice for the European Commission on crypto assets published on 9th January 2019, EBA report, 20-21.
[26] European Banking Authority, Report with advice for the European Commission on crypto-assets published on 9th January 2019, EBA report, 20-21.
[27] Valeriia Dyntu, 'Cryptocurrency in the system of money laundering', (2018), 4 5 Baltic Journal of Economic Studies, 75 77.
[28] Bitpay, non-custodial wallets v custodial wallets: know the difference, published on 14th November 2023 available at https://bitpay.com/blog/non-custodial-wallets-vs-custodial-wallets/. [Accessed in 25 February 2023]
[29] European Parliament and Council, Directive 2015/849 terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015], OJL 141 article 10.
[30] Ibid, article 13.
[31] PWC Luxembourg, Anti-Money laundering services, asset & wealth management and alternatives, (2020), Price Water House Coopers, 5
[32] ComplyAdvantage, 'A Guide to Anti-Money Laundering for Crypto Firms A step-by-step guide to risk mitigation and regulatory compliance best practices, (2023) 4.

III. Determining the uses of artificial intelligence against cryptolaundering

Gatekeepers institutions must unveil the content of transactions when they originate from cryptocurrency platforms before they are integrated in the financial circuit. Since not all these transactions constitute cryptolaundering, credit institutions must operate a distinction between instances of laundering and licit transactions. In this context, artificial intelligence provides a path in ensuring that these transactions are detected and identified. It can be emphasized that artificial intelligence will not have a single use; but many uses against cryptolaundering (A). However, such uses would impact the rights of persons targeted by such measures that need to be clarified (B).

A. The extent of uses of artificial intelligence against cryptolaundering

Gatekeepers would be the main users of artificial intelligence, but their use would differ. It would differ on the target for such use. As such, credit institutions can introduce such technology to monitor clients that own cryptocurrencies[33]. Another use for VASP would target their clients to monitor the funds they receive on their platforms. Since the EU is only compassing gatekeepers, VASP would focus their monitoring on transactions they receive or transfer into fiat currency[34]. Under European law, VASP do not have to extend such monitoring on exchange of cryptocurrencies, although some national frameworks extended the scope to such services.

Under AML obligations, two types of due diligence coexist: the simplified and enhanced customer due diligence (EDD)[35]. According the FATF, cryptocurrencies require credit institutions to adopt EDD meaning a closer monitoring of clients and their transactions[36]. Artificial intelligence would thus be a mean to fulfil such EDD. What differentiates artificial intelligence from detection software is the capacity to assert by itself, whether a transaction is part of cryptolaundering. More than detecting an objective criterion it interprets pre-determined criteria to assess, by itself, whether a transaction is considered as suspicious. Its output would represent the result of such interpretation.

Jingguang Han, Yuyun Huang, Sha Liu and Kieran Towey addressed four stages for artificial intelligence as mean to prevent money laundering relying on fiat currencies[37]. **The transaction-screen** to assess whether a transaction is complying with established sanctions; **the name-screening** to identify persons included in the transactions and whether they are potential money launderers; **the transaction monitoring** aims at identifying suspicious transactions pattern and to complete a report accordingly, and the **client profile-monitoring** to provide for an overview of the client profile and its transactions history[38]. These stages occur in real-time, allowing for an adapted and rapid measure to be taken[39].The challenges for artificial intelligence applied to cryptolaundering lies in the encryption of the transactions. Artificial intelligence itself cannot read through the blockchain cryptography.

---

[33] Deloitte, The case for artificial intelligence in combating money laundering and terrorist financing A deep dive into the application of machine learning technology, (2018), SEA Financial Services, 9-10.

[34] Jason Scharfman, 'Anti-Money Laundering Compliance for Cryptocurrencies' (2022) in Cryptocurrency Compliance and Operations Digital Assets, Blockchain and DeFi 98; Meera Ragha and Diego Ballon Ossio, Unravelling the Travel Rule: AML requirements for crypto asset businesses, (2021), 36 11, Butterworths Journal of International Banking and Financial Law, 784 784.

[35] European Parliament and Council, Directive 2015/849 terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015], OJL 141 article 15 and 18.

[36] Financial Action Task Force, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, (2021), FATF report, pp1-111, p40

[37] Jingguang Han, Yuyun Huang, · Sha Liu and Kieran Towey, Artificial intelligence for anti-money laundering: a review and extension, (2020), Digital Finance, volume 2, pp211-239*,* 219

[38] *Ibidem,* 218-219.

[39] *Ibidem.*

Another advanced technology, relying on blockchain analytic can neutralise the pseudonymity of transactions. In this perspective, artificial intelligence, equipped with such software, can read through the blockchain technology to ensure whether the funds had a licit origin[40]. Such tracing is part of the obligations established by the European Union in the coming crypto market regulation[41]. Under European Law, credit institutions and VASP must be able to trace the history of funds and to qualify it as suspicious accordingly. Such suspicion can be presumed for transactions wired from cryptocurrencies platform that do not offer the adequate standards of protection, whether by their compliance framework or by the national framework they thrive in. Traceability needs only to give the compliance department of cryptocurrency platform information that would raise a suspicious transaction to fulfil its obligations under AML[42]. In this context, artificial intelligence must contain such a tracing and blockchain analytic tool to comply with AML obligations.

Such applications have managed to read through the blockchain of cryptocurrency transactions to detect patterns of cryptolaundering in the United-States[43]. Such algorithms are protected by intellectual property and do not reveal the methodology of their functioning[44]. Nevertheless, some artificial intelligence developers revealed that their model is using 166 features to detect cryptolaundering allowing to separate illicit from licit transactions[45]. Artificial intelligence has demonstrated its efficiency capacity to detect such illicit transactions through traceability. In the case of Bitcoin, since "*Each transaction represents a real transaction of the Bitcoin blockchain and has a unique ID that is determined by its predecessor*"; artificial intelligence would retrace such ID[46]. Hence, despite the lack of knowledge of the inner working of the algorithm; one can assess that it can fulfil credit institutions obligations to detect an illicit origin of funds. Whereas the crypto market is shrouded in mystery for credit institutions, financial authorities, and practitioners, artificial intelligence could bring clarity in such exchanges[47].

The Financial Action Task Force (FATF) provides for a list of red flag indicators for virtual assets to qualify a transaction as suspicious under six subcategories tagged as red flags for: transactions, transactions patterns, anonymity, about senders or recipients, the source of funds or wealth and geographical risks. The content of such categories regroups 72 criteria[48]. Artificial intelligence used by credit institutions and VASP could rely on such criteria to assess cryptolaundering.

---

[40] Eric Pettersson Ruiz and Jannis Angelis, "Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchange"s, 24 11, journal of money laundering control 769 773.

[41] European Commission, Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto assets (recast), published on 29th November 2021, 2021/0241 (COD), p3.

[42] European Parliament and Council, Directive 2015/849 terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015], OJL 141, article 33.

[43] Eric Pettersson Ruiz and Jannis Angelis, "Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges' 24 11, journal of money laundering control, 766 773

[44] Elliptic, Ellitpic Data set, published in 2019 available at: <https://www.kaggle.com/datasets/ellipticco/elliptic-data-set [Accessed on 6th March 2023].

[45] *Ibidem*.

[46] Eric Pettersson Ruiz and Jannis Angelis, "Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchange"s, 24 11, journal of money laundering control 769 773.

[47] Financial stability institute, FSI Insights on policy implementation n°: 31 Supervising crypto assets for anti-money laundering, published in April 2021, 21.

[48] Financial Action Task Force, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, published in September 2020, FATF report.

B. Identifying the impacts of artificial intelligence used against cryptolaundering.

Once a transaction has been flagged as suspicious by the artificial intelligence, compliance departments must report it to the Financial investigative unit (FIU) for it to adopt measures and investigate whether this transaction is money laundering[49]. In this perspective, the FIU can take administrative measures while assessing whether such transaction is money laundering. It can oppose the transaction for a certain duration or take a freezing order[50]. Such order is defined as a "*decision issued or validated by an issuing authority in order to prevent the destruction,* ***transformation, removal, transfer or disposal of property*** *with a view to the confiscation thereof*"; this issuing authority is not limited to courts but can comprise FIU as well[51]. In this last case however, it needs to be validated later by a judge or a public prosecutor[52]. The legal effects of such order "*can be general and affect all transactions linked to a business relationship, or it can be partial and only relate to specific transactions, which are specified by the FIU*"[53]. Such measure thus aims at freezing the transaction, or a set of transactions to assess their legality. The challenge for such framework is not the administrative measure itself, but its basis: the artificial intelligence output. As such, an administrative decision could fully or partially be based on the output of an artificial intelligence software used by another entity than the public decision-maker.

Such approach is challenging, in the case where the flagging by the credit institutions would only or mainly rely on such output[54]. This could also be extended to the FIU; whose administrative measures could be taken based on such a report and indirectly on the artificial intelligence output[55]. The practical challenge is that artificial intelligence becomes the basis for both the credit institution reporting and an administrative decision. However, artificial intelligence is not a panacea. It makes probabilities not certainties and errors during its functioning could lead to flawed decisions by public authorities[56]. Not only would this impact the finance of the targeted person but would also impact the redress against such decision. One must understand why a measure was held against him according to the theory of argumentative justice[57]. The understanding is often based on the necessity for the decision to be reasoned, allowing to discard any taint of arbitrariness[58]. This reasoning might however be impacted by the intrinsic nature of artificial intelligence and its lack of intelligibility[59]. This "*black box*" represents a technical and legal challenge inherent to all artificial intelligence software[60]. It is defined as one ***"can***

[49] *Ibidem*.
[50] Cellule de renseignement financier, freezing of suspicious transactions, published on 1st of April 2021, Parquet general du Grand-Duché de Luxembourg, 3.
[51] European Parliament and Council, Regulation (EU) 2018/1805 of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, [2018] OJL 303 article 2, (8), (a), ii.
[52] *Ibidem*.
[53] Cellule de renseignement financier, freezing of suspicious transactions, published on 1st of April 2021, Parquet general du Grand-Duché de Luxembourg, 3.
[54] Julie Gerlings and Ioanna Constantioun, 'Machine Learning in Transaction Monitoring: The Prospect of xAI', (2023), Proceedings of the 56th Hawaii International Conference on System Sciences, 3474 3476
[55] Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era', (2017), 105, Georgetown Law Journal, 1147 1170
[56] Eirini Ntoutsi and others, 'Bias in data-driven artificial intelligence systems—An introductory survey', (2019), , L3S Research Center & Faculty of Electrical Engineering and Computer Science, Leibniz University Hannover, Hannover, Germany 4.
[57] Adrien van den Branden, Juge humain v Juge robot, (2019) *Les Robots à l'assaut de la Justice, l'intelligence artificielle au service des justiciables,* Bruylant edition, 18.
[58] *Moreira v. Portugal,* App no 47940/99 (ECtHR 25th February 2020), para 72.
[59] Jenna Burrell, How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms, (2016), Big data & society, 3 < https://journals.sagepub.com/doi/full/10.1177/2053951715622512> accessed 23 February 2023
[60] Yavar Bathaee, 'The artificial intelligence black box and the failure of intent and causation, (2018), 31 2, Harvard Journal of Law & Technology, 889 906

observe its inputs and outputs, but we cannot tell how one becomes the other"[61]**.** It means that the output is decided on unknown parameters. Such perspective leads for decision-takers to over-rely on a technology that does not establish the reasons for its decision.

Under the AML and human rights frameworks, there is a right to redress against a freezing order[62]. However, how can such right be effective with such opacity? The effectiveness of remedies against an artificial intelligence software is a major human right issue[63]. However, such opacity would impair the effectiveness of remedies, in the context of a flagging report and an administrative measure.
Such challenges entail the necessity for establishing principles for the use of artificial intelligence as a mean to prevent cryptolaundering.

IV. Framing the principles for AI against cryptolaundering

The inner working of artificial intelligence makes its reasoning opaque, while its advanced technology increases its influence of its output on the compliance officer[64]. As demonstrated earlier, this influence could lead to base private and public decisions solely on artificial intelligence output. Moreover, the opaqueness of artificial intelligence thus leads to take a flagging report or an administrative measure on unknown basis. Such prospect would not satisfy European standards on the use of artificial intelligence[65]. For allowing an effective use of artificial intelligence while preserving European standards, it is required to frame its use under robust principles. Hence one needs to firstly frame the principles regarding the human-AI relationship in the fight against cryptolaundering (A); before framing the extent under which financial institutions need to understand the artificial intelligence reasoning and output (B).

A. *The human-AI relationship in the fight against cryptolaundering*

The core principle would focus on the relationship between the artificial intelligence and its user. A cross reading approach of the forthcoming artificial intelligence act (AIA) and the AML framework favours a decision in the hands of humans (1). However, such principle would be challenging considering the very process of cryptolaundering (2).

1. An adapted principle for the AML framework

If the principle of human in command makes little doubt under European law[66]; one should however assess its extent of the in the context of artificial intelligence against cryptolaundering?

---

[61] Frank Pasqual, *the black box society: The Secret Algorithms That Control Money and Information*, (2015), Harvard University Press, 3.
[62] Article 9-3 of the AML/CFT Law (Luxembourg); European Parliament and Council, Regulation (EU) 2018/1805 of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, [2018] OJL 303, article 33.
[63] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial intelligence, human rights, democracy, and the Rule of Law a primer', (2021) Council of Europe and The Alan Turing Institute, 15.
[64] Charvi Rastogi, Yunfeng Zhang, Dennis Wei, Kush R. Varshney, Amit Dhurandhar, and Richard Tomsett , 'Deciding Fast and Slow: The Role of Cognitive Biases in AI-assisted Decision-making', (2022), 6 Proceedings of the ACM on Human-computer interaction, 83 85
[65] European Parliament and Council, Regulation 2016/679 (EU), on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJL 119, [2016] article 22.
[66] European Parliament and Council, Proposal for a regulation 2021/106 on laying down harmonized rules on artificial intelligence (Artificial intelligence act) and emending certain union legislative acts, published on 21st April 2021, COM/2021/206 final, p7; European Parliament and Council, Regulation 2016/679 (EU), on the

Under the AML framework, credit institutions and VSAP need to inform the "*FIU, **including by filing a report**, **on their own initiative**, where the obliged entity knows, suspects or **has reasonable grounds** to suspect that funds, regardless of the amount involved, **are the proceeds of criminal activity or are related to terrorist financing***"[67]. Such report is conditioned by the obligation to contain "***all necessary information***" for reporting a suspicious transaction[68]. One could theorize that such information needs to at least demonstrate "*reasonable grounds to suspect that money laundering or terrorist financing is being committed […] **its development, the origin of the funds, the purpose, nature and procedure of the operation***"[69]. However, such list is far from being exhaustive, and the means on how such a report must be established is not mentioned as it only requires a substantive information obligation. A flagging would thus not be considered without such substantive information. One could theorize that the report for suspicious transaction could comprise the artificial intelligence output but only if it would contain the reasons for flagging the transaction as cryptolaundering. Thus, an output based on unknown parameters would not fulfil such an obligation under the AML framework.

However, can such the report, that can impact the rights of persons be taken solely on artificial intelligence output even if it answers such obligation? The EU framework stands in a negative answer, requiring a meaningful human intervention in its relationship with such an output. It establishes the principle of a meaningful intervention in the context of high-risk artificial intelligence[70]. They are defined "*in the light of their intended purpose, they pose a high risk of harm to the health and safety or the **fundamental rights of persons**, taking into account both the severity of the possible harm and its probability of occurrence*"[71]. Artificial intelligence software programmed to identify criminal activities falls in this category[72]. Thus, by extension and by its above-mentioned impacts, artificial intelligence software to detect instances of cryptolaundering would fall in such category.

Such software will be subjected to human oversight in and forbids that the humans mechanically repeat the result of the algorithm[73]. It thus calls for a human oversight on the artificial intelligence output. Human oversight entails that user "*remain aware of the possible **tendency of automatically relying or over-relying on the output produced** by a high-risk AI system*"[74]. Compliance officers must therefore balance the weight of the output "*rather than just a token gesture*"[75]. Hence, it is expected that they use supplementary information to assess the suspicious character of a given transaction. Artificial intelligence could be the starting point for suspecting a transaction but cannot be the whole basis for under this framework, they are not allowed to simply reproduce the flagging of cryptolaundering.

---

protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJL 119, [2016] article 22.

[67] European Parliament and Council, Directive 2015/849 terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015], OJL 141 Article 33

[68] *Ibidem*.

[69] Cellule de renseignement financier, Suspicious operations report, published on 1st of January 2017, Parquet general du Grand-Duché de Luxembourg, pp1-6, p3.

[70]European Parliament and Council, Proposal for a regulation 2021/106 (EU) on laying down harmonized rules on artificial intelligence (Artificial intelligence act) and emending certain union legislative acts, published on 21st April 2021, article 14.

[71]. European Parliament and Council, Proposal for a regulation 2021/106 on laying down harmonized rules on artificial intelligence (Artificial intelligence act) and emending certain union legislative acts, published on 21st April 2021, COM/2021/206 final (32).

[72] *Ibid* recital 38

[73] Ibid article14.4

[74] *Ibidem*.

[75] Article 29 Data protection working party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, 17/EN WP 251, 10

Compliance departments must thus weight the balance of the cryptolaundering detection and not base their entire report on such flagging. However, this theorical framework is challenged by the reality of the flagging of cryptolaundering instances.

2. The limits of human control in the AML framework

Despite this meaningful human intervention obligation, the challenge lies on its extent in the cryptolaundering preventive framework. The rapid and effective identification of cryptolaundering transactions is vital for the overall prevention framework of AML[76]. This entails the need for a diligent decision-making to report or not to report. In practice, this might lead compliance officers to report suspicious transaction following the algorithmic output or heavily anchored by it. The efficiency of artificial intelligence to detect cryptolaundering weights the balance in favour of heavily relying on it. Traditional methods fall short for such laundering and artificial intelligence presents a pathway toward a more effective preventive money laundering framework.

Hence, on one hand, the AIA requires credit institutions not to automatically follow the output; while on the other hand their due diligence obligations under the AML framework require them to report as soon as possible instances of cryptolaundering. One could assume that credit institutions could favour following the output of artificial intelligence to comply with their obligations to report in due manner instances of cryptolaundering over the risk of letting a laundering transaction to occur. This would prioritize the security of the financial market and preserve the integrity of their AML obligations. However, this approach might increase false positives flagging and ultimately drown FIU and law enforcement under reports, agencies rendering the whole AML framework paralyzed[77]. Compliance officers need to weight the output themselves in order to assess the veracity of the output. Hence, for such principle to be effective, it must be accompanied with the requirement of understanding the reasoning leading to the output.

B. Understanding the flagging of the artificial intelligence algorithm: the path to justification

Scholars and European institutions have long considered transparency as a main principle in the artificial intelligence life cycle[78]. The AIA does not refer to explainability but to transparency as a main obligation for providers[79]. Transparency entails the full disclosure of the code of the software. However, compliance officers are not computer scientists; their knowledge is limited, and the full disclosure of the code is irrelevant to understand how it reached its output. Full transparency is thus not desirable for such a use.

A preferable path toward enabling an understanding of the artificial intelligence output is to for artificial intelligence to be explainable: to understand how it reached its output. Whereas there is no common definition for explainability in artificial intelligence, one could encompass it as "*the process of describing one or more facts, such that it* ***facilitates the understanding of aspects related to said facts***"[80]. The AIA approaches the notion of transparency as to "*enable users to* ***interpret the system's***

---

[76] Eric Pettersson Ruiz and Jannis Angelis, "Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges' 24 11, journal of money laundering control, 766 773.

[77] Court of Appeal of Luxembourg, held on 11th January 2017, n°14/17.

[78] Nicholas Diakopoulos, 'Transparency, (2020)', The Oxford Handbook of Ethics of AI, Oxford University press, 197 198; European Parliament and Council, Proposal for a regulation 2021/106 on laying down harmonized rules on artificial intelligence (Artificial intelligence act) and emending certain union legislative acts, published on 21st April 2021, COM/2021/206 final, (43).

[79] *Ibid*, (45) (47) (69) (70) ; article 1 (c) ; article 13, article 52.

[80] Sebastian Palacio, Adriano Lucieri, Mohsin Muni, Jorn Hees , Sheraz Ahmed , Andreas Dengel , 'XAI Handbook: Towards a Unified Framework for Explainable AI' (2021), 1 5 ; https://arxiv.org/abs/2105.06677 accessed on 15 February 2023

output *and use it* ***appropriately****. An* ***appropriate type and degree of transparency*** *shall be ensured, with a view to achieving compliance with the relevant obligations of the user"*[81]. The reference to an appropriate transparency could be referred as explainability. Nevertheless, explainability does not entail a full disclosure of the inner working, but rather a possibility to explain the inner working without disclosing it. Such explainability stems from its own programming or from a post hoc technique using another algorithm that generate explanations on the artificial intelligence reasoning[82]. What would the requirement of explanation be under the prevention of cryptolaundering?

The core explanation will have to focus on how the artificial intelligence flagged the transaction as suspicious. This explanation is deriving from the obligation of financial institutions that "*he/she should ensure that the information is transmitted* ***in a format and through means which comply with any guidelines*** *issued by the national FIU,* ***in an effective manner***"[83]. The requirement of effectiveness entails a certain understanding of the algorithmic decision for non-computer scientist. One could however challenge such explanation by assessing whether such extent would satisfy AML obligations. The AML framework indicates that credit institutions must be provide *"the FIU, directly or indirectly, at its request,* ***with all necessary information****"* when reporting a suspicious transaction[84].

To meet this obligation, one could assert that artificial intelligence not only has to explain its output, but needs to justify it. Justification can be differentiated from explainability by its purpose; whereas explainability delivers insights on the inner working " *justification explains* ***why a decision is a good one****, but it may or may not do so by explaining exactly how it was made. Unlike introspective explanations, justifications* ***can be produced for non-interpretable systems***"[85]. Justification encompasses a wide range of artificial intelligence models whereas explainability is more limited in range. Justification allows a pathway for both using the most effective models while also having insights on its inner working.

The concept of justification entails the convincing that the output is the good one indicating the reasons to flag a transaction and why its output makes sense[86]. Justification could reveal the reasons for the flagging as to the origin of the transaction, its history, and the identity of the persons and other relevant factors. This justification would offer the "*necessary information*" requirement under AML obligation; allowing to understand the logic of the output. This justification allows a more effective interpretation from the credit institutions, whether the decision was taken on relevant criteria and verifying them.

---

[81] European Parliament and Council, Proposal for a regulation 2021/106 on laying down harmonized rules on artificial intelligence (Artificial intelligence act) and emending certain union legislative acts, published on 21st April 2021, COM/2021/206 final article 13.

[82] Alejandro Barredo Arrieta, Natalia Díaz-Rodríguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador García, Sergio Gil-López, Daniel Molina, Richard Benjamins, Raka Chatila and Francisco Herrera, 'Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI', (2020), 58 Information Fusion, , 82 84

[83] European Banking authority, Guidelines On policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849P25, 25

[84] European Parliament and Council, Directive 2015/849 terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015], OJL 141 Article 33

[85] Or Biran and Courtenay Cotton, Explanation and Justification in Machine Learning: A Survey (2017), 1 4. < https://www.semanticscholar.org/paper/Explanation-and-Justification-in-Machine-Learning-%3A-Biran-Cotton/02e2e79a77d8aabc1af1900ac80ceebac20abde4#cited-papers> accessed on 4th February 2023
; Clement Henin, Daniel Le Métayer, 'A Framework to Contest and Justify Algorithmic Decisions', (2021), AI and Ethics, 463 463.

[86] Or Brian and Kathleen McKeown, 'Human-centric justification of machine learning predictions' (2017), Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence 1461 1462.

More than explanation, justification is more desirable to assess the quality of the output and its decision-making process. It is also relevant for it can transmit the information in an intelligible format to both the compliance officer and the FIU. Justification lies as core principle for artificial intelligence the prevention of cryptolaundering. Only by understanding the basis of the output can one avails it or contradict it thus rendering efficient the principle of meaningful human intervention. Justification allows contestability and "*contestability transfers knowledge about how the machine is reasoning to the professional, and it allows the professional to collaborate, critique, and correct the predictive algorithm* [87]. Justification would thus free credit institutions compliance department from an automatic dependence from the output of artificial intelligence.

Justification would give a certain legitimacy for flagging a transaction. Such information could later be verified by the financial authorities to assess the relevance of the flagging. Justification would serve as a nexus toward assessing the veracity of the flagging. The artificial intelligence output would constitute the starting point of the assessment for cryptolaundering by financial authorities. Compliance departments must thus enforce these principles in their reporting obligations.

C. Framework to redress

What if a person invests on a cryptocurrency platform and decide to exchange his virtual currencies to fiat currency? This is the normal course for crypto assets transactions. However, what if during this transaction, an artificial intelligence model used by the credit institution flags it as cryptolaundering and a report to the FIU is transmitted. Moreover, if the FIU decides to take measures, it will be based a report partially or wholly based on an artificial intelligent output. The AML framework entails the protection of *"the right to an effective remedy and to a fair trial"*[88]. One could however question the extent of such provision, for the very nature of the preventive framework is to take administrative measures, thus before any trial. The CCBE determined that such provisions confer notably *"the right to notification of rights and the right to legal assistance"*[89]. Such procedural rights thus aim at offering legal defence against such a decision.

Under the AML framework and the Charter of fundamental rights of the European Union, persons targeted by an administrative measure from the FIU have the right to an effective remedy against such measure[90]. This entails the possibility of challenging it before competent courts. However, the challenge lies when the decision of the FIU is based on the credit institutions report relying on the output of the algorithm. If the FIU measure complies with the output of the algorithm, one should have an effective right to defence and the targeted person would need to understand the algorithmic reasoning[91]. Hence one could affirm that the principles of justification extend to the person targeted by FIU measures.

This further entails that justification is a core principle not only for financial authorities and institutions, but for the targeted person as well. The rationale is however different. For credit institutions and

[87] Deirdre K. Mulligan Daniel N. Kluttz Nitin Kohli, 'Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions', (2019), in *After the Digital Tornado*, Cambridge University Press, 15: "*contestability transfers knowledge about how the machine is reasoning to the professional, and it allows the professional to collaborate, critique, and correct the predictive algorithm*.

[88] European Parliament and Council, Directive 2015/849 terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015], OJL 141 (65).

[89] Council of Bars and Law Societies of Europe, Proportionality in anti-money laundering regulation: Balancing the fight against laundering proceeds of crime with protective rights of the citizen, published on 26th June 2020, 3.

[90] European Union, Charter of fundamental rights of the European Union, published on 18th December 2000, [2009], 2000/C 364/01 OJC 326, article 47.

[91] *Pélissier and Sassi v France*, App no 25444/94 (ECtHR, 25th March 1999) para 51.

authorities, justification is necessary to assess the quality of the decision; for the targeted person, it is a mean for legal defence. However, the extent of this justification would also vary; for the AIA clearly states that the transparency obligations "*will be limited only to the **minimum necessary information** for individuals to exercise their right to an effective remedy*"[92]. This limit also from intellectual property protection of the provider of artificial intelligence[93]. One could ask, who would give this minimum necessary information and what it means in the context of cryptolaundering. Bearing in mind the use of cryptolaundering; the minimum necessary information would encompass the suspicion of an illicit origin and its basis.

This minimum necessary information obligation should at least encompass the reasons for the qualification of the funds as suspicious, for the person to have the capacity to redress against the decision based on it. These principles are needed during the use of artificial intelligence and its aftermath. However, one cannot let any software be used by credit institutions in the fight against cryptolaundering. The developers must answer to principles as well, to ensure an adequate development.

V. Conclusions

The identification of these principles makes artificial intelligence for detecting cryptolaundering compatible with the current and future frameworks. The ultra-risk perspective that this technology brings make these principles vitals and must be enforced by compliance departments when dealing with cryptocurrencies. The prevention of cryptolaundering had brought the necessity to adapt the means of detecting its instances as such artificial intelligence presents a further step in effectively preventing such laundering. These principles are vitals in the prevention of the laundering; but will ultimately be as relevant in the context of criminal proceedings as evidence for cryptolaundering. It will thus be relevant for assessing the quality of the evidence; in a context where it can be an effective mean to assess such laundering. Once more, artificial intelligence will play a fundamental role, but needs to answer to a compatible approach under European law.

[92] European Parliament and Council, Proposal for a regulation 2021/106 on laying down harmonized rules on artificial intelligence (Artificial intelligence act) and emending certain union legislative acts, published on 21st April 2021, COM/2021/206 final, 11.

[93] Committee on Legal affairs, Report on intellectual property rights for the development of artificial intelligence technologies, published on 2nd October 2020, 20202015/INI, (18) ; European Parliament and Council, Regulation 2016/679 (EU), on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJL 119, [2016] (63).

References:

Academic articles :

- Alejandro Barredo Arrieta, Natalia Díaz-Rodríguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador García, Sergio Gil-López, Daniel Molina, Richard Benjamins, Raka Chatila and Francisco Herrera, 'Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI', (2020), 58 Information Fusion.
- Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era', (2017), 105, Georgetown Law Journal
- Chad Albrecht and Kristopher McKay Duffin, Steven Hawkins and Victor Manuel Morales Rocha, The use of cryptocurrencies in the money laundering process, (2019), 22 2, Journal of Money Laundering control
- Charvi Rastogi, Yunfeng Zhang, Dennis Wei, Kush R. Varshney, Amit Dhurandhar, and Richard Tomsett , 'Deciding Fast and Slow: The Role of Cognitive Biases in AI-assisted Decision-making', (2022), 6 Proceedings of the ACM on Human-computer interaction
- Daniel Holman and Barbara Stettner, 'Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches', Allen & Overy, LLP
- Deirdre K. Mulligan Daniel N. Kluttz Nitin Kohli, 'Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions', (2019), in *After the Digital Tornado*, Cambridge University Press
- Eirini Ntoutsi and others, 'Bias in data-driven artificial intelligence systems—An introductory survey', (2019), L3S Research Center & Faculty of Electrical Engineering and Computer Science, Leibniz University Hannover, Hannover, Germany
- Er Puneet Er. Deepika and Er. Rajdeep Kaur, 'Cryptocurrency: trends, perspectives, and challenges', (2017), 4, International Journal of Trends in Research and Development
- Eric Pettersson Ruiz and Jannis Angelis, "Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchange"s, 24 11, journal of money laundering control
- Ethem Ilbiz and Christian Kaunert, 'Sharing Economy for Tackling Crypto-Laundering: The Europol Associated 'Global Conference on Criminal Finances and Cryptocurrencies'' (2022), Sustainability MPDI
- Fan Fang, Carmine Ventre, Michail Basio, Hoiliong Kong, Leslie Kanthan, David Martinez-Rego, Fan Wu, and Lingbo Li, Cryptocurrency Trading: A Comprehensive Survey, (2021) 8 13, Financial innovation
- Gaspare Jucan Sicignano, 'Money Laundering using Cryptocurrency: The Case of Bitcoin!' , (2021), 7, 2, Athens Journal of Law
- Geoffrey Barnes 'Focusing Police Resources: Algorithmic Forecasting in Durham', paper presented to the 9th International Conference on Evidence-Based Policing, Cambridge, United Kingdom, 16th July 2016
- Jason Scharfman, 'Anti-Money Laundering Compliance for Cryptocurrencies' (2022) in Cryptocurrency Compliance and Operations Digital Assets, Blockchain and DeFi
- Julie Gerlings and Ioanna Constantioun, 'Machine Learning in Transaction Monitoring: The Prospect of xAI', (2023), Proceedings of the 56th Hawaii International Conference on System Sciences
- Mahmoud Mostafa, 'Bitcoin's Blockchain Peer-to-Peer Network Security Attacks and Countermeasures', 13 7 Indian journal of science and technology (2020).

- Marion Oswald, Jamie Grace, Sheena Urwin & Geoffrey C. Barnes, 'Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, (2018), 27, Information & Communications Technology Law
- Meera Ragha and Diego Ballon Ossio, Unravelling the Travel Rule: AML requirements for crypto asset businesses, (2021), 36 11, Butterworths Journal of International Banking and Financial Law
- Nicholas Diakopoulos, 'Transparency, (2020)', The Oxford Handbook of Ethics of AI, Oxford University press
- Or Brian and Kathleen McKeown, 'Human-centric justification of machine learning predictions' (2017), Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence.
- Sebastian Palacio, Adriano Lucieri, Mohsin Muni, Jorn Hees , Sheraz Ahmed , Andreas Dengel , 'XAI Handbook: Towards a Unified Framework for Explainable AI' (2021),
- Sonia M. Gipson Rankin, 'Technological Tethereds: Potential Impact of Untrustworthy Artificial Intelligence in Criminal Justice Risk Assessment Instruments', (2021), 78, 2 Washington and Lee Law review
- Valeriia Dyntu, 'Cryptocurrency in the system of money laundering', (2018), 4 5 Baltic Journal of Economic Studies
- Yavar Bathaee, 'The artificial intelligence black box and the failure of intent and causation, (2018), 31 2, Harvard Journal of Law & Technology

Books :

- Loren Jolly, 'Les cryptomonnaies perçues comme la nouvelle menace légitimant un droit pénal de contrôle : l'exemple du dispositif anti-blanchiment', (2022) in la réglementation des cryptomonnaies, l'émergence d'un droit en réseau dans une société globalisée, 1st edition, Bruylant edition
- Adrien van den Branden, Juge humain v Juge robot, (2019) *Les Robots à l'assaut de la Justice, l'intelligence artificielle au service des justiciables,* Bruylant edition
- Frank Pasqual, *the black box society: The Secret Algorithms That Control Money and Information*, (2015), Harvard University Press

Studies :

- Laura E. Jehl, Blockchain Primer, (2018), Bloomberg Law, The Bureau of National Affairs
- World Bank Group, Cryptocurrencies and Blockchain, (2018), Office of the Chief Economist, Europe, and Central Asia Economic Update
- Joint Money Laundering Steering Group, Prevention of money laundering/ combating terrorist financing (2020), Guidance for the UK financial sector part II: Sectorial guidance
- Bitpay, non-custodial wallets v custodial wallets: know the difference, published on 14th November 2023 available at https://bitpay.com/blog/non-custodial-wallets-vs-custodial-wallets/. [Accessed in 25 February 2023].
- Or Biran and Courtenay Cotton, Explanation and Justification in Machine Learning: A Survey (2017), 1 4. < https://www.semanticscholar.org/paper/Explanation-and-Justification-in-Machine-Learning-%3A-Biran-Cotton/02e2e79a77d8aabc1af1900ac80ceebac20abde4#cited-papers> accessed on 4th February 2023

European Union documents:

- Committee on Legal affairs, Report on intellectual property rights for the development of artificial intelligence technologies, published on 2nd October 2020, 20202015/INI, (18)
- European Banking authority, Guidelines On policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849P25.
- European Banking Authority, Report with advice for the European Commission on crypto assets published on 9th January 2019, EBA report
- European Central Bank, Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures, published in May 2019, ECB Crypto-Assets Task Force
- European Central Bank, Opinion of the European Central Bank of 18 December 2020 on the application of money laundering and terrorist financing requirements to virtual currency service providers, CON/2020/35
- European Commission, Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto assets (recast), published on 29th November 2021, 2021/0241 (COD)
- European Parliament and Council Directive (EU) 2018/843 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 [2018] OJ L156.
- European Parliament and Council, Directive 2015/849 terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015], OJL 141
- European Parliament and Council, Proposal for a regulation 2021/106 on laying down harmonized rules on artificial intelligence (Artificial intelligence act) and emending certain union legislative acts, published on 21st April 2021, COM/2021/206 final
- European Parliament and Council, Regulation (EU) 2018/1805 of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, [2018] OJL 303
- European Parliament and Council, Regulation 2016/679 (EU), on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJL 119, [2016].
- European Union, Charter of fundamental rights of the European Union, published on 18th December 2000, [2009], 2000/C 364/01 OJC 326
- Europol, Cryptocurrencies: tracing the evolution of criminal finances, (2021) European Union Agency for Law Enforcement Cooperation Europol spotlight.

Reports and guides:

- Article 29 Data protection working party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, 17/EN WP 251
- Cellule de renseignement financier, freezing of suspicious transactions, published on 1st of April 2021, Parquet general du Grand-Duché de Luxembourg
- Cellule de renseignement financier, Suspicious operations report, published on 1st of January 2017, Parquet general du Grand-Duché de Luxembourg
- ComplyAdvantage, 'A Guide to Anti-Money Laundering for Crypto Firms A step-by-step guide to risk mitigation and regulatory compliance best practices, (2023).
- Council of Bars and Law Societies of Europe, Proportionality in anti-money laundering regulation: Balancing the fight against laundering proceeds of crime with protective rights of

the citizen, published on 26th June 2020David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial intelligence, human rights, democracy, and the Rule of Law a primer', (2021) Council of Europe and The Alan Turing Institute

- Deloitte, The case for artificial intelligence in combating money laundering and terrorist financing A deep dive into the application of machine learning technology, (2018), SEA Financial Services.
- Financial Action Task Force, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, (2021), FATF report,
- Financial Action Task Force, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, published in September 2020, FATF report
- Financial action task force, Virtual Currencies Key Definitions and Potential AML/CFT Risks, published in June 2014, FATF report
- Financial stability institute, FSI Insights on policy implementation n°: 31 Supervising crypto assets for anti-money laundering, published in April 2021
- PWC Luxembourg, Anti-Money laundering services, asset & wealth management and alternatives, (2020), Price Water House Coopers

National law:

- Luxembourg, Law of 20th May 2004

Cases:

European court of human rights:

- *Moreira v. Portugal,* App no 47940/99 (ECtHR 25th February 2020)
- *Pélissier and Sassi v France*, App no 25444/94 (ECtHR, 25th March 1999)

Luxembourgish courts:

- Court of Appeal of Luxembourg, held on 11th January 2017, n°14/17.