Università degli Studi di Padova

Sede Amministrativa: Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

---

CORSO DI DOTTORATO DI RICERCA IN GIURISPRUDENZA

XXXV CICLO

VIRTUAL ASSETS AND TERRORISM FINANCING STRUCTURE, EVOLUTION AND LAW ENFORCEMENT STRATEGIES

Coordinatore: Ch.ma Prof.ssa Paola Lambrini

Supervisore: Ch.mo Prof. Riccardo Borsari

Dottoranda : Marta Barcellona

List of Contents

VIRTUAL ASSETS AND TERRORISM FINANCING
STRUCTURE, EVOLUTION AND LAW ENFORCEMENT STRATEGIES

CHAPTER II

EVOLUTION OF TRENDS, SOURCES AND METHODS OF TERRORISM FINANCING: THE POSSIBLE ROLE OF VIRTUAL ASSETS

CHAPTER III

VIRTUAL ASSETS, TERRORISM FINANCING AND THE INTERNATIONAL REGULATORY ARCHITECTURE: AN ASSESSMENT

CHAPTER IV

STEMMING THE FLOW OF FUNDS VIA ASSET FREEZE AND ASSET RECOVERY: WHERE DO VIRTUAL ASSETS STAND?

Introduction

Everyone has heard of Bitcoin. Since their first appearance, however, the world of Virtual Assets has greatly expanded and evolved, posing significant challenges in terms of regulation and assessment of the risks involved on multiple levels.

The present work focuses on the possible role of Virtual Assets for terrorism financing purposes by exploring the role that they could play as means of collecting and moving funds, as well as the issues they could pose in terms of preventive and repressive measures.

In order to do so, it appears necessary to clarify what terrorism financing is and how its criminalisation has evolved over the years, according to the evolution of the terrorist threat. For this reason, Chapter I illustrates the evolution of the crime of terrorism financing, which appears to be the result of a complex multi-level process started at the supranational level. Given the limited action on terrorism due to the disagreements surrounding its complex nature and troubled definition, until the end of the Nineties terrorism financing was not specifically addressed in the international agenda; things, however, started to change first with the 1999 UN Convention for the Suppression of Terrorism Financing, and then with UN Security Council Resolution 1373 (2001), adopted in the aftermath of the 9/11 attacks. On the wake of the Global War on Terror, indeed, the international attention on disrupting the flow of funds for terrorist purposes soared, and over the years many actors endorsed and reinforced the 1999 UN Convention and Resolution 1373 (2001), such as the Financial Action Task Force, the Council of Europe, and the European Union. In particular, while in the first decade after the 9/11 attacks (2001-2011) efforts were devoted to reach a shared criminal definition of terrorism financing, during the second decade (2012-2022) efforts have been focused on expanding its criminalisation to include the new forms of terrorist threat, namely lone terrorists and foreign fighters. The approach emerged at the supranational level largely influenced the development of the Italian criminal framework on terrorism

financing, and, throughout Chapter I, particular emphasis is posed on the interaction among the actors involved, ,as well as on the connections and intersection of terrorism – and terrorism financing – with other serious forms of crime.

Since the funding methods and strategies are strictly connected with the structure of terrorist groups and the kind of terrorist acts carried out, Chapter II offers an overview of the current international geopolitical scenario on terrorism, mapping the current trends in relation to the geographical distribution of terrorist groups and the changes in their structure and goals, namely examining the Salafi-jihadist terrorist threat (Africa, Middle East and Asia), and the new phenomenon of domestic terrorism that is rising in the Western world. Overall, the decline of State-sponsored terrorism and the progressive dissolution of rigid hierarchical structures in favour of flexible networks and cells have affected terrorists' methods of financing, both in relation to the strategies adopted to raise and move funds. With regard to the sources of funding, indeed, terrorists mainly rely on private channels, both legitimate and illegitimate; however, the choice of what method to resort to can vary, going from personal savings and donations to the abuse of non-profit organisations, as well as petty crimes or larger criminal schemes – also depending on whether terrorists are in control of territories or not. Moreover, multiple strategies to move funds can be used, including cash movements, the exploitation of formal banking system or informal value transfer systems, as well as new online payment methods. In this perspective, Chapter II analyses how Virtual Assets could be employed in these two different moments of the conducts of financing – raising and moving: tracing back the origins of Bitcoin, the Chapter examines Virtual Assets' recent developments by focusing on the features that are likely to be the most attractive to terrorists: (*pseudo*)anonymity, transnationality, decentralisation, and uneven legislative frameworks across jurisdictions.

Accordingly, the last two Chapters are dedicated to the study of the regulatory responses to the threats posed by Virtual Assets and to law enforcement strategies.

Chapter III illustrates how Virtual Assets are being progressively included in the AML/CFT framework, highlighting the primary role played by the Financial Action Task Force (FATF) in this field. Standing out as a global standard-setter, indeed, the FATF relies on an effective peer pressure system based on the implementation of hard-soft Recommendations, enjoying a large endorsement by other influential Standard-Setting Bodies that significantly contribute to the global spread of the FATF work. In particular, efforts are concentrated to address Virtual Assets' vulnerabilities, establishing customer due diligence measures and strengthening international cooperation – although struggling to tackle the issues posed by decentralised and enhanced-anonymity tools. In this context, particular attention is paid to the work of the European Union, especially with regard to the V AML Directive and the new package of Proposals aimed at boosting the European action in the AML/CFT field; after a slow start, indeed, the European Union is now aligning with the work of the FATF and responding to the need of a comprehensive regulation of the world of Virtual Assets. In addition, the Chapter analyses how the Italian AML/CFT has included Virtual Assets within its scope.

Finally, Chapter IV focuses on the instruments adopted to stem the flow of terrorists' funds, under the double perspective of asset freezing measures established pursuant to targeted sanctions, and of the extension of confiscation measures to terrorist offences. The first part analyses the evolution of United Nations targeted sanctions against terrorism – namely the sanctions regime created by Resolution 1267 (1999) and the autonomous sanctions regime established by Resolution 1373 (2001) – and their transposition at the European Union level, highlighting the changes in the legal basis adopted over the years and the issues regarding the difficult task to provide effective sanctions while ensuring the protection of individual fundamental rights. The second part examines the application of confiscation measures to terrorism, illustrating their evolution at the international level, the two-fold approach of the European Union – focused on the harmonisation of national legislation and reinforcing cooperation among Member States – and illustrating the complex and ever-evolving Italian legal framework,

which includes multiple forms of confiscation and specific provisions with regard to the confiscation of proceeds and instrumentalities related to the commission of terrorist offences.

Finally, Chapter IV includes some considerations on the application of asset freezing and confiscation measures to Virtual Assets and the possible issues that could emerge given their peculiar features.

CHAPTER I

THE CRIMINALISATION OF TERRORISM FINANCING: FROM THE INTERNATIONAL APPROACH TO THE ITALIAN LEGAL FRAMEWORK

SUMMARY: 1. A preliminary question: what is terrorism? 2. Terrorism financing at the international level before the 9/11 attacks 2.1 The United Nations approach 2.2 The 1999 United Nations International Convention for the Suppression of the Financing of Terrorism 3. The 9/11 attack and the Global War on Terror: from 2001 to 2011 3.1 The United Nations response: the Security Council Resolution 1373 (2001) ... 3.1.1 and the UN Global Counter-Terrorism Strategy 3.2 The extension of the FATF mandate on terrorism financing 3.3 The Council of Europe approach 3.4 The European Union contribution to the criminalisation of terrorism financing 3.4.1 The 2002 Council Framework Decision on combating terrorism 3.4.2 The expansion of Anti-Money Laundering tools to terrorism financing: the III AML Directive 4. The 9/11 attack and the Global War on Terror: from 2012 to 2022 4.1 The United Nations Security Council action 4.1.1 The UN Global Counter-Terrorism Strategy Reviews 4.2 The FATF updated Recommendations 4.3 The Council of Europe revisions: the 2015 Riga Protocol 4.4 The European Union initiative 4.4.1 The EU Directive 2017/541 on combating terrorism 4.4.2 A look at the development of the EU regulatory framework 4.4.3 The European Union strategies on terrorism financing 5. The evolution of the Italian criminal framework on terrorism: an overview 5.1 The criminalisation of financing pursuant to art. 270 *bis* c.p. 5.2 The financing of travels for terrorist purposes pursuant to art. 270 *quater*.1 c.p. 5.3. An autonomous form of financing: art. 270 *quinquies*.1 c.p. 5.4 The responsibility of legal entities for terrorism financing 6. Terrorism financing, organized crime and money laundering: a holistic approach

1. A preliminary question: what is terrorism?

Traditionally traced back to the attacks perpetrated by the Sicarii and the Zealots, terrorism acquired a renovated attention with Robespierre's Reign of Terror[1]. Since then, however, modern terrorism took different forms, aiming at different targets, employing different tactics and developing new forms of organisation[2], engaging scholars, national and international actors in the quest for a shared definition[3]. The term terrorism, indeed, appears to be fluid and elusive, substantially relying on a political choice which implies a moral problem, that is choosing between which acts of political violence can be justified and others that cannot[4]; effectively conveyed by the well-known expression "one man's terrorist is another man's freedom fighter", this tension has hampered the efforts made at the international level to agree on a shared definition in order to build ad efficient international cooperation[5].

---

[1] For an historical perspective on the evolution of terrorism: F. BENIGNO, "Terrore e terrorismo: Saggio storico sulla violenza politica", Einaudi, Torino, 2018.

[2] According to RAPOPORT, modern terrorism can be divided into four waves: the Anarchist Wave (1880-1920), the Anti-Colonial Wave (1920-1960 ca.), the New-Left Wave (1960-2000 ca.), and the Religious Wave (1929-today): D. C. RAPOPORT, "The four waves of modern terror. International dimensions and consequences", in "An international history of terrorism: Western and non-Western experiences", edited by J. Hanhimäki and B. Blumenau, Routledge, 2013.

[3] To the point that some scholars claim that the search for a definition of terrorism is clueless: R. R. BAXTER, "A skeptical look at the concept of terrorism", in *Akron Law Review*, 1974 Vol. 7(3), 380-387: "*We have cause to regret that a legal concept of "terrorism" was ever inflicted upon us. The term is imprecise; it is ambiguous; and above all, it serves no operative legal purpose*", and, more recently: D. BRYAN, L. KELLY, S. TEMPLER, "The failed paradigm of 'terrorism'", in *Behavioral Sciences of Terrorism and Political Aggression*, 2011, Vol. (3)2, 80-96. Others, instead, emphasise the importance to achieve a shared definition: B. GANOR, "Defining terrorism: is one man's terrorist another man's freedom fighter?", in *Police Practice and Research*, 2002, Vol. (3) 4, 287-304. For a comprehensive overview of the problems in defining terrorism: A. P. SCHMID, "Terrorism. The Definitional Problem", in *Case Western Reserve Journal of International Law*, 2004, Vol. (36) Issues & 3, 375-420. For an overview of the definitions of terrorism: J. EASSON, A. P. SCHMID, in "250-plus Academic, Governmental and Intergovernmental Definitions of Terrorism", in "The Routledge Handbook of Terrorism Research", edited by Alex P. Schmid, Taylor & Francis Group, 2011, 99-158. Lastly, given the specific features of terrorism, it has been suggested that terrorism would constitute a *different dimension of crime*: G. P. FLETCHER, (2006), "Indefinable concept of terrorism", in *Journal of International Criminal Justice*, 2006, Vol. (4) 5, 894-911.

[4] It is clear, however, that labelling someone as a "terrorist" entails a negative judgement: B. HOFFMAN, "Inside Terrorism", 3rd ed., Columbia University Press, New York, 2017, 24. In this regard, it is interesting to remind that the Jacobins appear to have used the term "terrorist" in a positive sense until the 9th of Thermidor: W. LAQUEUR, "Terrorism", Weidenfeld and Nicolson, London, 1977, 6.

[5] In this sense: G. WARDLAW, "Political Terrorism: theory, tactics, and counter-measures", Cambridge University Press, 1982, 4: "*at the international level, the political support given to sectional interests militates against a universal definition that could form the basis for international law and action*". On the

Nevertheless, there is some level of agreement on the main features of modern terrorism, which can be described as a "*deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change*", which is "*specifically designed to have far-reaching psychological effects beyond the immediate victim(s) or object of the terrorist attack*"[6]. This concise definition effectively depicts the modalities as well as the ultimate goals of terrorists, and it could serve as a useful starting point to reflect on the problems of reaching a satisfactory criminal legal framework on terrorism and, as a consequence, of terrorism financing as well. In the following paragraphs, indeed, it will be illustrated the long and complex process that interested several actors at international and regional level, and that led to the current legal framework in relation to the criminalisation of the conducts of terrorism financing.

2. Terrorism financing at the international level before the 9/11

The first attempt to build an international suppressive framework in the field of terrorism dates back to 1937, when the League of Nations presented the draft of the Convention for the Prevention and Punishment of Terrorism[7]. Article 2 of the Convention provided a list of conducts which should be held as acts of terrorism[8]

need to reach a definition in order to build a strong international legal framework: A. BIANCHI, "Security Council's Anti-terror Resolutions and their Implementations by Member States", in *Journal of International Criminal Justice*, 2006, Vol. 4 (5), 1048; A. CASSESE, "The Multifaceted Criminal Notion of Terrorism in International Law", in *Journal of International Criminal Justice*, 2006, Vol. (4) 5, 934.

[6] B. HOFFMAN, *Ibid.*, 44.

[7] Convention for the Prevention and Punishment of Terrorism, League of Nations, Geneva, 1937.

[8] Art. 2: "*Each of the High Contracting Parties shall, if this has not already been done, make the following acts committed on his own territory criminal offences if they are directed against another High Contracting Party and if they constitute acts of terrorism within the meaning of Article 1:*

(1) Any wilful act causing death or grievous bodily harm or loss of liberty to:

(a) Heads of States, persons exercising the prerogatives of the head of the State, their hereditary or designated successors;

(b) The wives or husbands of the above-mentioned persons;

(c) Persons charged with public functions or holding public positions when the act is directed against them in their public capacity.

when committed "*against a State and intended or calculated to create a state of terror in the minds of particular persons, or a group of persons or the general public*" (art. 1 (2)), and, urging State Parties to qualify as criminal offence – among others – the "*wilful participation in any such act*" (art. 3, par. 1, 4)) and the "*assistance, knowingly given, towards the commission of any such act*" (art. 3, par. 1, 5)). Therefore, the conducts of financial support could only be relevant as forms of participation or assistance, and, although not explicitly recognising them an autonomous nature, it did not preclude this option to State Parties which would have deemed necessary to do so in order to "*prevent an offender escaping punishment*" (art. 4)[9].

Although never entered into force, the draft represents an interesting – yet isolated – attempt of providing a comprehensive framework in the field of terrorism at the international level[10]. In fact, the Conventions adopted afterwards show a clear sectoral approach, in this way refusing to achieve a consensus on the definition of terrorism and focusing on the practical needs of the moment: this is the case, indeed, both of the United Nations sectorial conventions adopted in response to specific

(2) *Wilful destruction of, or damage to, public property or property devoted to a public purpose belonging to or subject to the authority of another High Contracting Party.*
(3) *Any wilful act calculated to endanger the lives of members of the public.*
(4) *Any attempt to commit an offence falling within the foregoing provisions of the present article.*
(5) *The manufacture, obtaining, possession, or supplying of arms, ammunition, explosives or harmful substances with a view to the commission in any country whatsoever of an offence falling within the present article*".

[9] Art. 4: "*Each of the offences mentioned in Article 3 shall be treated by the law as a distinct offence in all cases where this is necessary in order to prevent an offender escaping punishment*".

[10] Nonetheless, some regional conventions managed to overcame the sectoral approach, namely the Arab Convention for the Suppression of Terrorism (1998) and Organization of African Unity Convention on the Prevention and Combating of Terrorism (1999): R. BORSARI, "Diritto punitivo sovranazionale come sistema", CEDAM, Padova, 2007, 79. Yet, these two regional anti-terrorism tools explicitly exclude from the scope of terrorism those acts carried out in the struggle for freedom: T. WEIGEND, "Universal Terrorist", in *Journal of International Criminal Justice*, Vol. 4 (5), 2006, 922.

issues[11] and of the 1977 European Convention on the Suppression of Terrorism[12], which, at that time being, was the only instrument available within the Council of Europe system in relation to the fight against terrorism, and, similarly to the sectoral UN Conventions, merely listed a series of conducts which should be considered falling under the umbrella of "acts of terrorism", mainly focusing on extradition procedures[13].

2.1 The United Nations approach

During the first half of the Nineties, the United Nations addressed the problem of terrorism through the action of the Security Council, which focused on targeting State-sponsored terrorism[14] in response to contingent needs, adopting *ad hoc*

[11] They can be here recalled: Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo, 1963); Convention for the Suppression of Unlawful Seizure of Aircraft (the Hague, 1970); Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal, 1971) and its supplementary Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (Montreal, 1988); Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); International Convention against the Taking of Hostages (1979); Convention on the Physical Protection of Nuclear Material (Vienna, 1980); Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (Rome, 1988); Convention on the Marking of Plastic Explosives for the Purpose of Detection (Montreal, 1991); International Convention for the Suppression of Terrorist Bombings (1997); International Convention for the Suppression of Acts of Nuclear Terrorism (New York, 2005). Besides, an attempt to tackle terrorism in a broader manner was represented by the General Assembly Resolution A/RES/27/3034 (1972), adopted on 18 December 1972, which established an Ad Hoc Committee on International Terrorism, consisting of 35 members. However, the Resolution did not condemn terrorism, rather urged states to eliminate the underlying causes of it and still reaffirmed the right to self-determination: M. HALBERSTAM, "The evolution of the United Nations position on terrorism: from exempting National Liberation Movements to criminalizing terrorism wherever and by whomever committed", in *Columbia Journal of Transnational Law*, 2003, Vol. 41(3), 573-574.

[12] European Convention on the Suppression of Terrorism (ETS No. 090), adopted on 27 January 1977 and entered in force on 4 August 1978.

[13] For this reason, the 1977 Convention could be held as an example of the application of the so-called "inductive approach": G. LEVITT, "Is terrorism worth defining?", in *Ohio Northern University Law Review*, Vol. 13, Issue 1 (1986), 97-116.

[14] Indeed, it was already a well-known phenomenon, as "*after the First World War it became the fashion among some governments to finance terrorist groups*" (…) and "*this fashion became even more popular after the Second World War*": W. LAQUEUR, *Ibid.*, 87-88.

Resolutions[15]. These include the UNSC Resolution 748 (1992)[16], addressed to the Libyan government in relation to the Lockerbie case, in which the Security Council reaffirmed that "*every State has the duty to refrain from organizing, instigating, assisting o participating in terrorist acts in another State*"; UN SC Resolution 1044 (1996)[17], adopted in response to the attempted assassination of the President of the Arab Republic of Egypt, in Addis Ababa on 26 June 1995, that called upon Sudan to "*desist from engaging in activities of assisting, supporting and facilitating terrorist activities*", and UN SC Resolution 1189 (1998)[18], issued in response to the attacks that took place on 7 August 1998 in Nairobi and Dar-es-Salaam against the U.S. embassies, which stressed that "*every Member State has the duty to refrain from organizing, instigating, assisting or participating in terrorist acts in another State*". These Resolutions share a common concern about the forms of State-sponsored assistance to terrorist acts, yet their scope remains limited to the specific circumstances they refer to, and they refrain from making any explicit reference to terrorism financing, including it implicitly in the conducts of assistance to terrorist acts.

By the second half of the Nineties, however, the United Nations started to expand its action: with Resolution 49/60 (1994)[19] the General Assembly approved the "Declaration on Measures to Eliminate International Terrorism", and the term "terrorist financing" made its first appearance at the international level[20]. The General Assembly indeed, did not only affirm that States must "*refrain from*

[15] It is interesting to notice, however, that the Security Council used the term "terrorism" for the first time in Resolution S/RES/579 (1985), adopted by at its 2637th meeting, on 18 December 1985 in relation to the Achille Lauro seizure. For an overview of the UN Security Council practice on terrorism until the early 2000s: B. SAUL, "Defining Terrorism in International Law", Oxford University Press, 2006, 213-250.

[16] S/RES/748 (1992), adopted by the Security Council at its 3063rd meeting on 31 March 1992. For the first time, the Security Council qualified acts of international terrorism as threats to international peace and security – a practice that continued in the following years: A. BIANCHI, *Ibid.*, 1045.

[17] S/RES/1044 (1996) adopted by the Security Council at its 3627th meeting, on 31 January 1996.

[18] S/RES/1189 (1998) adopted by the Security Council at its 3915th meeting, on 13 August 1998.

[19] A/RES/49/60 "Measures to eliminate international terrorism", adopted on 9 December 1994.

[20] The Security Council, instead, used the term "terrorist financing" for the first time in Resolution S/RES/1269 (1999) (*infra* Chapter IV § 1.2) – which was not related to state-sponsored terrorism: I. BANTEKAS, "The International Law of Terrorist Financing, in The American Journal of International Law", Vol. 97, 2003, 315-332.

organizing, instigating, assisting or participating in terrorist acts in territories of other States, or from acquiescing in or encouraging activities within their territories directed towards the commission of such acts", but specified that they must "*refrain from organizing, instigating, facilitating, financing, encouraging or tolerating terrorist activities and to take appropriate practical measures to ensure that their respective territories are not used for terrorist installations or training camps, or for the preparation or organization of terrorist acts intended to be committed against other States or their citizens*".

Moreover, this Resolution marks a significant step ahead in the international approach to the terrorist threat, as it condemns terrorism regardless of the reasons behind it – in this way taking a clear position on the debate about whether some acts could be justified in the name of the struggle for self-determination.[21]

Therefore, it can be argued that the Declaration reinforced the position of the United Nations on terrorism by expressively referring to terrorist financing and unequivocally condemning acts of terrorism; still, it merely addressed the phenomenon of State-sponsored terrorism.

In this respect, the General Assembly took a stand two years later, with the adoption of Resolution 51/210 (1996)[22], which established an Ad Hoc Committee (the Sixth Committee) in order to "*elaborate an international convention for the suppression of terrorist bombings and an international convention for the suppression of acts of nuclear*

[21] Declaration on Measures to Eliminate International Terrorism, art. 1, par. 1: "*The States Members of the United Nations solemnly reaffirm their unequivocal condemnation of all acts, methods and practices of terrorism, as criminal and unjustifiable, wherever and by whomever committed, including those which jeopardize the friendly relations among States and peoples and threaten the territorial integrity and security of States*", and art. 1, par. 3: "*Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them*". In this sense: M. HALBERSTAM, *Ibid*, 573-584. The Author underlines that previous UN General Assembly Resolutions reaffirmed the right to self-determination, "*without explicitly condemning terrorism regardless of the cause*" – such as A/RES/32/147 (1977), A/RES/34/145 (1979), A/RES/36/109 (1981) and A/RES/38/130) – noticing that this trend stopped first with Resolutions A/RES/48/122 (1993) and A/RES/49/185 (1994), and it then set off with the 1994 Declaration.

[22] A/RES/51/210, adopted at its 88th plenary meeting on 17 December 1996.

terrorism"[23], and called upon States to " *take steps to prevent and counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations, whether such financing is direct or indirect through organizations which also have or claim to have charitable, social or cultural goals or which are also engaged in unlawful activities such as illicit arms trafficking, drug dealing and racketeering, including the exploitation of persons for purposes of funding terrorist activities, and in particular to consider, where appropriate, adopting regulatory measures to prevent and counteract movements of funds suspected to be intended for terrorist purposes without impeding in any way the freedom of legitimate capital movements and to intensify the exchange of information concerning international movements of such funds*", and reiterated States to "*refrain from financing, encouraging, providing training for or otherwise supporting terrorist activities*"[24].

So, while until the mid-Nineties the United Nations included the conducts of financing under the umbrella of "assistance", considering them as forms of participation to terrorist acts, and limited its action to State-sponsored terrorism, in the last years of the decade an effort towards a broader action can be appreciated; a trend, indeed, has then been followed with the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism, which can be undoubtedly considered as one of the international cornerstones in the fight against terrorism financing.

2.2 The 1999 United Nations International Convention for the Suppression of the Financing of Terrorism

The kick-start for the adoption of the 1999 United Nations International Convention (1999 UN Convention) for the Suppression of the Financing of Terrorism was a draft presented by the Permanent Representative of France to the United Nations on 3

[23]The United Nations International Convention for the Suppression of Terrorist Bombings was adopted in New York, on 15 December 1997, while the UN International Convention for the Suppression of Acts of Nuclear Terrorism was adopted in New York, on 13 April 2005.

[24] The first practical application of this new expanded scope is represented by UN SC Resolution S/RES/1267, adopted at its 4051st meeting on 15 October 1999: *infra* Chapter IV § 1.1.

November 1998, which invited State Members to take action to address the specific issue of terrorism financing[25]. Following this input, the General Assembly appointed the Sixth Committee established pursuant to Resolution 51/210 (1996) (*supra* §2.1)[26] to start the *travaux préparatoires*[27], which resulted in the adoption of the Convention with Resolution 54/109 on 9 December 1999, entered into force on 10 April 2002[28].

Focusing on the criminal law provisions of the Convention, article 2, paragraph 1 criminalises terrorism financing as follows:

> *"Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:*
>
> *(a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or*
>
> *(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to*

[25] Letter dated 3 November 1998 from the Permanent Representative of France to the United Nations addressed to the Secretary-General - Draft international convention for the suppression of terrorist financing, adopted by Sixth Committee of the General Assembly on 4 November 1998 (A/C.6/53/9).

[26] At that time, the Sixth Committee had already finished the draft of the International Convention for the Suppression of Terrorist Bombings, and it has been remarked that many provisions of the 1999 Convention draw on its provisions: R. LAVALLE, *Ibid.,* 494-495. Moreover, it is interesting to notice that Resolution A/RES/62/71 of 6 December 2007 charged the Sixth Committee to work on a comprehensive convention on international terrorism, and a year later a dedicated Working Group was set up. However, the elaboration of the draft is still ongoing: in its Resolution A/RES/76/121, adopted on 17 December 2021 the General Assembly recommended the Committee to establish a working group aimed, *inter alia*, to complete a draft of the Convention.

[27] A/RES/53/108 (1998), adopted at its 83rd plenary meeting on 8 December 1998.

[28] It is interesting to remark that the *travaux* were particularly rapid. However, despite the fact that the UN had already expressed its view (*supra,* note 21), the issue concerning whether terrorism could be sometimes justified has been long debated, as some States were divided on the opportunity to consider as acts of terrorism those acts carried out by national liberation movements or activities of resistance against the occupation of a foreign country: P. KLEIN, "International Convention for the Suppression of the Financing of Terrorism", in *United Nation Audiovisual Library of International Law*, 2009, 2.

intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."

While subparagraph *(a)* criminalised the funding of specific acts identified by nine sectoral conventions already in place[29], subparagraph *(b)* extended the criminalisation of financing when linked to terrorist activities, setting out some specific elements[30] which have been held establishing a mini-definition of "terrorism" [31].

According to the Convention, the conducts of financing may consist of both in the *provision* or *collection*[32] of funds, where *funds* are to be intended as "*assets of every*

---

[29] Namely: Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973; International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979; Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988; Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988; International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997 (Annex). Doubts were raised on the effectiveness of this provision, as "*not all countries are bound by the full set of annexed treaties; the consequence is that Article 2(1)(a) has a different reach in every State Party*": M. PIETH, "Criminalizing the financing of terrorism", in *Journal of International Criminal Justice*, 2006, Vol. (4) 5, 1079.

[30] In this sense: P. KLEIN, *Ibid.*, 2. Moreover, it has been remarked that, unlikely the previous sectoral UN Convention on terrorism-related issues, the 1999 Convention for the Suppression of Terrorism Financing "*besides setting out the objective elements of criminal conduct, also place emphasis on the* purpose *pursued by the perpetrators*" – among the sectoral Convention, a similar approach can be observed only in the 1979 UN Convention against the Taking of Hostages (art. 1): A. CASSESE, *Ibid.*, 942-943.

[31] A. AUST, "Counter-Terrorism: A New Approach. The International Convention for the Suppression of the Financing of Terrorism", in *Max Planck Yearbook of United Nations Law*, 2001, Vol. 5, 294-295. Moreover, it has been remarked that this is a mere *indirect* definition of terrorism, which exclusively serve for the purposes of defining terrorism financing: A. GIOIA, "The UN Conventions on the Prevention and Suppression of International terrorism", in "International Cooperation in Counter-terrorism. The United Nations and Regional Organizations in the Fight Against Terrorism", ed. by G. Nesi, Ashgate, 2005, 13, who, commenting on the lack of a shared definition of terrorism, points out that "*it seems paradoxical that the financing of terrorism as a whole is considered to be an offence, whereas terrorism itself is only criminalized if it consists of specific acts covered by the 'sectoral' treaties*".

[32] While the provision suggests an active action, the collection would refer a more passive one. In this regard, it has been pointed that during the *travaux préparatoires* it had been suggest to add also

kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit" (art. 1 par. 1), in this way providing a broad definition, covering any tangible or intangible asset[33].

At a closer look, the stretch towards a far-reaching criminalisation of terrorism financing seems to be reaffirmed by the fact that it covers the conducts carried out by *any person* – in this way including both private individuals and public officials, as well as legal entities as set in art. 5 – and *by any means, directly or indirectly*, thus including also the use of intermediaries[34]. Yet, it shows a particular concern in delimiting its scope, requiring the conducts to be carried out *unlawfully* – in order to exclude those cases where financial aid was made available to organizations which also have legit purposes[35] - and *wilfully*, emphasising that the financing has to be carried out in a deliberate manner[36]. In fact, the *mens rea* requires the conduct to be carried out with the *intention* that the funds should be used or in the *knowledge* that they are to be used in order to carry out the conducts described in subparagraphs *(a)* and *(b)*, and, even if the choice of including these two variants is debatable[37], it is quite clear that the Convention excluded negligence to be sufficient to integrate the offence of terrorism financing.[38]

---

the conduct of receiving funds, but this option was excluded to not unduly extend the criminalization: A. AUST., *Ibid.*, 295.

[33] R. LAVALLE, "The International Convention for the Suppression of the Financing of Terrorism", in *Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht*, 2000, 496: the Author thus suggests that this definition of "funds" resembles to some sort of "material assistance".

[34] A. AUST, *Ibid.*, 294.

[35] In this sense: A. AUST, *Ibid.*, 294-295; R. LAVALLE, *Ibid.*, 500.

[36] A. AUST, *Ibid.*, 294-295.

[37] In this sense LAVALLE, who remarks that, even if it could be argued that the element of intent would display the wish and belief that those funds are going to be used for terrorist purposes, while the element of knowledge would imply an element of certainty, there is not a real difference between the two options: R. LAVALLE, *Ibid.*, 498-500.

[38] However, it is arguable whether this dual formulation would allow to go beyond the element of the direct intent, including also the *dolus eventualis*: R. LAVALLE, *Ibid.*, 499; M. PIETH, *Ibid.*, 1081-1082: the Author, anyway, underlines that "*both intent and knowledge may well be interpreted as representing a standard of firm, direct intent*".

Moreover, the Convention explicitly states that also the attempt to commit any of the offences set out at article 1 shall be punishable (art. 2, par. 4), as well as anyone who participates, organizes or direct others or intentionally contributes to their commission (art. 2, par. 5).

The rich framework depicted by the Convention is completed by requiring State Parties to establish the liability of legal entities – even if it leaves the choice to each State Party to decide whether this liability should be criminal, civil or administrative – and to identify, detect, freeze or seize and forfeiture the funds used or allocated for the purposes of terrorism financing, as well as the proceeds derived from such offences (art. 8.), clarifying that *proceeds* are to be intended as "*funds derived from or obtained, directly or indirectly, through the commission of an offence set forth in article 2*" (art. 1)[39].

Although the Convention covers only the conducts aimed at financing acts of terrorism, in this way not covering those conducts aimed at supporting terrorist organisations themselves (*structural financing*), it marks a big step ahead in the suppression of terrorism financing, shaping it as an autonomous offence[40], heavily relying on the subjective element and punishable also in those case where the funds were not actually used to carry out a terrorist act[41], since "*it is the intent to further the commission of an act of terrorism, which gives rise to prosecution under the Convention*"[42],

---

[39] On this point, however, it has been remarked that the Convention does not require to criminalise the laundering of such funds; a gap closed in 2001 by the FATF Special Recommendations on the financing of terrorism (*infra* § 3.2): W. GILMORE, "Money laundering", in "Routledge Handbook of Transnational Criminal Law", edited by N. Boister, R. J. Currie, 2015, 342. On the confiscation of proceeds related to terrorist offences: *infra* Chapter IV.

[40] In this sense: S. DE VIDO, "Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione Europea", CEDAM, Padova, 2012, 55 ss.; A. GARDELLA, "Fighting the Financing of Terrorism: Judicial Cooperation", in Freezing the Assets of International Terrorist Organisations", in "Enforcing International Law Norms against Terrorism", ed. By A. Bianchi, Hart, 2004, 437. *Contra*: V. ARAGONA, "Il contrasto al finanziamento del terrorismo. Criticità e innovazioni della nuova disciplina italiana", in *Diritto Penale Contemporaneo*, Vol. 1, 2017, 97, who states that terrorism financing was still shaped as an ancillary offence to terrorism.

[41] Art. 3: *"For an act to constitute an offence set forth in paragraph 1, it shall not be necessary that the funds were actually used to carry out an offence referred to in paragraph 1, subparagraph (a) or (b)"*.

[42] P. KLEIN, *Ibid.*, 2. In so doing, the subjective element plays as *discrimen* between legal and illegal behaviour: M. PIETH, *Ibid.*, 1081.

constituting one of the first and most significant examples of preventive criminal paradigm[43].

3. The 9/11 attack and the Global War on Terror: from 2001 to 2011

In the morning of 11 September 2001 a series of coordinated terrorist attacks stroke the U.S. territory: two hijacked planes hit the World Trade Center in New York City, another one hit the west side of the Pentagon in Arlington, while another attack directed to Washington, D.C. failed and resulted in the crush of the hijacked plane in Pennsylvania[44]. These attacks – which resulted in almost three thousand deaths – marked a crucial turning point in the fight against terrorism, starting the so called "Global War on Terror"[45], announced by President George W. Bush a few days later:

> "***Our war on terror begins with al Qaeda, but it does not end there***. *It will not end until every terrorist group of global reach has been found, stopped and defeated* (…) *Americans should not expect one battle, but a* ***lengthy campaign***, *unlike any other we have ever seen. It may include dramatic strikes, visible on TV, and covert operations, secret even in success. We will* ***starve terrorists of funding***, *turn them one against another, drive them from place to place, until there is no refuge or no rest. And we will pursue nations that provide aid or safe haven to terrorism. Every nation, in every region, now has a decision to make.* ***Either you are with us, or you are with the terrorists***. *From this day*

[43] F. ROSSI, "Il contrasto al terrorismo internazionale nelle fonti penali multilivello", Jovene, Napoli, 2022, 100.

[44] For the complete U.S. government report on the 9/11 events, see "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Report)", U.S. Government, 22 July 2004.

[45] For an analysis of the "war on terrorism" *discourse* as an exercise of power: R. JACKSON, "Writing the war on terrorism. Language, politics and counter-terrorism", Manchester University Press, 2005. For an analysis of the changes in the U.S. Presidents' speeches on the War on Terror over the years: B. CHING, "Echoes of 9/11: Rhetorical Analysis of Presidential Statements in the "War on Terror"", in *Seton Hall Law Review*, Vol. 51 (2), 2020, 431-460.

forward, any nation that continues to harbor or support terrorism will be regarded by the United States as a hostile regime (…) *This is not, however, just America's fight. And what is at stake is not just America's freedom.* ***This is the world's fight***. ***This is civilization's fight***. *This is the fight of all who believe in progress and pluralism, tolerance and freedom*"[46].

As outlined when analysing the UN Resolutions adopted during the Nineties, terrorism was not a novelty. However, these attacks exposed the vulnerability of the U.S. and of the Western world as a whole, causing a strong reaction on different levels. While the NATO invoked the principle of collective defence (art. 5)[47] for the first time in its history, Bush presidency strongly reacted both at the domestic level – with the adoption, among others, of the controversial USA Patriot Act[48] – and at the international level, launching military operations in Afghanistan and Iraq[49]. Based on the dichotomy between good and evil and adopting a pre-emptive

[46]G. W. BUSH, Address to the Joint Session of the 107th Congress, 20 September 2001, in *Selected Speeches of President George W. Bush 2001 – 2008*, White House Archives, 65-75.

[47] Art. 5 of the North Atlantic Treaty (1949): "*The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.*
Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security".

[48] For an analysis: D. COLE, "Enemy Aliens", in *Stanford Law Review*, 2002, Vol. (54) 5, 953-1004.

[49] In this way trying to relaunch the U.S. as the leader of international security: B. BUZAN, "Will the 'global war on terrorism' be the new Cold War?", in *International Affairs*, 2006, Vol. (82) 6, 1102: "*the main significance of the GWoT is as a political framing that might justify and legitimize US primacy, leadership and unilateralism, both to Americans and to the rest of the world*".
While the war against Afghanistan was generally supported by the international community, the invasion of Iraq raised more criticism, accused of being a political choice not backed by a real necessity: M. EVANGELISTA, "Law, Ethics, and the War on Terror", Polity Press, Cambridge, 2008, 103 ss.

approach[50], the War on Terror has largely informed Western securitisation policies[51], which, although not sharing the war-like features of the U.S. approach, have led to a rapid growth of the international, regional and national measures adopted in fight against terrorism and terrorism financing, starting a "Financial War on Terror" as well under the well-known motto of "follow the money". In particular, the international counter-terrorism action post-9/11 is characterised by the replacement of the traditional instruments of multilateral treaties with the faster adoption of global standards, which have been then legitimised at the regional level with the adoption of multilateral conventions, such as the one elaborated by the Council of Europe, and, in the case of the European Union, by traditional binding instruments[52] (*infra* Chapter III § 1).

---

[50] The pre-emptive approach was applied both on the military side ("pre-emptive self-defence" doctrine) and on the legislative side. For an analysis of Bush's ""pre-emptive self-defence" doctrine outlined in the 2002 U.S. National Security Strategy: C. BROWN, "After 'Caroline': NSS 2002, practical judgment, and the politics and ethics of pre-emption", in "The Ethics of Preventive War", edited by D. K. Chatterjee, Cambridge University Press, 2013, 27-45; R. JERVIS, "Understanding the Bush doctrine: Preventive Wars and Regime Change", in *Political Science Quarterly*, 2016, Vol. (131) 285-311; S. D. MURPHY, "The doctrine of preemptive self-defense", in *Villanova Law Review*, 2005, Vol. (50) 3, 699-748. On prevention, see also: M. WALZER, "Just and Unjust Wars", 5th edition, Basic Books, New York, 2015. For an analysis of the pre-emptive approach at the legislative level: L. STAMPNITZKY, Disciplining terror: how experts invented "terrorism", Cambridge University Press, 2013, 165-232. The Author also remarks how the war narrative had already been used to govern terrorism during the Reagan administration, albeit "*in contrast to the preemptive "war on terror" that would arise after 9/11, this first war on terror was driven by a logic of retaliation, in which military counterterrorism strikes were akin to punishment for a crime*": L. STAMPNITZKY, *Ibid*, 110. On Reagan's legacy on combating terrorism, see also: P. KENGOR, "Reagan's "March of Freedom in a Changing World" and K. K. SKINNER, "The Beginning of a New U.S. Grand Strategy. Policy on Terror during the Reagan Era", in Reagan's Legacy in a World Transformed, edited by J. L. Chidester and P. Kengor, Harvard University Press, 2015, 76-97 and 101-123 respectively.

[51] On securitisation: O. WAEVER, "Securitization and Desecuritization", in "On Security", by R. D. LIPSCHUTZ, Columbia University Press, 1995, 46-86. In particular, according to the Author,"*the use of the security label does not merely reflect whether a problem is a security problem, it is also a political choice, that is, a decision for conceptualization in a special way. When a problem is "securitized", the act tends to lead to specific ways of addressing it: threat, defense, and often state-centered solutions*" (p. 65). Besides, the acceptance by the target audience is crucial: "*What is essential is the designation of an existential threat requiring emergency action or special measures and the acceptance of that designation by a significant audience*": O. WAEVER, B. BUZAN, J. DE WILDE, "Security: a new framework for analysis", Lynne Rienne Publishers, 1998 27. On the centrality of the role of the audience, see also: T. BALZACQ, "A theory of securitization. Origins, core assumptions, and variants", in "Securitization theory. How security problems emerge and dissolve", edited by T. Balzacq, Routledge, London, 2011, 1-30.

[52] See V. MITSILEGAS, "Transnational Criminal Law and the Global Rule of Law", in "The Global Community: Yearbook of the International Law and Jurisprudence 2016", Oxford University Press, 2017, 47-80.

3.1The United Nations response: the Security Council Resolution 1373 (2001)…

On 12 September 2001 the Security Council condemned the 9/11 attacks with Resolution 1368[53] and, a couple of weeks later, took a big step ahead in counter-terrorism financing with the unanimous adoption of the Resolution 1373 (2001)[54]. Considering the 9/11 attacks as a threat to international peace and security, the Resolution requires all States to "*prevent and suppress the financing of terrorist acts*" (par. 1 a)), to "*criminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts*" (par. 1 b)), and to immediately freeze funds and any other financial asset or economic resource related to persons involved in the commission of terrorist acts (par. 1 c))[55], as well as to "*prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities*

[53] S/RES/1368 (2001), adopted by the Security Council at its 4370th meeting, on 12 September 2001. Although advocating a law enforcement-type response, the Resolution did not state that 9/11 attacks constituted an "armed attack": M. WILLIAMSON, "Terrorism, War and International Law. The Legality of the Use of Force Against Afghanistan in 2001", Ashgate, 2009, 178-179. On the ambiguity of the Resolution, stretched between the right to self-defence claimed by the U.S. and the traditional response of collective security: A. CASSESE, *Ibid*., 993-1002; B. FASSBENDER, "The Un Security Council and International Terrorism", in "Enforcing international Law Norms Against Terrorism", edited by A. Bianchi, Hart Publishing, 2004, 86-89. For a different point of view: C. GRAY, "International Law and the Use of Force", 4th edition, Oxford University Press, 2018, 206: emphasizing the importance of the reference to self-defence in the preamble, the Author affirms that "*it seems arguable that the members of the Security Council were in fact willing to accept the use of force in self-defence by the USA"*. On the nature of self-defence within the United Nations system: H. KELSEN, "Collective Security and Collective Self-Defense Under the Charter of the United Nations", in *The American Journal of International Law*, 1948, Vol. (42), 784: "*Self-defense is that minimum of of self-help which, even within a system of collective security based on a centralized force monopoly of the community, must be permitted*".

[54] S/RES/1373 (2001) adopted by the Security Council at its 4385th meeting, on 28 September 2001.

[55] For an analysis of the implications of par. 1, c): *infra*, Chapter IV § 1.2.

owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons" (par. 1 (d)).

In so doing, Resolution 1373 (2001) expanded the criminalisation of terrorism financing: indeed, while art par. 1, b) corresponds to art. 2, par. 1 of the 1999 Convention, the provisions of par. 1, d) enable to include not only the criminalisation of financing of terrorist organisations overall (*structural financing*), given the omission of the element of the "intention" that such funds are to be used to carry out terrorist acts[56].

Moreover, the Resolution requires States to not provide any form of support to persons or entities involved in terrorist acts, to exchange information with other States in order to prevent the commission of terrorist acts, to deny safe havens, to prevent the use of their territories for terrorist purposes, to ensure that people involved in terrorist activities are brought to justice, to cooperate in criminal investigations and proceedings and to implement effective border controls (par. 2).

The Resolution was adopted pursuant to Chapter VII of the UN Charter[57], which notably enables the Security Council to make recommendations or take measures in order to maintain or restore international peace and security in case of any threat to the peace, breach of the peace, or act of aggression (art. 39 UN Charter)[58]; however, such Resolutions do not constitute a manifestation of a specific legislative power of

[56] In this sense: S. DE VIDO, "Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione Europea", *Ibid*., 65-66. V. ARAGONA, *Ibid*., 97; M. A. MANNO, "Il contrasto al finanziamento del terrorismo internazionale. Tra prevenzione sanzionatoria e punizione preventiva", Giappichelli, Torino, 2020, 73.

[57] On the different functions of the Security Council acting under Chapter VI or Chapter VII: B. CONFORTI, C. FOCARELLI, "The Law and Practice of the United Nations", 5th ed., BRILL, 2016, 190-193.

[58] Here, "threat" should be interpreted as an objective, concrete and current threat, on the basis of a combined lecture of article 39 and 33 of the UN Charter: L. PASCULLI, "Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali", Padova University Press, 2012, 204. With regard to the measures article 39 refers to, they are namely those measures not involving force established by art. 41 (i.e., sanctions) and, those measures involving force established by art. 42. For an analysis of the use of sanctions pursuant to art. 41 in relation to terrorism: see, *infra* Chapter IV.

the Security Council, but rather an expression of its political power, which results in the adoption of individual enforcement measures[59].

Nevertheless, this assumption has been challenged by Resolution 1373, which differs from the ones previously adopted for several reasons. First of all, while the previous Resolutions were issued in response to specific events, the scope of Resolution 1373 goes beyond the 9/11 attacks – although they are explicitly recalled in the preamble – encompassing all acts of terrorism[60]. Indeed, the Resolution seems to be aimed at compensating the voluntary basis set out by the 1999 UN Convention, making some of its provisions binding for all UN Member States – namely the provisions set out at articles 1 and 2 – regardless of whether they had already joined the Convention or not[61]; in fact, although the Security Council does not gather all State Members[62], its Resolutions are mandatory for all the 191 Members, in this way displaying a unilateral nature[63]. Therefore, the combination of the unilateral nature of the measures adopted with Resolution 1373 and their long-term and broad scope, has led scholars to argue that the UN Security Council acted as a real legislator,

---

[59] In this sense: A. MARSCHICK, "The Security Council as a World Legislator? Theory, Practice & Consequences of an Expanding World Power", in *Institute for International Law and Justice New York University School of Law*, Working Paper 2005/18, 6. However, it has been affirmed that the Security Council would have always had a legislative authority when acting in response to a threat or breach of peace or act of aggression: F. L. KIRGIS JR., "The Security Council's first fifty years", in *The American Journal of International Law*, 1995, Vol. (89) 3, 506-539. For a detailed comment – and criticism – on the alleged legislative powers of the Security Council: G. ARANGIO-RUIZ, "On the Security Council's 'Law Making'", in *Rivista di Diritto Internazionale*, Vol. 2, 2000, 609-726.

[60] In this sense: A. BIANCHI, Security Council's Anti-terror Resolutions *Ibid.*, 1047; A. MARSCHICK, *Ibid.*, 15, who remarks that the preamble of the Resolution expresses the determination of the Security Council to prevent all *such* acts – and not only *these* acts - in this way extending its action to all terrorist acts.

[61] At the time of the adoption of Resolution 1373 (2001), only four states had already ratify the 1999 UN Convention – namely, Botswana, Sri Lanka, the United Kingdom, and Uzbekistan). Interestingly, the article 3, (d) of Resolution 1373 merely calls States to "*become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999*", not obliging them to do so. Apparently, this was due to a lack of political willingness of the States to be so bound, as Resolution 1373 (2001) does not cover all the provisions set out by the Convention: P. C. SZASZ, "The security council starts legislating", in *American Journal of International Law*, 2002, Vol. (96) 4, 903.

[62] The UN Security Council is composed of fifteen Members: five permanent Members (China, France, Russian Federation, the United Kingdom, and the United States) and ten non-permanent Members elected for two-year terms by the General Assembly (art. 23 UN Charter).

[63] In this sense: M. HAPPOLD, "Security Council Resolution 1373 and the Constitution of the United Nations", in *Leiden Journal of International Law*, 2003, 16(3), 593-610.

establishing abstract and general binding obligations upon all States, and in this way going beyond its mandate[64].

Nonetheless, the alleged lack of legal basis appears to have been legitimised by the large consensus that States manifested welcoming its adoption[65], which has been confirmed by the broad participation showed by State Members in the implementation of the Resolution under the guidance of the Counter-Terrorism Committee (CTC), established by the Resolution itself to help State Members in the implementation of the new obligations established[66].

3.1.1 and the Global Counter-Terrorism Strategy

Along with the adoption of binding Resolutions, the United Nations deemed necessary to reinforce the policy framework against terrorism with the adoption of a Global Counter-Terrorism Strategy, adopted by consensus with General Assembly Resolution 60/288 (2006)[67] . With the Strategy – to be updated every two years –Member States agreed to a common strategic and operational framework in the fight against terrorism, notably founded on four pillars: i. measures to address the conditions conducive to the spread of terrorism, ii. measures to prevent and combat terrorism, iii. measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard;

---

[64] This trend appears to have been followed by Resolution 1540 (2004): A. MARSCHICK, *Ibid*., 16 ss.

[65] In this respect, however, it has been noticed that the Security Council has a broad discretion in the exercise of its powers, which already manifested itself in different occasions: B. SAUL, *Ibid*., 239.

[66] On the tasks of the CTC: N. ROSTOW, "Before and after: the changed UN response to terrorism since September 11th", in *Cornell International Law Journal*, 2002 Vol. (35) 3, 475-490. For a comment on the first achievements of the CTC: E. ROSAND, "Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight against Terrorism", in *American Journal of International Law*, 2003, Vol. 97(2), 333-341; E. ROSAND, "Resolution 1373 and the CTC: The Security Council's Capacity-building", in "International Cooperation in Counter-Terrorism. The United Nations and Regional Organizations in the Fight Against Terrorism", edited by G. Nesi, Ashgate, 2005, 81-88. Moreover, it has been remarked that the CTC would stand out for its activism and its influence, channelled especially through its best practice standards, which would make of it a sort of an "administrative legislator": C. DI STASIO, *Ibid*., 150.

[67] A/RES/60/288 (2006) adopted by the General Assembly, on 8 September 2006.

and iv. measures to ensure respect for human rights for all and the rule of law as the fundamental basis for the fight against terrorism.

Providing a guidance definition of terrorism in its preamble[68], the 2006 Strategy counted more than fifty recommendations and, with regard to the financing of terrorism, reiterated the commitment of Member States in refraining from financing terrorist activities and to fully cooperate in the detection and in the denial of safe havens and either to prosecute or extradite any person who finances such acts. Moreover, the Strategy stressed the importance of the cooperation among the United Nations bodies involved in the implementation of the counter-terrorist strategy, and established the new United Nations Counter-Terrorism Implementation Task Force (CTITF) to support States in the implementation of the Strategy and to collaborate with the relevant UN bodies, such as the United Nations Centre for Counter-Terrorism (UNCCT), the United Nations Office of Drugs and Crime (UNODC), as well as the Counter-Terrorism Committed (CTC) and its Counter Terrorism Committee Executive (CTED)[69] – as well as among States Members and international bodies involved in the fight against money laundering and terrorism financing, namely the International Monetary Fund and the World Bank. In particular, the Strategy invited Member States to welcome the work of the Financial Action Task Force (FATF), which, starting from 2001, plays an important role in the fight against terrorism financing, closely cooperating with the United Nations.

In the following years, efforts were made in order to stabilise and reinforce the newly established framework, underlining the importance of the role of the United Nation in coordination with the other relevant international, regional and

[68] The Strategy states that all forms and manifestations of acts, methods and practices of terrorism are "*activities aimed at the destruction of human rights, fundamental freedoms and democracy, threatening territorial integrity, security of States and destabilizing legitimately constituted Governments*". However, it has been pointed out that this definition would cover not what terrorism is, rather its consequences: M. EVANGELISTA, *Ibid.*, 45: "*equating terrorism with its consequences, when other actions can yield similar consequences, is no substitute for a definition*".

[69] Established in 2004 by S/RES/1535 (2004) adopted by the Security Council at its 4936th meeting, on 26 March 2004. Its mandate has been renewed until 2025 by Resolution S/RES/2617 (2021), unanimously adopted by the Security Council on 30 December 2021.

subregional organisations[70], institutionalising the Counter-Terrorism Implementation Task Force[71] and calling for cooperation on terrorism-related matters[72].

3.2 The extension of the FATF mandate on terrorism financing

Established by the G-7 Summit held in Paris in 1989, the Financial Action Task Force (FATF) was originally a small body[73] with a one-year mandate aimed at stopping the laundering activities of drug-trafficking proceeds through the adoption of *ad hoc* Recommendations, first issued in 1990[74]; however, its mandate has been continuously renovated[75], and its members as well as its action continuously expanded, in this way achieving a global reach and becoming the global standard-setter in the anti-money laundering and terrorist financing regulatory field (AML/CFT)[76]. Already in 1996, indeed, the Recommendations were updated to

[70] A/RES/62/272 (2008), adopted at its 120th plenary meeting on 5 September 2008 (1st Review), Recital No. 5.
[71] A/RES/64/235 (2009), adopted at its 68th plenary meeting on 24 December 2009.
[72] A/RES/64/297 (2010), adopted at its 117th plenary meeting on 8 September 2010.
[73] In addition to the G-7 members (United States, Japan, Germany, France, United Kingdom, Italy, Canada) the other FATF's founding members include Australia, Austria, Belgium, Luxembourg, Netherlands, Spain, Sweden and Switzerland, as well as the European Commission.
[74] "The Forty Recommendations of the Financial Action Task Force on Money Laundering", FATF, 1990. During the Eighties, the international drug trafficking activities were perceived as a great security concern, as already mentioned.
[75] Until in 2019 it became permanent: in 2019 the Ministers of the FATF agreed to make the Mandate open-ended starting in 2020, in the light of the fact that "*the FATF has evolved from a temporary forum to a sustained public and political commitment*": FATF, Mandate – Approved by the Ministers and the Representatives of the Financial Action Task Force, 12 April, 2019, Washington D.C.
[76] Nowadays, the FATF 39 members, which include the European Commission and the Gulf Cooperation Council. In addition, 30 countries and organizations participate as observers (among others: the International Monetary Fund, the World Bank, the OECD, the UN Office on Drugs and Crime and the UN Counter-Terrorism Committee Executive Directorate). Moreover, in the implementation of its mandate, the FATF is supported by nine FATF-Style Regional Bodies (FSRBs): the Asia/Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), the Eurasian Group (EAG) based in Moscow, Russia; the Eastern & Southern Africa Anti-Money Laundering Group (ESAAMLG), the Central Africa Anti-Money Laundering Group (GABAC), the Latin America Anti-Money Laundering Group (GAFILAT), the West Africa Money Laundering Group (GIABA), the Middle East and North Africa Financial Action Task Force (MENAFATF) and the Council of Europe Anti-Money Laundering Group (MONEYVAL),

include all money laundering activities[77], and, following the 9/11 attacks, the FATF decided to extend its mandate to the fight against terrorism financing by issuing Eight Special Recommendations during the extraordinary Plenary held in Washington D.C. on 29-30 October 2001. Reflecting a strong connection with the work of the United Nations, the first Special Recommendation urged Member States to "*take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism*" and to "*immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373*". Accordingly, the II Special Recommendation required members to "*criminalise the financing of terrorism, terrorist acts and terrorist organisations*" – omitting any reference to the subjective element of funding a specific terrorist act, in this way following Resolution 1373 and criminalising also the conducts of structural financing[78] – as well as "*ensure that such offences are designated as money laundering predicate offences*".

Overall, the Special Recommendations called upon State Members to take measures to freeze funds or assets used by terrorists, and to implement measures to seize and confiscate property which is the proceeds or used – or intended to be used for terrorism purposes (S. Rec. III)[79]; to request financial institutions to report suspicious transactions (S. Rec. IV); to strengthen international cooperation (S. Rec. V); to ensure that legal entities, including agents, which provide money or value transfer services are licensed or registered and subject to FATF Recommendations relating to banks and non-bank financial institutions (S. Rec. VI); to require financial institutions and money remitters to store complete originator information on funds transfers and related messages and to monitor those activities that do not display

established within the Council of Europe. For a deeper analysis of the nature and structure of the FATF, see *infra* Chapter III, §1.

[77] "The Forty Recommendations", FATF, 1996.

[78] M. A. MANNO, *Ibid*., 74.

[79] *Infra* Chapter IV.

complete information (S. Rec. VII), and to pay particular attention when monitoring the activities of non-profit organisations (S. Rec. VIII)[80].

The FATF Recommendations were comprehensively updated in June 2003[81], and in October 2004 a IX Special Recommendation was added, focusing on the threats posed by cash couriers. Moreover, always in 2004 an Interpretive Note to Special Recommendation II was issued, which further specified that "*terrorist financing offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist*" (par. 3), and confirmed the criminalisation of financing both terrorist acts and terrorist organisations[82]. In addition, the Interpretive Note seemed to call States in a more decisive manner than before (i.e., 1999 UN Convention) to establish criminal liability of legal persons, stating to resort to civil or administrative liability only in case where resorting to criminal law was not possible (par. 12)[83].

As we can see, there are many similarities between the FATF Special Recommendations and the measures required by UN SC Resolution 1373 (2001), this meaning that compliance with FATF measures mirrors the compliance with the Resolution itself. Besides, this tie has been clearly acknowledged by the UN Security Council, which with Resolution 1617 (2005)[84] strongly urged Member States "*implement the comprehensive international standards embodied in the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering and the FATF Nine*

[80] It is interesting to notice that article 18, par. 1, b) of the 1999 Convention already required financial institutions to adopt due diligence and know your customer measures.

[81] "The Forty Recommendations", FATF, 20 June 2003.

[82] Int. Note to Special Recommendation II, par. 6: "*terrorist financing offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s)*".

[83] FATF Interpretive Note to Rec. 5, par. B, 9: "*Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons*".

[84] S/RES/1617 (2005) adopted by the Security Council at its 5244th meeting, on 29 July 2005.

Special Recommendations on Terrorist Financing", and, as we will see hereinafter, will continue in the following years.

3.3 The Council of Europe approach

As abovementioned, the Council of Europe had already tried to provide some essential rules for cooperation in the field of terrorism with the 1977 European Convention on the Suppression of Terrorism (*supra* § 2); yet, the Convention had a limited scope, and it was not a sufficiently effective tool to create an harmonised framework for the fight against terrorism in the wake of the 9/11 attacks. Therefore, following the initiatives taken at the international level and recognising the need of strengthening the tools for the fight against terrorism[85] , the Council of Europe decided to update of the Convention by issuing the "Protocol amending the European Convention on the Suppression of Terrorism" (ETS 190) on 15 May 2003 (2003 Protocol)[86], which expanded the list of offences constituting terrorist acts and introducing, among others, the offences "*within the scope of the International Convention for the Suppression of the Financing of Terrorism, adopted at New York on 9 December 1999*" – but refraining to make any reference to Security Council Resolution 1373 (2001), thus addressing only the conducts of financing terrorist acts. However, if on the one hand the Protocol extended the scope of the Convention, both broadening the list of offences and clarifying that also the attempt to commit any of those offences, the participation as an accomplice of the organisation or the

[85] On 12 September 2001, at its 763rd meeting the Committee of Ministers issued a Declaration on the fight against terrorism which explicitly invited Member States to join the Convention: Declaration of the Committee of Ministers on the fight against international terrorism, Council of Europe – Committee of Ministers, 12 September 2001. The Committee reiterated the invitation with the Decision adopted on 21 September 2001 during its 765*bis* meeting, which also encouraged Member States to join other related Conventions and considered the chance to open the ratification of the 1977 Convention also to non-member States: Decision on the fight against international terrorism (Committee of Ministers' Declaration of 12 September 2001), Council of Europe – Committee of Ministers, 21 September 2001.

[86] The Protocol currently counts 35 ratifications, while 12 State Members signed but not ratified.

directing others to commit them shall be held as offences, on the other hand it still maintained an inductive approach.

Therefore, considering the framework still not solid enough, two years later two new Conventions were issued, namely the Convention on the Prevention of Terrorism (CETS 196) and Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198), both adopted in Warsaw on 16 May 2005.

Drafted by the Council of Europe Committee of Experts on Terrorism (CODEXTER)[87], in respect to terrorism financing the 2005 Convention on the Prevention of Terrorism did not make any significant progress, as it merely included the 1999 UN Convention in the list of treaties whose offences constitute "terrorist offence" (art. 1)[88], in this way reaffirming the choice made with the 2003 Protocol. Besides, if in relation to terrorism financing the Council of Europe seemed to be running behind, under other aspects it actually forerun the other supranational actors, namely in the criminalisation of terrorism-related conducts, such as public provocation to commit a terrorist offence (art. 5), recruitment for terrorism (art. 6) and training for terrorism (art. 7)[89].

The 2005 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, instead, focused on terrorism financing within the framework of money laundering, updating and extending the scope of the 1990 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS 141) to terrorism financing – thus

---

[87] Established in 2003, the CODEXTER was an intergovernmental body aimed at coordinating the Council of Europe's action against terrorism. Preceded by the Multidisciplinary Group for International Action Against Terrorism (GMT) – which drafted the 2003 Protocol amending the 1977 Convention – in 2018 CODEXTER was replaced by the Council of Europe Counter-Terrorism Committee (CDCT).

[88] In the Preamble, the Convention qualified terrorist acts as those acts that "*have the purpose by their nature or context to seriously intimidate a population or unduly compel a government or an international organisation to perform or abstain from performing any act or seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation*".

[89] Criminalised by the European Union three years later, with Council Framework Decision 2008/919/JHA (*infra* § 2.4.1).

following the path traced by the FATF[90]. With regard to the definition of terrorism financing, it is interesting to notice that, although the preamble of the Convention explicitly recalls both the 1999 UN Convention, "*particularly its Articles 2 and 4, which oblige States Parties to establish the financing of terrorism as a criminal offence*" and the UN Resolution 1373(2001) – especially its paragraph 3 (d)[91] – article 1 of the Convention refers to the definition set forth at art. 2 of the 1999 UN Convention, thus once again covering only the financing of terrorist acts and not welcoming the extension to the structural financing achieved by Resolution 1373 (2001), in this way not making any progress in relation to the 2005 Convention on the Prevention of Terrorism and the 2003 Protocol[92].

3.4 The European Union contribution to the criminalisation of terrorism financing

The European Union responded to the international inputs by taking action on two different levels[93]. On the one hand, it tried to reach a harmonised framework in the criminalisation of terrorist-related offences, especially with the adoption of 2002 Framework Decision. On the other hand, following the work of the FATF, and similarly to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198), it extended and updated the tools already in place against money laundering activities in order to apply them also for counterterrorism financing purposes, notably with the adoption of the III AML Directive.

---

[90] For a deeper analysis, *infra* Chapter IV.

[91] Resolution 1373 (2001), par. 3 (d) calls upon all States to: "*Become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999*".

[92] S. DE VIDO, "Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione Europea", *Ibid.*, 98.

[93] Before 2001, the European Union had addressed the issue of terrorism financing by issuing the Council Recommendation of 9 December 1999 on cooperation in combating the financing of terrorist groups (1999/C 373/01), which called State Members to intensify cooperation and to enhance the exchange of information.

3.4.1 The 2002 Council Framework Decision on combating terrorism

Following the Action Plan elaborated by the extraordinary European Council meeting on 21 September 2001[94], and the two Common Positions adopted on 27 December 2001[95], in 2002 the Council issued a Framework Decision on combating terrorism[96]. Aimed at providing a harmonised approach to the fight against terrorism[97], the Framework Decision listed a series of acts which should be held as "terrorist offences" (art. 1) and distinguished between "offences relating to a terrorist group" (art. 2) and "offences linked to terrorist activities" (art. 3).

Including the conducts of financing under the umbrella of article 2, par. 2, b), the Framework Decision covered both the financing of terrorist acts and terrorist organisations, since it required State Members to criminalise the funding "*in any way*" of the "*activities*", "*with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group*"[98], where "terrorist group" was to be intended as "*a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of*

---

[94] Calling for a coordinated and inter-disciplinary approach, the Action Plan identified four main areas of action: i. enhancing police and judicial cooperation, ii. developing international legal instruments, iii. putting an end to the funding of terrorism; and iv. strengthening air security and coordinating the European Union's global action: Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001, (SN 140/01).

[95]Council Common Position of 27 December 2001 on combating terrorism (2001/930/CFSP) and Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP); for a deeper analysis, see *infra* Chapter IV § 2.1.

[96] Council Framework Decision of on combating terrorism of 13 June 2002 on combating terrorism (2002/475/JHA). It is interesting to notice that the Proposal was issued by the Commission just few days after the 9/11 attacks, on 19 September 2001 (COM(2001)521 final).

[97] The instrument of the Framework Decision was created in order to implement the Third Pillar (area of freedom, security and justice), established by the Treaty of Amsterdam. In particular, the 2002 Council Framework Decision is meant to approximate substantive criminal law in the field of terrorism; however it has been pointed out that "*Member States retain the discretion to maintain or adopt new legislation entailing broader incriminations or grounds of jurisdiction as well as higher penalties*": F. GALLI, "Terrorism", in "Research Handbook on EU Criminal Law", ed. by V. Mitsilegas, M. Bergström, T. Konstadinides, 2016, 404.

[98] Art. 2, par. 2: "*Each Member State shall take the necessary measures to ensure that the following intentional acts are punishable:*
(a) directing a terrorist group;
(b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group".

its membership or a developed structure" (art. 2, par. 1)[99]. Yet, it has been remarked that it did not recognise the autonomous nature of such conducts, considering them as forms of participation to terrorist offences[100]. An interesting aspect of the Framework Position, however, is the provision relating to the liability of legal persons: establishing their liability "*for any of the offences referred to in Articles 1 to 4*" (art. 7), it encompasses also the conducts of terrorism financing, although not taking position on the nature of such liability, - just like the 1999 UN Convention (*supra* §2.1) – simply stating that sanctions could consist in "*criminal or non-criminal fines*" (art. 8).

Given the rapid evolution of the terrorist threat and the adoption of the 2005 Council of Europe Convention on Prevention of Terrorism, the Framework Decision has been updated in 2008[101]: the architecture has been enriched by introducing new offences linked to terrorist activities, namely public provocation – both direct and indirect – to commit a terrorist offence, recruitment for terrorism, training for terrorism – but did not introduced any novelty in relation to terrorism financing conducts[102].

---

[99] This definition corresponds to the one adopted by art. 1, par. 3 of the Council Common Position (2001/931/CFSP), which has been suggested to be inspired by the definition of "criminal organisation" set out by art. 1 of the Joint Action of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union (98/733/JHA): F. GALLI, *Ibid*., 406. Still, these two definitions are not identical, since 2002 Council Framework Decision – unlike 1998 Joint Action – does not require formally defined roles for its members, continuity of its membership or a developed structure – in this way expanding its scope: F. ROSSI, "Il contrasto al terrorismo internazionale nelle fonti penali multilivello", *Ibid*., 137.

[100] In this sense: M. A. MANNO, *Ibid*., 75-76. Moreover, criticisms have been raised in relation to the wording of art. 2, par. 2 (b), accused to be too broad, in this way leaving EU Members wide discretion in its implementation: A. BIANCHI, *Ibid*., 1054.

[101] Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. In particular, Recital No. 3 states that: "*The terrorist threat has grown and rapidly evolved in recent years, with changes in the modus operandi of terrorist activists and supporters including the replacement of structured and hierarchical groups by semiautonomous cells loosely tied to each other. Such cell inter-link international networks and increasingly rely on the use of new technologies, in particular the Internet*".

[102] For a comment on the influence of the 2005 Council of Europe Convention on the Prevention of Terrorism on the 2008 Council Framework Decision recalls the provisions on the criminalisation of public provocation, recruitment and training for terrorism set out by: F. ROSSI, "La circolarità dei modelli nazionali nel processo di armonizzazione europea delle legislazioni penali antiterrorismo",

3.4.2 The expansion of Anti-Money laundering tools to terrorism financing: the III AML Directive

In order to align the European framework with the recent amendments made by the FATF to its Recommendations (*supra* §3.2), in 2005 the European Union issued the third Anti-Money Laundering Directive[103], which extended its scope beyond the mere fight against money laundering, covering also terrorism financing[104], as "*the misuse of the financial system to channel criminal or even clean money to terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system*" (Recital No. 8). The definition of terrorism financing provided by the Directive on the one hand slightly differed from the one elaborated by the 1999 UN Convention, as it did not require the elements of unlawfulness and willingness[105] (*supra* §2.1), and on the other hand explicitly recalled the 2002 Framework Decision, as it defined terrorism financing as "*the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism*" (art. 1, par. 4)[106].

---

in *Diritto Penale Contemporaneo*, Vol. 1, 2017, 179-180. See also: F. ROSSI, "Il contrasto al terrorismo internazionale nelle fonti penali multilivello", *Ibid.*, 140-142.

[103] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[104] The Council Directive of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (91 /308/EEC) (I AML Directive) substantially transposed the 1988 UN Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, in this way limiting its scope to the drug-related predicate offences and imposing obligations only to financial institutions. The Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (II AML Directive) extended its scope to organised crime offences and included professionals among the subjects required to adopt customer due diligence measures and to report suspicious transactions.

[105] V. MITSILEGAS, B. GILMORE, "The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards", in *International and Comparative Law Quarterly*, 2007, Vol. 56 (1), 126 (note 45).

[106] It is interesting to notice that art. 1, par. 1 of the Directive does not require the criminalisation of money laundering and terrorism financing, rather their prohibition; this choice of words can be explained on the basis that the Directive belonged to the first pillar and not to the third one: E.

Therefore, if at the international level, thanks to the work of the United Nations and of the FATF, consensus was reached on the autonomous nature of the crime of terrorism financing and on the need of its criminalisation both when aimed at funding terrorist acts and when directed to support terrorist organisations, at the European level we can appreciate a blurred approach. Indeed, on the one hand the Council of Europe acknowledged its autonomous nature, yet only covered the financing of terrorist acts; on the other hand, the European Union established the criminalisation of the conducts of financing terrorist acts as well as the organisation, but struggled with recognising its autonomous nature.

3.4.3 The European Counter-Terrorism Strategy

Alongside the legislative initiatives taken in order to tackle the threat of terrorism and terrorism financing, the European Union showed a significant commitment in building an effective counter-terrorism framework: the 2003 European Security Strategy identified terrorism as one of the key threats to tackle and to stay ahead of[107], and following the 2004 Declaration on combating terrorism, adopted after the Madrid bombings[108], a specific Counter-Terrorism Strategy was issued in 2005, which, similarly to the one elaborated by the United Nations, was founded on four principal points: Prevent, Protect, Pursue and Respond[109]. The Strategy displayed a broad scope, going from foreign policy, defence, and borders controls to preventing radicalisation and recruitment, protecting European citizens and infrastructures, and effectively bring to justice persons involved in terrorist acts or organisations[110].

CASSESE, P. COSTANZO, "La terza direttiva comunitaria in materia di antiriciclaggio e antiterrorismo", in *Giornale di Diritto Amministrativo*, Vol. 1, 2006, 6.

[107] European Security Strategy – A secure Europe in a better world, Council of the European Union, 8 December 2003 (15895/03).

[108] Declaration on Combating Terrorism, European Council, Brussels, 25 March 2004.

[109] The European Union Counter-Terrorism Strategy, Council of the European Union, 14469/4/05 REV 4, 30 November 2005 (adopted by the European Council in December 2005).

[110] For a comprehensive analysis of the Strategy: C. DI STASIO, *Ibid*., 238-257.

Moreover, the goals of the Counter- Terrorism Strategy are to be read in combination with the goals set first by the Hague Programme (2005-2010)[111], which called for a global response, and an integrated and coherent approach to address terrorism.

4. The 9/11 attack and the Global War on Terror: from 2011 to 2022

After the 9/11, other terrorist attacks have shaken the world, contributing to the pursuing of the War on Terror began in 2001.

However, whereas during the 2001-2011 decade the efforts at the international level focused on establishing shared fundamental points in the fight against terrorism and terrorism financing in order to build an effective international cooperation framework, in recent years the attention shifted to the need to implement the instruments adopted to address the evolution of the terrorist threat. Specific efforts have been devoted to tackle the phenomenon of foreign terrorist fighters – which resulted in the expansion both of terrorist offences and the conducts constituting terrorism financing – and, more recently, particular attention has been paid to the threats posed by new technologies and to the possible exploitation of virtual assets by terrorists. The following paragraphs are going to map the evolution the criminalisation of terrorism financing according to the structural evolution of terrorist organisations and terrorist threats; since the issues related to technological developments do not affect the criminal definition of terrorism financing, rather have consequences on the expansion of the regulatory framework and on law enforcement measures, they will be analysed in depth later on (*infra* Chapters III and IV).

[111] Communication from the Commission to the Council and the European Parliament, "The Hague Programme: Ten priorities for the next five years The Partnership for European renewal in the field of Freedom, Security and Justice", Brussels, 10.5.2005, COM(2005) 184 final.

4.1 The United Nations Security Council action

In the last decade the Security Council continued to require all Member States to criminalise terrorism financing following the path traced by Resolution 1373 (2001), and at the same time intensified the dialogue with the FATF, encouraging State Members to implement its Recommendations and to follow its reports. In particular, the Security Council focused on the growing phenomenon of Foreign Terrorist Fighters (FTFs), which, pursuant to 2178 (2014)[112], are to be identified with those "*individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict*". Specifically addressing this phenomenon, Resolution 2178 (2014), recalling Resolution 1373 (2001), decided to expand the set of terrorism-related offences by requiring all Member States to establish serious criminal offences in relation to: i. the travel – or the attempt to travel – to a State in order to carry out, planning, preparing or participating in terrorist acts, or to provide or receiving terrorist training; ii. the wilful organisation or facilitation, including acts of recruitment, of those travels; and, in order to disrupt the financial support to foreign terrorist fighters, "the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used" to finance such travels[113].

---

[112] S/RES/2178 (2014) adopted by the Security Council at its 7272nd meeting, on 24 September 2014.

[113] Recital No. 6: "(The Security Council) *Recalls its decision, in resolution 1373 (2001), that all Member States shall ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice, and decides that all States shall ensure that their domestic laws and regulations establish serious criminal offenses sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offense:*

(a) their nationals who travel or attempt to travel to a State other than their States of residence or nationality, and other individuals who travel or attempt to travel from their territories to a State other than their States of residence or nationality, for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training;

(b) the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to finance the travel of individuals who travel to a State other than their States of

The provisions set out by Resolution 2178 (2014) have then been reinforced by Resolution 2253 (2015)[114], which explicitly endorsed the work of the FATF on counter terrorism financing (Recitals No. 16-18) and clarifies the obligation set out by par. 1 d) of Resolution 1373 (2001) applies to making funds, financial assets, economic or financial resources or other related services available, directly or indirectly for terrorist organisations or individual terrorists, including recruitment, training, or travel purposes, even in the absence of a link to a specific terrorist act (Recital No. 19) as well as by Resolution 2368 (2017)[115], and Resolution 2396 (2017)[116], which once again recalled the obligation established by Resolution 2178 (2014) to establish serious criminal offences regarding the travel, recruitment, and financing of foreign terrorist fighters, (Recital No. 1) and urged Member States especially focus on border control measures.

4.1.1 The United Nations Global Counter-Terrorism Strategy

Over the decade, the UN Global Counter-Terrorism Strategy has been regularly updated, and continued to build on the four pillars first set out in 2006. Responding – and adapting – to the current needs, over the years the Security Council while adopting the Reviews have reiterated the importance of preventing and suppressing terrorism financing[117], as well as the importance of full cooperation in order to deny safe havens and bring to justice any person involved in the commission, among others, of financing

residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training; and,

(c) *the wilful organization, or other facilitation, including acts of recruitment, by their nationals or in their territories, of the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training*".

[114] S/RES/2253 (2015) adopted by the Security Council at its 7587th meeting, on 17 December 2015.

[115] S/RES/2368 (2017), adopted by the Security Council at its 8007th meeting on 20 July 2017.

[116] S/RES/2396 (2017), adopted by the Security Council at its 8148th meeting on 21 December 2017.

[117] A/RES/66/282 adopted on 29 June 2012 (3rd Review), recital No. 23; A/RES/68/276 adopted on 13 June 2014 (4th Review), Recital No. 32; A/RES/70/291 adopted on 1 July 2016 (5th Review), Recital No. 55; A/RES/72/284 adopted on 26 June 2018 (6th Review), Recital No. 44.

terrorist acts[118], and expressed concern on different phenomena, going from the new threats posed by lone terrorists[119], to foreign terrorist fighters[120], to violent extremism[121], to the linkages between terrorism and transnational organised crime[122], to kidnapping for ransom in order to collect funds for terrorist purposes[123], as well as the use of information technologies – which constitute a constant concern for the development of effective counter-terrorism strategies[124] and are at the core of the last Review adopted[125] (*infra* Chapter II).

Finally, it is important to remark that the engagement of the United Nations in the fight against terrorism and terrorism financing is not limited to the updates of the Counter-Terrorism Strategy, rather it relies also on other parallel initiatives, such as the Madrid Guiding Principles, adopted in 2015 to stem the flow of foreign terrorist

[118] A/RES/68/276 adopted on 13 June 2014 (4th Review), Recital No. 22: A/RES/70/291 adopted on 1 July 2016 (5th Review), Recital No. 32; A/RES/72/284 adopted on 26 June 2018 (6th Review), Recital No. 28.

[119] A/RES/68/276 adopted on 13 June 2014 (4th Review), Recital No. 25: A/RES/70/291 adopted on 1 July 2016 (5th Review), Recital No. 36; A/RES/72/284 adopted on 26 June 2018 (6th Review), Recital No. 32.

[120] A/RES/68/276 adopted on 13 June 2014 (4th Review), Recital No. 31: A/RES/70/291 adopted on 1 July 2016 (5th Review), Recital No. 32; A/RES/72/284 adopted on 26 June 2018 (6th Review), Recital No. 22.

[121] A/RES/68/276 adopted on 13 June 2014 (4th Review); A/RES/70/291 adopted on 1 July 2016 (5th Review), Recital No. 38.

[122] A/RES/68/276 adopted on 13 June 2014 (4th Review); A/RES/70/291 adopted on 1 July 2016 (5th Review), Recital No. 56; A/RES/72/284 adopted on 26 June 2018 (6th Review), Recital No. 55.

[123] A/RES/66/282 adopted on 29 June 2012 (3rd Review), recital No. 20; A/RES/68/276 adopted on 13 June 2014 (4th Review), Recital No. 28; A/RES/70/291 adopted on 1 July 2016 (5th Review), Recital No. 46; Recital No. 32 of A/RES/72/284 adopted on 26 June 2018 (6th Review), Recital No. 43.

[124] A/RES/66/282 adopted on 29 June 2012 (3rd Review), recital No. 19; A/RES/68/276 adopted on 13 June 2014 (4th Review), Recital No. 27; A/RES/70/291 adopted on 1 July 2016 (5th Review), Recital No. 42; Recital No. 32 of A/RES/72/284 adopted on 26 June 2018 (6th Review), Recital No. 35.

[125] A/RES/75/291 adopted on 30 June 2021 (7th Review); the General Assembly decided in May 2020 to postpone the adoption of the 7th Review to 2021 due to the COVID-19 pandemic: (A/DEC/74/556), adopted on 20 May 2020.

fighters[126] and the creation of the new UN Office of Counter-Terrorism established by General Assembly Resolution 71/291 (2017)[127].

4.2 The FATF updated Recommendations

Working in close contact with the United Nations, the FATF has been particularly prolific. After two rounds of public consultations[128], in 2012 the FATF once again expanded its mandate to include counter-financing of weapons of mass destruction and comprehensively revised its Recommendations, implementing a risk-based approach and addressing new priority areas such as corruption and tax crimes[129]. With regard to terrorism financing, the IX Special Recommendations were integrated in the Recommendations – yet some of them remained still unique to terrorist financing, namely Recommendation 5 (SRII - terrorist financing offence), Recommendation 6 (SRIII - freezing and confiscating terrorist assets), and Recommendation 8 (SRI VIII - non-profit organisations). In particular, Recommendation 5 clearly reiterated countries

[126] With S/2015/939 (2015), the Security Council adopted 35 practical Guiding Principles to help Member States to address the foreign terrorist fighters' threat. Divided in three sections: I. Detection of, intervention against and prevention of the incitement, recruitment and facilitation of foreign terrorist fighters (1-14); II. Prevention of travel by foreign terrorist fighters, including through operational measures, the use of advance passenger information and measures to strengthen border security (15-21); III. Criminalization, prosecution, including prosecution strategies for returnees, international cooperation and the rehabilitation and reintegration of returnees (22-35). Following the request of UN SC Resolution 2396(2017) to review the 2015 Madrid Guiding Principles, the CCT issued an addendum on 28 December 2018 (S/2018/1177), which contains 17 additional guiding principles focusing on: border security and information-sharing (36-38); preventing and countering incitement and recruitment to commit terrorist acts consistent with international law, countering violent extremism conducive to terrorism and terrorist narratives, risk assessments and intervention programmes (39-40); judicial measures and international cooperation (41-49); protecting critical infrastructure, vulnerable or soft targets and tourism sites (50-51); preventing and combating the illicit trafficking of small arms and light weapons (52).

[127] A/RES/71/291 (2017), adopted at its 87th plenary meeting on 15 June 2017.

[128] Began in June 2009, the review process involved the participation of the private sector. It included two rounds of public consultation – respectively completed between October 2010 and June-September 2011 – and two private sector consultative forum meetings, held in November 2010 and December 2001.

[129] For an extensive analysis of the 2012 FATF Standards, see: G. W. SUTTON, "The new FATF Standards", in *George Mason Journal of International Commercial Law*, Vol. 4 (1), 2012, 68-136.

to criminalise the financing of terrorist acts, terrorist organisations and individual terrorists, regardless of the existence of a link to specific terrorist acts[130], and its Interpretive Note substantially transposed the provisions set out by the previous Interpretive Note to Special Recommendation II.

During the following years, the FATF regularly updated its Standards, and some relevant amendments have been made in relation to the definition of terrorism financing. In this sense, in October 2015 the FATF revised the Interpretive Note to Recommendation 5 to align it with UN SC Resolution 2178(2014), clarifying that the FATF requires countries to criminalise financing the travels of individuals to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training (Int. Note., B, 3) . In addition, a year later, the Interpretive Note was revised again in order to expand its scope by replacing "funds" with "funds or other assets", in order to have the same scope as Recommendation 6 (*infra* Chapter IV)[131].

4.3 The Council of Europe revisions: the 2015 Riga Protocol

In the last decade, the Council of Europe implemented the Convention on Preventing Terrorism (CETS 196) by adopting an Additional Protocol in 2015[132], that

---

[130] Recommendation 5: "*Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences*".

[131] At the same time, he FATF extended the Glossary definition of "funds or other assets", which now covers: "*any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services*".

[132] Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (CETS 217). Entered in force the 1st July 2017, it currently counts 23 ratifications, while 18 Member State

follows the UNSC Resolution 2178 (2014) – especially paragraphs 4 to 6 – in this way implementing the work of the United Nations[133]. Besides requiring State Parties to criminalise the conducts consisting in the participation in an association or group for the purpose of terrorism (art. 2), receiving training for terrorism (art. 3), travelling abroad for the purpose of terrorism (art. 4), and organising or facilitating travelling abroad for the purpose of terrorism (art. 6), the Additional Protocol requires State Parties to consider as a criminal offence also the funding of travelling abroad for the purpose of terrorism, defined as "*providing or collecting, by any means, directly or indirectly, funds fully or partially enabling any person to travel abroad for the purpose of terrorism, as defined in Article 4, paragraph 1, of this Protocol, knowing that the funds are fully or partially intended to be used for this purpose*" (art. 5, par. 1). Therefore, since art. 4, par. 1 specified that "travels abroad for the purpose of terrorism" covered only travels to a State other than the one of the traveller's nationality or residence[134] – like the United Nations provisions – pursuant to art. 5, par. 1, the Protocol requires the criminalisation of funding of travels to a State different from the traveller's nationality or residence and only when such funding is performed unlawfully and intentionally (art. 5, par. 2).

4.4 The European Union initiatives

Following the two-fold approach outlined above (*supra* § 3.3), the European Union implemented its instruments against the financing of terrorism both by enriching the criminalisation of the conducts of financing and by reinforcing the anti-money laundering and counterterrorism financing provisions. However, while both the

only signed, but not ratified. Austria, Azerbaijan, Georgia, Ireland, Liechtenstein and Serbia neither signed nor ratified.

[133] On the legitimisation role of the Council of Europe of international provisions which are adopted via non-traditional public law means: V. MITSILEGAS, "Transnational Criminal Law and the Global Rule of Law", *Ibid.*, 55.

[134] Art. 4, par. 1: "*For the purpose of this Protocol, "travelling abroad for the purpose of terrorism" means travelling to a State, which is not that of the traveller's nationality or residence, for the purpose of the commission of, contribution to or participation in a terrorist offence, or the providing or receiving of training for terrorism*".

2002 EU Council Framework Decision and the III AML Directive presented their own definition – although very similar – of the crime of terrorism financing, this parallel approach stopped first with the adoption of the IV AML Directive (art. 1, 5)), which did not amend the definition previously set out by the III AML Directive, and then ceased completely with the adoption of the Directive (EU) 2017/541, which finally set out a common understanding of the crime of terrorism financing, leaving no role to the AML/CFT rules on the matter, which therefore are let solely to manage regulatory challenges.

However, a little remark appears here to be necessary: while art. 1, par., 1, 5) of the IV AML Directive referred to articles 1 to 4 of the 2002 Council Framework Decision, in this way including the criminalisation of the financing of "offences linked to terrorist activities" (art. 3)[135], Directive (EU) 2017/541 did not include them within the scope of terrorism financing, as article 11 does not recall the "other offences related to terrorist activities" of article 12 – which contains the same provisions as art. 3 of the 2002 Council Framework Decision[136].

4.4.1 The Directive (EU) 2017/541 on combating terrorism

Taking into account the recent developments on the fight against terrorism elaborated at the international level, in 2017 the European Union replaced the 2002 Council Framework Decision with Directive (EU) 2017/541[137], which in its preamble

---

[135] 2002 Council Framework Decision, art. 3: "*Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following acts:*
(a) aggravated theft with a view to committing one of the acts listed in Article 1(1);
(b) extortion with a view to the perpetration of one of the acts listed in Article 1(1);
(c) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b)".

[136] P. GODINHO SILVA, "Recent developments in EU legislation on anti-money laundering and terrorist financing", in *New Journal of European Criminal Law*, Vol. 10 (1), 2019, 64-65.

[137] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. For a comprehensive analysis: S. SANTINI, "L'Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della Direttiva 2017/541", in *Diritto Penale Contemporaneo*, 2017, Vol. 7-8, 13-48. It is interesting to notice that, after

expressively recalls both the Security Council Resolution 2178 (2014), and the 2015 Council of Europe Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism.

With regard to terrorism financing, the Directive takes into consideration the conducts of financing under two different perspectives. On the one hand, according to article 4, b)[138], the conduct of funding a terrorist group[139] is held as a manifestation of a systematic and conscious involvement in a terrorist organisation[140]; on the other hand, according to article 11, terrorism financing is considered as an autonomous criminal offence, punishable when committed intentionally by "*providing or collecting funds, by any means, directly or indirectly, with the intention that they be used, or in the knowledge that they are to be used, in full or in part, to commit, or to contribute to the commission of, any of the offences referred to in Articles 3 to 10*" (art. 11, par. 1) – that is to commit a terrorist offence (art. 3)[141], a public provocation to commit a terrorist offence (art. 5), recruitment for terrorism (art. 6), providing training for terrorism (art. 7), receiving training for terrorism (art. 8), travelling for the purpose of terrorism (art. 9), and organising or

---

the Treaty of Lisbon, the legal instrument to address the criminal dimension of terrorism is the Directive, which, unlike the previous Council Framework Decisions, is subject to the control of the European Court and non-compliant countries could face infringement proceedings – thus enhancing its harmonisation power: I. J. PATRONE, "La legislazione dell'Unione Europea tra esigenze di armonizzazione e logiche emergenziali", in *Speciale Questione Giustizia*, 2016, 283-290.

[138] Directive (EU) 2017/541, art. 4: "*Member States shall take the necessary measures to ensure that the following acts, when committed intentionally, are punishable as a criminal offence:*
(a) directing a terrorist group;
(b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group".

[139] The definition of "terrorist group" at the article 1 of the 2017 Directive is identical to the one provided by the repealed Council Framework Decision 2002/475/JHA.

[140] M. A. MANNO, *Ibid*., 77; art. 4 of the 2017 Directive substantially reports art. 2, par. 2 of 2002 Framework Decision (*supra* § 3.4.1).

[141] The definition is taken by the 2002 Framework Decision, with the addition of a new conduct, consisting in:*"(i) illegal system interference, as referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council (1) in cases where Article 9(3) or point (b) or (c) of Article 9(4) of that Directive applies, and illegal data interference, as referred to in Article 5 of that Directive in cases where point (c) of Article 9(4) of that Directive applies*".

otherwise facilitating travelling for the purpose of terrorism (art. 10) [142]. Furthermore, art. 11, par. 2,

clarifies that in case of financing pursuant to art. 4, financing of terrorist offences (art. 3) or financing of travels for the purpose of terrorism (art. 9), "*it shall not be necessary that the funds be in fact used, in full or in part, to commit, or to contribute to the commission of, any of those offences, nor shall it be required that the offender knows for which specific offence or offences the funds are to be used*", in this way extending the scope of the criminalisation through the emphasis of the subjective element[143]. Besides, with regard to legal persons, art. 17 establishes their liability for, among others, conducts of terrorism financing in their double manifestation under art. 4, b) and art. 11.

4.4.2 A look at the development of the EU regulatory framework

At the same time, efforts to tackle terrorism financing within the anti-money laundering framework continued with the adoption of IV and V AML Directives which, however, as abovementioned did not bring any relevant novelty in relation to the definition of terrorism financing. Directive 2015/849[144] (IV AML Directive), indeed, remarked the importance of fully implementing the FATF Recommendations as revised in 2012, as well as the instruments developed by the international bodies, but did not touch the definition of terrorism financing set out by the III AML Directive, whereas it extended the definition of money laundering (art. 1, par. 3), and, following

[142] Articles 5-7 appear to be shaped on the basis of articles 5-7 of the Council of Europe Convention on the Prevention of Terrorism (CETS 196) – already transposed with Council Framework Decision 2008/919/JHA, whereas articles 8-10 appear to be shaped on the basis of the 2015 Riga Protocol, although they present some differences: F. ROSSI, *Ibid*., 130-131. However, it is interesting to remark that the European Union formally approved the 2015 Riga Protocol in 2018 (Council Decision (EU) 2018/890 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism) – after the adoption of the Directive (EU) 2017/541.

[143] V. MASARONE, "La 'lotta' al terrorismo", in "L'incidenza di decisioni quadro, direttive e convenzioni europee sul diritto penale italiano", ed. by A. Cavaliere, V. Masarone, Edizioni Scientifiche Italiane, Napoli, 2018, 43. It is interesting to notice that the definition of "funds" at art. 2 of the Directive is the same as the one set out art. 1, par. 1 of the 1999 UN Convention (*supra* §2.2).

[144] Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

the 2012 amended FATF Recommendations, included tax crimes among predicate offences, extended the number of obliged entities, and endorsed the risk-based approach, as well as strengthening client identification measures, modifying the definition and the regime applicable to the political exposed persons (PEPs), and establishing a new central national register and strengthened the reporting and record-retention obligations.

Three years later, the IV AML Directive has been amended by Directive 2018/843[145] (V AML Directive), which, acknowledging that the definitions of both terrorism financing and money laundering had been achieved, focused on the enhancement of the due diligence measures in relation to high-risk third countries, the reinforcement the transparency regimes required for the beneficial owners, the strengthen of the investigatory powers of the Financial Investigation Units (FIUs), and, what is more important for the purpose of the present work, the introduction in the AML/CFT regulatory framework of virtual assets (*infra* Chapter III).

4.4.3 The European Union strategies on terrorism financing

Over the years, the focus on terrorism financing (and anti-money laundering) issues has not weakened, rather it still constitutes one of the top priorities of the EU agenda. Following the Hague Programme, the Stockholm Programme fixed the policy priorities of the European Union for the 2010-2014 period in the area of freedom, security and justice and addressed terrorism, among others, as a serious threat[146]. In particular, in relation to terrorism financing it called Member States to address the vulnerabilities of the financial system, especially in relation to new payment methods, and called the European

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

[146] Besides terrorism, the Stockholm Programme was focused on tackling human trafficking, sexual exploitation of children and child abuse, cybercrime, economic crimes and corruption, drug trafficking and organised crime : "The Stockholm Programme - An open and secure Europe serving and protecting the citizen", European Council, 4 May 2010 (2010/C 115/01).

Commission to comply with the work of the FATF, especially in relation to Special Recommendation VIII on non-profit organisations.

Then, in recent years several initiatives have been developed in order to address terrorism financing, in its double dimension of criminal and regulatory issue. The European Union, indeed, has intensively worked to build a shared framework to address the threats to the internal security of the Union, including terrorism and terrorism financing by adopting the European Agenda on Security in 2015[147], which has been then followed by the Commission Action Plan for strengthening the fight against terrorist financing in 2016[148], which urged to trace terrorists through their financial movements, prevent them to move funds or other assets, disrupt their sources of revenues, and prevent them from moving funds or other assets.

More recently, both the two initiatives have been updated, and in the context of the newly adopted European Union Security Union Strategy[149], the European Commission issued a new Counter-Terrorism Agenda on 9 December 2020 – which constitutes the first official agenda since the 2005 Counter-terrorism Strategy – which, with regard to terrorism financing, reiterates the importance to implement and enforce the measures set at the European level, such as the Directive (EU) 2017/541 on combating terrorism, and calls for a closer cooperation with countries in the Southern Neighbourhood[150].

---

[147] Communication form the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2015) 185 final.

[148] Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing, 2 February 2016, (COM(2016) 50 final);

[149] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of Regions on the EU Security Union Strategy, 24.7.2020 (COM (2020) 605). In addition to terrorism, the Strategy focuses on organised crime, drugs trade and human trafficking, as well as cybercrime.

[150]Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee of the Regions: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 9.12.2020 (COM (2020) 795 final). However, it has been remarked that while objectives are clearly set out, "terrorism" remains largely unspecified, and policy measures remains vague and disperse: S. D'AMATO, A. TERLIZZI, "Strategic European counterterrorism? An empirical analysis", in *European Security*, Vol. 31 (4), 2022, 540-557.

On the other hand, the European Union addressed the challenges posed by terrorism financing by elaborating a specific Action Plan for a comprehensive Union policy on preventing money laundering and terrorism financing, built on six pillars: i. ensuring effective implementation of the existing EU AML/CFT framework; ii. establishing an EU single rulebook on AML /CFT; iii. establishing an EU-level AML/CFT supervision; iv. establishing a support and cooperation mechanism for Financial Intelligence Units; v. enforcing EU-level criminal law provisions and improving information exchange; and vi. strengthening the international dimension of the EU AML/CFT framework[151]. This Action plan has been followed by a package of proposals which are meant to renew the regulatory framework, and that expand on new technologies (*infra* Chapter III).

5. The evolution of the Italian criminal framework on terrorism: an overview

The term "terrorism" made its first appearance in the Criminal Code at the surge of the domestic terrorist threat (the so-called "years of lead")[152], with the introduction of a set of articles in Book II, Title I, Chapter I of the Criminal Code[153]: article 289 *bis* c.p., which criminalises the kidnapping with the purpose of terrorism or subversion through Law Decree 21/03/1978, No. 59[154], and articles 280 c.p. and 270 *bis* c.p. through Law Decree 15/12/1979 No. 625, respectively criminalising the attacks with

[151] Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, 13.5.2020 (2020/C 164/06).

[152] This phenomenon embraced both extreme-left (e.g. Brigate Rosse and Prima Linea), and extreme-right (e.g. Ordine Nuovo) terrorist organisations. Moreover, it has to be noted that this phenomenon involved also other European countries, such as Germany (Rote Armée Fraktion), Spain (ETA), and Ireland (IRA).

[153] Dedicated to the protection of the international personality of the State. However, according to a recent interpretation, terrorist offences should be considered first devoted to the protection of individual rights directly attacked (e.g. life, physical integrity, personal freedom, as well as individual and collective property), and, in second place, devoted to the protection of other values, that could change according to the acts concretely carried out: F: VIGANÒ, "La nozione di 'terrorismo' ai sensi del diritto penale", in "Sanzioni "individuali" del Consiglio di Sicurezza e garanzie processuali fondamentali", ed. by F. Salerno, CEDAM, Padova, 2010, 219.

[154] Article introduced by Law Decree 21/03/1978, No. 59, converted with amendments by L. 18/05/1978, n. 191.

the purpose of terrorism or subversion and the association with terroristic and democratic order subversion purposes[155]. The scope of these provisions, however, was quite narrow, as they were shaped on domestic terrorism with subversive purposes, and did not address the international terrorism – nor terrorism financing activities, which could only be punished in the form of participation ex art. 110 c.p. Moreover, article 1 of Law Decree 15/12/1979 No. 625 introduced a new common aggrieving circumstance applicable to any crime committed with "*purposes of terrorism or subversion of the democratic order*", which increased the penalty by half[156]. Following the 9/11 attacks, however, the attention on the phenomenon of terrorism in its international dimension soared, initiating a fervid period of legislative initiatives that resulted in a rich and complex framework – often accused of challenging the principles of legality, proportionality, materiality and offensiveness. In part, this is the consequence of the "war" and "fight" against terrorism promoted at the supranational level[157] and of the corresponding initiatives taken[158] – which have nonetheless the credit to have significantly contributed to achieve a certain degree of harmonisation at the European level[159]; at the same time,

[155] Articles introduced by Law Decree 15/12/1979 No. 625 (also known as "Legge Cossiga"), converted with amendments by L. 6/02/1980, No. 15. We remind that, pursuant to article 11 of Law 29 May 1982 No. 304, the purpose of subversion of the democratic order shall be interpreted as subversion of the Italian democratic order.

[156] After the adoption of Law Decree 21 March 2018, No. 21, this provision has been transferred into the Criminal Code under art. 270 bis.1 c.p.

[157] Largely used in relation to terrorism and organised crime overall at the international and European level: M. DONINI, "Diritto penale di lotta vs. diritto penale del nemico", in "Contrasto al terrorismo interno e internazionale", edited by R. E. Kostoris, R. Orlandi, Giappichelli, Torino, 2006, 20-24.

[158] In this respect, it has been affirmed that there is a "co-responsibility" of the European institutions: A. CAVALIERE, "Le nuove emergenze terroristiche: il difficile rapporto tra esigenze di tutela e garanzie individuali", in "Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali", ed. by R. Wenin, G. Fornasari, Editoriale Scientifica, Napoli, 2017, 40 ss. Notwithstanding its flaws, it is relevant to underline that the European approach is far from sharing the war-like features of the U.S. architecture: F. VIGANÒ, "Sul contrasto al terrorismo di matrice islamica tramite il sistema penale, tra 'diritto penale del nemico' e legittimi bilanciamenti", in *Studi Urbinati, A - Scienze Giuridiche, Politiche Ed Economiche*, Vol. *58* (4), 334-336. For a partially different position: F. FASANI, "Le nuove fattispecie antiterrorismo: una prima lettura", in *Diritto Penale e Processo*, Vol. 8, 2015, 927 ss.

[159] For a sample investigation on the criminalisation of terrorism financing across the European Union: C. CHINNICI, "Il contrasto al finanziamento al terrorismo: studio comparato sull´implementazione degli strumenti dell´Unione Europea", coordinated by V. Militello, Palermo,

it is interesting to notice that sometimes the Italian legislator anticipated them, thus spontaneously embracing – and reinforcing – this approach[160].

Indeed, if we look at the whole legislative framework on terrorism the Italian Legislator seems to have embraced a securitisation policy[161] inspired by an emergency logic[162], which sometimes draws near to the so-called "criminal law of the enemy" (*Feindstrafrecht*)[163] aimed at neutralizing the perpetrator[164]. In particular,

---

2018. On the role of the Council of Europe and of the European Union on the "Europeanisation" of criminal law: A. BERNARDI, "L'europeizzazione del diritto e della scienza penale", Giappichelli, Torino, 2004. For a recent analysis on the impact of the Council of Europe on criminal law: A. BERNARDI, "La sovranità penale tra Stato e Consiglio d'Europa", Jovene, 2019.

[160] Therefore, the relationship between supranational and national sources is better described as circular, rather than vertical: F. ROSSI, "La circolarità dei modelli nazionali nel processo di armonizzazione europea delle legislazioni penali antiterrorismo", *Ibid*., 188; for an extensive analysis on the top-down and bottom-up impact of supranational and national legislation: F. ROSSI, "Il contrasto al terrorismo internazionale nelle fonti penali multilivello", *Ibid*., 147 ss.

[161] On securitisation: *supra* note 51. For a deep analysis on the relationship between security and criminal law, in its double function as *securitas-protectio* and *securitas potestas* and on the role of objective and perceived security : F. FORZATI, "La sicurezza fra diritto penale e potere punitivo. Genesi e fenomenologia dell'illecito securitario postmoderno fra involuzioni potestative e regressioni al premoderno", Edizioni Scientifiche Italiane, Napoli, 2020. On the relationship between security and freedom and antiterrorism policies: M. BARBERIS, "Non c'è sicurezza senza libertà. Il fallimento delle politiche antiterrorismo", il Mulino, Bologna, 2017.

[162] On criminal law and emergency: S. MOCCIA, "La perenne emergenza. Tendenze autoritarie nel sistema penale", 2nd ed., Edizioni Scientifiche Italiane, Napoli, 2000.

[163] The concept of "criminal law of the enemy" has been elaborated by G. Jakobs, as counterposed to the "criminal law of the citizen" (*Bürgerstrafrecht*): unlike the citizen, the enemy does not enjoy the fundamental individual rights granted by the legal system, in this way creating a state of exception that stays outside of it: G. JAKOBS, "Diritto penale del nemico? Una analisi sulle condizioni della giuridicità", in "Delitto politico e diritto penale del nemico", edited by A. Gamberini, R. Orlandi, Monduzzi, Bologna, 2007. Criminal law literature on the possible applications of this theory and its consequences is immense; for a special focus on terrorism perspective: R. BARTOLI, "Lotta al terrorismo internazionale. Tra diritto penale del nemico *ius in bello* del criminale e annientamento del nemico assoluto", Giappichelli, Torino, 2008. On the state of exception from a philosophical perspective: G. AGAMBEN, "State of Exception", University of Chicago Press, 2005.

[164] In this sense, it has been remarked that the Italian Legislator has followed the schemes of the "criminal law of the enemy" by introducing criminal provisions with a marked anticipatory nature, both in the form of the criminalisation of preparatory acts and of the criminalisation of vague – and sometimes neutral – conducts: L. RISICATO, "Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?", Giappichelli, Torino, 2019, 50-52. However, others remark that the Italian criminal provisions on terrorism would not constitute an expression of criminal law of the enemy, rather would remain within the borders of an emergency logic: R. BARTOLI, "Le nuove emergenze terroristiche", in "Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali", *Ibid*., 62. For a specific analysis on the application of the emergency criminal law to terrorism within the Italian legal system: R. BARTOLI, "Legislazione e prassi in tema di contrasto al terrorismo internazionale: un nuovo paradigma emergenziale?", in *Diritto Penale Contemporaneo*, Vol. 3, 2017, 233-259. Similarly, it has been observed that in the field of terrorism we find a criminal law "at the limit", in the sense that it is shaped at the limits of the guarantees and

with regard to the terrorism related offences introduced in the Criminal Code, this approach led to the creation of a microsystem[165] characterised by the criminalisation of preparatory acts, vague description of the conducts and a particular emphasis on the subjective element - conveyed through the element of the specific intent[166] - rather than on the conducts concretely carried out[167], and whose overall coordination has proven difficult, thus risking to fall into a mere symbolical legislation.

Right after the adoption of UN SC Resolution 1373 (2001)[168], indeed, the Italian Legislator significantly expanded its action with Law Decree 18/10/2001 No. 374[169], which amended art. 270 *bis* c.p. – extending its scope to international terrorism (art. 270 *bis*, par. 3 c.p.), introducing terrorism financing among the criminalised conducts and raising the penalties – and introduced article 270 *ter* c.p., which criminalises the conducts of assistance to people belonging to the association of articles 270 and 270 *bis* c.p. [170]. Moreover, two years later, was introduced art. 280 *bis*

---

individual rights which are at the basis of the democratic order: M. PELISSERO, "Contrasto al terrorismo internazionale e il diritto penale al limite", in *Speciale Questione Giustizia*, 2016, 99-112.

[165] Looking in a broader manner to the criminal provisions introduced to address terrorism, it has been suggested that the Italian Legislator would display an approach similar to the one adopted in relation to the mafia phenomenon. According to DONINI, the "exceptional" rules adopted in relation to mafia and terrorism now constitute a new separated general part of criminal law: M. DONINI, "Mafia e terrorismo come "parte generale" del diritto penale", in *Meridiana*, No. 97, 2020, 203-228.

[166] A. CAVALIERE, "Le nuove emergenze terroristiche: il difficile rapporto tra esigenze di tutela e garanzie individuali", *Ibid*., 26-28. On the role of the specific intent in the criminal provisions on terrorism: L. PICOTTI, "Terrorismo e sistema penale: realtà, prospettive, limiti", in Diritto Penale Contemporaneo, Vol. 1, 2017, 254-257. For an extensive analysis of the specific intent within the Italian criminal law system: L. PICOTTI, "Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali", Giuffrè, Milano, 1993.

[167] Thus resulting in a type of criminal law based on the author of the crime (i.e., "*diritto penale d'autore*): in V. MILITELLO, "Terrorismo e sistema penale: realtà, prospettive, limiti", in *Diritto Penale Contemporaneo*, Vol. 1, 2017, 6. See also: G. MARINO, "Lo statuto del terrorista", in *Diritto Penale Contemporaneo*, Vol. 1, 2017, 44-52.

[168] It is interesting to notice, however, that Italy formally ratified the 1999 UN Convention only two years later through Law 14/01/2003, No. 7, "Ratifica ed esecuzione della Convenzione internazionale per la repressione del finanziamento del terrorismo, fatta a New York il 9 dicembre 1999, e norme di adeguamento dell'ordinamento interno".

[169] Law Decree 18/10/2001 No. 374, "Disposizioni urgenti per contrastare il terrorismo internazionale", converted with amendments by L. 15/12/2001, n. 438.

[170] In so doing, despite the disruptiveness of the 9/11 events and of subsequent international response, the Italian Legislator did not abandon the structure of the criminal response adopted in response to domestic terrorism, rather implemented it: V. MILITELLO, "Terrorismo e Sistema penale: realtà, prospettive, limiti", *Ibid.*, 6.

c.p., which criminalises acts of terrorism carried out by means of deadly or explosive devices[171].

After the 2005 London terrorist attacks, the Italian Legislator amended again the criminal provisions on terrorism, bringing some relevant novelties to the Criminal Code: Law Decree 27/07/2005 No. 144[172], introduced three new provisions, namely art. 270 *quarter* c.p., 270 *quinquies* c.p. and 270 *sexies* c.p, which on the one hand implemented the 2002 Council Framework Decision (*supra* §3.4.1), and on the other and anticipated the provisions set out by the 2008 Council Framework Decision, the Security Council Resolution 2178 (2014), and the Directive (EU) 2017/541 (*supra* §3.4.1; §4.1.1; §4.4.1).

For the first time in the Italian legal system, art. 270 *sexies* c.p. introduced a definition of "terrorist purposes", identified as "*acts which, by their nature or context, may cause serious harm to a country or an international organisation and are carried out with the aim of intimidating the population or forcing the public authorities or an international organisation to execute or refrain from executing any act or to destabilise or destroy fundamental political, constitutional, economic and social structures of a country or an international organization, as well as other conducts defined as terrorist or committed for the purpose of terrorism by conventions or other rules of international law binding for Italy*". Formulated on the basis of art. 1 of the 2002 Council Framework Decision, the first part of article 270 *sexies* c.p. appears to have an autonomous nature, while the last part seems to serve as a "closing norm", aimed at including those conducts that, although lacking the elements set out in the first part, are "*conducts defined as terrorist or committed for the purpose of terrorism by conventions or other rules of international law binding for Italy*"[173]. However, what is here relevant for the purpose of this work, is that art. 270 *sexies* c.p. represents the specific intent which informs the whole

[171] Introduced by L. 14/03/2003 No. 34, through which Italy ratified the UN 1997 Bombing Convention.

[172] "Misure urgenti per il contrasto del terrorismo internazionale" (also known as "Decreto Pisanu"), converted with amendments by L. 31/07/2005, n. 155.

[173] M. MANTOVANI, "Le condotte con finalità di terrorismo", in "Contrasto al terrorismo interno e internazionale", a cura di R. E. Kostoris e R. Orlandi, Giappichelli, Torino, 2006, 81-82.

microsystem on terrorism, and which often adds on the specific intent already required by the provisions themselves (i.e., double specific intent).

Articles 270 *quater* and 270 *quinquies* c.p. – expressively subsidiary to art. 270 *bis* c.p. – were aimed at filling the gaps of the existing microsystem by criminalising, respectively, the conducts of enlisting persons in terrorist groups – but not the enlistees – and the conducts of training, punishing both trainers and trainees[174]. These provisions raised multiple doubts in relation both to the vague description of the conduct[175] and their effectiveness, since, given the extensive interpretation adopted by the Courts of art. 270 *bis*, c.p. (*infra* § 5.1) they have seen little application[176].

Criticisms surrounding the criminal provisions on terrorism have not been solved by the following initiatives. Again, after the Charlie Hebdo attacks in Paris and in order to complete the implementation of the Security Council Resolution 2178 (2014) (*supra* § 4.1.1), with Law Decree 18/02/2015, No. 7[177] the Italian Legislator continued to respond to the terrorist threat by reinforcing and expanding criminal

---

[174] Thus going beyond the 2005 Council of Europe Convention on Preventing Terrorism, which did not establish the criminal responsibility of trainees – which was only added later on, with the 2015 Riga Protocol: R. WENIN, "Una riflessione comparata sulle norme in materia di addestramento per finalità di terrorismo", in *Diritto Penale Contemporaneo*, Vol. 4, 2016, 118. Besides, we remind that also at the European Union level the responsibility of the trainees has been established for the first time by Directive (EU) 2017/541. The reason behind the decision to treat differently the enlistee (not punished) and the trainee (punished) has been linked to the fact that training activities are more dangerous and logically subsequent to enlisting – a choice that was reflected also on the more severe punishment established for art. 270 *quinquies* c.p. and the subsidiary clause of art. 270 *quater* c.p. in favour of art. 270 *quinquies* c.p.: A. PRESOTTO, "Le modifiche agli artt. 270 *quater* e *quinquies* del codice penale per il contrasto al terrorismo", in *Diritto Penale Contemporaneo,* Vol. 1, 2017, 111.

[175] Particular doubts were raised definition of "enlisting" ex art. 270 *quater* c.p.; in this respect, Italian Supreme Court stated that the conduct of "enlisting" is realised when there is a "serious agreement" between the enlisted and the enlistee: Cass. pen., sez. I, 9 September 2015, n. 40699; for a comment, see: A. PRESOTTO, *Ibid.*, 110-111. Moreover, it has been remarked that art. 270 *quater* c.p. would represent an extreme form of anticipation of the criminal law intervention: G. MARINO, "Lo statuto del terrorista", *Ibid.*, 49.

[176] Moreover, problems of coordination arises also when looking at the sanctions established: art. 270 quater c.p. – subsidiary to art. 270 *bis* c.p. establishes the same punishment for the enlister as the one established by art. 270 *bis*, par. 1 c.p. – which is more severe than art. 270 *bis*, par. 2 c.p.

[177] "Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione", converted with amendments by L. 17/04/2015 n. 43 (also known as "Antiterrorism Law Decree").

provisions, which once again appear to be vague and extremely anticipatory, thus challenging the principle of legality and offensiveness[178]. In fact, the Legislator added a second paragraph to art. 270 *quater* c.p. to extend the criminal responsibility to the enlistee, yet providing a less severe punishment compared to the one applicable to the enlister pursuant to art. 270 *quater* par.1. c.p., as well as to art. 270 *quinquies* c.p., which now explicitly establishes the criminalisation of conducts of self-training – as long as they are followed by behaviours unequivocally aimed at carrying out one of the conducts of art. 270 *sexies* c.p.[179]. Moreover, the Law Decree introduced article 270 *quater*.1 c.p., which criminalises the conducts of organising, financing or promoting travels for terrorist purposes, in this way introducing a new form of financing – yet subsidiary to art. 270 *bis* c.p. (*infra* § 5.2).

A year later, following another string of serious terrorist attacks (Bataclan Paris 2015, Nice, Berlin and Brussels 2016), new provisions were added to the Criminal Code through Law 28/07/2016 No. 153 [180], namely financing conducts with terrorist purposes (art. 270 *quinquies*.1 c.p.), theft of seized goods or money (art. 270 *quinquies*.2 c.p.), acts of nuclear terrorism (art. 280 *ter* c.p.), and introducing a new form of mandatory confiscation for any crime committed with terrorist purposes (art. 270 *septies* c.p.)[181].

Focusing the attention specifically on the conducts of terrorism financing, it can be argued that the Criminal Code basically contains three provisions which are

---

[178] A. CAVALIERE, "Considerazioni critiche intorno al D.L. Antiterrorismo, n. 7 del 18 febbraio 2015", in *Diritto penale Contemporaneo*, Vol. 2, 2015, 228. Some pointed out that the Law Decree displays a neutralising attitude: G. MARINO, "Il sistema antiterrorismo alla luce della L. 43/2015: un esempio di 'diritto penale del nemico'?", in *Rivista Italiana di Diritto e Procedura Penale*, Vol. 3, 2016, 1388-1426.

[179] Thus requiring a *quid pluris* for the punishing of the self-trained, consisting in preparatory acts: A. VALSECCHI, "Le modifiche alle norme incriminatrici in materia di terrorismo", in edited by R. E. Kostoris, F. Viganò, Giappichelli, Torino, 2015, 11. In this way, it has been pointed out that the Legislator has significantly anticipated the intervention of criminal law: A. PRESOTTO, *Ibid.*, 112-113.

[180] Law 28/07/2016, No. 153, through which Italy ratified Council of Europe Convention on Preventing Terrorism (16 May 2005), UN International Convention for the Suppression of Acts of Nuclear Terrorism (14 September 2005), Protocol amending the European Convention on the Suppression of Terrorism (15 May 2003), Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (16 May 2005), Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (22 October 2015).

[181] See *infra* Chapter IV § 9.2.

devoted to its criminalisation, namely art. 270 *bis* c.p., 270 *quarter*.1 c.p. and 270 *quinquies*.1 c.p. However, although theoretically aimed at suppressing different forms of financing, the coordination of the provisions contained in these three articles, as well as the little application they have concretely had, raise some doubts about their effectiveness.

5.1 The criminalisation of financing pursuant to art. 270 *bis* c.p.

As already mentioned, terrorist organisations have evolved from rigid hierarchical structures to flexible and adaptive schemes. This structural shift could have represented a significant obstacle for the concrete application of article 270 *bis* c.p., since, following the organisational approach developed in relation to the mafia-structured organised crime requiring the proof of a stable and structured organisation governed by precise rules and roles (i.e., "strong" organisational model), the proof of the participation to the terrorist association could almost be impossible to reach. Therefore, in order to ensure the concrete applicability of the provision – which was at risk to be a dead letter – Italian courts have adopted a "weak" organisational model (similar to the one adopted in relation to drug-trafficking)[182], which does not require the proof of a structured organisation: what counts is the ideological connection among members and the ability to carry out a violent programme - that can also be not defined yet[183]: the proof of participation is inferred both by the ideological/psychological adherence to the criminal programme and by the effective integration in the organisation[184].

---

[182] A. VALSECCHI, "Le modifiche alle norme incriminatrici in materia di terrorismo", *Ibid*., 2015, 6.

[183] However, it has been remarked that, in order to be punished, the members should carry out preparatory activities: F. VIGANÒ, "Il contrasto al terrorismo di matrice islamico-fondamentalistica: il diritto penale sostanziale", in "Terrorismo internazionale e diritto penale", edited by C. De Maglie, S. Seminara, CEDAM, Padova, 2007, 134.

[184] Cass. pen., sez. I, 15 June 2006; Cass. pen., sez. I, 11 October 2006. Besides, the Italian Supreme Court recently clarified that the proof of the participation could consist of merely indirect contacts, provided that the ideological adherence exists: Cass. Cass., Sez. V, 18 December 2020 (dep. 4 March 2021), n. 8891. For a comment: A. VALSECCHI, "Per la prova della partecipazione all'Isis sono

Looking specifically at terrorism financing, art. 270 *bis* c.p. criminalises the financing of the association itself, as par. 1 states that: "*any person who promotes, constitutes, organises, directs or finances associations whose aim is to carry out acts of violence with terrorist or subversive democratic order purposes, is punished with imprisonment from seven to fifteen years*"[185]. The choice of including the conduct of financing among the conducts punished in the first paragraph could be read as the intention of the legislator to criminalise the conducts of financing in a more severe manner compared to the conducts of participation pursuant to the second paragraph, punished with imprisonment from five to ten years (art. 270 *bis*, par. 2, c.p.).

Requiring the specific intent in order to be integrated – to be verified on two different levels[186]: the perpetrator has to have the intent of carrying out acts of violence in order to realise the terrorist purposes, given the its expansive nature, both due to its structure[187] and to the broad interpretation allowed by the Courts, art. 270 *bis* c.p. leaves barely no room for application for the other conducts of terrorism financing criminalised by the Italian Legislator.

5.2 The financing of travels for terrorist purposes pursuant to art. 270 *quater*.1 c.p.

Introduced in 2015, art. 270 *quater*.1 c.p. criminalises the conducts of organising, financing or promoting travels for terrorist purposes, and it is subsidiary to art. 270 *bis* and art. 270 *quater* c.p.: "*Any person, when articles 270 bis and 270 quater do not*

---

necessari e sufficienti contatti anche indiretti fra adepto e membri dell'organizzazione (accompagnati dall'adesione ideologica al programma terroristico)", in *Sistema Penale*, 15 March 2021.

[185] In order to once again underline the links between the legislative techniques adopted in relation to transnational crimes, it is interesting to underline that in the Italian system a similar wording can only be found at art. 74, d.P.R. No. 309/1990, which criminalises the association for drug-trafficking purposes: M. A. MANNO, *Ibid*., 108.

[186] F. VIGANÒ, "Il contrasto al terrorismo di matrice islamico-fondamentalistica: il diritto penale sostanziale", *Ibid*., 142.

[187] In this sense: In this sense: A. CAVALIERE, "Le nuove emergenze terroristiche: il difficile rapporto tra esigenze di tutela e garanzie individuali", *Ibid.*, 28: "*the structure of the association works as : a) amplifier of criminal liability, casting a shadow of suspect to those who have not participated in the commission of a crime; b) multiplier of punishment, based on the subjective dangerousness in relation to those that are already responsible for one or more crimes; c) a shortcut in relation to the proof needed, and, always in relation to procedural level; d) as means for the application of special procedures, which display weakened guarantees*".

apply, who organises, finances or promotes travels towards foreign territories in order to carry out conducts with terrorist purposes pursuant to art. 270 sexies, is punished with five to eight years of imprisonment"[188].

Aimed at targeting those conducts that would escape from the scope of articles 270 *bis* c.p. and 270 *quater* c.p., this provision, which, similarly to art. 270 *bis* c.p., requires the author to display a double specific intent[189] - the intent of alternatively organising, financing or promoting travels towards foreign territories in order to carry out conducts with terrorist purposes - has actually seen little concrete application due to the extensive interpretation adopted by the Italian Courts in relation to art. 270 *bis* c.p.[190].

The conducts of financing, indeed, could fall under the scope of art. 270 *quater*.1 c.p. only in those cases where neither the financier, nor the person who receives the funds are involved in a terrorist association, and only if the funds are to be used for the organisation of travels; were they aimed to other terrorist purposes, the conduct would fall under the scope of art. 270 *quinquies* c.p.[191] – which, although being subsidiary to art. 270 *quater*.1 c.p., establishes a more severe punishment.

However, it is interesting to notice that there are still doubts about the exact definition of "travels": it is not clear, indeed, if the destination of the travel has to be the place where the terrorist act will take place, or if the destination could also merely be the place where the person will be trained. Following the position expressed by the Security Council Resolution 2178 (2014) and of the Directive (EU)

---

[188] The structure of art. 270 *quater*.1 c.p. appears to have been shaped on the basis of art. 600 *quinquies* c.p.: R. BORSARI, "Articolo 270 *quater*.1 c.p.", in "Commentario breve al codice penale", ed. by G. Forti, S. Seminara, G. Zuccalà, 6th ed., CEDAM, Padova, 2017.

[189] It has been pointed out that here the specific intent bears the entire offensiveness of the provision, as the conduct is *per se* neutral: G. MARINO, "Il 'filo di Arianna'. Dolo specifico e pericolo nel diritto penale della sicurezza", in Diritto Penale Contemporaneo, Vol. 6 (2018), 59.

[190] At the moment, art. 270 *quater*.1 c.p. has only been applied once, namely in the case relating to the so-called "first Italian foreign fighter": Court of Assise of Milan, 19 December 2016, No. 8. For a comment: D. ALBANESE, "Le motivazioni della Corte d'Assise di Milano sul "caso Fatima": spunti di riflessione su terrorismo internazionale e organizzazione di trasferimenti ex art. 270-*quater*.1 c.p", in *Diritto Penale Contemporaneo*, Vol. 3 (2017), 346-355.

[191] In this sense: E. DOLCINI, G. L. GATTA, "Codice penale commentato", Wolters Kluwer, 2021, Vol. II, 200.

2017/541, the first solution could seem preferable[192]; however, it raises concerns about the marked anticipated criminalisation that it would entail[193]. Similarly, in order to limit the anticipatory force of art. 270 *quater*.1 c.p., in case the travel is not directed to the final destination, art. 270 *quater*.1 c.p. will apply only if sufficient information on how to reach the final destination was given[194]. Lastly, while the wording of the provision would suggest that only those who finance (or organise or promote) multiple travels could be punished according to art. 270 *quater*.1 c.p., the Italian Court has stated that one travel is sufficient[195].

5.3 An autonomous form of financing: art. 270 *quinquies*.1 c.p.

Introduced in order to implement the 1999 UN Convention and the III AML Directive[196], art. 270 *quinquies*.1 c.p. punishes with seven to fifteen years of imprisonment "*any person, when articles 270 bis and 270 quater.1 do not apply, who collects, distributes or makes available goods or money, in any manner whatsoever made, which intended to be used, in whole or in part, for the purpose of carrying out those acts of terrorism referred to in article 270 sexies (…) regardless of the actual use of the funds for the commission of the aforementioned conducts*" (art. 270 *quinquies*.1, par. 1 c.p.) and with five to ten years "*any person who deposits or safeguards the goods or money referred to in the first paragraph shall be punished with imprisonment of between five and ten years*" (art. 270 *quinquies*.1, par. 2 c.p.).

Presenting itself as a subsidiary form of criminalisation of the autonomous financing conducts, art. 270 *quinquies*.1 c.p. contains two distinct provisions: the first one established by par. 1, which criminalises the collection, distribution or making

---

[192] S. CRISPINO, "Finalità di terrorismo, snodi ermeneutici e ruolo dell'interpretazione conforme", in *Diritto Penale Contemporaneo*, Vol. 1, 2017, 237.

[193] A. VALSECCHI, "Le modifiche alle norme incriminatrici in materia di terrorismo", in "Il nuovo 'pacchetto' antiterrorismo", *Ibid.*, 15.

[194] A. VALSECCHI, *Ibid.*, 16.

[195] Court of Assise of Milan, 19 December 2016, No. 8 (*supra*, note 190).

[196] In this sense: M. A. MANNO, *Ibid.*, 112.

available goods or money, and the second one established by par. 2, which criminalises – in a less severe manner – their mere deposit or custody.

Overall, the structure of art. 270 *quinquies*.1 c.p. has raised numerous concerns. First of all, par. 1 it has been pointed out that the wording used to describe the two alternative conducts – collection and distribution – is imprecise, since it first refers to "goods or money" – "in any manner whatsoever made"[197] – and then it uses the term "funds"[198].

Moreover, art. 270 *quinquies*.1 c.p. appears to be structured on a marked teleological tension of the conduct, whose criminalisation is based on the use of the funds for terrorist purpose – use that does not have to actually take place for art. 270 *quinquies*.1 c.p. to apply[199], in this way representing a clear example of criminalisation of preparatory acts, which is far from any concrete offensiveness and is based on the aim perpetrated by the author[200].

Besides, criticisms have been raised in relation to the penalties established by art. 270 *quinquies*.1 c.p. On the one hand, criticisms have been raised in relation to the fact that the conducts described at par. 2 are punished in a less severe manner than the ones described at par. 1, notwithstanding the fact that usually the conducts described at par. 2 would take place after the collection but before the distribution

---

[197] This choice is meant to remind that their origin – whether licit or illicit – has no relevance in order to integrate the conduct of terrorism financing, unlike money laundering activities: E. DOLCINI, G. L. GATTA, "Codice penale commentato", *Ibid*., 213. However, others have remarked that this specification appears to be redundant: F. FASANI, "Un nuovo intervento di contrasto al terrorismo internazionale", in *Diritto Penale e Processo*, Vol. 12, 2016, 1558-1559.

[198] In this respect, it has been suggested that the scope of the norm should be read through the lenses of the international sources, which intend "financing" as the provision of "assets", thus putting emphasis on the economic nature: M. A. MANNO, *Ibid*., 112. In the same sense: F. FASANI, "Un nuovo intervento di contrasto al terrorismo internazionale", in *Diritto Penale e Processo*, Vol. 12, 2016, 1558, who suggests that "goods" should be interpreted as goods that can be easily converted into money, on the basis of the term of "financing" itself, the use of the term "funds" at par. 2, supranational sources and the Italian AML/CFT framework as well; an interpretation that appears to be confirmed also by the wording Directive EU 2017/541: F. FASANI, "L'impatto della direttiva antiterrorismo sulla legislazione penale sostanziale italiana" in *Diritto Penale e Processo*, Vol. 1, 2018, 16.

[199] Since the structure of the provision is shaped on the specific intent – which already make the criminal provision integrated even if the scope is not committed, the fact that the Legislator specified that par. 1 is integrated "*regardless of the actual use of the funds*" has been considered redundant: F. FASANI, "Un nuovo intervento di contrasto al terrorismo internazionale", *Ibid*., 1559.

[200] M. A. MANNO, *Ibid*., 114-117.

of the funds[201]. On the other hand, criticisms have been raised in relation to the fact that the conducts of par. 1 are punished in the same manner as the ones established by art. 270 *bis*, par. 1 c.p. and, therefore, in a more severe manner than the conducts of participation set out at art. 270 *bis*, par. 2 c.p. – notwithstanding the fact that art. 270 *quinquies*.1 c.p. is subsidiary to art. 270 *bis* c.p.; besides, both pars. 1 and 2 of art. 270 *quinquies*.1 c.p. establish a more severe punishment than the one established for the conducts of art. 270 *quater*.1 c.p., to which, once again, art. 270 *quinquies*.1 c.p. is subsidiary[202].

However, given its subsidiary nature and the broad interpretation adopted in relation to art. 270 *bis* c.p., art. 270 *quinquies*.1 c.p. could apply only in case of lone wolves - if the funds are not meant for travel purposes; in that case, art. 270 *quater*.1 c.p. would apply. – or in case the proof of the elements integrating art. 270 *bis* c.p. is not met[203].

5.4 The responsibility of legal entities for terrorism financing

As previously pointed out, the 1999 UN Convention required State Parties to establish the liability of legal entities – yet not taking a position on the nature of such liability. This approach had been endorsed by the 2002 EU Council Framework Decision, and later by the 2005 Council of Europe Convention on the Prevention of Terrorism, as well as Directive (EU) 2017/541; in this context, the position of the FATF stood out, since from the outset the Interpretive Note to Special Recommendation II invited countries to establish a criminal liability for legal entities – a position later confirmed by the Interpretive Note to Recommendation 5.

---

[201] For a critical comment on the choice of the Legislator to differentiate the punishment of conducts of pars. 1 and 2: F. FASANI, "Un nuovo intervento di contrasto al terrorismo internazionale", *Ibid*., 1562

[202] R. BORSARI, "Articolo 270 quinquies. 1 c.p.", in "Commentario breve al codice penale", *Ibid*., 915.

[203] R. BERTOLESI, "Ancora nuove norme in materia di terrorismo", in *Diritto Penale Contemporaneo*, 19 October 2016.

With the implementation of the Convention through Law No. 7 of 14 January 2003, article 25 *quater* was introduced to the system outlined by Legislative Decree No. 231/2001. This provision presents some peculiar characteristics, starting by the fact that, unlike the other dispositions included in the list of predicate offences, art. 25 *quater* does not explicitly lists the criminal provisions involved, rather it comprehensively refers to the "*commission of crimes with terrorist or subversive purposes included in the Criminal Code and established by special legislation*", as well as the "*commission of other crimes in violation of art. 2 of the 1999 UN Convention*". This structure raises some concerns in relation to the identification of the scope of article 25 *quater*, which could be theoretically immense: art. 270 *sexies* itself displays an expansive nature, since it openly refers to "*other conducts defined as terrorist or committed for the purpose of terrorism by conventions or other rules of international law binding for Italy*", and, in addition, the aggravating circumstance of "terrorist purpose" established by art. 270 *bis*.1 c.p.[204] is applicable to every crime committed[205]. Besides, the generic structure of art. 25 *quater* has serious repercussions on the capacity of legal persons to effectively identify and map the risk areas and to apply the provisions of d. lgs. 231/2001[206]; not to mention the fact that it seems unlikely that the two alternative objective elements necessary for the legal entity to respond of the crime committed, namely the interest or advantage of the legal entity, could actually verify, as only a criminal legal entity could benefit from the commission of crime with terrorist purposes[207].

[204] Previously located at art. 1 Law 6/2/1980 No. 15 (*supra* note 155).
[205] R. SABIA, "Delitti di terrorismo e responsabilità da reato degli enti tra legalità e esigenze di effettività", in *Diritto Penale Contemporaneo*, Vol. 1 (2017), 215-216.
[206] In this sense, it has been suggested that entities could establish models similar to the one put in place in order to prevent the commission of money laundering offences (art. 25 *octies,* L. 231/2001): M. PALMISANO, "Prevenzione del finanziamento al terrorismo e congelamento dei capitali", in "Mobilità, sicurezza e nuove frontiere tecnologiche", edited by V. Militello, A. Spena, Giappichelli, Torino, 2018, 311.
[207] M. PALMISANO, *Ibid*., 311-312.

6. Terrorism financing, organised crime and money laundering: a holistic approach.

In the light of the development of the criminalisation of terrorism financing, both at supranational and national level, a few remarks appear here to be necessary. The approach and legislative techniques adopted, indeed, show clear influences stemming from a variety of other forms of crimes, which are held to be tightly linked to terrorism financing or to show a similar structure and posing similar risks.

First of all, we find multiple linkages between terrorism financing and transnational organised crimes. As a fact, although their motives differ[208], since the decline of state sponsorship of terrorism terrorists increasingly turned to organised criminal activities in order to generate new funds, both via forming short or long-term alliances and/or starting to share operational and operational and organisational similarities[209]. Accordingly, these two phenomena are frequently jointly addressed in the international agenda. The connection between organised crime, especially drug trafficking, and terrorism had been already pointed out by the United Nations General Assembly Resolution 49/60 (1994)[210]: the fight against drug trafficking, indeed, was one of the top priorities during the Eighties, and the results achieved on international cooperation in that matter have been partially employed to address the issues raised by the terrorist threat[211] and also served as a basis for the development of international anti-money laundering regulations.

---

[208] Organised crime is motivated and guided by profits, whereas terrorism by ideological/political motives. On the characteristics of organised crime and transnational organised crime: M. C. BASSIOUNI, "Introduzione", in "La cooperazione internazionale per la prevenzione e repressione della criminalità organizzata e del terrorismo", edited by M. C. Bassiouni, Giuffrè, Milano, 2005, 1 ss.

[209] To the point that they could eventually converge, thus creating an organisation that would display both criminal and terrorist characteristics at the same time: T. MAKARENKO, "The Crime-Terror Continuum: Tracing the Interplay between Organised Crime and Terrorism", in "Global crime today: The changing face of organised crime", edited by M. Galeotti, Routledge, 2007, 129-145.

[210] I. BANTEKAS, *Ibid.*, 317-318. Indeed, in the Preamble the General Assembly claimed the "*desirability for closer coordination and cooperation among States in combating crimes closely connected with terrorism, including drug trafficking, unlawful arms trade, money laundering and smuggling of nuclear and other potentially deadly materials*".

[211] Indeed, the 1999 UN Convention displays a structure similar to the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances: M. C. BASSIOUNI, in La cooperazione internazionale per la prevenzione e la repressione della criminalità organizzata e del terrorismo, a cura di M. C. Bassiouni, Giuffré, Milano, 2005, 69. Besides, the link between drug

Looking at the development of the Italian framework, we can appreciate a similar approach, especially in relation to the similarities remarked in the legislative response to terrorism overall, including terrorism financing, and the legislative strategies employed to tackle mafia-structured organisations, especially in the development of special preventive and procedural measures.

Perhaps the most evident tie, however, is represented by the international legal framework against money laundering, which was developed in response to the need of combating drug trafficking. This link is apparent when looking at the original text of the FATF Forty Recommendations issued in 1990 (*supra* §3.2*)* and at the I AML Directive (*supra* §3.4.2), both addressed at tackling money laundering activities linked to the proceeds derived from drug trafficking[212]. Similarly, counterterrorism financing measures have been shaped on the basis of anti-money laundering regulations: the FATF Recommendations, the AML Directives issued by the European Union, as well as the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism blend anti-money laundering and counterterrorism financing measures together. Nevertheless, the two phenomena present structural differences, as money laundering is a process aimed at "laundering" illicit proceeds in order to use them in the market[213], whereas terrorism financing can be described as a *money dirtying* process[214], as, regardless of the legitimate or illegitimate origin of the funds, they are meant to be used for a criminal purpose – terrorism financing, indeed.

---

trafficking and terrorism can be seized also when looking at the national level, namely at UK antiterrorism legislation: L. K. DONOHUE, "The Cost of Counterterrorism", Cambridge University Press, 2008, 122 ss.

[212] In addition to the 1990 FATF Recommendation and I AML Directive, we recall also the work of the Inter-American Drug Abuse Control Commission (CICAD), a technical body of the Organization of American States, which in 1992 approved its Anti-Money Laundering Model Regulations.

[213] The laundering process is traditionally identified in three stages: i. placement, ii. layering, iii. integration.

[214] Or "reverse money laundering": E. JURITH, "Acts of Terror, Illicit Drugs and Money Laundering", in *Journal of Financial Crime*, Vol. 11 (2), 2003, 159.

Looking specifically at the United Nations Security Council Resolutions, Resolution 1373 (2001) already underlined the "*close connection between international terrorism and transnational organized crime, illicit drugs, money-laundering, illegal arms trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials*", calling for enhancing coordination national, subregional, regional and international levels. Over the years, these concerns have been not only constantly reaffirmed, but also expanded to address other forms of transnational organised crimes, such as human trafficking[215] and frequently recalling State Members to ratify and implement the relevant Conventions[216] .

This comprehensive approach can be explained on the fact that these crimes are often empirically linked one to another, as they can mutually serve one another, but it is also interesting to notice that they are expressions of that securitisation process which first inform drug trafficking and then extended to terrorism. Indeed, at the political level these crimes have been elevated to security threat[217], and, by declaring "war" and engaging "fight" against these threats, both at the international and national levels have been created permanent states of emergency[218], which have served as a justification for the adoption of far-reaching measures[219].

---

[215] They can be here recalled: S/RES/2195 (2014); S/RES/2199 (2015); S/RES/2253 (2015); S/RES/2322 (2016); S/RES/2331 (2016); S/RES/2368 (2017); S/RES/2370 (2017); S/RES/2388 (2017); S/RES/2462 (2019); S/RES/2482 (2019).

[216] Such as the Single Convention on Narcotic Drugs of 1961 as amended by the 1972 Protocol, the Convention on Psychotropic Substances of 1971, the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, UN Convention against Transnational Organized Crime and the related Protocols, the United Nations Convention against Corruption of 2003.

[217] V. MITSILEGAS, "Transnational Criminal Law and the Global Rule of Law", *Ibid*., 50.

[218] For a comment on the implication of this trend in the U.S. legislation: T. A. DURKIN, "Permanent States of Exception: A Two-Tiered System of Criminal Justice Courtesy of the Double Government Wars on Crime, Drugs & Terror", in *Valparaiso University Law Review*, 2016, Vol. 50 (2), 419-492.

[219] See V. MITSILEGAS, "Countering the chameleon threat of dirty money. 'Hard' and 'soft' law in the emergence of a global regime against money laundering and terrorist financing", in "Transnational Organised Crime", Taylor & Francis, 2003, 195-211.

CHAPTER II

EVOLUTION OF TRENDS, SOURCES AND METHODS OF TERRORISM FINANCING: THE POSSIBLE ROLE OF VIRTUAL ASSETS

SUMMARY: 1. Geopolitics of terrorism: an overview 1.1 The Middle-East 1.2 Africa 1.3 South Asia and South-East Asia 1.4 Western countries: the rise of ethnically and racially motivated terrorism 2. The purposes of terrorism financing 3. Who finances terrorism? 3.1 State sponsors of terrorism 3.2 Private sources of terrorism financing 3.2.1 Legitimate private sources of funding 3.2.2 Illegitimate private sources of funding 4. Terrorism financing methods 4.1 The oldest method of all: the use of cash couriers 4.2 The exploitation of the formal banking system 4.3 Informal Value Transfer Systems: *Hawala* and terrorism financing 4.4 The use of new payment methods 5. The possible impact of Virtual Assets on terrorism financing 5.1 Virtual Assets ecosystem: defining the conceptual framework 5.2 Where it all began: the rise of Bitcoin 5.2.1 How does Bitcoin work? 5.2.2 The debated nature of Bitcoin 5.2.3 Beyond Bitcoin: the new forms of non-backed Altcoins 5.3 The growing phenomenon of Stable Coins and Global Stable Coins 5.4 Monetary Central Authorities' response: the rise of Central Bank Digital Currencies 5.5 Virtual Assets and Terrorism Financing: the possible vulnerabilities 5.5.1 (*pseudo*)Anonymity 5.5.2 Transnationality 5.5.3 Decentralisation 5.5.4 Different regulation across countries 6. Using Virtual Assets to raise funds 7. Using Virtual Assets to move funds

1. Geopolitics of terrorism: an overview

Since the beginning of the War on Terror, terrorist groups have spread across regions, expanding their action and modifying their structure. Overall, terrorists have taken advantage of areas characterised by political instability, which represent a prolific environment for recruiting and raising, moving and hiding funds, as well as to settle strategic alliances with criminal organisations[220]. In particular, the

[220] Domestic conflicts interrupt social control systems, thus offering organised crime and terrorist groups new opportunities to expand and reinforce their network. This is even more true in case of emergent States and democracies: M. C. BASSIOUNI, *Ibid*., 20-27. On a similar note, Makarenko notes that in most cases alliances between terrorists and organised crime take place in regions characterised by instability, which is in the interest of both parties to preserve; eventually, weak or

Middle-East, Africa, Asia and South Asia host several terrorist organisations motivated by ideological and political reasons and sometimes backed by formal affiliations to Al-Qaeda or ISIL cores, which have spread their regional presence by establishing new groups both with local and g-local ambitions. After the 9/11 attacks, indeed, the Salafi-jihadist threat has become increasingly decentralised, spreading through Islamic States provinces (*wilayat*), Al-Qaeda affiliates, new Salafi-jihadist and allied groups and inspired networks and individuals; often in competition against each other, these groups show a substantial fluidity, as individual fighters and supporters move among groups according to leaders' and territory changes[221].

In recent years, the Salafi-jihadist threat in the Western world has evolved, resulting in terrorist attacks perpetrated by single individuals (i.e., lone wolves), and in the growing phenomenon of foreign fighters. Moreover, a new terrorist phenomenon appears to be on the rise in Western countries, which is linked to extreme and far-right groups and it is making its way within national and international agendas.

Bearing in mind the fact that the conducts of raising and moving funds aimed at terrorism financing can take place all over the world – and not only within the countries that present a high risk of terrorist activities[222] - it seems worth to briefly map the geographic distribution of the main active terrorist groups, since they are

failed states could boost their convergence and create safe havens (i.e. "black holes"): T. MAKARENKO, *Ibid*., 138-140. See also, B. H. STANISLAWSKI., K. PEŁCZYŃSKA-NAŁĘCZ , K. STRACHOTA, M. FALKOWSKI, D. M. CRANE, M. LEVITSKY, "Para-States, Quasi-States, and Black Spots: Perhaps Not States, but Not "Ungoverned Territories," Either", in *International Studies Review*, Vol.(10)2, 2008, 366-396.

[221] For a deeper analysis: JONES G., VALLEE C., NEWLEE D., HARRINGTON N., SHARB C., BYRNE H., "The Evolution of the Salafi-Jihadist Threat. Current and Future Challenges from the Islamic State, Al-Qaeda, and Other Groups", Center for Strategic and International Studies, November 2018, 1-72. According to the Authors, Syria would count the highest number of Salafi-Jihadist fighters (43.650 – 70.550), followed by Afghanistan (27.000 – 64.000), Pakistan (17.500 – 39.540), Iraq (10.000 – 15.000), Libya (4.900 – 9.900), Somalia (3.095 – 7.240), Nigeria (3.450 – 6.900) and Yemen (2.300 – 3.500).

[222] Given the transnational nature of terrorism financing, a jurisdiction that presents a low terrorism risk may present a high terrorism financing risk level: the fact that terrorists do not carry out domestic terrorist attacks, indeed, does not imply that they are not involved in terrorism financing operations through the exploitation of regulatory and supervisory vulnerabilities: "Terrorist Financing Risk Assessment Guidance", FATF, July 2019.

often linked to local organised crime and their location can affect the strategies and methods of financing they resort to.

1.1 The Middle-East

The Middle-East region is known to face long-lasting political issues, which have favoured the rise and settlement of various terrorist groups. Two of the most notorious terrorist organisation operating in the area are Hamas[223] - active since the end of the Eighties in the West Bank and the Gaza Strip - and Hezbollah, a Shiite Muslim political party and militant group active in Lebanon founded during Lebanon's civil war[224].

However, since the rise of Islamic State of Iraq and the Levant (ISIL)[225], the international attention has focused on the territories encompassing Iraq and Syria (commonly referred to as the "Syraq" region). Emerged from Abu Musab al Zarqawi's Al-Qaeda in Iraq (AQI), ISIL officially formed in Iraq in 2006 and, under the new leadership of Al-Baghdadi, expanded in Syria in late 2011, also thanks to the withdrawal of U.S. forces from Iraq. After reaching its maximum expansion in 2014 with the occupation of the city of Mosul, however, ISIL suffered severe setbacks and has been forced to consistently downsize its presence in Syraq[226].

---

[223] Hamas (Harakat al-Muqawama al-Islamiya - Islamic Resistance Movement) is a militant Palestinian nationalist and Islamist movement stemmed from the Muslim Brotherhood Movement in 1987. Operating in West Bank and Gaza Strip, it aims at encompassing Israel, the West Bank and the Gaza Strip. Hamas is well established in the social fabric of the region, and it pursues its goals both through political activity and guerrilla and terrorist attacks, endorsing jihad as a mean to reach its goals – which include also international ambitions: M. LEVITT, "Hamas: Politics, Charity, and Terrorism in the Service of Jihad", Yale University Press, 2006, 8 ss.

[224] It is interesting to notice that the terrorist nature of Hezbollah is not globally recognized. While the United States, the United Kingdom, Canada, Australia, Germany and Israel have designated Hezbollah as a terrorist group, the European Union has only designated its military wing, while the United Nations has not listed Hezbollah at all. This is a further proof of the difficulties posed by the political implications surrounding terrorism. For a deeper analysis of the articulate structure and purposes of Hezbollah: N. QASSEM, "Hizbullah. The story from witihin", SAQI, London, 2010.

[225] Also known as IS (Islamic State), ISIS (Islamic State of Iraq and Syria) or Daesh, which stands for its Arabic acronym (al-Dawlah al-Islamiyah fi al-'Iraq wa al-Sham).

[226] For an extensive analysis on the roots and history of ISIL: F. A. GERGES, "ISIS: a history", Princeton University Press, 2016.

Alongside ISIL, another significant terrorist presence in the region is represented by Hay'at Tahrir al-Sham (HTS) (formerly known as Al-Nusrah Front for the People of the Levant/Jabhat al-Nusra, which dissolved in 2016) which, once affiliated to Al-Qaeda, declared to no longer have any ties with it[227].

1.2 Africa

Aggrieved by political, social, environmental and economic instability, Africa appears to be a particular fertile area for the proliferation of terrorist groups: ISIL and Al-Qaeda have expanded their presence across the whole continent by establishing alliances with local militant and terrorist groups and founding new local branches, which eventually collaborate with one another – as well as with violent political and armed groups and criminal organisations – including for funds flowing purposes[228].

While terrorists' presence in North Africa seems to be declining[229], terrorist activities have soared in the Sahel region[230], which has been lately labelled as "the new epicentre of terrorism"[231]. Since the military coup taken place in Mali in 2012, indeed, the instability of the region progressively escalated[232] and contaminated

---

[227] C. LISTER, "How al-Qa`ida Lost Control of its Syrian Affiliate: The Inside Story", in *CTC Sentinel*, Vol. 11 (2), 2018, 1-9; J. DREVONA, P. HAENNI: "Redefining Global Jihad and Its Termination: The Subjugation of al-Qaeda by Its Former Franchise in Syria", in *Studies in Conflict & Terrorism*, 2022, 1-16.

[228] Report on "Terrorist Financing in West and Central Africa", FATF-GIABA-GABAC, 2016, 8-9.

[229] Twenty-nineth report of the Analytical Support and Sanctions Monitoring Team pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities, 3 February 2021 (S/2022/83), 10-11.

[230] The Sahel region stretches from East to West Sub-Sahara, encompassing northern Senegal, southern Mauritania, Mali, Burkina Faso, extreme south Algeria, Niger, northeastern Nigeria, south-central Chad, and Sudan, extreme north South Sudan, Eritrea and extreme north Ethiopia.

[231] Global Terrorism Index 2022 (March 2022), Institute for Economics and Peace.

[232] Despite the international peace-keeping operations launched to help the stabilisation of the region – such as the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), launched in 2013 and still operative – two new military coups took place in 2020 and 2021. Moreover, in November 2022 France has formally ended the "Operation Barkhane", launched in 2014 to help the G5 Sahel countries (Burkina Faso, Chad, Mali, Mauritania and Niger) to tackle terrorist networks and to prevent the creation of terrorist safe-havens.

neighbouring countries, notably Burkina Faso, Niger, Benin and Cote d'Ivoire[233], thus favouring the establishment of terrorist groups, such as the Al-Qaeda linked Jama'at Nusrat al-Islam wal-Muslimeen (JNIM)[234], and the two ISIL affiliated Islamic State of the Greater Sahara (ISGS)[235] and Islamic State West Africa Province (ISWAP)[236] - the latter operating across Sahel and West Africa. Alongside Sahel, in fact, West and Central Africa gather numerous terrorist groups, the biggest ones being Boko Haram[237] - which formalised its alliance with ISIL in 2015[238] - and Al-Qaeda in the Islamic Maghreb (AQIM), which spread its presence from North Africa to West and Central Africa, thus encompassing Libya, southern Algeria, Mali and the Sahel itself[239].

---

[233] A. OROSZ, "Violent extremism in the Sahel is strengthening its grip in West Africa", London School of Economics Blog, 15 February 2022.

[234] Formed in 2017, JNIM is the result of the merger of four Salafi-jihadist groups active in Sahel: Ansar Dine, Katiba Macina, al-Mourabitoun, and the Sahara branch of al Qaeda in the Islamic Maghreb (AQIM): THOMPSON J., "Examining Extremism: Jama'at Nasr al-Islam wal Muslimin", Center for Strategic & International Studies, 15 July 2021. Although JNIM presents itself as a united front for Salafist jihad in the Sahel, it operates in four distinct areas, with different dynamics: northern Mali, Central Mali and Northern Burkina Faso, Eastern Burkina Faso and Niger Borderlands, Southwestern Burkina Faso: D. EIZENGA, W. WILLIAMS, "The Puzzle of JNIM and Militant Islamist Groups in the Sahel", in *Africa Security Brief*, The Africa Center for Strategic Studies, No. 38, December 2020, 1-8.

[235] The Islamic State in the Greater Sahara is active in the Liptako-Gourma region of the Sahel, which crosses parts of Burkina Faso, Mali, and Niger territories. Trying to create a Salafi-jihadist caliphate, ISGS declared his adherence to the Islamic State in May 2015, although ISIS recognised it only in October 2016: J. THOMPSON, "Examining Extremism: Islamic State in the Greater Sahara", Center for Strategic & International Studies, 22 July 2021.

[236] Stemmed from Boko Haram in 2016, ISWAP holds the monopoly in the Lake Chad Basin region and has increasingly demonstrated an affiliation with ISIL through its propaganda. Although in competition one against each other, since 2020 ISWAP and ISGS propaganda have become increasingly aligned, as ISGS (pushed by Al-Qaida-affiliated JNIM) has tried to strengthen itself through its links to ISWAP: Report on Civil Society Perspectives: ISIL in Africa – Key Trends and Developments, United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), April 2022, 10.

[237] Often translated as "Western education/culture is forbidden", Boko Haram was founded in 2002 by Mohammed Yusuf as a Salafi movement that preached the rejection of democracy and Western-style education; the movement became openly aligned with jihadism in July 2009. For an extensive analysis: A. THURSTON, "Boko Haram: The History of an African Jihadist Movement", Princeton University Press, 2018.

[238] Thus expanding ISIL's influence to Nigeria: Report on "Terrorist Financing in West and Central Africa", *Ibid*, 7.

[239] Report on "Terrorist Financing in West and Central Africa", *Ibid.*, 8. Founded in 1998 under the name of "Salafist Group for Preaching and Combat" (GSPC) as a splinter of the Armed Islamic Group (GIA), the group adopted the name of Al-Qaeda in the Islamic Maghreb (AQIM) after becoming a

Together with Sahel and West-Central Africa, also the East side of the continent constitutes an area of great concern in relation to terrorism: based in Somalia, al-Shabaab[240] - which has formally declared its alliance with Al-Qaeda in 2012 - is one of the most powerful terrorist groups in the region[241], together with the ISIL affiliated Islamic State Central African Province (ISCAP)[242], which is active in the Democratic Republic of Congo and Mozambique.

1.3 South Asia and South-East Asia

Being the cradle of Al-Qaeda[243], Afghanistan has long been held as one of the most dangerous hot-spots for terrorism and, even if after the occupation of the country in 2001 Al-Qaeda has gradually reduced its presence and decentralised its structure, the recent return of the Taliban regime could provoke a revival of the terrorist threat

formal affiliate of Al Qaeda in 2006: Z. LAUB, J. MASTERS, "Al-Qaeda in the Islamic Maghreb", Council of Foreign Relations, 27 March 2015.

[240] Harakat Shabaab al-Mujahidin (Al Shabaab) stemmed from the Islamic Courts Union (ICU) in 2006. Publicly supporting Al Qaida since 2009, the two organisations formalised their allegiance in 2012: J. HARRINGTON, J. THOMPSON, "Examining Extremism: Harakat al Shabaab al Mujahideen (al Shabaab)", Center for Strategic & International Studies, 23 September 2021. In 2007 the United Nations launched the peace-keeping operation "African Union Mission in Somalia" (AMISOM), which has recently been replaced with the "African Union Transition Mission in Somalia" (ATMIS) in April 2022.

[241] As further proof of the marriages of convenience among terrorist groups, reports show that Al-Shabaab would be collaborating with Boko Haram. More precisely, Boko Haram would be sending its fighters to Somalia for training purposes: Report on "Terrorist Financing in West and Central Africa", *Ibid.*, 7.

[242] ISCAP seems to have links with the insurgent group ISIL affiliated Allied Democratic Forces (ADF), active in Uganda and in the Democratic Republic of the Congo as well. It is worth to notice that, as already seen in relation to Mali and Somalia, the United Nations are present in the Democratic Republic of the Congo with the peace-keeping operation called "United Nations Organization Stabilization Mission in the Democratic Republic of the Congo" (MONUSCO), launched in 2010.

[243] The origins of Al-Qaeda trace back in the Eighties, during the Soviet-Afghan civil war. Promoting international jihadism in order to establish an Islamic caliphate, Al-Qaeda enjoyed protection and hospitality of the Taliban regime in Afghanistan, as well as of Saudi Arabia, Pakistan and Sudan during the Nineties. For an extensive analysis of the roots of Al-Qaeda: C. HELLMICH, "Al-Qaeda: From Global Network to Local Franchise", Bloomsbury, 2011.

in the country[244] and in the neighbouring areas[245]. At the moment, ISIL Khorasan – the regional ISIL's branch – represents the major terrorist threat in the area, extending its action in north-eastern Iran, southern Turkmenistan, and northern Afghanistan, together with the Al-Qaeda branch based in Yemen, known as Al-Qaeda in the Arabian Peninsula (AQAP) [246].

Shifting the attention to South-East Asia, the Philippines and Indonesia appear to display the highest terrorist threat in the region. In particular, the Abu Sayyaf Group (ASG)[247] is held as one of the most violent groups operating in the area, together with Al-Qaeda-affiliate Jemaah Islamiyah (AJAI)[248]. Both aiming at establishing an

[244] Although the agreement signed in 2020 between the U.S. and the Taliban leadership clearly states that "*the Islamic Republic of Afghanistan reaffirms its continued commitment not to cooperate with or permit international terrorist groups or individuals to recruit, train, raise funds (including through the production or distribution of narcotics), transit Afghanistan or misuse its internationally recognized travel documents, or conduct other support activities in Afghanistan, and will not host them*", the U.S. manifested concern about the possible evolution of the terrorist threat in the area: "Annual Threat Assessment of the U.S. Intelligence Community", Office of the Director of National Intelligence, 7 February 2022. Moreover, the UN recently reported that, despite the fact that only few foreign fighters are moving to Afghanistan, "*there are no recent signs that the Taliban has taken steps to limit the activities of foreign terrorist fighters in the country*", noting that "*Member States are concerned that terrorist groups enjoy greater freedom in Afghanistan than at any time in recent history*": "Fourteenth Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat", 28 January 2022, (S/2022/63), 7.

[245] Specific concerns are showed in relation to Pakistan: L. O'DONNELL, "Pakistan Sponsored Terror Next Door. Now, It's Back to Roost", Foreign Policy, 31 May 2022.

[246] According to UN, ISIL-Khorasan has increased from earlier estimates of 2,200 fighters to now approaching 4,000 following the release by the Taliban of several thousand individuals from prison: Fourteenth Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat, 28 January 2022 (S/2022/63), par. 33, 7.

[247] Formally founded by Abdurajak Abubakar Janjalani in 1991, ASG's main goal is to establish an independent Islamic State in southern Philippines. After its pledge to ISIL, ASG intensified its terrorist activities: V. S. KALICHARAN, "An Evaluation of the Islamic State's Influence over the Abu Sayyaf", in *Perspectives on Terrorism*, Vol. (13) 5, 2019, 90-101. However, the motives at the basis of this alliance would rely more on practical needs than ideological beliefs: J. FRANCO, P. HOLTMANN, "Pledges to Islamic State: Weak and Strong Alliances", in *RSIS Commentary*, No. 221, 2014, 1-2.

[248] Established in the late Eighties in Indonesia, AIJI aims at establishing an Islamic state based on Sharia across Southeast Asia. In particular, AIJI was responsible of the 2002 Bali bombing attacks, which resulted in the death of over 200 people. Although apparently less active in recent years, experts have warned that the threat would still be concrete: C. VALLEE, "Jemaah Islamiyah: Another Manifestation of al Qaeda Core's Global Strategy", in *New Perspectives in Foreign Policy*, Vol. 15, 2018, 63-68. On the roots of AIJI: B. SINGH, "The Talibanization of Sutheast Asia. Losing the war on terror to Islamist extremists", Praeger Security International, Westport, 2007, 50-99.

independent Islamic State, ASG and AJAI appear to occasionally cooperate - although in competition one against each other[249].

1.4 Western countries: the rise of ethnically and racially motivated terrorism

The Salafi-jihadist threat still covers a central role in the national and international agendas, since in recent years multiple terrorist attacks have taken place – especially in Western countries – and the alarming attractiveness of their narratives, which foster the alarming phenomenon of foreign fighters. However, in recent years scholars and policy makers have begun to appreciate the rise of a new form of terrorism, often referred to as "ethnically or racially motivated terrorism" (ERMT) which is apparently spreading in the Western world – namely Europe, U.S. and Australasia. Linked to far-right environments and motivated by racial or ethnic beliefs[250], this new phenomenon has emerged as a manifestation of domestic terrorism characterised by attacks perpetrated by local lone actors – such as the ones that took place in 2019 in Christchurch (New Zealand)[251], El Paso (Texas)[252], Halle (Germany)[253] and in 2020 in Hanau (Germany)[254]. Overall, the concern surrounding this phenomenon is growing: while in Europe the number of individuals arrested

[249] B. SINGH, "The Talibanization of Sutheast Asia. Losing the war on terror to Islamist extremists", *Ibid*., 85 ss.

[250] Given its multifaceted nature, this phenomenon is also referred to as "right-wing extremism" or "far-right-terrorism". For an analysis of the far-right phenomenon: C. MUDDE, "The far right today", Polity Press, 2019.

[251] On 15 March 2019, Brenton Harrison Tarrant - linked to the far-right and inspired by white supremacist beliefs - carried out two consecutive mass shootings in two mosques in Christchurch, New Zealand, which resulted in the death of 51 people and in the injury of 40 others.

[252] On 3 August 2019, Patrick Wood Crusius, linked to the far-right, killed 23 people and injured 23 others in a mass shooting at a Walmart store in El Paso, Texas.

[253] On 9 October 2019, Stephan Balliet tried to carry out a shooting in a synagogue in Halle, Germany. Failing in his purpose, the attacker shot and killed two people nearby and injured two others.

[254] On 19 February 2020, eleven people were killed and five others injured during a shooting in two bars in Hanau, Germany. After the attack, the perpetrator, linked to the far-right, killed his mother and then killed himself.

on suspicion of involvement in right-wing terrorist activity is increasing[255], the U.S. government assessed that racially or ethnically motivated violent extremists are likely to carry out mass-casualty attacks against civilians, stating that this phenomenon is very likely to continue to constitute a threat in the future[256].

2. The purposes of terrorism financing

As already underlined when analysing the evolution of the criminalisation of terrorism financing, the conducts of financing encompass both the collection and provision of fund linked to the perpetration of terrorist attacks and the collection and provision of funds aimed at generally supporting terrorists and terrorist organisations[257]. Of course, these costs can considerably vary according to the nature of the attack perpetrated and the structure of the terrorist groups. In this respect, in recent years it has been witnessed a general shift from structured attacks requiring a considerable amount of funds and people involved, usually directed against symbols of power – like the 9/11 attacks – towards attacks committed by lone actors – often self-funded – and directed against soft targets – such as a street market – which can be carried out with a limited amount of funds, and still being effective and achieving great media resonance[258].

---

[255] Although no concrete attack has been registered in Europe in 2021, State Members authorities arrested 64 individuals suspected of planning right-wing terrorist or extremist attacks, thus marking a clear increase compared to the 34 arrested made in 2020 and the 21 completed in 2019. At the same time, the age of people suspected of being involved in such activities continued to decrease, following a trend already registered in 2021: European Union Terrorism Situation & Trend Report (TESAT), EUROPOL, 14 July 2022.

[256] "Annual Assessment of the U.S. Intelligence Community", *Ibid.*, 27. In this context, it is interesting to notice that some countries have already designated some of these groups as terrorist adding them to their own blacklists. This is the case of the United Kingdom, which has listed four extreme-right groups (National Action, Scottish Dawn, Sonnenkrieg Division and NS131), and Canada, which has proscribed Blood & Honour and Combat groups: "Member States concerned by the growing and increasingly transnational threat of extreme right-wing terrorism", UN CTED Trends Alert, United Nations Security Council Counter-Terrorism Committee Executive Directorate, April 2020, 8.

[257] *Supra* Chapter I.

[258] Although there is no internationally agreed definition of "soft target", the UN reports that "*the term has typically been used to describe public spaces or other locations that are easily accessible and predominantly civilian in nature, often with limited security measures in place*", and that such locations have been chosen by terrorists because they offer terrorist the "*the opportunity to maximize casualties*

Similarly, as mapped above (*supra* §1), the decentralisation of terrorist groups led to a reshaping of their structure, which generally resulted in the abandon of rigid hierarchies in favour of fluid networks. However, the support of a terrorist organisation still implies considerable costs, especially for those still existing state-like organisation which present complex bureaucratic structures. Some of these costs are fixed, such as the support of active members and their families, and the costs related to training activities, travels and logistics. For instance, ISIL's largest expenditures are represented by the salaries paid to the fighters and to the families of imprisoned or deceased fighters[259]. Others, instead, can eventually vary, as the ones devoted to the promotion of the ideology and to recruitment activities. Recruitment methods and techniques and their costs, indeed, seem to change according to the social and political context of the region: while in Eurasia terrorist groups mostly rely on structured recruitment networks which require financial support, in Africa and in parts of the Middle-East they focus their recruitment campaigns in the territories they have control over or influence to some extent; in Europe, instead, terrorists prefer to reach out to new members through social contacts in lower urban areas – including specific religious gatherings and prisons – and online[260].

Indeed, in recent years the role of the Internet has steadily increased, as it not only allows terrorists to spread their propaganda globally and recruiting new members at lower expenses through websites, platforms and social media[261], but it also has

and generate widespread publicity": "Responding to terrorist threats against soft targets", UN CTED Analytical Brief, United Nations Security Council Counter-Terrorism Committee Executive Directorate, 2019, 2.

[259] "2022 National Terrorist Financing Risk Assessment", U.S. Treasury Department, February 2022, 6.

[260] Report on "Financing of Recruitment for Terrorist Purposes", FATF, January 2018, 6. However, the FATF notes that Boko Haram is known to recruit also outside its territories, namely from the lower North Central states of the country and from countries within the regions of West and Central Africa, including Senegal, Mali, Mauritania, Niger, Chad and Cameroon.

[261] Notwithstanding the fact that, the higher the quality of the contents created, the higher the investments required: Report on "Financing of Recruitment for Terrorist Purposes", *Ibid.*, 19. For instance, ISIL is known to have put a great effort in spreading its propaganda through self-published online magazines in different languages in order to reach the largest public possible, such as Dabiq

proven to be an effective vehicle both for collecting (e.g. fundraising and crowdfunding activities) and transfer of funds[262].

3. Who finances terrorism?

Financiers of terrorism are traditionally divided into two categories: States that sponsor terrorist groups and private individuals and entities – including terrorists themselves – that provide financial support. Whereas during the past century forms of active State-sponsored terrorism were widely acknowledged[263], after the end of the Cold War and the 9/11 attacks the role of States in financing terrorist activities seems to have diminished; nonetheless, it can still be relevant[264].

Furthermore, it has been suggested that some elements could be relevant when it comes to choose on what source of funding rely on, namely: quantity, legitimacy, security, reliability, control, and simplicity. Of course, not all of these criteria will cover the same importance for all terrorists; according to their needs and capacities, terrorists will evaluate what sources will be the best choice[265].

(English and others), Dar-al-Islam (French), Istok (Russian), Konstantiniyye (Turkish) and Rumyia (English and others).

[262] For a comprehensive analysis on the use of the Internet for terrorist purposes, including terrorism financing: Report on "The Use of the Internet for terrorist purposes", United Nations Office on Drugs and Crime (UNODC), New York, September 2012. See also: M. JACOBSON, "Terrorist Financing and the Internet", in *Studies in Conflict & Terrorism*, Vol. 33 (4), 2010, 353-365. For an analysis on how Al Qaeda exploits internet for spreading propaganda, recruiting, training and financing: M. RUDNER, "'Electronic Jihad': the Internet as Al Qaeda's Catalyst for Global Terror", in *Studies in Conflict & Terrorism*, Vol. 40 (1), 2017, 10-23.

[263] See *supra* Chapter I, § 2.1.

[264] S. D. COLLINS, "State-Sponsored Terrorism: In Decline, Yet Still a Potent Threat", in *Politics & Policy*, Vol. (42) 1, 2014, 131-159.

[265] See M. FREEMAN, "The sources of terrorist financing: theory and typology", in *Studies in Conflict & Terrorism*, Vol. 34, 2011, 461-475.

3.1 State sponsors of terrorism

States can be interested in supporting terrorism for multiple reasons. First, they can decide to back terrorist organisations in order to fulfil their strategic purposes, such as the destabilisation of a neighbour country or to expand their power beyond borders. Second, States can be pushed by ideological motivations, such as exporting their political system and to enhance their prestige. Lastly, supporting terrorism can be seen as a mean to bolster and reinforce domestic power[266].

Exploiting terrorism for one - or more - of these reasons, "rogue states"[267] that have contributed to the survival and maintenance of terrorist organisations have done so on different levels, ranging from simply tolerating terrorists' presence on their territory to actively help them to reach their goals by providing them weapons, funds, diplomatic backing, training, organisational assistance, ideological direction and even serving as safe havens[268]. Over the years, States that have been accused of supporting terrorism include Cuba, North Korea, Syria, Libya, Sudan, Yemen, Qatar, Afghanistan and Iran; however, most of them largely stopped their sponsorship activities in recent years[269]. Nonetheless, some terrorist groups still greatly benefit from States' support: this is the case of Hezbollah, which is considered to be enjoying support from Iran since the Nineties to these days[270] - to the point that Iran funding is estimated represent the biggest source of income for

[266] For an extensive analysis on the motives that can push a State to sponsor terrorism: D. L. BYMAN, "Deadly connections: states that sponsor terrorism", Cambridge University Press, 2005, 36-52.

[267] Used for the first time in 1994 by President Clinton in relation to Iran and Lybia, the term "rogue states" has then been used by the U.S. to refer also to Cuba, Sudan, Syria and North Korea: P. MINNEROP, "Rogue States – State Sponsors of Terrorism?", in *German Law Journal*, Vol. 3, 2002. On the creation of the "rogue States" category in response to the void left by the end of the Cold War: N. CHOMSKY, "Rogue States. The Rule of Force in World Affairs", Pluto Press, London, 2000, 19 ss.

[268] D. L. BYMAN, *Ibid.*, 59-66.

[269] On this point, it is interesting to report the changes over the years on the U.S. State sponsors of terrorism list. The list has included: South Yemen (1979-2000), Libya (1979-2006), Iraq (1979-1982 and 1990-2004), Cuba (1982-2015 and 2021 to this day), Iran (1984 to this day), North Korea (1988-2008 and 2017 to this day), Sudan (1993-2020).

[270] For a detailed overview of the ties between Iran and Hezbollah: E. OTTOLENGHI, "State sponsors of terrorism: an examination of Iran's Global Terrorism Network", Congressional Testimony: Foundation for Defense of Democracy, 17 April 2018.

Hezbollah, supplying it with weapons and funding[271]. Iran, in addition, is held to be one of the major supporters of Hamas as well[272].

3.2 Private sources of terrorism financing

With the reduced role played by States in supporting terrorism, nowadays terrorists appear to rely mainly on private channels, receiving funds by donors or directly financing themselves both through licit and criminal activities. In this respect, both the structure and the geographical location of terrorist organisations affect the choice of means employed to raise funds: while lone actors are more inclined to rely on personal revenues or commit petty crimes to collect the funds needed, structured organisation can resort to more sophisticated means, such as setting up legitimate businesses or complex crime schemes. In the same way, terrorists which are in control of territories are likely to exploit them to raise funds, whereas lone actors or fluid networks turn to other forms of funding which do not depend on their physical location, such as donations.

---

[271] "Country Reports on Terrorism 2020", U.S. Department of State, December 2021, 113: "*Iran's annual financial backing to Hizballah — which in recent years has been estimated to be in the hundreds of millions of dollars — accounts for most of the group's annual budget*". However, due to economic difficulties, Iran has lately reduced its financial support to Hezbollah, thus possibly forcing Hezbollah to increase its involvement in criminal activities: "2022 National Terrorist Financing Risk Assessment", *Ibid.*,11.

[272] For a deeper analysis: M. LEVITT, "Hamas: Politics, Charity, and Terrorism in the Service of Jihad", Yale University Press, 2006. See also: I. LEVY, "How Iran Fuels Hamas Terrorism", The Washington Institute for Near East Policy, 1 June 2021.

3.2.1 Legitimate private sources of funding

As highlighted in Chapter I, the peculiar feature of terrorism financing is that while the funds raised are destined to criminal use, their origin can be both illegitimate and legitimate. With regard to the possible legitimate sources of funding, terrorists can collect funds on small scale through personal savings, salaries, pensions, rents and welfare payments, as well as on a larger scale thanks to donations or by exploiting legitimate businesses and charities, thus posing significant challenges in terms of detection of the financial flow[273].

The use of small legitimate personal revenues poses particular issues, as their misuse is very difficult to prevent, especially when the amounts needed are small and not detectable through the AML/CTF procedures. In recent years, indeed, we have acknowledged the rise of low-budget terrorist attacks, carried out by self-funded individuals who use their own money to buy the weapons needed and to organise and effectively carry out the whole attacks. This is the case, for instance, not only of the latest jihadist-linked attacks that have taken place in Europe, but also of the ERMT *modus operandi* displayed so far (*supra* § 1.4).

Furthermore, members and sympathizers of terrorist organisations can contribute to the terrorist cause by using their savings for donations, both aimed at funding a specific attack or generally to help the survival and prosperity of the organisation. Among terrorist groups that benefit the most from donations, we find Al Qaeda[274] and its affiliates - such as AJAI[275] - as well as ERMT groups, the latter being particularly active on social media, forums, gaming chatrooms and other online platforms, where they carry out crowdfunding initiatives. Indeed, these groups use

---

[273] I. BANTEKAS, *Ibid.*, 320. For instance, a recent report revealed that the majority of U.S. ISIL's supporters that engaged in fundraising activities chose licit means – mostly through donations – while a minority engaged in illegal tactics, mostly consisting of financial aid fraud: L. VIDINO, J. LEWIS, A. MINES, "Dollars for Daesh. Analyzing the Finances of American ISIS Supporters", The Georgetown Washington University, 2020.

[274] Report on "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", FATF, February 2015.

[275] AJAI is known to receive funds both from internal and external donors: B. SINGH, "The Talibanization of Sutheast Asia. Losing the war on terror to Islamist extremists", *Ibid*., 79.

crowdfunding in a similar way to terrorist organisations, that is to say exploiting popular crowdfunding platforms to expand their reach and soliciting funding on their websites or social networks - with the big difference that they often do not need to disguise the true aim of their crowdfunding campaigns[276].

Another possible legitimate source of funds to support terrorist activities is represented by the proceeds deriving from legitimate businesses. Terrorists, indeed, could find convenient to set up a licit business, especially in those cases where no formal qualifications or great initial investments are required, and diverting the proceeds to terrorist purposes[277]. Similarly, charitable activities are often used by terrorists to misguide and hide the collection of funds for terrorist purposes, and, as early as with Resolution 21/210 (1996), the United Nations General Assembly expressed concern on their possible exploitation[278] - a concern the reaffirmed by the FATF Special Recommendation VIII (now transposed to Rec. 8)[279]. In this sense, non-profit organisations (NPOs) display some features that can be attractive to terrorists – that is to say, terrorist financing vulnerabilities - which substantially consist in the possible exploitation of their extended logistical networks, large transitory workforces, operational capacity and organisational culture[280]. Benefitting from public trust, indeed, charities can collect considerable amounts of

---

[276] According to the FATF, indeed, extreme right-wing groups may feel less need to hide their activities, especially if the group has not been designated as terrorist or officially banned. In this respect, the FATF suggests that designating these actors as terrorists could be useful in terms of denying them access to the regulated financial system and disrupting their public fundraising capabilities: Report on "Ethnically or Racially Motivated Terrorism Financing", FATF, June 2021, 10.

[277] Report on "Terrorist Financing Typologies", FATF, 2008, 13.

[278] Especially, A/RES/21/210 (1996) par. 3 (d) called upon States to "*investigate, when sufficient justification exists according to national laws, and acting within their jurisdiction and through appropriate channels of international cooperation, the abuse of organizations, groups or associations, including those with charitable, social or cultural goals, by terrorists who use them as a cover for their own activities*". In this respect, it is interesting to underline that also the 1999 Convention at Recital no. 6 recalled the concern expressed by A/RES/21/210 (1996) on the misuse of charitable organisations.

[279] On this point, it is interesting to notice that the FATF Recommendation 8 does not apply to all the NPOs, but only to those that display characteristics and carry out activities which put it at risk of terrorist financing abuse. For this purpose, the NPOs FATF functional definition includes "*legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works""*: FATF Recommendations, March 2022, 58.

[280] Report on "Risk of Terrorist Abuse in Non-Profit Organisations", FATF, June 2014, 24-26.

money – often in cash – that can be diverted for funding terrorist activities, exploiting legitimate charities as conduits for terrorism financing or to conceal the illegal diversion of funds originally intended for legitimate purposes to terrorist ones, or by establishing sham charities, entirely devoted to raise funds for terrorism - in this way setting up an entirely illegitimate business[281]. In this respect, over the years authorities have identified multiple charities networks linked to terrorist organisations, such as Al-Qaeda[282] and Hamas[283] and, although for a while seemed that terrorists had diminished the abuse of charities as means of funding, nowadays they seem to have return to rely on such schemes[284].

3.2.2 Illegitimate private sources of funding

The proceeds deriving from criminal activities represent a large source of income for terrorist organisations, going from petty crimes to larger criminal schemes.

In particular, terrorist organisations that enjoy control over territories tend to make the most of their revenues from the exploitation of their natural resources – including oil, gas, agriculture, fishing, wildlife trade, minerals and precious metals[285] - and of local population, imposing illicit taxes or engaging in criminal activities such as human trafficking, smuggling and kidnapping for ransom. This is the case of Al-Shabaab, JNAIM, and HTS[286]. Al-Shabaab, for instance, appears to

[281] For examples of cases of terrorism financing through sham charities: N. RAPHAELI, "Financing of terrorism: sources, methods, and channels", in *Terrorism and Political Violence*, Vol. 15 (4), 2003, 62 ss.
[282] M. LEVITT, "Charitable Organizations and Terrorist Financing: A War on Terror Status-Check", The Washington Institute for Near East Policy, 19 March 2004.
[283] M. LEVITT, "Hamas : Politics, Charity, and Terrorism in the Service of Jihad", *Ibid*., 142 ss.
[284] In this sense: K. BAUER, M. LEVITT, "Funding in Place: Local Financing Trends Behind Today's Global Terrorist Threat", in *Evolutions in Counter-Terrorism*, The International Centre for Counter-Terrorism – The Hague (ICCT), Vol. 2, 2020, 47-76.
[285] "Concern over the use of proceeds from the exploitation, trade, and trafficking of natural resources for the purposes of terrorism financing", UN CTED Trends Alert, United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), June 2022.
[286] 2022 National Terrorist Financing Risk Assessment, *Ibid*., 9.

domestically rely on a "taxation" system organised in multiple checkpoints across Somalia[287], on extortion schemes and on the collection of *zakat*[288].

Similar dynamics were appreciated in relation to ISIL at the time of its maximum expansion, when its primary source of revenue consisted in the illicit proceeds from bank looting, extortion, control of oil fields and refineries, agriculture, robbery of economic assets – which allegedly included also historical and archaeological artefacts[289] - and illicit taxation of cash and goods that would transit across their territories[290]. As a consequence of the territorial losses suffered, ISIL shifted towards others sources of income, which include looting local civilians and businesses, kidnapping for ransom, extortion of oil networks, and possibly through the trafficking of artifacts previously looted and human trafficking activities[291]. Indeed, ISIL's provinces and allies in Africa have been known to engage in kidnapping for

---

[287] The taxation checkpoints are located across the main supply routes in southern and central Somalia. According to UNSC, the amount of the tax varies according to the type of vehicle and the goods carried. For instance, in case of a new vehicle, a registration tax is required, which could range from $200 to $500 depending on the type of vehicle: Final Report of the Panel of Experts on Somalia, adopted by the Security Council on 28 September 2020 (S/2020/949), 8.

[288] *Zakat* is an obligation for Muslims to donate 2.5% of their wealth when it exceeds a minimum level, with the aim of reducing poverty and redistribute incomes among the community. Being one of the five pillars of Islam, it is often used by terrorist groups as a means to collect funds: for instance, reports show that also ISWAP would resort to *Zakat* to raise money in north-eastern Nigeria: A. THURSTON, "Why Jihadists are collecting Zakat in the Sahel", in *Political Violence at a Glance*, 12 July 2021. Moreover, it has been remarked that criminal activities have enhanced the prosperity of Al-Shabaab: K. PETRICH, "Cows, Charcoal, and Cocaine: Al-Shabaab's Criminal Activities in the Horn of Africa", in *Studies in Conflict & Terrorism*, 2019, 1-22.

[289] Although obtaining data about the real extension of artefacts and historical goods is difficult, the international attention on the matter is high. For instance, we recall here the adoption of Security Council Resolution 2199 (2015) which, following ISIL's expansion, extended to Syria the prohibition of trade in cultural objects already in place for Iraq (Security Council Resolution 1483 (2003)). In addition, the European Union recently adopted a new Regulation on the introduction and import of cultural goods having regard – among others – that: "*In light of the Council Conclusions of 12 February 2016 on the fight against the financing of terrorism, the Communication from the Commission to the European Parliament and the Council of 2 February 2016 on an Action Plan for strengthening the fight against terrorist financing and Directive (EU) 2017/541 of the European Parliament and of the Council, common rules on trade with third countries should be adopted so as to ensure the effective protection against illicit trade in cultural goods and against their loss or destruction, the preservation of humanity's cultural heritage and the prevention of terrorist financing and money laundering through the sale of pillaged cultural goods to buyers in the Union*": Regulation (EU)2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods, Recital No. 1.

[290] Report on "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", FATF, 2015.

[291] Public Statement on the Financing of ISIL, Al Qaeda and Affiliates, FATF, 21 October 2021.

ransom, as well as Boko Haram and Al-Shabaab[292], and terrorist groups may raise funds also by contributing in smuggling of migrants to raise funds, especially when the territories they control are located on smuggling routes - such as Burkina Faso, Niger and Mali, Syria, Iraq and Afghanistan - requesting them to pay 'tolls' for passage or in exchange for security[293]. With regard to South-East Asia, criminal activities appear to be a major source of funding for ASG, which engages in kidnaping for ransom, drug trafficking, arms smuggling, extortion and assassination[294].

4. Terrorism financing methods

Just like the choice on how to raise funds depends on terrorists' needs, abilities, location and organisation, similar considerations guide terrorists when it comes to decide how to move the funds collected. Taking into account their volume, the level of risk, the general convenience, as well as simplicity, costs and speed[295], terrorist may resort to a number of different means, which include the physical transportation of money or goods across borders, the transfer of funds through the formal banking system, the use informal transfer systems – which do not depend on banks or financial institutions – or to transfer funds online via new payment methods.

[292] Report on "Financial Flows from Human Trafficking", FATF, July 2018, 15.
[293] Report on "Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling", FATF, March 2022, 27.
[294] B. SINGH, "Crime-Terror Nexus in Southeast Asia: Case Study of the Abu Sayyaf Group", in *Counter Terrorist Trends and Analyses* - International Centre for Political Violence and Terrorism Research, Vol. (10) 9, 2018, 6-10.
[295] M. FREEMAN, M. RUHESEN, "Terrorism Financing Methods: An Overview", in *Perspectives on Terrorism*, Vol. (7) 4, 2013, 5-26.

4.1 The oldest method of all: the use of cash couriers

Ensuring anonymity, quick transactions and wide acceptance, cash still enjoys a high degree of popularity. Despite the development of digital payments, indeed, cash is still extensively used not only in less developed countries, but also among advanced economies[296] and, even if COVID-19 pandemic has accelerated the digitalisation process, cash continues to play a central role[297].

Therefore, it is not surprising that the oldest and easiest method used by terrorists to transfer funds across borders is the movement of cash[298]. The physical transportation of cash can be particularly attractive in case of jurisdictions with porous borders, where terrorists may possibly rely on the connivance of border controllers, and, while on the one hand it does not allow to transfer a lot of money at one time – or at least makes it more difficult and more dangerous – on the other hand in this way terrorists avoid the controls and the restrictions put in place by countries to monitor the flows of money through the banking system. For instance, Al-Qaeda and JNAIM both used to rely on cash couriers to move money during the Nineties[299], and, more recently, foreign fighters joining ISIL have been reported to be explicitly requested to bring cash with them when traveling to their final destination[300], and ISIL would still be using networks of cash couriers to transfer cash between and among Iraq, Syria and Turkey[301].

---

[296] According to a survey carried out by ECB in 2019, the share of cash usage for day-to-day transaction in the euro area is 73%: "Study on the payment attitudes of consumers in the euro area (SPACE)", European Central Bank, December 2020.

[297] F. PANETTA, "Cash still king in times of COVID-19" – Keynote speech at the Deutsche Bundesbank's 5th International Cash Conference – "Cash in times of turmoil", European Central Bank, 15 June 2021.

[298] We remind that the FATF added a specific Recommendation on cash couriers in 2004 (Special Recommendation IX), now transposed into Recommendation 32.

[299] M. FREEMAN, M. RUHESEN, *Ibid.*, 8-9.

[300] Report on "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", FATF, 29.

[301] 2022 National Terrorist Financing Risk Assessment, *Ibid.*,6.

4.2 The exploitation of the formal banking system

After the 9/11 attacks, the banking and financial sector have been at the centre of multiple sets of regulations aimed at reinforcing the controls over the flows of money, with the explicit aim of deterring and disrupting the financing of terrorism and money laundering schemes. Nevertheless, formal banking system appear to still be a vulnerable sector[302], subject to the possible exploitation for terrorist purposes through a number of means, including the help of complicit employees, the use of intermediaries to complete transactions and setting up accounts in off-shore banks. Hezbollah, for instance, appears to regularly resort to the international banking system to receive and send funds[303], and in recent years the U.S Office of Foreign Assets Control (OFAC)[304] has designated numerous financial institutions involved in terrorism financing activities for Hezbollah, the latest being the Lebanese Jammal Trust Bank (JTB) in 2019[305]. Also Al-Qaeda seems to continue to use the regulated financial system to support its terrorist activities[306]: for instance, in 2021 Al-Qaeda associates sent money to a Turkish bank account to support Al-

[302]Joint Report of the Counter Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team on actions taken by Member States to disrupt terrorism financing, adopted by the Security Council on 3 June 2020 (S/2020/493), 16, par. 55: "*more than half of responding States identified the formal banking system as the most frequently used terrorism-financing channel*".

[303] This has been linked in part to the fact that there is no international agreement on the status of Hezbollah as a terrorist organisation: while the United States, the United Kingdom, Canada, Australia, Germany and Israel have designated Hezbollah as a terrorist group, the European Union has only designated its military wing, while the UN does not provide for targeted sanctions against Hezbollah. In this sense: 2022 National Terrorist Financing Risk Assessment, *Ibid*., 17.

[304] Established in 1950 in Washington D.C., the Office of Foreign Assets Control (OFAC) is the agency of the US Department of the Treasury charged of the administration and enforcement of economic and trade sanctions.

[305] "Treasury Labels Bank Providing Financial Services to Hizballah as Specially Designated Global Terrorist", U.S. Department of the Treasury – Press Release, 19 August 2019. Other financial institutions linked to Hezbollah that have been designated in recent years include: Chams Exchange Company SAL (2019); Kassem Rmeiti & Co. For Exchange (2013); Halawi Exchange (2013); Hassan Ayash Exchange (2011); Ellissa Exchange Company (2011); New Line Exchange Trust Co. (2011); Lebanese-Canadian Bank (2011). For a deeper analysis: T. BADRAN, E. OTTOLENGHI, "Hezbollah Finance in Lebanon. A Primary-Source Review", Foundation for Defense of Democracies, 23 September 2020.

[306] 2022 National Terrorist Financing Risk Assessment. *Ibid*., 8.

Qaeda terrorist operations in Syria[307]. With regard to ISIL, particular concerns were raised at the time of its maximum expansion, namely with regard to those financial institutions located in the territories fallen under its control in Iraq and Syria[308].
Lastly, it has been noticed ERMT actors could be more inclined to use regulated financial institutions to move funds since they have fewer operational security concerns, as many of these groups and activities are not considered illegal or, when they are, they require small amounts of funds[309].

4.3 Informal Value Transfer Systems: *Hawala* and terrorism financing

Also referred to as "Informal Funds Systems" or "Alternative Remittance Systems", Informal Value Transfer Systems (IVTS) can be described as "*any system or network of people facilitating, on a full-time or part-time basis, the transfer of value domestically or internationally outside the conventional, regulated financial institutional systems*". Relying on mutual trust and reputation, and often backed by strong ethnic, tribal or religious ties[310], examples of IVTS can be found in those regions where access to regulated financial system is not always guaranteed or trusted, thus serving as an instrument of financial inclusion or even representing the main system for transferring money[311]; these networks, indeed, are frequently used by immigrants

[307] "Treasury Designates Al-Qa'ida-Linked Financial Facilitators in Turkey and Syria", U.S. Department of the Treasury – Press Release, 28 July 2021.
[308] Indeed, numerous banks based in Syria have been designated both by the U.S. and the European Union, such as the Central Bank of Syria, Commercial Bank of Syria, and Syria International Islamic Bank: Report on Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL), FATF, February 2015, 27-28.
[309] Report on "Ethnically or Racially Motivated Terrorism Financing", FATF, June 2021, 21-22.
[310] M. VACCANI, "Alternative remittance systems and terrorism financing: issues in risk mitigation", World Bank Working Papers, 2010, 13.
[311] For this reason, it has been remarked that it would be incorrect to label these systems as "alternative", since they would actually constitute the rule and not the exception: N. PASSAS, "Informal Value Transfer Systems and Criminal Organizations; a study into so-called underground banking networks", 1999, 11.

to send money to their families[312] and also by human relief workers to reach war-torn and particularly unstable areas[313].

In the wake of the 9/11 attacks, Informal Value Transfer Systems began to receive increased attention and to be identified as one of the main possible channels of money transfers used by terrorists[314]. The attention focused especially on the *Hawala* system[315], given its presence across Southeast Asia, Middle-East and Africa[316] and still nowadays it is believed to be one of the channels terrorists resort to transfer their funds. Suspects on Hawala networks are mainly based to the fact that funds are transferred without any physical movement or traceability in the regulated financial system: if a person wishes to transfer money to another person located abroad, all he has to do is to contact an *Hawala* dealer (*hawaladar*) based in his country, who will contact the *Hawala* dealer operating in the country of destination, providing him with instructions to give the amount requested to the recipient, and the entire operation is secured by a password known only among the sender, the recipient and the two *Hawala* dealers[317]. However, it has been remarked that actually *Hawala* mostly serve as a useful system of financial inclusion, and that such networks are more connected and more similar to the banking system than they

---

[312] W. PERKEL, "Money Laundering and Terrorism: Informal Value Transfer Systems", in *American Criminal Law Review*, Vol. 41 (1), 2004, 200.

[313] E. A . THOMPSON, "Misplaced Blame: Islam, Terrorism and the Origins of Hawala", in *Max Planck Yearbook of United Nations Law*, Vol. 11, 2007, 280.

[314] We recall here that the FATF dedicated the Special Recommendation VI to money or value transfer services (now transposed into Recommendation 14). See also, FATF Report on "The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing", October 2013. For an overview of the possible AML/TF risks related to money transfer systems overall: FATF Guidance on a risk-based approach on money or value transfer systems", February 2016.

[315] *Hawala* is an Arabic term whose etymological meaning can be identified in "transform" or "change", in this way denoting a "transfer". Its origin are uncertain: E. A . THOMPSON, *Ibid.*, 288 ss. While our attention focuses on the *Hawala* system, it is interesting to notice that there are other IVTS used across the globe, which include: Hundi (India/Pakistan), Fei ch'ien , Hui k'uan , Ch'iao hui , Nging sing kek (China), Poey Kuan (Thailand), Bangelap (Indonesia): N. PASSAS, *Ibid.*, 8

[316] W. PERKEL, *Ibid.*, 185.

[317] For a deeper analysis: K. COOPER, C. WALKER, "Security from terrorism financing: models of delivery applied to informal value transfer systems", in *British Journal of Criminology*, Vol. (56) 6, 2016, 1125-1145.

appear, displaying some characteristics that regulated financial institutions aspire to – namely speed, trust, paperlesseness, global reach and fluidity[318].

4.4 The use of new payment methods

The development of new methods to transfer money and the rapid spread of the Internet brought new opportunities to quickly and securely the transfer of funds all over the globe – including for terrorist purposes. Indeed, it has been reported that terrorists have resorted to prepaid cards, mobile payments, and internet-based payment services (e.g. Paypal) [319], mostly in order to transfer funds to participate to fundraising activities promoted on online platforms and social media. Offering simpler and rapid way to transfer the funds globally and avoiding the more thorough controls of the traditional financial system methods, the appeal of this instrument can be easily understood. Besides, international actors such as the United Nations expressed a growing concern in recent years about the increased use of communications technology and internet by terrorists to finance their activities; among the most recent statements in this sense, we recall here Security Council Resolution 2462 (2019)[320], which stated that there is evidence of the growing role of communication technologies and of the internet, recognising that foreign terrorist fighters and terrorist groups could exploit emerging payments methods, including prepaid cards and mobile-payments or virtual-assets to move and transfer funds[321]. Furthermore, these concerns have been recently reiterated by the latest Review of the United Nations Counter-Terrorism Strategy[322], and overall urges members to "*enhance their efforts in the fight against the financing of terrorism by addressing the anonymity of transactions and by tracing, detecting, sanctioning and*

[318] In this sense: M. DE GOEDE, "Hawala discourses and the war on terrorist finance", in *Environment & Planning D: Society & Space*, Vol. (21) 5, 2003, 517, who states that labelling the *Hawala* system as the antithesis of normal banking has created a "financial enemy" – in this way reinforcing the enemy discourse within the war on terrorism.
[319] Report on "Emerging Terrorist Financing Risks", FATF, October 2015.
[320] S/RES/2462 (2019) adopted by the Security Council at its 8496th meeting, on 28 March 2019.
[321] S/RES/2462 (2019), 2.
[322] A/RES/75/291 (7th Review), 5.

effectively dismantling illegal money transmitters and tackling the risks associated with the use of cash, informal remittance systems, prepaid credit and debit cards, virtual assets and other anonymous means of monetary or financial transactions, as well as to anticipate and address, as appropriate, the risk of new financial instruments being abused for the purpose of terrorist financing" (Recital No. 57).

5. The possible impact of Virtual Assets on terrorist financing

"As technologies develop and virtual assets proliferate, there will be a growing appeal to use online transactions and cryptocurrencies for financing terrorism. This is a risk we must stay ahead of" [323].

Along the traditional sources and methods of terrorism financing abovementioned, in recent years the attention has progressively shifted towards the evolution of new technological solutions and their possible role for terrorism financing purposes. Initially focusing on their possible exploitation for money laundering schemes, indeed, the international concern relating to terrorism financing purposes has steadily increased, and it is currently at the core of both the international and national agendas, especially after the COVID-19 pandemic, which has led to the growth of digital payments and use of technology overall. Indeed, while evidences of terrorists using virtual assets for financing purposes is still little, things could rapidly change in the near future as technology becomes more accessible. Just like any other organisation, indeed, terrorists base their funding strategies on the basis of costs, capacity, and risk analysis[324]: while at the moment characteristics such as

[323]Peter Dutton, Chair of the 2019 "No Money for Terror" Ministerial Conference on Counter-Terrorism Financing, Melbourne, Australia, 7-8 November 2019.

[324] The appetite to implement new technological solutions broadly relies on four factors: i. technological awareness; ii. openness to new ideas; iii. attitudes towards risk; and, iv. nature of the environment: B. A. JACKSON, "Technology Acquisition by Terrorist Groups - Threat Assessment Informed by Lessons from Private Sector Technology Adoption, RAND Corporation, 2001. See also: R. MUGAVERO, V. SABATO, S. SOLDATELLI, "Analisi degli eventi terroristici e delle tecnologie

(pseudo) anonymity could be particularly attractive (*infra* § 5.5.1), others could deter terrorist to embark on the world of virtual assets – namely their still limited usability, security, acceptance and reliability.[325].

5.1 Virtual Assets ecosystem: mapping the conceptual framework

Before focusing on the possible role of Virtual Assets (VAs) in terrorism financing schemes, it essential to clearly understand their main characteristics and their functioning. Due to their complex technical features and to their constant evolution, indeed, there is often a certain degree of confusion surrounding the topic of Virtual Assets, starting with the names that have been used to refer to them, namely "virtual currencies", "cryptocurrencies", "cryptoassets" and "digital currencies". While each of these terms sheds a light on a specific feature, none of them can be held as a comprehensive definition of these new kind of tools. For this reason, for the purpose of this work it has been chosen to borrow the term "virtual assets" from the FATF, which constitutes a broad definition intended to include all the relevant feature of these new tools, and also to accommodate future developments. In this sense, "virtual assets" are intended as a

"*digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations*"[326].

impiegate", in "Terrorismo e Nuove Tecnologie", edited by R. Mugavero, R. Razzante, Pacini Giuridica, Pisa, 2016, 13-20.

[325] In this sense: C. DION-SCHWARZ, D. MANHEIM, P. B. JOHNSTON, "Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats", RAND Corporation 2019.

[326] This definition presents some points in common with the definition of virtual currencies provided in 2014 "Virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"),

It is interesting to notice that the FATF has very carefully avoided any references to the term "currency", choosing the term "value" instead, and, by including both payment/exchange and investment purposes, rightly specified that they can be digitally "transferred" or "traded". This choice of words reflects the uncertainties about the multi-faceted nature of virtual assets and their multiple possible functions, bearing in mind that the sector is evolving towards the integration of this tools in decentralised finance services, such as smart contracts[327] and decentralised applications (*infra* § 5.1.2).

As a result, the definition of virtual assets covers all those digital representations of value, whether centralised or decentralised, which are issued by private entities and that do not have legal tender[328]. Therefore, it is clear that virtual assets have to be distinguished from electronic money (e-money): indeed, even if both e-money and virtual assets are issued by a private entity, e-money does not constitute a separate currency and it is regulated by the central authority[329]. Accordingly, e-money has to be accepted as a means of payment by parties other than the issuer and it is redeemable at full face value upon demand, whereas virtual assets do not have legal tender[330].

---

which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status": Report on "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", FATF, June 2014, 4.

[327] The term "smart contract" first appeared in 1994, when Nick Szabo defined it as "*a computerized transaction protocol that executes the terms of a contract*": N. SZABO, "Smart Contracts", 1994.

[328] Of course, this include tokens, which are "*digital representations of VAs or rights and obligations, created, stored, and capable of being transferred electronically using distributed ledger technology (DLT) or similar technology and sometimes conferred during a sale to raise capital for a business or organization*" (e.g., ICOs). According to their function, four types of tokens can be distinguished: payment/exchange tokens, investment/security-type tokens – which provide rights such as shares, utility tokens – used to access applications or services and hybrid tokens – which can perform more than one function: Guidance Manual on "Virtual Assets and Virtual Assets Service Providers. ML/TF Risk Assessment Tool", World Bank Group, June 2022, 18-19.

[329] "Bitcoin Versus Electronic Money", World Bank, 2014.

[330] We remind that, according to the EU "E-money Directive", e-money is defined as "*electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive*

Moreover, virtual assets also do not include Central Bank Digital Currencies (CBDCs), which are currently being developed and tested by countries and represent a digital version of *fiat* money (*infra* § 5.1.3).

5.2 Where it all began: the rise of Bitcoin

In October 2008, a white paper called "A Peer-to-Peer Electronic Cash System" presented Bitcoin to the world[331], announcing that a new alternative transaction system based on distributed ledger technology (DLT), completely autonomous and independent from any central authority, would be implemented shortly. On 12 January 2009, the first Bitcoin transaction was registered[332] and, from that moment on, the interest for this new kind of technology has dramatically increased, leading to the birth of numerous other kinds of virtual assets (*altcoins*). Given that Bitcoin not only paved the way to the development of these new technologies, but is still by far the most common one, we are going to outline its main features, which are useful to understand the structure of Virtual Assets overall.

5.2.1 How does Bitcoin work?

Bitcoin is not the first attempt to use some sort of private currency as an alternative to *fiat* money: in the late Nineties two attempts had already taken place, namely the "e-gold" and the "Liberty Dollar", both shut down on the basis of possible misuse[333]. Unlike Bitcoin, however, they both relied on a centralised system, and that is where the real novelty of Bitcoin lies: the fact that it is based on decentralised system which

2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer" (Directive (EU) 2009/110, art. 2, n. 2).

[331] The paper was signed under the pseudonym of Satoshi Nakamoto; the real identity of the author is still unknown: NAKAMOTO S., " Bitcoin: A Peer-to-Peer Electronic Cash System".

[332] Carried out by the developer and computer scientist Hal Finney.

[333] F. M. AMETRANO, "Bitcoin: oro digitale per nuovi standard monetari", in "Dal sesterzio al bitcoin. Vecchie e nuove dimensioni del denaro", edited by A. Miglietta, A. Mingardi, Rubettino, 2020, 143.

does not need any central authority to operate[334]. Indeed, the architecture of Bitcoin is based on a public permissionless chain of independent nodes (*blockchain*)[335], meaning that everyone can connect to the blockchain without any authorisation[336], as the system auto-regulate itself through algorithms.

In fact, each node of the chain keeps a public and irreversible real time-shared register of all the transactions carried out and validates them thanks to a consensus algorithm called *proof of work*[337], which ensures that every Bitcoin is only spent once at a time – thus avoiding the phenomenon of *double spending*. Each transaction is verified by *mining* nodes, that create new nodes through the solution of algorithms, in this way carrying out the transaction and, since the solution of those algorithms requires a high level of expertise and resources[338], miners are remunerated for their work both with commissions and a prize in Bitcoin, the latter decreasing by half every 210.000 nodes[339]. Indeed, Bitcoin has been created in a limited number – the cap is set at 21 million – mocking the progressive scarcity of gold and enabling a system based on a total inelastic supply.

Moreover, users' Bitcoin are linked to addresses, which are managed through wallets. At the moment, five different types of wallets can be identified: i. hardware wallets, which allow users to store their keys online on physical devices; ii. software wallets, which consist in downloaded applications that can be stored on desktops or mobile devices, iii. hosted/custodial wallets, which are offered on websites by

---

334 We can distinguish three kinds of networks: centralised, distributed and decentralised. The terms "distributed" and "decentralised" are often used as synonyms, still they are not the same: while in decentralised systems nodes are only connected to peers, in distributed systems nodes distribute work to sub-nodes: N. ATTICO, "Blockchain. Guida all'ecosistema. Tecnologia, business e società", GueriniNEXT, 2018, 22-23.

335 For the sake of clarity, it is important to underline that blockchain is a type of distributed ledger technology (DLT), but not all DLTs rely on blockchains.

336 While public blockchains can be both permissionless and permissioned, private blockchains can only be permissioned.

337 Another consensus algorithm is the *proof of stake*, used, among others, by Cardano and Ethereum 2.0. Proof of work is basically a competition among miners to solve algorithms and validate the transaction, whereas proof of stake chooses random validators to confirm the transaction.

338 The activity of mining requires a great calculating capacity and consumes a great amount of energy.

339 And is estimated to terminate in 2140, when the last Bitcoin will be issued: the original amount of the prize was set at 50 Bitcoin; in 2012 decreased at 25 Bitcoin and in 2016 it was set at 12.5.

third-party service providers that have access to users' private keys; iv. hybrid wallets, which work like the hosted/custodial wallets except for the fact that the provider does not have access to users' private keys; and v. multi-signature wallets, which require the use of multiple keys to authorise the transactions, thus reducing the risk of thefts[340].

To ensure privacy, the addresses are protected by asymmetric cryptography through the use of a public and a private key: the public key identifies the address and it is – as the name suggests – public; the private key, instead, ensures the privacy of the address' owner identity.

5.2.2 The debated nature of Bitcoin

Despite the fact that Bitcoin made its first appearance fifteen years ago, debates on its nature are still ongoing.

First, if considered under the lens of a mean of transferring value, Bitcoin could constitute a new kind of money[341]. Money, indeed, is "*anything that people are willing to use in order to represent systematically the value of other things for the purpose of exchanging goods and services*"[342]: theoretically speaking, anything can be become "money", as long as it is accepted and trusted as medium of exchange. Looking back at the history of money, indeed, we can see how it hugely changed over centuries, going from objects whose acceptance was strictly linked to their intrinsic value, such as seeds, seashells, salt, and, later on, precious metals (e.g. copper, silver and gold) to the adoption of gold-backed money and then the complete emancipation from

[340] Study on "Virtual Currencies and Terrorism financing: assessing the risks and evaluating responses", European Parliament, 2018, 14.

[341] In this sense, Bitcoin has been associated to the Austrian school of Economics, namely with Van Hayek's theory on the effectiveness of a regime of currency competition, which would ensure a stable currency and thus a free society: European Central Bank, "Virtual Currency Schemes", 2012. However, it has been remarked that while Bitcoin is associated to gold, Hayek did not wish for a return to it: L. FANTACCI, "Cryptocurrencies and the Denationalization of Money", in *International Journal of Political Economy*, Vol. (48), 2019, 105-126.

[342] Y. N. HARARI, "Money", Vintage, London, 2018, 7.

any intrinsic value associated to it, achieved with the current *fiat* money[343]. "*Fiat*", indeed, means "created", and that refers to the fact that the value of money is not intrinsic, rather it relies on the fact that governments attribute to it the status of legal tender[344]. Similarly, virtual assets have no intrinsic value, so in this sense they could arguably be held as the ultimate form of money[345], as long as they manage to serve all the functions that are expected from currency, which notably are: medium of exchange, store value and unit of account.

As for medium of exchange, since at the moment Bitcoin does not have legal tender, all the transactions that have been – and are – carried out in order to purchase goods and services have been successful just on the basis of the agreement of the parties, since they lack mandatory acceptance[346].

But the biggest hesitations over Bitcoin as a new form of money are related to its high volatility, which has questioned its suitability to serve as store of value – especially in the short run[347] – and as unit of account, raising more than one concern in relation to the stability and integrity of financial markets and to monetary stability. Actually, this issue that involves not only Bitcoin, but all unbacked virtual assets, and, if until few years ago these concerns were limited, given that the number of users involved in virtual assets transactions was relatively small[348], nowadays this threat is considered to be much more concrete. In particular, it has been noted that

---

[343] For an overview of the history of money: S. AMMOUS, "The bitcoin standard: the decentralized alternative to central banking", Wiley, 2018, 11-72.

[344] In 1971, U.S. President Richard Nixon unilaterally ended the convertibility of the U.S. dollar to gold, in this way marking the beginning of the *fiat* money.

[345] In this sense: B. T. MCCALLUM, "The Bitcoin Revolution", in *Cato Journal*, Vol. 35(2), 2015, 347-356.

[346] We recall here the attempt made in this sense by Tesla, which in February 2021 announced to the U.S Securities and Exchange Commission to have invested 1.50 billion U.S. dollars in Bitcoin and that they would begin to accept Bitcoin as a form of payment: However, just a couple of months later Elon Musk stated that Tesla would stop to accept Bitcoin due to their intensive energy-consuming mining process.

[347] Over the long run, it has been remarked that their role as store of value will depend on their demand, that is to say to what users believe about its future success: E. GERBA, M. RUBIO, "Virtual Money: how much do Cryptocurrencies alter the fundamental functions of money?" in Monetary Dialogue Papers –European Parliament, December 2019, 19-20.

[348] E. GERBA, M. RUBIO, *Ibid.*, 23-24. In the same sense: ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", European Central Bank – Occasional Papers Series, No. 223, May 2019, 22: "*crypto-assets currently do not pose a material risk to financial stability in the euro area*".

Virtual Assets market is now bigger than the sub-prime mortgage market was when it started the 2008 financial crisis – which was estimated in 1.3 trillion dollars – and it would display similar dynamics[349]: in response to consumers' demand, indeed, also institutional activities are entering the market and investing in virtual assets (e.g. hedge funds), and nowadays virtual assets are considered as an emerging financial stability risk[350].

Given these characteristics, some suggested that Bitcoin should be considered as a speculative investment[351]. More precisely, Bitcoin used for speculative purposes may be considered a security, due to the investment of money, common enterprise, and expectation that profits will be derived from the efforts of third parties[352]. Others, instead, consider Bitcoin to fit under the big umbrella of commodities[353], since it can be used for commerce purposes, is interchangeable with other goods of the same type, and can be traded to hedge against economic risk[354]; more precisely, it has been noted that that Bitcoin would present some similarities with exhaustible commodity resources[355].

5.2.3 Beyond Bitcoin: the new forms of non-backed Altcoins

Bitcoin has been the first successful decentralised system that enabled peer-to-peer transactions, and it still holds its position as a leader in the virtual assets' ecosystem.

---

[349] F. PANETTA, "For a few cryptos more: the Wild West of crypto finance", Speech at Columbia University, 25 April 2022.

[350] For instance, in its latest report the Financial Stability Board remarked that virtual assets are rapidly evolving and could threaten global financial stability: "Assessment of Risks to Financial Stability from Crypto-assets", FSB, 16 February 2022.

[351] In this sense: D. YERMACK, "Is Bitcoin a real currency? An economic appraisal", National Bureau of Economic Research – Working Paper 19747, December 2013, 1-22.

[352] N. D. SWARTZ, "Bursting the Bitcoin Bubble: The Case to Regulate Digital Currency as Security or Commodity", in *Tulane Journal of Technology and Intellectual Property*, 2014, Vol. 17, pp. 319-336.

[353] M. PRENTIS, "Digital Metal: Regulating Bitcoin as a Commodity", in *Case Western Reserve Law Review*, Vol. 66 (2), 2015, 609-638.

[354] N. D. SWARTZ, *Ibid.*, 333 ss.

[355] M. GRONWALD, "Is Bitcoin a Commodity? On price jumps, demand shocks, and certainty of supply", in *Journal of International Money and Finance*, Vol. 97, 2019, 86–92.

Since its appearance, however, myriads of new models (commonly referred to as "altcoins") have been presented, attempting to improve Bitcoin's technology and to address different needs by presenting different solutions in their structure to enhance some technical features. For instance, Bitcoin has frequently been described as a near-instantaneous system to transfer value, operating 24/7. Still, the structure of Bitcoin blockchain does not allow to process approximately more than seven transactions per second (while Visa can perform up to 24, 000 transactions per second) and, as the number of Bitcoin users has grown, the speed of transactions has considerably decreased[356]. For this reason, over the years multiple Altcoins have been developed in order to offer quicker transactions, such as Litecoin (LTC)[357], DogeCoin (DOGE)[358] and Bitcoin Cash (BCH)[359].

Similarly, other Altcoins have been created to enhance the level of anonymity, also known as privacy coins. For instance, Dash, a Bitcoin spin-off launched in 2014 and formerly known as Dark Coin, has implemented the Bitcoin code with the addition of master nodes which perform mixing activities, thus making it more difficult to trace the amounts transferred and the users involved in the transaction[360]. Later, privacy coins emancipated from Bitcoin's protocol and developed specific protocols capable of ensuring a higher level of anonymity through encryption: this is the case of ZCash (ZEC) and ZCoin (now renamed FIRO),which rely on the Zero Knowledge Proof (ZKP) protocol[361] and Monero (XMR), which is based on CryptoNote protocol, that allows to obfuscate both the addresses and the amount of the transactions[362].

Besides, innovations have not only concerned the improvement of some features of Bitcoin and Bitcoin's blockchain, as some new systems parted ways from Bitcoin's

---

[356] Study on "Virtual Currencies and Terrorism Financing: assessing the risks and evaluating the responses", European Parliament, 2018, 15.

[357] Launched in 2011 by Charles Lee, Litecoin has a fixed cap of 84 million coins and it is capable of verifying the nodes more rapidly than Bitcoin.

[358] Launched in 2013 by Billy Markus, Dogecoin was created for payment purposes like Bitcoin, but unlike Bitcoin (and Litecoin) it does not have a fixed cap.

[359] Launched in 2017, Bitcoin Cash is a hard fork of Bitcoin that allows to process over 100 transactions per second.

[360] N. ATTICO, *Ibid*., 66-67.

[361] N. ATTICO, *Ibid*., 68. In 2020, ZCoin was rebranded as FIRO.

[362] Launched in 2017, Monero is one of the most popular privacy coins.

philosophy, offering virtual assets operating on public *permissioned* blockchain, such as Ripple (XRP)[363] or have expanded the range of services offered, such as Ether – currently the second most popular virtual asset[364] - which is based on the Ethereum blockchain, created to expand its functions beyond the transfer of value, including the development of decentralised applications (*dapps*) and smart contracts and based on a less energy-consuming algorithm for the verification of the transactions, namely the *proof of stake*[365], in this way joining the altcoins Cardano (ADA) and Solana (SOL)[366].

5.3 The growing phenomenon of Stablecoins and Global Stablecoins

As abovementioned, one of the main features of Bitcoin (and shared also by the others unbacked altcoins), is their unpredictable volatility, and, if on the one hand this trait could represent an attractive opportunity for those who are interested in exploiting market instability to carry out profitable speculations, on the other hand others may be reluctant to take such high risks.

Backed by physical or financial assets, including one or multiple *fiat* currencies or other virtual assets (*collateralised Stablecoins*), or using algorithms to regulate their supply according to changes in demand (*algorithmic Stablecoins*), Stablecoins aim exactly at overcoming this problem and ensure price stability[367], thus making them

[363] Founded in 2012 by Chris Larsen and Jed McCaleb, has a market capitalisation of about 16 billion EUR.

[364] Launched in 2015, Ether market capitalisation accounts around 145 billion EUR – which is nonetheless way behind Bitcoin, set around 300 billion EUR.

[365] The transition was completed on 15 September 2022.

[366] Developed by Charles Hoskinson and launched in 2017, Cardano has a market capitalisation of about 8 billion EUR. Solana was launched in 2020 as an alternative to Ethereum, and has a market capitalisation of more than 4 billion EUR.

[367] Although in public discussion the term "collateralised Stablecoins" is used in a broad, comprehensive manner, it refers to three different types of Stablecoins: i. tokenised funds, which are backed by funds or close substitutes (e.g. fiat-backed Stablecoins); ii. off-chain collateralised stablecoin, backed by assets held by an accountable entity; iii. on-chain collateralised stablecoins, backed by virtual assets held on the blockchain. For a deeper analysis: D. BULLMANN, J. KLEMM, A.

suitable to be used for digital cross-border payments and e-commerce purposes, and eventually function as a store of value[368]. While still representing a small part of the virtual assets market, Stablecoins – which can be both centralised or decentralised – are considerably growing[369], especially the "collateralised" ones, with Tether (USDT), USD Coin (USDC) and Binance USD (BUSD)[370] representing about the 90% of the total Stablecoin market. In fact, the largest Stablecoins appear to have achieved a critical role in the virtual assets' ecosystem, as they appear to be frequently used as liquidity providers in decentralised finance and in virtual assets trading operations, where they operate as a connection between *fiat* currencies and virtual assets[371].

Nevertheless, despite their alleged price stability, Stablecoins have shown some fluctuations – although being considerably lower than the ones showed by unbacked virtual assets[372] - and their suitability as means of payment has been questioned on the basis of their limited adoption in this sense and the general low speed of transactions[373]. Moreover, given the growing interconnection with the financial system, it has been pointed out that Stablecoins, just as unbacked virtual assets, could eventually pose financial stability, monetary policy transmission and

---

PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", European Central Bank – Occasional Papers Series, 2019, No. 230, 1-55.

368 "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements. Final Report and High-Level Recommendations", FSB, 13 October 2020;

369 M. ADACHI, P. BENTO PEREIRA DA SILVA, A. BORN, M. CAPPUCCIO, S. CZÁK-LUDWIG, I. GSCHOSSMANN, G. PAULA, A. PELLICANI, S. PHILIPPS, M. PLOOIJ, I. ROSSTEUSCHER, P. ZEOLI: "Stablecoins' role in crypto and beyond: functions, risks and policy", Macroprudential Bulletin, European Central Bank, Vol. 18, 2022, 1: "*although Stablecoins' market capitalisations increased from 23 billion euros in early 2021 to almost 150 billion in the first quater of 2022, they still only represent less than 10% of the total virtual asset market*

370 All pegged to the U.S. dollar with 1:1 ratio, Tether (launched in 2014) is currently the third largest virtual asset – after Bitcoin and Ether – with a market capitalisation of almost 63 billion EUR, followed by USD Coin with almost 42 billion EUR and Binance USD, with slightly less than 16 billion EUR.

371 M. ADACHI ET AL., *Ibid.*, 2.

372 D. ARNER, R. AUER, J. FROST, "Stablecoins: Risks, Potential and Regulation", BIS Working Papers, No. 905, Bank for International Settlements, November 2020, 7-8.

373 In this sense: M. ADACHI ET AL., *Ibid.*, 4.

money sovereignty risks[374]. This is even more true in case of the rise of the so-called Global Stablecoins, that is to say Stablecoins "*with a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume*"[375], capable of influencing the international market trends.

Nonetheless, the higher level of stability granted by Stablecoins could represent an attractive opportunity for terrorists, persuading also risk-averse subjects to join the world of virtual assets.

5.4 Monetary Central Authorities' response: the rise of Central Bank Digital Currencies

In response to the increasing appeal of virtual assets and to the growth of e-commerce and online transactions, countries are considering – and some of them are already implementing – the adoption of a digital version of *fiat* money, commonly referred to as Central Bank Digital Currency (CBDC)[376]. These new forms of fiat money could be used as: i. digital central bank tokens for financial institutions purposes, ii. accounts at the central bank, and iii. digital cash for retail payments[377]. Indeed, the latter function appears to be the main one that pushed China to take the first steps towards this direction[378], as already in 2017 announced the development

[374] CRYPTO-ASSETS TASK FORCE, "Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area", European Central Bank – Occasional Paper Series No. 247, September 2020.

[375] "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements. Final Report and High-Level Recommendations", FSB, 13 October 2020.

[376] For a deeper analysis: T. MANCINI GRIFFOLI, M. S. MARTINEZ PERIA, I. AGUR, A. ARI, J. KIFF, A. POPESCU, C. ROCHON, "Casting light on Central Bank Digital Currency", IMF, 2018. In particular, it is interesting to remark that the Authors suggest that "*CBDC seems to be natural next step in the evolution of official coinage (from metal-based money, to metal-backed banknotes, to physical fiat money*" (6).

[377] Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, FATF, June 2020, 26.

[378] The People's Bank of China (PBoC) has clarified that the e-CNY is fiat currency issued by the central bank, which relies on a centralised management model and a two-tier operational system and whose aim is to replace cash and to coexist with physical Renminbi, serving mainly for domestic

of the e-CNY[379] and, after testing it in selected areas, launched it during the Beijing Olympics Games in February 2022. But China is not the only country which is investing in the implementation of CBDC: at the moment, ten countries have already launched their CBDC, while 87 countries are considering their possible adoption[380]. Among them, we find the U.S. government, which has made public its intention to explore the possible adoption of a digital dollar[381]. Besides, also the European Union is considering the implementation of the digital euro: in October 2021 the Eurosystem opened the investigation phase for the possible introduction of electronic money issued by the central bank[382].

Since CBDC are *fiat* money, they do not fall under the umbrella of virtual currencies, and the FATF itself has stated that CBDCs are covered by the Recommendations applicable to cash or electronic payments[383]. However, some open questions remain, such as the protection of privacy and anonymity – at the moment guaranteed only via cash payments.

5.5 Virtual Assets and Terrorism Financing: the possible vulnerabilities

After having outlined the state of art of the evolution of virtual assets, we can try to assess which of their characteristics could pose new issues – or exacerbate some of

retail payment purposes: "Progress of Research & Development Development of E-CNY in China", People's Bank of China, July 2021.

379 Also known as digital yuan, e-Renminbi (e-RMB) or Digital Currency/Electronic Payments (DCEP) initiative.

380 According to the Atlantic Council, 105 countries – representing over 95% of global GDP – are exploring a CBDC, including nineteen of the G20 countries. At the moment, ten countries have fully implemented CBDCs, namely Nigeria, the Bahamas, the Eastern Caribbean Union (Antigua and Barbuda, Dominica, Grenada, Montserrat, St. Kitts and Nevis, Saint Lucia, and St. Vincent and the Grenadines) and Jamaica. See also: A. KOSSE, I. MATTEI, "Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies", in *BIS Papers*, May 2022, 1-23.

381 Executive Order 14067 on Ensuring Responsible Development of Digital Assets, 9 March 2022. At the moment, the MIT Digital Currency Initiative and the Federal Reserve Bank of Boston are working on the implementation of a digital U.S. dollar with Project Hamilton.

382 F. PANETTA, "The present and future of money in the digital age", European Central Bank, 10 December 2021.

383 Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, FATF, June 2020.

the already known difficulties in tackling terrorism financing. Notably, particular concerns surround the possible higher levels of anonymity offered by these new technologies, their global reach, the absence of a central authority in charge of their regulation and the presence of – sometimes substantial – differences regulation choices across jurisdictions.

5.5.1 (*pseudo*)Anonymity

One of the main concerns about virtual assets is represented by the fact that they would ensure a higher level of anonymity, in this way obfuscating the trail of the transactions carried out. However, what these new technologies actually offer is not the anonymity of the transactions *per se*, since the registers keeping the records of the transactions are public – so everyone can trace the transactions – and they are permanent, so they cannot be modified. Instead, what they ensure would be better described as pseudo-anonymity, as the identity behind the transactions can be more easily disguised compared to the regulated financial system[384].

Nevertheless, some mechanisms have been developed in order to enhance the level of anonymity by trying to hide the origin of the funds transferred and to hide the record of the transactions. This is the function of ring signatures, a tool that allows the obfuscation of the originator of a transfer by requiring multiple signature of randomly chosen virtual assets users, and of mixers and tumblers, which obfuscate the history of transactions by, indeed, mixing virtual assets of different users through a centralised system, such as Blender.io, or through a peer-to-peer

[384]Study on "Virtual Currencies and Terrorism financing: assessing the risks and evaluating responses", European Parliament, 2018, 30: "*Media reports frequently describe Bitcoin as 'anonymous' and 'untraceable' but this is oversimplified and inaccurate. Bitcoin is more appropriately described as 'pseudonymous': Bitcoin users are represented on the blockchain with alphanumeric addresses associated with their Bitcoin wallet. Whilst a user's actual identity is not visible on the blockchain, information about their transactions – such as dates, values, and the Bitcoin addresses of counterparties – are all recorded publicly. Furthermore, because the blockchain is a chronological record of transactions, it is possible to derive a reliable picture of the movement of Bitcoin*".

decentralised system, by using particular protocols, such as CoinJoin[385]. As it can be easily guessed, decentralised mixers could pose bigger concerns in terms of possible criminal exploitation, as they are more difficult to regulate, while centralised mixers can be more easily reached by authorities[386]. Besides, terrorists seem to have already acknowledged – at least theoretically – the possible benefits of mixing in order to hide the movement of funds[387] and evidences show that criminals are increasingly using these services[388].

Another way to achieve a higher level of anonymity is to use those altcoins which have been created exactly with the purpose of enhancing the level of anonymity granted through encryption and the use of obfuscated public ledgers – privacy coins (*supra* § 5.2.3). Reports show that privacy coins are particularly attractive for criminal purposes[389], and terrorists affiliated with ISIL and racially or ethnically motivated extremists have already been reported to use privacy coins to conceal their identities while conducting financial activities[390].

Besides the implementation of mixing technologies or privacy coins, an additional layer of anonymity can be achieved through the Dark Web, which can be accessed

---

[385] For example, Wasabi Wallet and Samourai-Whirlpool Wallet rely on CoinJoin protocol to ensure users' privacy.

[386] Recently the U.S. government sanctioned Blender.io for having laundered the equivalent of 20.5 U.S. dollars from North Korea "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats", U.S. Department of the Treasury – Press Release, 6 May 2022.

[387] Already in July 2014, ISIL supporters have been reported to promote the use of mixing technology to hide the movement of funds, notably via a blog post entitled "'Bitcoin and the Charity of Violent Struggle' which suggested to resort to services such as DarkWallet (an early attempt to improve the anonymity of transactions which has been later shut down in 2020): S. HIGGINS, "ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide", CoinDesk, 7 July 2014.

[388] Europol has recently underlined that privacy coins are becoming more and more popular, especially in the Dark Web: Internet Organised Crime Threat Assessment (IOCTA), EUROPOL, 2021.

[389] Already in 2018, the European Parliament reported that criminals were using privacy coins, especially crypto-jacking and ransomware attacks. For example, in 2017 the perpetrators of the famous WannaCry ransomware attack exchanged their Bitcoin for Monero through the Swiss exchange ShapeShift: Study on "Virtual Currencies: assessing the risks and evaluating the responses", European Parliament, 2018. More recently, Europol has underlined that privacy coins are becoming more and more popular, especially in the Dark Web: Internet Organised Crime Threat Assessment (IOCTA), EUROPOL, 2021, 9.

[390] S. DOBITSCH, "Terrorism and Digital Financing: how Technology is Changing the Threat", Statement at the U.S. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security, 22 July 2021, 8.

only through specific tools and uses technologies such as TOR protocol to hide IP addresses and to ensure the encryption of communication[391], thus representing an attractive opportunity for criminal activities: reports, indeed, show that some Dark Web marketplaces accept altcoins, including Monero[392], and terrorist already use Darknet platforms for propaganda and recruiting purposes, as well as trafficking illicit goods[393].

5.5.2 Transnationality

Another feature of virtual assets that could result attractive for criminal purposes, and, of course for terrorism financing, is their suitability for transnational transactions. In fact, as already underlined (*supra* § 1), while a region that present a high rate of terrorist activity is more likely to present a high risk of terrorism financing flows, this is not necessarily true as financing activities can take place all over the world. Therefore, terrorist could be attracted to virtual assets to carry out transactions across boarders avoiding the regulated financial system and the physical transportation of cash[394].

5.5.3 Decentralisation

Following Bitcoin's philosophy, many of the most common virtual assets rely on decentralised, permissionless systems, which enable anyone to access the network

[391] We remind that the Dark Web a subset of the Deep Web. The contents on Deep Web are simply not indexed by standard web search-engines, while the contents on the Dark Web can only be accessed through specific software or authorisations.
[392] Spotlight on "Cryptocurrencies: tracing the evolution of criminal finances", EUROPOL, 26 January 2022, 27. In this regard, we remind here the Alphabay case, a Darkweb marketplace that accepted Monero for the purchase of illicit goods and services shut down in 2017: "AlphaBay, the Largest Online 'Dark Market,' Shut Down", U.S. Department of Justice – Press Release, 20 July 2017.
[393] For a deeper analysis: N. MALIK, "Terror in the Dark: How terrorists use encryption, the Darknet and cryptocurrencies", The Henry Jackson Society, 2018.
[394] Study on "Virtual Currencies: assessing the risks and evaluating the responses", European Parliament 2018, 38.

without any kind of authorisation. This feature, of course, could be particularly attractive to terrorism financiers, since adopting effective measures – and especially enforce them – appears to be more challenging. However, it has been noticed that virtual assets ecosystem actually hosts several centralised intermediaries[395], such as exchanges platforms, which allow users to convert fiat money to virtual assets and vice versa and also to exchange different kinds of virtual assets[396], custodial wallet providers and some mixers as well (*supra* § 5.5.1). These services could represent chokepoints in the virtual asset ecosystem for law enforcement and AML/CTF measures, as they could be identified and stopped more easily; for instance, the U.S. government recently issued sanctions against SUEX, a centralised virtual currency exchange for facilitating ransomware payments and illicit financial operations[397].
Nonetheless, users can store and manage their Virtual Assets through unhosted wallets, and new solutions that enable users to convert their virtual assets without passing by centralised exchanges are under development. This is the case of decentralised exchange platforms (DEXs), which allow direct peer-to-peer exchanges without the need to rely on third parties' custody or funds, such as IDEX, Bitsquare, OpenLedger, CryptoBridge and Bitshares, and "atomic swaps" (or "atomic cross-chain trading"), which allow to convert virtual assets that work on

[395] Study on "Virtual Currencies: assessing the risks and evaluating the responses", European Parliament 2018, 40.
[396] Founded in 2010 by Jade McCaleb, Mt.Gox was the first virtual asset exchange, but stopped its activity in 2014. Currently, among the most used exchanges we find: Coinbase, Binance, Kraken, Bitpanda, Bitstamp, Bitfinex.
[397] "Treasury Takes Robust Action to counter Ransomware", U.S. Department of the Treasury – Press Release, 21 September 2021. Less than two months later, the exchange Chatex has been designated pursuant to Executive Order 13694, for providing material support to SUEX, together with IZIBITS OU, Chatextech SIA, and Hightrade Finance Ltd, linked to Chatex: U.S. Department of Treasury: "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange", U.S Department of the Treasury, 8 November 2021, We remind here that the Executive Order (E.O.) 13694 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" was signed on 1 April 2015 by U.S. President Barack Obama with the aim of combatting criminal cyber activities through the through the creation of a specific Specially Designated Nationals and Blocked Persons List (SDN List) and sanctions.

different blockchains[398]. Therefore, attention must be paid to the threats of decentralisation also in relation to terrorism financing risks [399].

5.5.4 Different regulation across countries

The development of virtual assets has provoked different reactions across the world. While at the beginning many jurisdictions hesitated to regulate the phenomenon, in recent years more and more countries have extended AML/CTF regulations to virtual assets and have implemented specific measures, yet the approaches greatly vary. China, for example, started to concretely impose restrictions on virtual asset activities with the ban of Initial Coin Offerings (*infra* §6) in September 2017[400], followed in April 2019 by the official disapproval of mining activities, ultimately resulted in the total ban of both mining and trading virtual assets in September 2021[401]. Besides, Russia is moving in an erratic way, often changing its position on the use of virtual assets and at the same time working on the launch of its own CBDC, the Digital Ruble[402].

On a different note, other countries tried to implement these new technologies, trying to develop their own national virtual asset, such as Venezuela's Petro, or directly giving the status of legal tender to a chosen virtual asset, thus requiring businesses to accept it as mean of payment. This is the case of El Salvador, which, after having passed the so-called Bitcoin Law in September 2021, has been the first

---

[398] Study on "Virtual Currencies: assessing the threat and evaluating the responses", European Parliament, 2018, 41.

[399] In this sense: J. EISERT, "Terrorism and Digital Financing: how Technology is Changing the Threat", Statement at the U.S. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security, 22 July 2021, 14.

[400] Announcement on Preventing Financial Risks from Initial Coin Offerings, 4 September 2017. As early as in 2013, the Chinese Government had issued a statement forbidding banks to involve in virtual assets activities, but this did not deter the private sector to show a significant interest.

[401] "Circular on Further Preventing and Disposing of Speculative Risks in Virtual Currency Trading", People's Bank of China, 15 September, 2021. Others jurisdictions that have explicitly banned virtual assets activities are: Algeria, Bangladesh, Egypt, Iraq, Morocco, Nepal, Qatar and Tunisia:, "Regulation of Cryptocurrency Around the World: November 2021 Update", U.S. Library of the Congress, November 2021.

[402] "A Digital Ruble", Consultation Paper, Bank of Russia October 2020.

country in the world to accept Bitcoin as legal tender. Although this decision has been widely criticised at the international level[403], El Salvador President Nayib Bukele not only did not step back, but kept encouraging other countries to follow this path, and in April 2022 the Central African Republic followed his example, provoking similar worried reactions[404].

Such variegated approaches constitute a concrete challenge for building an effective international cooperation on the matter, pushing criminal actors – including terrorism financiers – to operate in countries with no or loose regulation. This is particularly concerning, given the fact that some of these countries present a high risk of terrorist activities, such as Indonesia and the Philippines (*supra* § 1.3)[405].

6. Using Virtual Assets to raise funds

Although evidences of the use of virtual assets for financing terrorism purposes are still little, their peculiar features are increasingly being appreciated, in particular for donations and fundraising purposes[406].

Looking at jihadist terrorism, the first cases of collecting funds through virtual assets date back to 2012, when on the Dark Web appeared a website called "*Fund*

---

[403] In January 2022 the International Monetary Fund urged El Salvador to remove Bitcoin's legal status, worried by the risks associated to financial stability, financial integrity, consumer protection and fiscal liabilities: "IMF Executive Board Concludes 2021 Article IV Consultation with El Salvador", Press Release, No. 22/13, International Monetary Fund, 25 January 2022,

[404] Criticisms have been raised both by the International Monetary Fund and by the Bank of Central African States (BEAC), the latter declaring the adoption of Bitcoin as legal tender invalid, and on 26 July 2022 the Central African Republic froze the application of its law adopting bitcoin as an official currency: S. KEDEM, "Central African Republic freezes the adoption of Bitcoin", African Business, 26 July 20022. Nonetheless, the efforts the government in this direction have not stopped, and in July 2022 President Faustin Archange Touadéra announced the launch of Sango Coin, a new national virtual asset: R. SAVAGE, "Central African Republic launches 'Sango Coin' cryptocurrency amid industry rout", Reuters, 15 July 2022.

[405] A. MUZTABA HASSAN, S. NAWED NAFEES, "Cryptocurrency and Terrorist Financing in Asia", The Diplomat, 4 February 2022.

[406] S. DOBITSCH, "Terrorism and Digital Financing: how Technology is Changing the Threat", Statement at the U.S. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security, 22 July 2021, 4. In the same sense: EU Terrorism Situation & Trend Report (TESAT), EUROPOL, 14 July 2022.

The Islamic State Without Leaving a Trace" inviting to financially support the ISIL through Bitcoin donations. Even if it only managed to raise five Bitcoins (about $10, according to the Bitcoin rate at the time)[407], other attempts followed, both in the form of campaigns, such as the "Jahezona" campaign organised on Twitter by the Ibn Taymiyya Media Center (ITMC)[408], which managed to collect around 0.929 Bitcoin (about 677 U.S. dollars at the time)[409] or initiatives carried out by single individuals. This is the case, for example, of the young U.S. teenager Ali Shukri Amin, which published a link on his Twitter account (@Amreekiwitness) to a document he had written entitled "*Bitcoin wa' Sadaqat al-Jihad*" (Bitcoin and the Charity of Jihad), where he explained how to use Bitcoin and how jihadists could use them to fund themselves[410]. Besides, in recent years fundraising activities through virtual assets appear to be more sophisticated, such as the campaign set up by the al-Qaeda linked al-Sadaqah Organisation in order to build facilities in Syria, in Latakia province: initially accepting only Bitcoin, the organisers then expanded to other virtual assets, including Monero and Dash[411]. Moreover, in 2019 the U.S government dismantled a structured network spread across the United States, Canada, Russia, Germany and Saudi Arabia linked to Al-Qassam Brigades (Hamas's militant wing) that used Bitcoin to receive donations for a fundraising campaign[412].

---

[407] E. AZANI, N. LIV, "Jihadists' Use of Virtual Currency", International Institute for Counter-Terrorism (ICT), 20 June 2018.

[408] ITMC is the media wing of the Mujahideen Shura Council in the Environs of Jerusalem (MSC), composed by Salafi-jihadist groups based in Gaza and it supports the Islamic State.

[409] N. LIV, "Jihadists' Use of Virtual Currency 2", International Institute for Counter-Terrorism (ICT), 18 January 2018, 2.

[410] Amin has been sentenced in 2015 for conspiring to provide material support and resources to the Islamic State of Iraq and the Levant (ISIL) and for helping ISIL supporters to travel to Syria:, "Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL", U.S. Department of Justice – Press Release, 28 August 2015.

[411] It is interesting to notice that in this case terrorism financing activities have profited from Bitcoin's volatility, as on 30 November 2017 they received 0.075 Bitcoins worth 685 U.S. dollars, worth the next day 803 U.S. dollars: Study on "Virtual Currencies: assessing the risks and evaluating the responses", European Parliament, 2018, 34.

[412] J. EISERT, "Terrorism and Digital Financing: how Technology is Changing the Threat", Statement at the U.S. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security, 22 July 2021, 15.

Furthermore, also right-wing extremist groups have been reported to raise funds through virtual assets, especially through donations and the purchase of their merchandise[413]. For example, this is the case of the Nordisk Styrke group, which only display virtual assets addresses on its donations page[414], and one South African far-right organisation has even been reported to have created its own Stablecoin to receive funds across the world, while the Christchurch attacker (*supra* §1.4) resulted to have carried out several donations to extreme right-wing organisations overseas[415].

Besides fundraising and donations activities, another means to collect funds through Virtual Assets is offered by Initial Coin Offerings (ICOs), which can be described as the equivalent of the Initial Public Offerings (IPOs): selling tokens issued on the blockchain for various rights in exchange, they are frequently used by start-ups to raise funds, and terrorists could possibly try to exploit them, either openly or fraudulently.

7. Using Virtual Assets to move funds

Virtual assets can be also an effective tool when it comes to move funds. For instance, in 2017 it has been reported that Bahrun Naim, a jihadist involved in the 2016 attacks in Jakarta, used PayPal and Bitcoin to move funds from the Middle-East to the terrorist cells based in Java[416], and, in the same year, the U.S. citizen Zoobia Shahnaz committed several frauds to financial institutions in order to collect money for ISIL supporters (including using some fraudulently obtained credit

[413] For a deeper analysis: D. GARTENSTEIN-ROSS, V. KODUVAYUR, S. HODGSON, "Crypto-Fascists. Cryptocurrency Usage by Domestic Extremists", Foundation for Defense and Democracy, March 2022.

[414] Report on "Ethnic or Racially Motivated Terrorism", FATF, June 2021, 12.

[415] Report on "Ethnic or Racially Motivated Terrorism", *Ibid*., 25.

[416] Study on "Virtual Assets: assessing the risks and evaluating the responses", *Ibid*., 38.

cards), and then laundered them buying about 62,000 U.S. dollars in Bitcoin and other virtual assets[417].

In addition, it has been pointed out that also domestic extremists are turning to virtual currencies (including privacy coins) to transfer funds, since extreme right-wing platforms have been started to be blocked by social media networks and by linked methods of payment[418].

While the transfer of funds via virtual assets could be convenient, difficulties could arise in those areas where the access to these tools is limited. For instance, virtual assets' ATMs are mostly located in North America (which accounts for the 95% of ATMs locations), whereas in Asia, Africa and Middle-East – which are the areas most at risks when it comes to terrorism – have access to a very limited number of ATMs[419], in this way making it difficult also for terrorists and terrorist organisation to effectively profit from virtual assets for financing purposes.

[417] Shahnaz then transferred more than $150,000 to individuals and entities in Pakistan, China and Turkey that were connected with ISIS. In March 2020 she has been sentenced to 13 years in prison for providing material support to ISIS: "Long Island Woman Sentenced to 13 Years' Imprisonment for Providing Material Support to ISIS", U.S. Department of Justice – Press Release, 13 March 2020.

[418] Report on "Ethnically or Racially Motivated Terrorism Financing", *Ibid.*, 25.

[419] Asia and Africa have respectively the 0.2% and 0.1% of ATMs available across the world: Crypto ATM Distribution by Continents and Countries – Coin ATM Radar.

CHAPTER III

VIRTUAL ASSETS, TERRORISM FINANCING AND THE INTERNATIONAL REGULATORY ARCHITECTURE: AN ASSESSMENT

SUMMARY: 1. The international AML/CFT architecture: the FATF as global trend-setter 2. First reactions on the possible impact of Virtual Assets on the international regulatory framework 2.1 The integration of Virtual Assets among the FATF Standards 2.2 The application of the risk-based approach in the Virtual Assets ecosystem 2.2.1 Tackling Virtual Assets' (*pseudo*)anonymity 2.2.2 Responding to Virtual Assets' transnationality 2.2.3 The challenge of addressing decentralisation issues 2.2.4. The need of international cooperation to address regulatory gaps 2.3 The effectiveness of the FATF approach: first outcomes 3. The contribution of the other international standard-setting bodies 3.1 The International Monetary Fund 3.2 The World Bank 3.3 The Basel Committee on Banking Supervision 3.4 The International Organisation of Securities Commissions 3.5 The Financial Stability Board 4. Virtual assets' regulation at the regional level: the European Union approach 4.1 The Fifth Anti-Money Laundering Directive 4.2 The new proposals to boost the UE action on the regulatory side: 4.2.1 From "virtual currencies" to "crypto-assets": the choice made with the proposed MiCA Regulation 4.2.2 The proposed new EU AML/CFT framework: the impact on Virtual Assets regulation 4.2.3. The EU implementation of the FATF "Travel Rule" to Virtual Assets 5. The Italian AML/CFT regulatory framework on Virtual Assets

1. The international AML/CFT architecture: the FATF as global standard-setter

As outlined in Chapter I, the criminalisation of terrorism financing as it is nowadays shaped is the result of a long and articulated process, which has involved multiple actors at different levels. Therefore, it is no surprise that a similar multi-nodal scheme can be appreciated when looking at the development of regulatory anti-money laundering and counter terrorism financing measures, whose articulated framework relies on the work of the FATF: benefitting from the perception of illicit

finance as a major security threat, indeed, the FATF managed to establish transnational spaces of monitoring, surveillance and enforcement[420].

The core of the AML/CFT framework is represented by the FATF Recommendations, which constitute one of the most famous examples of soft law – or, more precisely, of *hard* soft law[421]. Indeed, on the one hand they are not legally binding, representing a mere political commitment[422]; on the other hand, thanks to an effective peer pressure system consisting in self-assessments, mutual evaluations and listing procedures in case of non-compliance (i.e., "naming and shaming" practice)[423], they have acquired a prescriptive dimension, and are applied automatically by members with barely no scrutiny. In this way, despite the concerns raised in terms of lack of transparency, accountability and democracy of its processes[424], the FATF succeeded in creating an effective harmonisation,

---

[420] In this sense, the FATF could be held as an example of "*multimodal security governance*": A. P. JAKOBI, "Governing illicit finance in transnational security spaces: the FATF and anti-money laundering," in *Crime, Law and Social Change*, Vol. 69 (2), 2018, 185.

[421] In general, there is evidence of soft law emerging as a possibly more powerful form of regulation then the traditional international law making: A. SLAUGHTER, "Sovereignty and power in networked world order", in *Stanford Journal of International Law*, Vol. 40 (2), 2004, 298. This is particularly true in the field of financial regulation, as soft law would offer rapid responses in case of crises and would overcome the lengthy process typical of traditional hard law instruments: N. W. TURNER, "The financial action task force: international regulatory convergence through soft law" in *New York Law School Law Review*, Vol. 59 (3), 2014, 549.

[422] J. WESSEL, "The Financial Action Task Force: study in balancing sovereignty with equality in global administrative law", in *Widener Law Review*, Vol. 13 (1),2006, 173.

[423] According to the level of non-compliance, jurisdictions can fall under "Increased Monitoring" list (i.e. "grey list"), which does not require enhanced due diligence measures, or "high-risk jurisdictions" list (i.e. "black list"), which urges for enhanced due diligence, and, in the most serious cases, to apply counter-measures to protect the international financial system. It is interesting to underline the a strict relationship between non-compliant lists and market behaviour has been observed: since engaging with non-compliant jurisdictions require additional scrutiny (i.e., additional costs and risks), the market pushes jurisdictions to be compliant, while at the same time listing procedures stigmatise them, thus underpinning this effect; hence, being listed should incentivise compliance: J. C. MORSE, "Blacklists, market enforcement, and the global regime to combat terrorist financing", in *International Organization*, Vol. 73 (3), 2019, 511-546.

[424] For a comprehensive analysis: S. GHOSHRAY, "Compliance Convergence in FATF Rulemaking: The Conflict between Agency Capture and Soft Law," in *New York Law School Law Review,* Vol. 59 (3), 2014-2015, 521-546. Among the remarks made, the Author points out that the FATF would display an "hegemonic subservience" of developing and underdeveloped jurisdictions to Western countries. On this point, another Author underlines that "*it is arguable that the FATF, like the World Bank and IMF, has become an instrument* of *Western States to manage and control a vast array of economic and social realities in the overwhelming majority of developing countries, which exercise little or no power over the agenda of these institutions*": J. GATHII, "The Financial Action Task Force and Global Administrative Law", in

enforcement and information network to promote compliance convergence[425] across the globe[426].

Besides, it is important to underline that this result has been achieved thanks to the support of other powerful international actors, such as the United Nations and the European Union, and of other relevant standard-setting bodies, such as the International Monetary Fund, the World Bank (which both are also FATF's observers), as well as the Basel Committee on Banking Supervision, the Financial Stability Board, and International Organisation for Securities Commission; all of them have endorsed the work of the FATF and significantly contributed to the spread and application of its Standard well beyond the FATF membership.

Before comprehensively analyse the regulatory approach to the World of Virtual Assets and its possible development resulting from the interaction of these different global standard-setting bodies, it is interesting to remark that, similarly to what we have seen in relation to the criminalisation of terrorism financing[427], also with regard to the development of the AML/CFT regulatory framework we can see the abandon of traditional international instruments (e.g. treaties) in favour of other quicker solutions – which in the AML/CFT field are represented by the adoption of

---

Journal of the Professional Lawyer, 2010, p. 202. In this context, it has been underlined the influence of the U.S., especially at FATF's early stages: N. W. TURNER, "The financial action task force: international regulatory convergence through soft law" in *New York Law School Law Review*, Vol. 59 (3), 2014, 557. Besides, similar criticisms revolves all around the War on Terrorism approach: *supra* Chapter I.

[425] J. WESSEL, "The Financial Action Task Force: study in balancing sovereignty with equality in global administrative law", in *Widener Law Review*, Vol. 13 (1),2006, 171-173. For an analysis of the FATF's government through the form of best practices, and promotion of learning and accepted benchmarks: Y. HENG, K. MCDONAGH, "The Other War on Terror Revealed: Global Governmentality and the Financial Action Task Force's Campaign against Terrorist Financing", in *Review of International Studies*, Vol. 34 (3), 2008, 553- 573.

[426] In this sense, the FATF can be rightly described as "a body with selective membership but with global reach": V. MITSILEGAS, "Transnational Criminal Law and the Global Rule of Law", in *The Global Community: Yearbook of the International Law and Jurisprudence 2016*, Oxford University Press, 2017, 61

[427] *Supra* Chapter I; we specifically refer to the central role played by the Security Council Resolutions, which seems to have replaced the traditional means of Conventions.

standards developed by highly specialised civil servants through procedure involving multiple stakeholders, including the private sector[428].

2. FATF's first reactions on the possible impact of Virtual Assets on the international regulatory framework

If at the beginning the world looked at virtual assets with scepticism and their impact to everyday life was far to be significant, public interest quickly increased, along with a certain degree of confusion about the real understanding of the functioning of these new tools and the threats that they could pose. For this reason, in 2014 the FATF issued some initial considerations on what it called at the time "virtual currencies", intended to serve as a general guide for both countries and the private sector to identify and manage these new tools by providing some key definitions and technical clarifications[429]. Interestingly, we can see that at this initial stage the choice of the term "virtual currencies" reflected a particular concern on their possible role as new kind of money, as the definition contextually provided identified them as "*a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value*", which *"does not have legal tender status"*, and it is *"not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of*

[428] Therefore, States are no longer the sole rule-makers in international law: J. GATHII, "The Financial Action Task Force and Global Administrative Law", in *Journal of the Professional Lawyer*, 2010, 201. However, it has been insightfully remarked that this does not mean that States now play a minor role; on the contrary, the power of States is expanding. In this sense: A. SLAUGHTER, *Ibid*.,, 327: " *in a world in which sovereignty means the capacity to participate in cooperative regimes in the collective interest of all states, expanding the formal capacity of different state institutions to interact with their counterparts around the world means expanding state power*". See, also: S. CASSESE, "Global Administrative Law: The State of the Art,", *in International Journal of Constitutional* Law, Vol. 13 (2), 2015, 467: "*states are managers of non-state authority, establish networks with international governmental and non-governmental organizations, and are indispensable instruments of global institutions*". On the phenomenon of Global Administrative Law: B. KINGSBURY, N. KRISCH, R. B. STEWART, "The Emergence of Global Administrative Law", in *Law and Contemporary Problems*, Vol. 68(3& 4), 15-62.

[429] Report on "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", FATF, June 2014.

users of the virtual currency" – and so distinct from fiat currency and e-money[430]. Accordingly, the related Guidance on their potential anti-money laundering and terrorism financing risks, issued shortly after (2015 FATF Guidance)[431], overtly decided to focus only on their possible role for payment purposes and, more generally, reflected a quite narrow approach, which resulted in the choice to address only those "virtual currencies" activities which intersected and provided gateways to and from the regulated fiat currency financial system – namely convertible "virtual currencies" exchangers[432]. Nonetheless, this first Guidance provides some hints for the development of the FATF future approach on the matter: in particular, the Guidance invited members to apply the relevant Recommendations following the risk-based approach set out by Recommendation 1, such as, among others, taking appropriate measures to manage and mitigate these risks before launching new products or developing new technologies, register or licensing legal or natural persons exchanges (Rec. 14), as well as subject them to adequate regulation and supervision and amend legal frameworks where needed (Rec. 26), to apply customer identification and recordkeeping requirements (Rec. 35) and to put efforts in building an efficient and effective international cooperation (Rec. 40), including considering the creation of inter-agency working groups (Rec. 2).

2.1 The integration of Virtual Assets among the FATF Standards

In 2018, the FATF stepped up a gear in the field of virtual assets regulation by officially including them among the FATF Standards. Invited by the G-20 Finance

---

[430] Report on "Virtual Currencies – Key Definitions and Potential AML/CFT Risks, *Ibid*, 4.

[431] "Guidance for a risk-based approach on Virtual Currencies", FATF, June 2015.

[432] 2015 FATF Guidance, 4: "*The Guidance focuses on VCPPS and related AML/CFT issues, and applies to both centralised and decentralised VCPPS. It primarily addresses convertible VC, because of its higher risks. The focus of this Guidance is on convertible virtual currency exchangers which are points of intersection that provide gateways to the regulated financial system (where convertible VC activities intersect with the regulated fiat currency financial system). It does not address non-AML/CFT regulatory matters implicated by VC payment mechanisms (e.g., consumer protection, prudential safety and soundness, tax, anti-fraud issues and network IT security standards). Nor does it address non-payments uses of VC (e.g., store-of-value products for savings or investment purposes, such as derivatives, commodities, and securities products) or the monetary policy dimension of VC activities*".

Ministers and Central Banks Governors to work in this direction[433], indeed, in October the FATF approved the amendment to Recommendation 15, now renamed "Recommendation 15 on New Technologies":

> *"Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.*
> *To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations".*

This amendment marked a new approach, with regard both to the terminology used and to extent of the reach of the FATF.

Recommendation 15, indeed, replaced the term "virtual currencies" in favour of the broader term "Virtual Assets" (VAs), and introduced the new term of "Virtual Assets Service Providers" (VASPs). Both accompanied by two new corresponding definitions added in the Glossary, VAs definition expands on the previous "virtual currencies" definition with the explicit aim to cover all the possible future technological evolutions[434], whereas the one dedicated to virtual assets providers appears to be brand new. In particular, the FATF identifies Virtual Assets Service

---

[433] Communiqué of Finance Ministers and Central Bank Governors, Buenos Aires, 20 March 2018: "*We commit to implement the FATF standards as they apply to crypto-assets, look forward to the FATF review of those standards, and call on the FATF to advance global implementation. We call on international standard-setting bodies (SSBs) to continue their monitoring of crypto-assets and their risks, according to their mandates, and assess multilateral responses as needed*". See, also: Report to G20 Finance Ministers and Central Bank Governors, FATF, July 2018: it is interesting to notice that we can already see a shift in the terms adopted, as the FATF referred to these new technologies by calling them "virtual currencies/crypto-assets", thus somehow preannouncing the shift adopted few months later.

[434] *Supra* Chapter II. For convenience, we report the definition of VA adopted in the FATF Glossary: "*A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations*".

Providers as those legal or natural persons that are not covered elsewhere under the Recommendations and conduct as a business 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. safe keeping 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 a virtual asset. Therefore, it is clear that with Recommendation 15 the FATF extended its reach well beyond the mere Virtual Assets – fiat activities, covering all the possible activities involving Virtual Assets.

Welcomed by the United Nations Security Council[435], the FATF further specified the provisions set out by the new Recommendation 15 by issuing a corresponding Interpretive Note in 2019[436]. Organised in eight paragraphs, the Note first specifies that countries should consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value" (par. 1), in this way achieving a double goal: on the one hand, it reinforces the terminological paradigm shift operated with Recommendation 15 by not including any reference to the function of "currency", on the other hand it covers all the possible different regulations across jurisdictions, thus clarifying that Virtual Assets are subject also to freezing measures and confiscation (Recommendations 6 and 4)[437]. Moreover, coherently with the whole approach of the FATF, it underlines the importance of

[435] S/RES/2462 (2019), Recital No. 21: "(The Security Council) *Welcomes in that regard FATF's ongoing work concerning virtual assets and virtual assets service providers, including its October 2018 amendments to the FATF standards and statement on the Regulation of Virtual Assets, and* encourages *Member States to apply risk-based anti-money laundering and counter-terrorist financing regulations to virtual asset service providers, and to identify effective systems to conduct risk-based monitoring or supervision of virtual asset service providers*".

[436] We note that the Interpretive Note to Recommendation 15 has been further amended in June 2021 in order to clarify that of proliferation financing measures apply to VA activities and VASPs. This amendment follows the one made to Recommendation 1 and its Interpretive Note in October 2020, which included the requirement for countries, FIs and DNFBPs to assess and mitigate proliferation financing (PF) risks as defined under the FATF Standards, and has been accompanied by the release of the "Guidance on Proliferation Financing Risk Assessment and Mitigation", FATF, June 2021.

[437] *Infra* Chapter IV.

implementing a risk-based approach in order to ensure that the relevant measures are proportionate with the risks identified (par. 2), and details how members should apply the provisions set out by the new Recommendation 15. In this respect, a particular emphasis is posed on the registration/licensing requirement: while the Note does not require countries to impose a separate licensing/registration system for those entities which are already registered as financial institution and whose registration/license covers also the performing of VASP activities (par. 4), it urges that specific registration/licence should be imposed on those entities that are not elsewhere regulated. More precisely, the Interpretive Note requires VASPs to be registered/licensed at least in the jurisdiction where they were created or, in the case where the VASP is a natural person, where their place of business is located; nonetheless, the Note precise that jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction and to take necessary measures to prevent criminals to be involved in the VASP sector and identify the entities that carry out VASP activities without being licensed or registered and apply appropriate sanctions (par. 3). Indeed, the Note warns countries to appoint a competent authority – different from a self-regulatory body – to monitor and supervise VASPs activities, providing them with the power to conduct inspections, require information and impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the license/registration (par. 5). In addition, countries should ensure a range of effective, proportionate and dissuasive sanctions – leaving the choice to countries whether they should have criminal, civil or administrative nature – which should be both applicable to VASPs and their directors and senior management in the case that they fail to comply with AML/CFT requirements (par. 6).

In addition, the Note underlines that FATF customer due diligence measures (namely Recommendations 10 to 21) apply to VASPs, although with some adjustments due to their particular nature. For instance, the threshold above which entities involved in Virtual Assets transactions are required to conduct costumer

due diligence is lowered at USD/EUR 1 000[438], and significant emphasis have been put to the application of Recommendation 16, which sets out the so-called "travel rule", by requiring countries to ensure that the originating entities dealing with Virtual Assets obtains and holds accurate information both on the originator and the beneficiary of the transaction, as well as sending those information to the receiving entity and makes it available to competent authorities upon request; likewise, beneficiary entities have similar duties.

Finally, the Note invites countries to rapidly set up a constructive and effective cooperation on the basis of Recommendations 37 to 40, underlining the fact that differences of nomenclature or status of VASPs shall not be an obstacle (par. 8).

2.2 The application of the risk-based approach in the Virtual Assets ecosystem

In the words of the FATF, the risk-based approach allows countries "*to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way*"[439]. Set out by Recommendation 1, this approach informs the whole work of the FATF, and virtual assets are no exception: after the first guidance on the application of the risk-based approach to "virtual currencies" in 2015, following the amendment to Recommendation 15 the FATF issued a new specific guidance on how to apply the risk-based approach to virtual assets and virtual assets providers in 2019, which extended the scope to VAs convertible to

[438] The threshold for occasional transactions carried out by financial institutions is set at USD/EUR 15 000: FATF Recommendation 10, par. 2, ii).

[439] FATF 2012 Recommendations, 8. In this respect, it has been remarked that the risk-based approach has moved part of the responsibility of identifying risks, developing countermeasures and risk managing to the private sector, thus allowing States to pass the costs of implementation and to expand the reach of criminal law: M. PIETH, G. AIOLFI, "Anti-Money Laundering: Levelling the Playing Field", in *Basel Institute on Governance Working Paper Series – Working Paper 1*, 2003, 13-15.

other VAs (2019 FATF Guidance)[440], soon after replaced by its updated version in 2021 (2021 FATF Guidance)[441]. Designed to help both countries and the private sector to identify, assess, and take effective action to mitigate AML/CTF risks posed by virtual assets, the Guidance supports an objective-based implementation of FATF Recommendations according to the needs of each jurisdiction (*functional equivalence and objective-based approach*), encourages flexible requirements that are not based on a specific technology and that can adjust to future developments (*technology neutrality and future-proofing*), and invites countries to treat different kinds of VASPs in the same way from the regulatory point of view when they provide similar services and pose similar risks, and to regulate them consistently with financial institutions, in order to avoid unequal treatment (*level-playing field principle*, i.e. *functional treatment*)[442].

Reminding the expansive approach that should be applied when determining whether an asset is a VA[443], the Guidance shows a particular concern for Stablecoins with the potential for mass-adoption[444], and underlines that there should not be a case where a relevant financial asset is not covered by the FATF Standards (either as a VA or another financial asset)[445], nor a case where an asset is both a VA and a financial asset at the same time[446]. Hence, jurisdictions should decide how to classify

---

[440] 2019 FATF Guidance, 8, par. 14: "(…) *the Guidance focuses on VAs that are convertible for other funds or values, including both VAs that are convertible to another VA and VAs that re convertible to fiat or that intersect with the fiat financial system, having regard to the VA and VASP definitions. It does not address other regulatory matters that are potentially relevant to VAs and VASPs (e.g., consumer protection, prudential safety and soundness, tax, anti-fraud or anti-market manipulation issues, network IT security standards, or financial stability concerns"*. It is worth to remark that this selective regulatory approach has been followed by the 2021 Guidance.

[441] The amendments made to the Guidance focused on six main areas: clarification of the definitions of virtual assets and VASPs, guidance on how the FATF Standards apply to stable coins, additional guidance on the risks and the tools available to countries to address the money laundering and terrorist financing risks for peer-to-peer transactions, updated guidance on the licensing and registration of VASPs, additional guidance for the public and private sectors on the implementation of the "travel rule", and principles of information-sharing and co-operation amongst VASP Supervisors.

[442] 2021 FATF Guidance, 13, par. 25.

[443] 2021 FATF Guidance, 22, par. 47.

[444] 2021 FATF Guidance, 17, Box 1.

[445] 2021 FATF Guidance, 22, par. 46.

[446] 2021 FATF Guidance, 23, par. 51.

assets pursuant to the functional and technological neutral approach[447], and, where such classification proves difficult, countries should consider which designation would best mitigate and manage the risk, as well as the commonly accepted usage of the asset[448]. On this point, is interesting to notice that, with regard to those assets that are not interchangeable and are used as collectibles, also known as non-fungible tokens (NFTs), they fall out of the scope of the Guidance; however, they could be covered by FATF Standards under some circumstances, such as in the case where they are used for payment or investment purposes in practice or are digital representations of other financial assets already covered by FATF Standards: in this case they would fall under the definition of financial asset[449].

Following the same expansive approach applied to VAs[450], the Guidance further details the interpretation of the VASP definition, clarifying that it covers not only the provision of a service, but also any facilitation that implies an active involvement[451], in this way leaving out of its scope only those who perform a VASP function on a very infrequent basis, or for non-commercial reasons or for themselves[452]. As a consequence, also VA escrow services, brokerage services, order-book exchange services, and advanced trading services could fall under the VASP definition if they conduct or provide the activity as a business on behalf of another person[453], as well as ATMs[454], and activities of safekeeping, administration and control of VAs, except for those ancillary infrastructures such as cloud data storage providers, integrity service providers which very signatures, software developers and providers of unhosted wallets which only perform these activities[455]. In this respect, it is interesting to underline that the VASP definition covers also the

[447] 2021 FATF Guidance, 22, par. 47.
[448] Thus, applying the technology neutral approach, it is possible that a blockchain-based asset could be defined as a financial asset and not as VA: 2021 FATF Guidance, 23, par. 52.
[449] 2021 FATF Guidance, 24, par. 53.
[450] 2021 FATF Guidance, 24, par. 56.
[451] Only those actors which play a passive role are left out, such as Internet providers or cloud services: 2021 FATF Guidance, 25, par. 59.
[452] 2021 FATF Guidance, 25, par. 60.
[453] 2021 FATF Guidance, 28, par. 70.
[454] 2021 FATF Guidance, 28, par. 71.
[455] 2021 FATF Guidance, 29, pars. 72-76.

activities related to ICOs, unlike the mere acts of issuing VAs, or creating a software to issue VAs[456].

Before analysing how the Guidance addresses the specific risks posed by VAs, a few considerations have to be made. First, it is essential to clarify that the Guidance refers not only to Virtual Assets Providers, but to any entity which happens to be involved in Virtual Assets operations and transactions at some level, namely financial institutions and the FATF wide category of Designated Non-Financial Businesses and Professions (DNFBPs)[457]; and, of course, vice versa, when VASPs engage in traditional fiat-only activities or fiat-to-fiat transactions they are subject to the same measures as the others traditional institutions or entity[458]. Second, the Guidance should be taken into account not only by those countries which allows VAs activities in their jurisdictions, but also by those countries that have decided to prohibit them, in order to prevent illicit activities[459]. Third, given the interconnectedness of the risks posed by VAs and VASPs, the FATF Standards should be read through the lens of an holistic approach, since all the measures are aimed at addressing the multi-faceted issues that they pose.

2.2.1 Tackling Virtual Assets' (*pseudo*)anonymity

The Guidance shows a specific concern about the higher levels of anonymity offered by Virtual Assets[460]. In order to try to reduce the blind spots in the VAs' market, the Guidance details how the licensing/registration requirement set out by Recommendation 15 and its Interpretive Note could apply, reiterating the

[456] 2021 FATF Guidance, 30, pars. 77-78.

[457] According to the FATF Glossary, DNFBPs include casinos, real estate agents, dealers in precious metals and precious stones, legal professionals and accountants, and Trust and Company Service Providers.

[458] 2021 Guidance, 15, par. 30.

[459] 2021 Guidance, 21, par. 43.

[460] 2021 FATF Guidance, 7, par. 4: *"(…) the virtual asset ecosystem has seen the rise of anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralized platforms and exchanges, privacy wallets, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows*".

suggestion for host jurisdiction cover VASPs accessible in their territories, especially in view of the "*inherent cross-border availability of VAs*"[461] and suggesting that countries should consider to designate VASPs from countries which do not effectively implement licensing/registration requirements as higher risk[462]. Moreover, it urges the implementation of the full set of what the FATF generally calls "preventive measures", which include due diligence and know your costumer measures, recordkeeping and suspicious transaction reporting (Recs. 10 to 21)[463]. In this context, Recommendation 10 is of particular interest, as par. 7 of the Interpretive Note to Recommendation 15 lowered the threshold above which VASPs have to carry out Customed Due Diligence (CDD) for occasional transactions to USD/EUR 1000: on this point, the Guidance by suggesting that, given the peculiar characteristics of VAs, countries could further lower the threshold of USD/EUR 1000[464]. Moreover, pursuant to Recommendation 10, there are circumstances that require a more severe CDD framework (enhanced CDD), which could require measures to verify identity information, tracing the IP addresses, the use of analysis products, and Internet research to find information consistent with the customer's profile[465]. In this respect, the FATF underlines that country/geographic specific risk factors could play a central role, whose indicators may include: countries or geographic areas providing funding or support for terrorist activities or that have designated terrorist organisations operating within their territories, countries that show significant levels of organised crime, corruption or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling and illegal gambling, countries that are subject to sanctions, embargoes, or similar measures and countries characterised by weak governance, law enforcement and regulatory regimes[466].

---

[461] 2021 FATF Guidance, 44, par. 127.
[462] 2021 FATF Guidance, 46, par. 137.
[463] These Recommendation have direct applicability to VAs and VASPs, however also Recommendation 9, 22, and 23 are relevant: 2021 FATF Guidance, 48, par. 145.
[464] 2021 FATF Guidance, 49, par. 152.
[465] 2021 FATF Guidance, 50-51, pars. 156-158.
[466] 2021 FATF Guidance, 50, par. 154.

2.2.2 Responding to Virtual Assets' transnationality

The cross-border nature of Virtual Assets constitute a serious concern in regulatory terms, and the Guidance deals extensively on how to address this aspect. In this context, two Recommendations appear to be of particular interest, namely Recommendations 13 and 16.

Recommendation 13 specifically applies only to cross-border correspondent relationships and requires financial institutions to take some additional measures CDD measures[467]. When it comes to VASPs, the Guidance specifies that a "*corresponded relationship" is "the provision of VASP services by one VASP to another VASP or FI*", and, like in the case of financial institutions, is characterised by an on-going repetitive nature[468]. With regard to the assessment of the AML/CFT risks, the Guidance underlines that cross-border relationships with jurisdictions that have weak or non-existent AML/CFT regulation or supervision of VASPs are likely to present a higher risk[469]. Of course, Recommendation 13 in relation to VASPs does not apply to domestic equivalent of correspondent relationships[470].

Recommendation 16, instead, applies to both domestic and cross-border wire transfers. Aimed at preventing terrorists, and criminals in general, to have illimited access to wire transfers for moving funds[471], it requires financial institutions to

---

[467] FATF Rec. 13: "*Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to: (a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action; (b) assess the respondent institution's AML/CFT controls; (c) obtain approval from senior management before establishing new correspondent relationships; (d) clearly understand the respective responsibilities of each institution; and (e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.*
Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks".

[468] 2021 FATF Guidance, 53, par. 165.

[469] 2021 FATF Guidance, 53-54, par. 167.

[470] 2021 FATF Guidance, 54, par. 168. However, we remind that in those cases VASPs should carry out risk-based customer due diligence under Recommendation 10.

[471] FATF Int. Note to Rec. 16, par. A, p. 1.

obtain, store, and submit required and accurate originator and required beneficiary information associated with wire transfers in order to identify and report suspicious transactions, take freezing actions and prohibit transactions with designated persons and entities, as well as sanctions screening.

Pursuant to the functional approach, Recommendation 16 also applies to VASPs[472], and it is commonly referred to as the "travel rule"; however, as seen in relation to Recommendation 10, the peculiar characteristics of VAs make Recommendation 16 to apply to VAs and VASPs with some adjustments: only when VASPs carry out transactions (whether in fiat or VA) that involve a traditional wire transfer or a VA transfer between a VASP and another obliged entity, the full requirements of Recommendation 16 will apply, whereas in the case of transactions between a VASP and a non-obliged entity, some amendments are in put in place. In particular, where the transfer occurs between two VASPs or obliged entities, the Guidance underscores the importance of submitting the information immediately and securely, especially given the rapid and cross-border nature of VA transfers, meaning that those information should be transmitted prior, simultaneously pr concurrently with the transfer and in a manner that ensures their integrity and availability[473]; this, however, while still allows to submit batch information, prohibits post facto submission[474]. Nonetheless, in the case that countries adopt the lowered threshold set by Recommendation 10, less stringent requirements are required, as VASPs should only collect the name of the originator and the beneficiary and the VA wallet addresses or a unique transaction reference number, with no further action if there are no suspicious circumstances[475]. While the same requirements apply in case of a VA transfer involving an intermediary VASP, things are different in the case of a transfer between a VASP and not obliged entities, such as an unhosted wallet provider: in these cases, countries should ensure that the

[472] 2021 FATF Guidance, 55-56, par. 175.
[473] 2021 Guidance, 59 pars. 184-186.
[474] 2021 FATF Guidance, 60, par. 187.
[475] 2021 FATF Guidance, 61, pars. 191-192.

obliged entities adhere to Recommendation 16 with regard to their customer; however, they do not have to submit the required information to the non-obliged counterpart – anyway, they should obtain the required originator and beneficiary information from their customer[476].

2.2.3 The challenge of addressing decentralisation issues

Perhaps the most challenging aspect of the virtual assets ecosystem in terms of regulation is represented by those activities that are carried out without the involvement of any intermediary, in this way escaping from the jaws of the FATF.
This is the case of peer-to-peer (P2P) transactions, which are "*VA transfers conducted without the use or involvement of a VASP or other obliged entity*"[477] and thereby not subject to AML/CFT measures, in this way posing significant risks in terms of criminal abuse – to the point that, if they were to grow they could potentially challenge the effectiveness of the FATF architecture[478]. Since they are not covered by the AML/CFT framework, indeed, the Guidance merely suggests how countries could understand the risks associated[479], and recommends some measures that countries could adopt to mitigate such risks[480].
However, things are different for P2P platforms, which enable users to perform P2P transactions. Indeed, given the expansive nature of the VASP definition, these platforms could escape the AML/CFT measures only when they provide a very

[476] 2021 FATF Guidance, 65, pars. 203-204.
[477] 2021 FATF Guidance, 18, par. 37.
[478] 2021 FATF Guidance, 19, par. 40.
[479] Namely by cooperating with the private sector, training supervisory authorities, FIUs and law enforcement personnel, and supporting the development of technologies such as blockchain analytics: 2021 FATF Guidance, 39, par. 105.
[480] These measures may include controls on visibility, ongoing risk-based enhanced supervisions of VASPs and entities focused on unhosted wallet transactions, requiring VASPS to facilitate transactions only between verified addresses and sources and only to/from VASPs and other obliged entities, putting additional AML/CFT requirements on VASPs that allow transactions to/from non-obliged entities, as well as issuing public guidance and raise awareness of risks associated to P2P transactions: 2021 FATF Guidance, 39, par. 106.

limited functionality and do not carry out activities such as exchanges, transfers, storing, administration, control and the provision of financial services - regardless of their self-description or the technology used (i.e. functional and technology neutral approach)[481]. Accordingly, the Guidance considers to be VASPs also those platforms that merely provide "matching" or "finding" services, as well as self-labelled P2P platforms that have been involved at some stage of the product's development and launch[482], and those platforms that have implemented automated processes for their future development (e.g. smart contracts)[483].

A similar approach should be adopted with regards to decentralised exchanges or platforms, such as *Dapps*, which can perform or facilitate VAs transfer or exchange and are commonly referred to as DeFi[484]. In the light of the FATF technological neutral approach, DeFi applications themselves do not fall under the VASP definition; however, persons who maintain control or sufficient influence on in the DeFi arrangements, may be covered by VASP definition if they provide or actively facilitate a VASP service, regardless of how they self-label themselves (i.e functional approach)[485].

2.2.4 The need of international cooperation to address regulatory gaps

Considering the cross-border and mobile nature of virtual assets, together with the ever-evolving landscape of Virtual Assets regulations, one of the most problematic issues is represented by their uneven legal status and regulation across jurisdictions

[481] FATF Guidance 2021, 35, par. 90: "*For example, this may include websites which offer only a forum for buyers and sellers to identify and communicate with each other without offering, even in part, those services which are included in the definition of VASP*".

[482] 2021 FATF Guidance, 35, par. 91.

[483] 2021 FATF Guidance, 36, par. 92.

[484] 2021 FATF Guidance, 26-27, par. 66.

[485] 2021 FATF Guidance, 27, pars. 67-68. On this point, it is interesting to remark that some authors doubts DeFi's complete decentralised nature, as, in order to take strategic and operational decisions, some form of centralisation would be inevitable: S. ARAMONTE, W. HUANG, A. SCHRIMPF, "DeFi risks and the decentralisation illusion", in BIS Quarterly Review, December 2021.

(*supra* Chapter II, § 5.5.4). In this respect, international cooperation is crucial to design an effective regulatory framework and to limit and prevent jurisdictional arbitrage, "forum shopping" phenomena, unfair competition, and the exploitation of virtual assets for criminal purposes. On this point, the Guidance expands on par. 8 of the Interpretive Note to Recommendation 15, and stresses the importance of mutual assistance (Rec. 37), the cooperation in identification, freezing, seizing and confiscation procedures – which, of course, could directly involve virtual assets as well as other traditional assets (Rec. 38), and the provision of effective extradition assistance (Rec. 39), as well as cooperation among national competent authorities (Rec. 40), which are requested to promptly and constructively exchange information among them[486].

2.3 The effectiveness of the FATF approach: first outcomes of the application of FATF Standards on VAs and VASPs

Since the release of the first version of the Guidance in 2019, the FATF periodically monitored the national implementation of the new Recommendation 15. In 2020, already most of FATF (and FSRBs) jurisdictions introduced a regulatory regime permitting VASPs and, among those who had not adopted a regime yet, the majority manifested the willingness to do so in the near future[487]. However, stages and choices in the implementation greatly varied[488], and, while the implementation of the registration/licensing requirements and of a supervisory regime was widely introduced, the implementation of the "travel rule" proved to be particularly

[486] 2021 FATF Guidance, 68-69, pars. 221-226.

[487] Data are based on a self-assessment survey conducted in 2020, which saw the participation of a total number of 54 FATF (and FSRBs) members. Thirty-two members introduced a regulatory regime permitting VASPs, while three members had prohibited VASPs; among the nineteen members that reported not have a regime for VASPs yet, thirteen of them manifested their intention to regulate them, while two reported to intend to prohibit them and four did not take a position: First 12th Month Review, 8, pars. 23-25.

[488] First 12th Month Review, 8, par. 26.

problematic, as only less than a half of them applied it[489]: especially, a number of issues was raised in relation to the counterparty timely and secure identification, peer-to-peer transactions via private/unhosted wallets, batch and *post facto* submission of data, interoperability of the systems, as well as the fact that jurisdictions implement the travel rule at different times and in different manners (i.e., sunrise issue), and adopt different terminological choices[490].

The following year, the Second Review reported significant progress, both with regard to members participation – the number tripled, for a total of 128 members - and in the implementation of Recommendation 15[491], although significant gaps remained, especially in relation to the implementation of Recommendation 16. In fact, even if there seems to have been progress on the technology needed to perform the requirement effectively, they do not seem to be sufficient, and most jurisdictions and most VASPs are not compliant, thus creating a "*self-reinforcing conundrum*". Indeed, only 23 members reported to have introduce the travel-rule: only eight more than the previous assessment[492].

Similar concerns appear to keep concerning the FATF, as since June 2021 only limited progress were reported in the implementation of Recommendation 15[493],

---

489 First 12th Month Review, 12, par. 43.

490 First 12th Month Review, 16-18, pars. 60-68.

491 Fifty-eight members reported that they regulated VAs and VASPs (six of them prohibiting VASPs), and thirty-five of them 35 jurisdictions (30 jurisdictions permitting VASPs and five jurisdictions prohibiting VASPs) reported that their regimes were operational. Twenty-six members reported that they were passing the necessary regulatory framework, while twelve members stated that they still have to begin the regulatory process, and thirty-two members have still not taken any position: Second 12th Month Review, 43-44, pars. 25-29.

492 Second 12th Month Review, 18-19, pars. 58-61.

493 Report on "Targeted update on implementation of the FATF Standards on Virtual Assets and Virtual Assets Service Providers", FATF, June 2022. From June 2021 to May 2022, the FATF and its Global Network have published 53 Mutual Evaluation Reports and Follow-Up Reports, which include assessments of country compliance with the FATF's requirements on VAs and VASPs. Overall, most jurisdictions assessed during this period have received a partially compliant (PC) rating14, , showing there is a continued need to strengthen technical compliance with R.15. Since June 2021, no jurisdiction has received a fully compliant rating with R.15. Only 12 jurisdictions out of 53 (23%) have been assessed as largely compliant with R.15, with 6 of these jurisdictions being FATF members and 6 being a member of an FATF regional body (either the Asian Pacific Group, the Caribbean Financial Action Task Force, or MONEYVAL). Similarly, in line with the second 12-month review, jurisdictions also continue to face challenges for sub-criterion 15.9, which requires jurisdictions to apply AML/CFT preventative measures to VASPs, such as customer due diligence

and the travel rule continues to represent a major concern: while the number of jurisdictions implementing it is slowly growing (from 23 to 29), only 11 jurisdictions have started enforcement and supervisory measures[494]. However, in order to tackle the sunrise issue some jurisdictions are demonstrating a certain flexibility for domestic requirements and providing guidance to domestic VASPs[495].

3. The contribution of other Standard-Setting Bodies (SSBs)

As abovementioned, the FATF enjoys the endorsement of other important global international standard-setting bodies, which help the implementation of FATF Recommendations by further spreading them through their members. According to their mandate, these actors operate at different levels, namely different to the AML/CFT regime – yet still relevant to it, as the AML/CFT measures involve multiple sectors. In particular, the International Monetary Fund and World Bank play an important role, as they conduct periodical assessments based on a common methodology shared with the FATF[496] – of which they are also Observers; nonetheless, also other side actors contribute effectively by developing guidelines and best practices.

---

and the Travel Rule. 41 out of 53 jurisdictions (77%) do not meet, or partly meet, this requirement. 10. Notably, the mutual evaluation results on R.15 compliance are consistent with feedback received through an FATF survey to members in March 2022, which collected feedback on jurisdictions' progress in licensing and registering VAs and VASPs. The March 2022 survey found that of the 98 responding jurisdictions, 42 jurisdictions (or 43%) had introduced a licensing or registration regime for VAs and VASPs, in comparison to 39% (52 out of 128) in June 2021. This suggests there is a continued need for both FATF and FSRBs members to accelerate compliance with the FATF Standards on VAs and VASPs in order to prevent criminal misuse.

[494] Report on "Targeted update on implementation of the FATF Standards on Virtual Assets and Virtual Assets Service Providers", *Ibid.*, 10, par. 12,

[495] Report on "Targeted update on implementation of the FATF Standards on Virtual Assets and Virtual Assets Service Providers", *Ibid*., 13, par. 17-18.

[496] The Methodology used is the FATF "Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems"; first published in 2004, it has been revised in 2013 following the revision of the FATF Standards in 2012, and again in 2019 in order to welcome new Recommendation 15; the last amendment dates back to 2021.

Before mapping out how this complex network of international bodies has reacted to the rise of Virtual Assets and the role they are playing in shaping the regulatory framework, it is interesting to notice that, although working close one to another, the terminology they use still vary. In fact, only the World Bank uses the terminology used by the FATF (virtual assets and virtual assets service providers), while the other bodies chose to use the term of crypto-assets – still, this choice does not seem to have relevant consequence on their scope, which appears to be the same as the one of the FATF definitions.

3.1 The International Monetary Fund

Starting to engage in the field of anti-money laundering in 2000, after the 9/11 attacks the International Monetary Fund (IMF) included counter-terrorism financing in the scope of its work, and, given its nature of "*collaborative institution with near universal membership*", it is nowadays particularly helpful in achieving a global reach and ensuring a minimum standard of harmonisation across countries[497]. In particular, the IMF action in the AML/CFT field is expressed through assessment programs – namely the Financial Sector Assessment Program (FSAP) and the Offshore Financial Centers Program – as well as providing technical assistance, and developing policies[498]. Although not having issued a specific official guidance on Virtual Assets, informal discussions started as early as in 2016, with the issue of preliminary considerations on the types and feature of virtual assets and depicting the possible risks associated, which, similarly to the 2014 FATF Report, were referred to as "virtual currencies" – yet underlining that they failed to be

[497] "*As a collaborative institution with near universal membership, the IMF is a natural forum for sharing information, developing common approaches to issues, and promoting desirable policies and standards -- all of which are critical in the fight against money laundering and the financing of terrorism*": International Monetary Fund Official Website – Topics: Anti-Money Laundering/Combating the Financing of Terrorism.

[498] Assessment programs and technical assistance in the AML/CFT field are part of IMF's regular work since March 2004.

classified as money or currencies both from a legal and economic perspective[499]. More recently, the FATF approach on Virtual Assets' ecosystem has been welcomed, encouraging to adapt the national frameworks to keep up the pace and calls for an effective cooperation across jurisdictions, both in relation to VAs[500] and VASPs[501] and calling for a coordinated, consistent and comprehensive global response[502]. However, some gaps in the state of art of the regulatory framework have been underlined, such as the urgent need to develop common taxonomies, the difficult access to consistent and reliable data, and the necessity to establish additional requirements in case such entities or activities become systemic[503].

3.2 The World Bank

Following the work of the FATF, the World Bank recently released a Virtual Assets – Risk Assessment Tool and a related Guidance in order to help countries in the ML/TF risk assessment related to the VA and VASP sector[504]. Indeed, the World Bank recognises that the unique features of virtual assets overall reflect on the money-laundering and terrorism financing risks that they pose, and thus require a

[499] D. HE, K. HABERMEIER, R. LECKOW, V. HAKSAR, Y. ALMEIDA, M. KASHIMA, N. KYRIAKOS-SAAD, H. OURA, T. S. SEDIK, N. STETSENKO, C. VERDUGO-YEPES, "Virtual Currencies and Beyond: Initial Considerations", IMF Discussion Note, January 2016, p. 16: "*VCs fall short of the legal concept of currency or money*".

[500] N. SCHWARZ, K. CHEN, K. POH, G. JACKSON, K. KAO, F. FERNANDO, M. MARKEVYCH, "Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1). Some Legal and Practical Considerations", in *Fintech Notes*, International Monetary Fund, No. 2, October 2021.

[501] N. SCHWARZ, K. CHEN, K. POH, G. JACKSON, K. KAO, F. FERNANDO, M. MARKEVYCH, "Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2). Some Legal and Practical Considerations", in *Fintech Notes*, International Monetary Fund, No. 2, October 2021.

[502] A. NARAIN, M. MORETTI, "Regulating Crypto. The right rules could provide a safe space for innovation", in *Finance and Development*, International Monetary Fund, September 2022.

[503] P. BAINS, A. ISMAIL, F. MELO, N. SUGIMOTO, "Regulating the crypto ecosystem. The case of unbacked crypto assets", in *Fintech Notes*, Vol. 7, September 2022, 2-47.

[504] Guidance Manual on "Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool", World Bank Group, June 2022.

specific structure and approach[505], in particular in understanding the threats and vulnerabilities variables that both VAs and VASPs pose[506].

Similarly to the position of the FATF, the Guidance expresses particular concern in relation to higher level of privacy offered by some types of VAs and some dedicated tools (e.g., mixers and tumblers), peer-to-peer transactions, and decentralised exchanges – which in the future could gain significant volumes[507], and reiterates that all actors that perform any of the activities that fall under the FATF VASPs definition, should be covered by AML/CFT regulatory framework. Looking specifically at terrorism financing, the Guidance states that the nature of VAs could be used to fund terrorism even "*more efficiently than is done today with fiat currencies*", especially through donations, transfer of funds and crowdfunding initiatives, and suggesting that transfers to less-developed regions where terrorist groups operate should be treated as a higher threat[508].

---

[505] Guidance Manual on "Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool", *Ibid*., 28-29: "*Virtual asset ML and TF differ from conventional ML and TF. The VA industry is not confined to one jurisdiction; it operates globally and exists locally, with exchanges and mining operations unconstrained by national borders. With the inconsistencies in the definition of VAs in many countries and variation in designated legislation, the approach adopted for this VA-RA exercise looks at the risk of VAs separately from VASPs; the vulnerability of both would affect national vulnerability*".

[506] The Guidance distinguishes two categories of variables: intermediate variables, which are broad and high-level factors (namely: VA nature and profile, accessibility to criminals, source of funding VAs, operational features of VAs, ease of criminality, and economic impact), and input variables, which include AML control variables (general AML controls and product-specific AML controls) and inherent vulnerability variables: Guidance Manual on "Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool", *Ibid*., 35-37.

[507] Guidance 2022, p. 31: "*Several VA start-ups have argued that the centralized model of VA exchanges was a necessary first step to develop the market, but the next evolution will come from decentralized exchanges. Although this type of venue currently represents trivial volumes, if it gains significant attention it might represent the next evolution and/or addition in the VA exchange landscape*".

[508] Guidance Manual on "Virtual Assets and Virtual Assets Service Providers. ML/TF Risk Assessment Tool", *Ibid.*, 48.

3.3 The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (Basel Committee)[509] plays a concrete role in the implementation of the FATF Recommendations and contributes to the international regulatory framework by developing its own standards and guidelines[510]. With regard to terrorism financing, its Core Principles[511], which are endorsed and followed by the International Monetary Fund and by the World Bank while carrying out their assessment programmes, require supervisors to assess that "*banks have adequate policies and processes, including strict customer due diligence rules to promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities*" (Core Principle No. 29).

Like the other relevant international actors involved in the regulatory framework, in recent years the Basel Committee started to pay attention to the Virtual Assets phenomenon, and developed its approach according to the technological evolutions: starting from an initial statement on the possible impact of "crypto assets" – in which occasion the Basel Committee expressed concerns on their possible future impact on financial stability and their unfitness to provide the functions of money and to serve as a medium of exchange or store of value[512], nowadays the digital world surged to be one of the two main current – and future

[509] Founded in 1974 by central banks governors of G10 countries, the Basel Committee on Banking Supervision is one of the main trend setter organisations for the prudential regulation of the banking system, currently counting 45 members and covering 28 jurisdictions.

[510] For a comment on the functioning of the Basel Committee: M. S. BARR, G. P. MILLER, "Global Administrative Law: The View from Basel", in *The European Journal of International Law*, Vol. 17 (1), 2006, 15-46.

[511] The Core Principles for Effective Banking Supervision are part of the Basel Committee Fourteen Standards. First drawn up in 1997, they have been revised in 2006 and 2011. Used by countries, as well as the International Monetary Fund and the World bank during their assessments, they serve to assess the effectiveness the quality of countries' supervisory systems and practices.

[512] Interestingly, the Statement explain the choice of words "crypto-assets", as "*While crypto-assets are at times referred to as "crypto-currencies", the Committee is of the view that such assets do not reliably provide the standard functions of money and are unsafe to rely on as a medium of exchange or store of value*": "Statement on crypto assets", Basel Committee on Banking Supervision, 13 March 2019.

– concerns of the Committee[513]. Accordingly, it recently intensified its efforts in this sense, and issued two consultative documents within a short timeframe, which include some considerations that, although addressed to banks, raise interesting points[514]. In particular, the Committee encourages a "same risk, same activity, same treatment" approach – which appears to recall the FATF functional and technological neutral approach (*supra* § 2.2) – and calls for a minimum standard approach, leaving to the single jurisdiction whether to adopt additional measures. Moreover, it is interesting to notice that the Basel Committee suggests a different regulatory approach according to the kind of "crypto-assets" involved: crypto-assets with effective stabilisation mechanisms (e.g. stablecoins) that meet specific prudential classification conditions would be subject to a less severe scrutiny, while other crypto-assets – believed to pose higher risks –, including stablecoins that fail to meet classification conditions, would be submitted to more extended prescriptions[515].

Overall, it is interesting to remark that the work of the Basel Committee is valued by the FATF[516], which also in the Guidance referred to it in multiple occasions, namely when it comes to cooperation among jurisdictions and cross border nature (Principles 3 on cooperation and collaboration and 13 on home-host relationships)[517] and with reference to the Basel guidelines for managing the risks related to money

[513] Together with climate-related financial risks: P. HERNÀNDEZ DE COS, "Computers and money: the work of the Basel Committee on cryptoassets", Keynote speech at the 36th Annual General Meeting of the International Swaps and Derivatives Association, Madrid, 12 May 2022.

[514] "Prudential treatment of cryptoasset exposure – Consultative document", Basel Committee on Banking Supervision, June 2021; and its update: "Second consultation on the prudential treatment of cryptoasset exposures", Basel Committee on Banking Supervision, June 2022.

[515] "Second consultation on the prudential treatment of cryptoasset exposures", Basel Committee on Banking Supervision, June 2022. Interestingly, the document suggests the introduction of an exposure limit for the second group of riskier crypto-assets.

[516] The relationship between the work of the two bodies was very clear since the beginning, as the FATF's First Annual Report (1990) included the Basel Principles among the international instruments to combat money laundering.

[517] 2021 FATF Guidance, 47-48, par. 143.

laundering and financing of terrorism, especially in relation to beneficial ownership[518].

3.4 The International Organisation of Securities Commissions

Among the international actors which significantly contribute to the development of the international regulatory framework, we find the International Organisation of Securities Commissions (IOSCO), which is recognised as the global standard setter for the securities sector. Starting to ponder the possible impact of financial technologies (FinTech) in 2017[519] and of ICOs in 2018[520], in 2019 IOSCO released a consultation paper on how to regulate crypto-assets trading platforms (i.e., exchanges)[521], first followed by the release of some initial consideration on the possible impact of Global Stablecoins[522] and later by the adoption of a final report on how to address the regulatory issues posed by the Crypto-Asset Trading Platforms (2020 IOSCO Report)[523]. Valuing the work of the FATF[524], the Guidance was aimed at helping IOSCO members in the evaluation of the associated issues and risks, the Guidance provides some key considerations[525] and related toolkits in order to protect investors. In particular, it underlines the need to ensure the

---

[518] "Guidelines on sound management of risks related to money laundering and financing of terrorism", Basel Committee on Banking Supervision, January 2014 (rev. July 2020).

[519] Research Report on Financial Technologies (Fintech), IOSCO, February 2017.

[520] Communication on Concerns related to Initial Coin Offerings (ICOs), IOSCO Board, Madrid, 18 January 2018 (IOSCO/MR/01/2018).

[521] Consultation Report on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms, IOSCO Board, CR02/2019, May 2019.

[522] Public Report on Stablecoins Initiatives, IOSCO, March 2020 (OR01/2020).

[523] Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms Final Report, IOSCO, February 2020.

[524] 2020 IOSCO Report, 47: "*Amendments have been made in the Final Report to reflect updated FATF standards relating to KYC/AML/CFT*". Besides, it is worth to underline that this endorsement is reciprocal, as the 2021 FATF Guidance refers to the work of IOSCO, namely at par. 143,in terms of international cooperation in the VAs field and at par. 237, in relation to the assessment of the level of risk posed VA services, products or activities.

[525] The key considerations are related to: i. access to Cryptoassets Trading Platforms, ii. safeguard of participant assets, iii. conflicts of interest, iv. operations of Cryptoassets Trading Platforms, v. market integrity; vi. price discovery; and vii. technology.

protection of investors, fairness, efficiency and transparency of markets, and the reduction of systemic risk, as exchanges appear to perform similar functions of Trading Venues[526]. Moreover, the Guidance identifies the relevant IOSCO principles, namely those related to cooperation (Principles 13 to 15), which are particularly important given the cross-border nature of VAs, those dedicated to "Secondary and Other Markets" (Principles 33 to 37), those relating to "Market Intermediaries", and those devoted to "Clearing and Settlement", since some exchanges may act in similar ways of intermediaries (Principles 29 to 32), as well as principle 38, in order to ensure the fairness and efficiency of the regulatory and supervisory requirements and reducing systemic risks.

Overall, the Guidance highlights that regulatory approaches in relation to exchanges differ among jurisdictions, as well as their actions to mitigate the related issues and risks[527], and invites members to set up and efficient cross-border information sharing, both at global and regional levels[528].

The work of IOSCO, however, did not stop with the 2020 Guidance: in March 2022 it has been established a Board-level Fintech Task Force[529] with the task of developing, monitoring and implementing IOSCO's agenda in the field of Fintech and crypto-assets, as well as managing the coordination with the Financial Stability Board and other relevant standard setting bodies[530]. Accordingly, in July 2022, it has been released the "Crypo-asset Roadmap for 2022-2023"[531], which drafts the future steps to be taken in relation to the world of Virtual Assets: in particular, the new

[526] 2020 IOSCO Report, 6.

[527] 2020 IOSCO Report, 8.

[528] 2020 IOSCO Report, 26 ss.

[529] At the moment the Task Force counts 27 members from Board member jurisdictions: AMF France, ASIC Australia, BaFin Germany, SC Bahamas, CVM Brazil, CSRC China, CNBV Mexico, CONSOB Italy, FRA Egypt, ESMA, FSMA Belgium, FSS Korea, SFC Hong Kong, FSA Japan, SC Malaysia, AMMC Morocco, OSC Ontario, AMF Quebec, CMA Saudi Arabia MAS Singapore, CNMV Spain, FI Sweden, FINMA Switzerland, CMB Turkey, FCA United Kingdom, CFTC United States, SEC United States.

[530] Moreover, in the same month it has been established the DeFi Working Group 2, to understand and address the potential opportunities as well as the potential risks for investors and markets in the field of DeFi.

[531] Crypto-Asset Roadmap for 2022-2023, IOSCO,7 July 2022.

Task Force will be engaged in parallel to work on the challenges posed by Virtual Assets and DeFI in the view of their possible impact on market integrity and investor protection, adopting a coherent, coordinated cross-sectoral approach. Moreover, the Roadmap highlights the strong connection of IOSCO with the work of the other relevant standard setting bodies, namely the Financial Stability Board, the Basel Committee, and the FATF, explicitly recalling their critical importance – in this way once again confirm the tight connection among these international actors.

3.5 The Financial Stability Board

The Financial Stability Board (FSB) promotes the international financial stability by coordinating national financial authorities and international standard-setting bodies, and by monitoring and elaborating recommendations[532]. Being particularly concerned about both FinTech and virtual assets' implications for financial stability, in 2018 it concluded that they did not pose a material risk at that time[533]; however, shortly after it started to show some a specific concern to the phenomenon of Global Stablecoins. In 2020, indeed the FSB adopted High-Level Recommendations to respond to the main challenges related to Global Stablecoins , namely the uneven regulatory frameworks across countries, including the different legal classifications and consequent monitoring difficulties, the insufficient risk mitigation tools in place and risks for investors and unfair competition[534].However, the implementation of such Standards did not proceed as fast as expected[535], and, given the rapid

[532] For a comparison between FATF and FSB structure and functioning: S. DE VIDO, "Soft Organizations, Hard Powers: The FATF and the FSB as Standard-Setting Bodies", in *Global Jurist*, Vol. 19, November 2018, 1-12.

[533] "Crypto-asset markets Potential channels for future financial stability implications", FSB, 10 October 2018.

[534] "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements Final Report and High-Level Recommendations", FSB, 13 October 2020.

[535] "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements Progress Report on the implementation of the FSB High-Level Recommendations", FSB, 7 October 2021.

technological developments, the Financial Stability Board has recently released a consultative document on their review – which has seen the participation, among others, of the FATF, Basel Committee and IOSCO – from which clearly emerged the need of an effective regulation and supervision on Global Stablecoins[536].

At the same time, the Financial Stability Board stated that, unlike to what previously assessed in 2018, crypto-assets are likely to represent a threat for financial stability[537], and after recalling the crucial importance of the full and timely implementation of the existing international standards, expressively referring to FATF Recommendations 15 and 16[538], announced to be currently working to develop a framework dedicated to unbacked crypto-asset, recalling the same approach based on Recommendations used in relation to Global Stablecoins[539].

4. Virtual assets' regulation at the regional level: the European Union approach

As underlined in Chapter I, the European Union addresses anti-money laundering and terrorism financing issues under a double perspective. With regard to the regulatory framework designed by anti-money laundering Directives, we find that the European Legislator has encountered some difficulties in keeping the pace with the technological evolutions investing the market and the corresponding international regulatory approached undertaken at the international level. The struggle is quite clear when looking at the fact that proposals for new Directives

[536] "Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements" - Consultative Report, FSB, 11 October 2022.

[537] "Assessment of Risks to Financial Stability from Crypto-assets", FSB, 16 February 2022: "*crypto-assets markets are fast evolving and could reach a point where they represent a threat to global financial stability* ".

[538] July 2022 Statement on International Regulation and Supervision of Crypto-asset Activities, Financial Stability Boars, 11 July 2022.

[539] Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets Consultative document, 11 October 2022 and International Regulation of Crypto-asset Activities A proposed framework – questions for consultation, 11 October 2022.

have been issued before the transposing period into national legislation of the previous ones had expired, in this way provoking confusion and disorientation and hampering the efforts to reach a minimum level of harmonisation across Member States, creating a gap between countries that manage to promptly incorporate the new measures in their national framework and those that are not as fast – which result in inconsistences and fragmentation across the Union.

4.1 The EU Fifth Anti-Money Laundering Directive

Although the FATF had already started to consider the possible risks posed by "virtual currencies" in 2014 (*supra* § 2), the European Union response did not follow as quickly as expected. Indeed, the text of the IV AML Directive[540] – designed to introduce the 2012 FATF revised Recommendations and issued only a couple of months before the 2015 FATF Guidance on Virtual Currencies – did not contain any reference to "virtual currencies" nor to the entities involved in such activities (e.g., exchanges, wallet providers), thereby leaving State Members free to qualify and regulate them as they preferred – or to not regulate them at all.

However, given the rapid evolution and spread of these new tools, the European legislator soon started to work in order to update and enhance the regulatory framework, and, less than a year after the adoption of the IV AML – and more than a year before the deadline for its transposition at national levels[541]– a new proposal for the V AML Directive was adopted[542]. The Proposal underlined the need to

[540] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or 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.

[541] The deadline fixed for the implementation of the IV AML Directive was fixed on 26 June 2017.

[542] COM (2016) 450: Proposal for a Directive of the European Parliament and of the Council 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 Directive 2009/101/EC.

improve transparency, specifically in relation to offshore jurisdictions, and – what is of the most interest for the purpose of this work – put particular emphasis on the need to tackle the financing of terrorism, highlighting the evolution and the growth of the terrorist threat and pointing out the gaps in the oversight of the numerous means by terrorist to finance themselves, including "virtual currencies"[543].

After two years of intensive work on the proposal, on 30 May 2018 Directive (EU) 2018/843 (V AML Directive)[544], amending – not replacing – the IV Directive was adopted.

Looking specifically to virtual assets regulation, the V AML is the first legal instrument to address the risks of money laundering and terrorist financing posed by virtual assets in the European Union. Yet, the Directive shows a quite narrow approach, carefully selecting the areas of intervention and refusing to regulate the phenomenon in its entirety[545], and, if on the one hand this could be appreciated in the light of a balanced and proportionate approach aiming at protecting economic freedoms, on the other hand it has been accused of merely "fencing" the virtual currencies (i.e., virtual assets) market, in this way lacking of long-term outlook[546].

First of all, it is worth to notice that the European legislator chose to adopt the term "virtual currencies" by defining them as "*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,*

---

[543] This proposal integrated the European Agenda on Security (COM(2015) 185 final) and followed the 2016 Commission Action Plan for strengthening the fight against terrorist financing (*supra* Chapter I, § 4.4.3).

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

[545] Recital No. 9 of the V AML Directive clearly states this choice: *"(…) the inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers*".

[546] G. SOANA, "Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?", in *Economic Notes*, Wiley Online, 2021, 3: "*this approach is questionable not only from a criminal policy standpoint it is also of arguable efficacy*".

stored and traded electronically" (art. 1, al. 2, d), 18). The choice of using the term "virtual currencies" could suggest that the European Legislator built on the 2014 FATF definition. However, in spite of agreeing on what virtual currencies are not – namely, not issued or guaranteed by any authority, do not have legal tender, it is not e-money nor, of course, fiat currency – their understanding on their nature does not completely coincide: even if both call them virtual *currencies*, the FATF explicitly recalled the three functions of money, whereas the European legislator does not seem to recognise them as actual currency[547], thus leaning towards the position of the European Banking Authority expressed in 2014[548]. In fact, this definition merely refers to the function of virtual currencies as "means of exchange", raising some questions about the concrete understanding of the scope of application. This choice, indeed, seems to be in contrast with Recital 10, which acknowledges the multi-purpose nature of virtual currencies and expresses the willingness to cover all of them[549]. According to some commentators, the choice of naming only "means of exchange" in the wording of art. 1, par. 2, d), 18 would therefore suggest a narrow interpretation, meaning that it would include only currency tokens[550]; thus, what

[547] S. LOOSVELD, The 5th Anti-Money Laundering Directive: virtual currencies and other novelties", in *Journal of International Banking Law and Regulation*, Vol. 33 (9), 3. Indeed, during the works on the Proposal, the ECB clearly stated that "*virtual currencies are not in fact currencies*": Opinion of the European Central Bank of 12 October 2016 on a proposal for a directive amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101.

[548] V. COVOLO, "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", in *European journal of crime, criminal law and criminal justice*, Vol. 28, 2020, 229. For convenience, we report the definition proposed by the EBA: "*VCs are defined as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically. VCs can therefore be characterised along the distinguishing features specified below. Although some of the features resemble activities or products that are already within the remit of the EU EMoney Directive, these products are not intended to be included here, as e-money is a digital representation of FC, which VCs are not*": EBA, Opinion on 'virtual currencies', 4 July 2014, EBA/Op/2014/08.

[549] Recital No. 10: "*(…) Although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of value products or use in online casinos. The objective of this Directive is to cover all the potential uses of virtual currencies*".

[550] In this sense, L. HAFFKE, M.FROMBERGER & P. ZIMMERMANN, "Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them", *Journal of Banking Regulation*, Vol. 21 (2), 2020, p. 133. Moreover, the Authors point that, if on the one hand the

would matter for the application of the Directive would be the "*de facto* acceptance of the currency as means of payment"[551] – although not being a real currency.

But the V AML Directive not only establishes the first definition of virtual currencies in EU law: it also, and maybe most importantly, adds two new obliged entities under the umbrella of the AML/CFT framework, namely the "*providers engaged in exchange services between virtual currencies and fiat currencies*" (art. 1, par. 1, c), g)) and "*custodian wallet providers*" (art. 1, par. 1, c) h)). In so doing, the European Legislator refused to provide any customised measure in relation to their specific features, preferring to include them under the "traditional" framework[552]. Actually, it has been pointed out that the applicable AML/CFT regime to these new obliged entities appears to be more limited than the traditional one, as the V AML Directive does not establish an obligation for Member States to set up a central database to register the issuers identities and wallet addresses accessible by the national Financial Intelligence Units (FIUs)[553].

With regard to the exchanges providers between virtual ad fiat currencies, it is clear that the Directive covers centralised exchanges, which convert virtual currencies to fiat and vice versa against payment of a fee, including ATMs and kiosks[554]. More uncertainties, however, surround the possible inclusion of decentralised exchanges, which merely provide the platform where users perform such transactions: while some commentators underline the essential role of the provision of the platform and the fact that some decentralised exchanges also charge transaction fees to argue in

---

Directive does not require the global acceptance of virtual currencies in order to include them under its scope, Recital 11 expressly states that currencies that "'are used in very limited networks such as a city or region and among a small number of users" (i.e., local or complementary currencies) cannot be considered as virtual currencies under the meaning of the Directive, thereby leaving uncertainty on the minimum number of users required for a virtual currency to be classified as medium of exchange.

[551] S. DE VIDO, "All that Glitters is not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive", in . DPCE Online, Vol. 38 (1), April 2019, 72.

[552] G. SOANA, *Ibid.*, 7.

[553] S. LOOSVELD, *Ibid*, 2.

[554] V. COVOLO, *Ibid.*, 235.

favour of their inclusion under the V AML umbrella[555], others claim that this extension is not evident and question its opportunity[556].

In regard to custodian wallet providers, the Directive defines them as "*entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies*" (art. 1, al. 2, d), 19)). Again, the European Legislator decided to cover only certain types of wallet providers, choosing to regulate only those that keep the private keys of the users and thereby leaving a great number of entities involved in such services out of the scope of the Directive. On this basis, it has been pointed out that while virtual currencies-to-virtual currencies exchanges are not covered as exchange providers, they could fall under the application users[557]; however, others underline how this would go beyond the scope of the Directive[558].

Undoubtedly, the Directive leaves out numerous actors involved in virtual currencies (i.e., virtual assets) activities, and while some exclusions seems to be justified in the light of a balanced and proportionate approach (such as miners[559] and users[560]), others have been criticised. This is the case of tumbler services[561], and especially of ICOs, whose importance in the virtual assets market is growing.

---

555 L. HAFFKE, M. FROMBERGER & P. ZIMMERMANN, *Ibid.*, 134.

556 In this sense, G. SOANA, *Ibid*.,6: "*this extension is not automatic, especially when such platforms perform this bulletin board activity not only for cryptocurrencies but for a wide array of goods. It is also questionable whether it is correct to burden such basilar services with demanding duties as those provided by the anti-money laundering legislation*".

557 L. HAFFKE, M. FROMBERGER & P. ZIMMERMANN, *Ibid.*, 134. On this point, the Authors remark that it would be sufficient that the VC-to-VC exchange requires its users to manually enter their private keys every time they want to carry out a transaction, without storing them, to escape the EU regulatory framework. In this way, theoretically the AML/CFT measures would be unapplied; however, the Authors do not wish for a regulation which would encompass all the types of wallet providers, since this would be an overregulation as cash can still be anonymous.

558 See, V. COVOLO, *Ibid.*, 237.

559 In this sense: L. HAFFKE, M. FROMBERGER & P. ZIMMERMANN, *Ibid.*, 137-138. See also COVOLO, who highlights the fact that during the draft of the Proposal the Commission pointed out that the massive location of miners in China 'would make any initiative largely impossible to enforce': V. COVOLO, *Ibid.*, 238.

560 Interestingly, the V AMLD invites the commission to ponder the possibility to establish a system for self-declaration that would enable VC users to voluntarily identify themselves to the competent authorities. However, its effectiveness in terms of prevention of criminal activities has been questioned: V. COVOLO, *Ibid.*, 238.

561 L. HAFFKE, M. FROMBERGER & P. ZIMMERMANN, *Ibid.*, p. 129.

Indeed, the fact that the V AML Directive is limited to virtual-fiat exchanges exclude from its scope the majority of ICOs, as most of them sell tokens for other virtual currencies (i.e. virtual assets) and not for fiat currencies[562], in this way creating a situation of inequal treatment in terms of AML/CFT scrutiny between ICOs and IPOs, their corresponding in the fiat world[563].

In the light of the analysis of the V AML Directive, the current European framework on virtual assets appear to be not sufficient to address their complexity and leaves numerous gaps an open questions, not only in relation to the selective approach in the choice of the new obliged entities – which has been accused of deviating from the FATF risk-based approach in favour of a rule-based approach[564] - but also on its concrete applicability, since the territorial location of exchanges and wallet providers, and therefore the applicability of V AML Directive, is not always easy to determine[565].

Overall, despite being adopted in 2018 – just few months before the amendment to FATF Recommendation 15 – it clearly shows an approach based on the prior work of the FATF, both in the terminology used and in the choice to merely target the points of intersection between fiat and virtual currencies, in this way embracing the same approach of the 2015 FATF Guidance – an approach that the FATF would abandon shortly afterwards.

---

562 V. COVOLO, *Ibid.*, 236.

563 In fact, while IPOs are launched by financial institutions scrutinised for AML/CFT purposes, in the case of ICOs the users buy directly from the issuer, which is not subjected to any AML/CFT scrutiny: L. HAFFKE, M.FROMBERGER & P. ZIMMERMANN, *Ibid.*, 137.

564 P. GODINHO SILVA, "Recent developments in EU legislation on anti-money laundering and terrorist financing", *Ibid.*, 62.

565 S. DE VIDO, "All that Glitters is not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive", *Ibid.*, p. 74 : the Author underlines that a provisional similar to the one included in the GDPR would have been highly desirable in order to expand the territorial reach of the V Directive: "*A provision that would have mirrored the one included in the regulation would have been a huge step forward, and would have been an important attempt to respond to the challenges posed by the virtual world*".

4.2 The new initiatives to boost the UE AML/CFT regulatory framework

In the light of rapid evolution and growth of Virtual Assets, the European Union has worked intensively to expand its action and to cover the vulnerable areas interested by the rise of Virtual Assets, as the measures set out by the V AML Directive soon appeared to be too limited[566].

Following the 2020 Action Plan (*supra* Chapter I, § 4.4.3), on 20 July 2021 the European Commission issued a package of new proposals in order to deeply amend the AML/CFT regulatory framework, which has been favourably welcomed both by the European Parliament[567] and by the Council[568]. With the aim to enhance the scope and the effectiveness of the EU action and to improve harmonisation and cooperation among Member States, the package contains four proposals, which operate at different levels, namely: i. a proposal for the for the creation of a new Union Anti-Money Laundering Authority (AMLA)[569], ii. a proposal for a new Regulation on AML/CFT[570], iii. a proposal for a new VI AML Directive[571] - which

[566] Even before the deadline for the transposition of the V AML Directive, indeed, the need to enhance the legislative framework had already emerged: Communication from the Commission to the European Parliament and the Council "Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework" 24.7.2019 COM(2019) 360 final. On the same note, the 2019 Supranational Risk Assessment directly addressed the need to extend the regulatory scope in the field of Virtual Assets: "*while the 5th Anti-Money Laundering Directive provisions on virtual currency providers and custodian wallet providers are a first regulatory step, the increasing use of such instruments is posing higher risks and further regulatory steps may be needed"*: Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities COM(2019) 370 final.

[567] European Parliament Resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission's Action Plan and other recent developments (2020/2686(RSP))

[568] Council Conclusions on anti-money laundering and countering the financing of terrorism (12608/20).

[569] COM (2021) 421 final Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010.

[570] COM (2021) 420 final Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[571] COM (2021) 423 final Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849.

would repeal the IV AML Directed as amended by the V AML Directive – , and iv. a proposal for the revision of the 2015 Regulation on Transfers of Funds[572].

The creation new central Authority is of particular interest, since it will replace the current State-based AML/CFT supervision, whose quality and effectiveness proved to be uneven across Member States and inadequate to address cross-border issues: it will represent the centrepiece of an integrated AML/CFT supervisory system, provided with coordination powers, and also with direct supervision in case of risk cross-border financial sector obliged entities.

However, for the purpose of this work, the other three proposals appear to be particularly relevant, as they address the challenges posed by Virtual Assets to the AML/CFT regulatory framework. Nonetheless, alongside the proposals included in this package, another EU legislative initiative appears to be relevant in the regulation of Virtual Assets, as it provides definitions that are used also by the Proposals, namely the Proposal for a Markets in Crypto-Assets Regulation (MiCA)[573].

4.2.1 From "virtual currencies" to "crypto-assets": the choice made with the proposed MiCA Regulation

Being part of the Digital Finance package[574], the proposal for a MiCA Regulation is aimed at establishing a sound legal framework while supporting innovation and fair competition, as well as ensuring investor protection, market integrity, and financial stability. More precisely, MiCA sets out harmonised requirements for

[572] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

[573] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937 (COM/2020/593 final).

[574] The Digital Finance Package includes a new Strategy on Digital Finance for the EU (COM(2020)591), a proposal for a Regulation on a Pilot Regime for market infrastructures based on distributed ledger technology (COM(2020)594), a proposal for a Regulation on digital operational resilience for the financial sector (COM(2020)595), and a proposal for a Directive to clarify or amend certain related EU financial services rules (COM(2020)596).

issuers that seek to offer their crypto-assets across the Union and crypto-asset service providers wishing to apply for an authorisation to provide their services in the Single Market, and establishing different rules for the specific subset of asset-referenced tokens and significant asset-referenced tokens (i.e., Stablecoins and Global Stablecoins)[575].

Issued in 2020, after slightly more than two years the agreed text of MiCA Regulation has been released, bringing amendments to the original proposal which are relevant also for the purpose of this work, as they amend the terminology and the definitions to be applied to the world of virtual assets in the context of the EU regulation – including the AML/CFT sector[576].

Article 3 of the agreed text, indeed, establishes the definitions of crypto-assets, crypto-assets providers, and crypto-assets services, thus embracing the terminology already used by most of the standard setting bodies involved in virtual assets markets (*supra* § 3).

Article 3, par. 1, 2) defines crypto-assets as the "*digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology*", while "*crypto-asset service provider' means legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset*

[575] In this respect, it is interesting to notice that the EU shares the same concerns showed by the 2021 FATF Guidance and remarked by the Basel Committee, which suggests a differentiated approach. On this point, the EU Legislator considered to regulate under the E-Money Directive Stable Coins "*whose value is backed by one single currency that is legal tender are close to the definition of e-money under the Electronic Money Directive. The aim of many 'stablecoins' is to create a "means of payments" and, when backed by a reserve of assets, some 'stablecoins' could become a credible means of exchange and store of value. In that sense, 'stablecoins' can arguably have common features with e-money*". However, the E-Money Directive would not address all the challenges posed by stable coins – and especially the potential systemic risks posed by Global Stable Coins; hence, the EU Legislator opted for a tailored framework, which integrates some aspects of the E-Money Directive nonetheless. For an overview of the structure of the proposal of MiCA Regulation: D. A. ZETZSCHE, F. ANNUNZIATA, D. W. ARNER, R. P. BUCKLEY, "The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy", in *Capital Markets Law Journal*, Vol. 16 (2), 2021, 203-225.

[576] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA) - Letter to the Chair of the European Parliament Committee on Economic and Monetary Affairs, Council of the European Union, 13198/2.

services to third parties on a professional basis, and are allowed to provide crypto-asset services in accordance with Article 53"[577], such services being: " *(a) the custody and administration of crypto-assets on behalf of third parties; (b) the operation of a trading platform for crypto-assets; (c) the exchange of crypto-assets for funds; (d) the exchange of crypto-assets for other crypto-assets; (e) the execution of orders for crypto-assets on behalf of third parties; (f) placing of crypto-assets; (fa) providing transfer services for crypto-assets on behalf of third parties; (g) the reception and transmission of orders for crypto-assets on behalf of third parties (h) providing advice on crypto-assets; (hb) providing portfolio management on crypto-assets*"(art. 3, par. 1 , 9))[578].

Despite not choosing not to borrow the FATF terminology, it is clear that the definitions set above respond to the same approach; however, while the original Proposal itself stated that "*any definition of 'crypto-assets' should therefore correspond to the definition of 'virtual assets' set out in the recommendations of the Financial Action Task Force (FATF)*", and that crypto-assets*"should also encompass virtual asset services that are likely to raise money-laundering concerns and that are identified as such by the FATF*" (Recital No. 8), and the agreed text confirms merely recalls the importance of promoting convergence in the treatment of cryptoassets and crypto-asset, recalling the FATF, as well as the Financial Stability Board and the Basel Committee (Recital No. 5 c)).

[577] Whereas the original text of the Proposal defined crypto-assets service providers as "*any person whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis*". Article 53 establishes the requirement for obtaining the authorisation to provide crypto-assets services.

[578] Art. 3, par. 9, c) stated: "the exchange of crypto-assets for fiat currency that is legal tend"; letters fa) and hb) have been added by the Agreed text. Moreover, Nos. 10 to 17b establishes definitions of the services listed by No. 9.

4.2.2 The proposed new EU AML/CFT framework: the impact on Virtual Assets regulation

Until now, the European Legislator chose to regulate the AML/CFT field through the instrument of the Directive, which allows for a higher degree of flexibility in the choice of the national instruments and strategies to achieve the goals set at the EU level. The new package of proposals, however, marks a decisive shift: indeed, it splits the regulation in two different initiatives with different scopes, and does so through two different instruments, namely a proposed Directive, which will repeal the V AML Directive, and a proposed Regulation.

Interestingly, while the proposed Directive appears to be presented as the next VI AML Directive, it merely focuses on the organisation of the institutional AML/CFT system at national levels, especially on the functioning of the FIUs[579]: therefore, the regulation of the private sector – which is the most relevant for the purpose of the present work – is left to the proposed Regulation (Proposal). The choice to resort for the first time to the instrument of Regulation in the AML/CFT field, can be explained on the basis of the need to level out regulatory differences in a more incisive manner than the instrument of the Directive would allow, also in the light of the challenges posed by virtual assets, which constitute one of the main focuses of the proposed Regulation. Indeed, given the rapid technological developments and the further steps taken by the FATF since the adoption of the V AML Directive, the Proposal acknowledges the need to bolster the regulation on virtual assets[580], and brings some relevant novelties.

---

[579] For a comment on the role of FIUs in the light of the new proposals: F. A. SIENA, "The European anti-money laundering framework – At a turning point? The role of financial intelligence units", in *New Journal of European Criminal Law*, Vol. 13 (2), 2022, pp. 216-146.

[580] Recital No. 6 of the Proposal: "*Technology keeps evolving, offering opportunities to the private sector to develop new products and systems to exchange funds or value. While this is a positive phenomenon, it may generate new money laundering and terrorist financing risks, as criminals continuously manage to find ways to exploit vulnerabilities in order to hide and move illicit funds around the world. Crypto-assets service providers and crowdfunding platforms are exposed to the misuse of new channels for the movement of illicit money and are well placed to detect such movements and mitigate risks. The scope of Union legislation should therefore be expanded to cover these entities, in line with the recent developments in FATF standards in relation to crypto-assets*".

First of all, some considerations on the change in the terminology and definitions adopted are necessary. The proposed Regulation, indeed, expressively recalls the definitions of crypto-assets, crypto-assets service providers, and crypto-assets services elaborated by the proposed MiCA Regulation (respectively, article 3, par. 1, 2), 8), 9)), which replace the previous definition adopted in the context of the AML/CFT framework with the V AML Directive. A part from the terminology used, the definition of "crypto-assets" appears to be broader than the definition of "virtual currencies" established by the V AML Directive: the new definition of crypto-assets, indeed, does not refer to the lack of issue or guarantees of a central bank or a public authority, nor to the lack of legal tender; rather it underlines its double nature of digital representation not only of value, but also of *rights*, which can simply be transferred and store electronically – without classifying it as means of exchange – using a distributed ledger or similar technology. On the other hand, while the definition of "virtual assets service providers" laconically stated that referred to "*providers engaged in exchange services between virtual currencies and fiat currencies*" (art. 1, par. 1, c), g)) of V AML Directive), the new definition of "crypto-asset service providers", to be read together with the definition of "crypto-asset services", appears to be tailored to the one elaborated by the FATF, also on the fact that wallet providers are now included in the bigger category of "crypto-asset service providers".

Accordingly, by introducing crypto-assets providers among the obliged entities (art. 3, par. 1, 3), g), the proposed Regulation extends its reach to crypto-to-crypto activity, in this way aligning with the position of the FATF and significantly expanding on the V AML Directive.

However, the proposed Regulation does not seem to overcome the limit already encountered by the V AML Directive and by the work of the FATF as well, namely the regulation of unhosted wallet providers; nonetheless, it seems to have taken a little step ahead by prohibiting the provision and the custody of anonymous crypto-asset wallets. Showing a specific concern in relation to the risks posed by the higher level of anonymity granted by crypto-assets, indeed, article 58 forbids credit and

financial institutions, as well as crypto-asset service providers from "*keeping anonymous accounts, anonymous passbooks, anonymous safe-deposit boxes or anonymous crypto-asset wallets as well as any account otherwise allowing for the anonymisation of the customer account holder"* and establishes that *"owners and beneficiaries of existing anonymous accounts, anonymous passbooks, anonymous safe-deposit boxes or crypto-asset wallets shall be subject to customer due diligence measures before those accounts, passbooks, deposit boxes or cryptoasset wallets are used in any way".* Besides the novelties brought in relation to the AML/CFT regulation of Virtual Assets, it is worth to underline that the proposed Regulation also focuses on crowdfunding platforms –which, as seen in Chapter II, are more and more used as a mean to collect funds, also for terrorist purposes – by extending its scope to those crowdfunding platforms which are not licensed under Regulation (EU) 2020/1503[581].

While the Proposal is yet to be approved, some criticism have already been raised, as it has been suggested that the European Union, instead of solely implementing the work of the FATF, could have chosen to adopt a new approach based on the characteristics of the blockchain technology[582].

[581] Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937.

[582] G. SOANA, *Ibid*, p. 11: "*By customizing the regulation to the characteristics of blockchain technology, shifting the focus from the intermediaries towards the ledger, there would not only be a relevant amelioration in the effectiveness of control there would also be an economic effect. Indeed, the expansion of the regulated entities under the FATF guidelines entails that a whole set of nascent players will need to build the capacity to guarantee compliance with the AML legislation. This implies a relevant burden on any new venture in the cryptocurrency market and, therefore, a strong check to the market development. The European Union, by introducing a legislation that harnesses the opportunities of blockchain's ledger in terms of financial integrity and reduces the pressure on intermediaries could become an attractive market for blockchain ventures. A favorable, while fair, regulation is a key factor for the development of a market. In this sense, the EU could become a global standard-setter in this field while also creating a favorable regulatory environment for cryptocurrencies' related start-ups. Unfortunately, the EU does not seem inclined to seize this opportunity. Indeed, based on the proposal presented by the Commission on July 2021 on a new regulatory package on AML/CFT, the Commission simply aims at adapting to the new FATF guidelines, this way perpetuating this incomplete policy approach*".

4.2.3 The EU implementation of the FATF "Travel Rule" to crypto-assets

The last piece of the package proposals is represented by the proposal for a Regulation for the revision of the 2015 Regulation on Transfers of Funds, which will enable to trace transfers of crypto-assets[583].

This proposal represents a further step in the alignment with the work of FATF, as it introduces into the EU legislation the information-sharing obligations set by the Recommendation 16, which now applies also to virtual assets transfers (s*upra* § 2.2.2). Borrowing the new terminology established by the proposed MiCA Regulation in relation to crypto-assets and crypto-asset service providers, in fact, the proposal extends the scope of the V AML Directive – in order to include the transfers of crypto performed through crypto-asset service providers, as they currently apply only to "funds", defined as "*banknotes and coins, scriptural money and electronic money*" (art. 4, par. 1, 25) of Directive 2015/2366)[584]. As a consequence, the Proposal establishes that its provisions "*shall apply to transfers of funds, in any currency, or crypto-assets which are sent or received by a payment service provider, a crypto-asset service provider, or an intermediary payment service provider established in the Union*" (art. 2, par. 1), and defines "transfer of crypto-assets" as "*any transaction at least partially carried out by electronic means on behalf of an originator through a crypto-asset service provider, with a view to making crypto-assets available to a beneficiary through a crypto-asset service provider, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator and that of the beneficiary are one and the same*" (art. 3, par. 1, 10) – in this way excluding person-to-person transfer of crypto-assets from its scope.

Therefore, on the one hand the obligations of crypto-asset service provider of the originator when performing a transfers of crypto-assets will be the following: giving the name, the account number – where it exists and is used to process the

[583] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (COM(2021) 422 final).

[584] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

transaction, the address, the official personal document number, and the customer identification number of the date and place of birth of the originator, as well as ensuring that transfers of crypto-assets are accompanied by the name of the beneficiary and the beneficiary's account number - where it exists and is used to process the transaction. On the other hand, the crypto-asset service provider of the beneficiary must ensure that the information on the originator is included in, or follows, such transfers, as well as implementing effective procedures to detect whether the required information on the originator or the beneficiary is missing.

5. The Italian AML/CFT regulatory framework on Virtual Assets

The centrepiece of the Italian regulatory framework on anti-money laundering and terrorism financing is represented by the Legislative Decree 21 November 2007, No. 231, through which the Italian Legislator transposed the III AML Directive[585]: from that moment on, indeed, it has been periodically amended in order to welcome the evolution of the AML/CFT legislative framework at the supranational level.

With regard to Virtual Assets, as early as in 2015, the Bank of Italy issued a warning on their possible risks, recalling the 2014 FATF Report on virtual currencies[586], and, given the growing concerns around their possible use and misuse, the Italian Legislator has been particularly proactive to seek to fit these new instruments within the regulatory framework. Indeed, Legislative Decree of 25 May 2017 No. 90, through which Italy amended Legislative Decree 231/2007 in order to transpose the IV AML Directive[587], anticipated the European Legislator. In fact, as

[585] Legislative Decree 21 November 2007, No. 231, "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione".

[586] Avvertenza sull'utilizzo delle cosiddette "valute virtuali", Banca d'Italia, 30 gennaio 2015.

[587] Legislative Decree 25 May 2017, No. 90, "Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e

abovementioned, the European Union started to address the challenges posed by Virtual Assets to the AML/CFT framework only with the V AML Directive – yet, Legislative Decree 90/2017 not only introduced a first definition of virtual currencies, identified as "*digital representation of value, not issued by a central bank or public authority, not necessarily backed by a legal tender currency, used as means of exchange for the purchase of goods and services and transferred, stored and negotiated electronically*" (art. 1, par. 2, lett. qq)[588], but it also added "service providers related to the use of virtual currencies" among the list of obliged entities, and defined them as "*every physical or legal person that professionally provides third parties services in order to use, exchange, storage virtual currencies and their conversion to or from fiat currencies*" (art. 1, par. 1, ff))[589], and also required them to be registered in a special section the register of the "*Organismo degli Agenti e dei Mediatori*" (OAM) (art. 8, par. 1).

These provisions undoubtedly represented a remarkable standpoint of the Italian Legislator; still, the scope of the Legislative Decree 90/2017 on Virtual Assets was quite limited, as it covered only those exchanges converting virtual currencies from or into fiat currencies and did not address the role played by wallet providers.
This gap was filled two years later with the transposition of the V AML Directive through Legislative Decree of 4 October 2019, No. 125[590]: pursuant to the provisions contained in the V AML Directive, the Italian Legislator updated the regulatory framework on Virtual Assets by amending the definition of virtual currencies previously set out, extending its reach to cover virtual currencies service providers

attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006".

[588] Art.. 1, par. 1, qq): "*valuta virtuale: la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*".

[589] Art. 1, par. 1, ff): "*prestatori di servizi relativi all'utilizzo di valuta virtuale: ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale*".

[590] Legislative Decree of 4 October 2019, No. 125, "Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonché attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE".

which perform virtual-to-virtual operations, and adding custodian wallet providers to the list of obliged entities (art. 1, par. 1 g))[591].

Looking closer to the definition of virtual currencies, now it goes as follows: "*digital representation of value, not issued nor guaranteed by a central bank or public authority, not necessarily backed by a legal tender currency, used as means of exchange for the purchase of goods and services or for investment purposes and transferred, stored and negotiated electronically"*(art. 1, par. 1, h))[592]. It is interesting that – although choosing to maintain the term of "virtual currencies" instead of adopting the term of "virtual assets" developed by the FATF with the new Recommendation 15 at the time recently adopted – the amendments brought to it can be read in the sense of a deeper understanding of their nature, as it is clarified that they are nor issued nor guarantee by central banks or public authorities, and that the possible functions of these technologies is not limited to payment or exchange functions, but could also serve as "means of investment".

Shifting the attention on obliged entities, on the one hand now the definition of "virtual currencies providers" covers all the five functional activities as set out by the FATF: " *any physical or legal person which professionally provides to third parties, also online, services in order to use, exchange, or store virtual currency and to convert them to fiat value or to digital representation of value, including those convertible to other virtual currencies, as well as issuing, offering, transfer and compensation services, as well as any other service in order to acquire, negotiate or intermediate in the exchange of the currencies themselves"* (art. 1, par. 1, f))[593]. On the other hand, the Legislative Decree has included custodian wallet providers among obliged entities, yet limited to

---

[591] Art. 1, par. 1, g): "*all'articolo 1, comma 2, dopo la lettera ff) è aggiunta la seguente: "ff-bis) prestatori di servizi di portafoglio digitale: ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*"".

[592] Art. 1, par. 1, h): "*all'articolo 1, comma 2, lettera qq), dopo le parole «non emessa» sono inserite le seguenti: «né garantita» e dopo le parole «di beni e servizi» sono inserite le seguenti: «o per finalità di investimento*".

[593] Art. 1, par. 1, f): "*all'articolo 1, comma 2, lettera ff), dopo le parole «a titolo professionale,» sono inserite le seguenti: «anche online,» e dopo le parole «aventi corso legale» sono aggiunte le seguenti: «o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute»*".

custodian ones, which are " *any physical or legal person which professionally provides third parties, also online, private cryptographic storage services on the behalf of their clients, with the purpose of holding, memorising and transferring virtual currencies"* (art. 1, par. 1, ff-bis))[594].

Therefore, nowadays exchanges and custodian wallet providers are subject to are subject to the full set of AML/CFT measures, know your customer measures, information storage, suspicious transactions reports, in this way being on the same page with the V AML Directive. Nevertheless, this framework cannot be deemed as entirely effective to tackle the challenges posed by the ever-evolving technological developments surrounding the world of Virtual Assets, and much has to be expected from the transposition at the national level of the EU package proposal on the AML/CFT framework.

[594] Art. 1, par. 1, ff-bis): "*prestatori di servizi di portafoglio digitale: ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*".

CHAPTER IV

STEMMING THE FLOW OF FUNDS VIA ASSET FREEZE AND ASSET RECOVERY: WHERE DO VIRTUAL ASSETS STAND?

SUMMARY: *Section I – Stemming the flow of funds: asset freezing measures via targeted sanctions* 1. 1. The development of the United Nations sanctioning system: from general to targeted sanctions 1.1 Targeted sanctions against terrorism: the blacklisting system designed by Resolution 1267 (1999)… 1.2 And the autonomous sanctions under Security Council Resolution 1373 (2001) 2. The FATF endorsement of asset freezing measures 3. The implementation of the United Nations targeted sanctions at the European Union level 3.1 Before the Treaty of Lisbon 3.2 After the Treaty of Lisbon 3.3 The tension between UN and EU orders: finding the right balance 4. The Italian legal framework on the implementation of targeted sanctions *Section II – Stemming the flow of funds: the application of confiscation to terrorist offences* 5. The expansion of confiscation: from profit-driven crimes to terrorist offences 6. The Council of Europe Conventions on confiscation 7. The FATF focus on cross-border asset recovery 8. The development of the European Union legal framework on confiscation 9. The Italian legal framework on confiscation 9.1 Confiscation and terrorism financing terrorism *Section III – Virtual Assets, asset freezing and confiscation measures: key issues* 10. The application of targeted sanctions and confiscation to Virtual Assets: possible challenges

Section I – Stemming the flowof funds: asset freezing measures via targeted sanctions

1. The development of the United Nations sanctioning system: from general to targeted sanctions

Under Chapter VII of the UN Charter, article 41 establishes the power of the Security Council to "*decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures*", which may consist of *"complete or partial interruption of economic*

relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations". Aimed at maintaining or restoring international peace and security (art. 39 UN Charter), these measures – commonly referred to as "sanctions"[595] – have been rarely applied until the beginning of the Nineties[596], when the Security Council adopted a consistent set of heavy general sanctions directed against Iraq (1990-2003)[597]. Due to the significant humanitarian consequences suffered by the population (i.e., collateral damages), the Security Council slowly shifted to targeted sanctions[598], also known as "smart" sanctions on the basis of their capacity to hit only the desired target – just like "smart" bombs. Indeed, while general sanctions are directed against States, targeting their economy (e.g., total embargoes or commercial sanctions), targeted sanctions are directed against specific individuals – both natural and legal persons – and usually include restrictions to their freedom of movement and asset freezing measures[599].

At a closer look, however, targeted sanctions entail a number of issues too[600]. In this respect, it has been pointed out that, while States are usually able to defend their position in public sessions of the Security Council before the sanctions were imposed, individuals do not have this chance, either before or after their imposition, and sanctions are applied to them only on the basis of suspicion, whereas usually

---

595 As there is no universal definition of "sanctions", often "sanctions" and "measures" are interchangeably used, both by the United Nations and the European Union: L. PASCULLI, *Ibid.*, 195 ss.

596 Until that moment, only two sets of sanctions had been adopted, namely against Southern Rhodesia (S/RES/232 (1966); S/RES/2S3 (1968)) and South Africa (S/RES/418 (1977)).

597 Started with S/RES/661 (1990), adopted by the Security Council at its e 2933rd meeting on 6 August 1990 and terminated with S/RES/1483 (2003), adopted by the Security Council its 4761st meeting on 22 May 2003. However, few months later a new sanctions committee – establishing only targeted sanctions – was created: S/RES/1518 (2003), adopted by the Security Council at its 4872nd meeting on 24 November 2003.

598 For a comment on the alleged "humanitarian" shift from general to targeted sanctions: M. CRAVEN, "Humanitarianism and the Quest for Smarter Sanctions", in *European Journal of International Law*, Vol. 13 (1), 2002, 43-61.

599 On the distinction between the different typologies of UN sanctions: A. CIAMPI, "Sanzioni del Consiglio di Sicurezza e diritti umani", Giuffré, 2007, 26 ss.

600 For a critical analysis of targeted sanctions as a modern practice of banishment: M. DE GOEDE, "Blacklisting and the ban: Contesting targeted sanctions in Europe", in *Security Dialogue*, Vol. 42 (6), 2011, 500.

the responsibility of a State is much more documented[601]. Furthermore, a distinction has to be made between targeting political leaders or élites, and targeting common civilians, as the asymmetry of powers is even more striking in the latter case: information at the basis of the decision of targeting civilians, indeed, are not disclosed, while in case of political leaders the reasons are public and often debated, and leaders have institutional ways of challenging such allegations[602].

At the end of the Nineties, the practice of smart sanctions started to be tested against political leaders and rebel groups, (e.g. members of Uniao Nacional para a Independencia Total de Angola-UNITA)[603], and, with the famous Security Council Resolution 1267 (1999), against the Taliban to counter the terrorist threat.

However, the adoption of smart sanctions as a strategy to counter terrorism acquired a new, bigger dimension after the 9/11 attacks, which led to the creation of another wider sanctions system pursuant to Resolution 1373 (2001) and in the update of the sanctions regime established by Resolution 1267 (1999), which first resulted in targeting also common civilians suspected of being associated with Al-Qaeda and in the removal of the territorial link to the territory of Afghanistan, and then in the extension of the terrorist threat addressed. In particular, the sanctions system of 1267 Committee has called attention to the issues related to application of targeted sanctions – namely the protection of individual rights – which, due to its peculiar characteristics, resulted to be amplified[604].

---

[601] L. VAN DEN HERIK, N. SCHRIJVER, "Eroding the Primacy of the UN System of Collective Security: The Judgment of the European Court of Justice in the Cases of Kadi and Al Barakaat", in *International Organizations Law Review*, Vol. 5 (2), 332.

[602] A. ADDIS, "Targeted Sanctions as a Counterterrorism Strategy", in *Tulane Journal of International and Comparative Law*, Vol. 19 (1), 2010, 194-195.

[603] S/RES/1127 (1997), adopted by the Security Council at its 3814th meeting on 28 August 1997; S/RES/1173 (1998), adopted by the Security Council at its 3891st meeting on 12 June 1998; S/RES/1176 (1998), adopted by the Security Council at its 3894th meeting on 24 June 1998.

[604] Indeed, we remind that within the Security Council there are multiple Sanctions Committee, aimed at tackling different situations. Currently there are other thirteen ongoing sanctions regime, namely concerning Somalia (S/RES/751 (1992)), Iraq/Kuwait (S/RES/1518 (2003)), the Democratic Republic of the Congo (S/RES/1533 (2004), Sudan (S/RES/1591/2005)), Lebanon (S/RES/1636 (2005)), Democratic People's Republic of Korea (S/RES/1718 (2006)), Libya (S/RES/1970 (2011)), Afghanistan (S/RES/1988 (2011), Guinea-Bissau (S/RES/2048 (2012)), the Central African Republic (S/RES/2127 (2013), Yemen (S/RES/2140 (2014)), South Sudan (S/RES/2206 (2015)), and Mali (S/RES/2374 (2017)).

Besides, it is interesting to remark that the United Nations practice of preventive counter-terrorism sanctions displays similar characteristics as seen in relation to the criminalisation of terrorism financing and the evolution of the AML/CFT framework, that is to say the abandon of traditional international law instruments[605].

1.1 Targeted sanctions against terrorism: the blacklisting system designed by Resolution 1267 (1999)…

The cornerstone of the current blacklisting and sanctioning system in relation to terrorism is represented by UN Security Council Resolution 1267 (1999)[606], which, acting under Chapter VII of the UN Charter, urged Taliban to immediately stop providing safe havens and training for terrorist purposes, to take effective measures to ensure that their territory was not used to host terrorist installations and camps or for the preparation of terrorist acts, and to immediately turn over Usama Bin Laden – which was suspected to be linked to the U.S. embassies bombings in Nairobi and Dar-es-Salem (*supra* Chapter I § 2.1). Moreover, Resolution 1267 (1999) imposed a ban on travel (par. 4, a)) and, what is more important for the purpose of the present work, the freeze of Taliban's funds and other financial resources, "*including funds derived or generated from property owned or controlled directly or indirectly by the Taliban, or by any undertaking owned or controlled by the Taliban*" and "*ensure that neither they nor any other funds or financial resources so designated are made available, by their nationals or by any persons within their territory, to or for the benefit of the Taliban or any undertaking owned or controlled, directly or indirectly, by the Taliban*" (par. 4, b). In order to do so, at the same time the Resolution established a Sanctions Committee (also known as "1267 Committee") to draw and update the list of targeted individuals and entities subject to asset freezing measures, to process the

[605] For the practice of preventive counter-terrorism sanctions by the Security Council as a primary example of Global Administrative Law: V. MITSILEGAS, "EU criminal law after Lisbon : rights, trust and the transformation of justice in Europe", Hart, Oxford, 2016, 238.
[606] S/RES/1267 (1999), adopted by the Security Council at its 4051st meeting on 15 October 1999.

requests of delisting and to review the implementations report released by states (par. 6).

Therefore, Resolution 1267 (1999), inaugurated the practice of "smart sanctions" to terrorism - a trend that has been pursued and reinforced over the following years. A year after the establishment of the 1267 Committee, indeed, the Security Council adopted Resolution 1333 (2000)[607] to reiterate and expand the provisions previously set out: among others, it reinforced travel ban measures (par. 5, a)), imposed an arms embargo over the Afghan territories controlled by the Taliban (pars. 3 and 5), and demanded Taliban to stop illicit drug trafficking activities where linked to terrorism financing purposes (par. 9), and, above all, extended asset freezing measures to include the funds of Usama Bin Laden and persons and entities associated with him, including those being part of Al Qaeda (par. 8, c))[608]. Again, with Resolution 1363 (2001)[609] the Security Council requested to set up a mechanism to monitor the implementation of the measures established by resolutions 1267 (1999) and 1333 (2000) (par. 3, a)), to support states bordering Afghanistan (par. 3, b)), and to collect and evaluate reports and formulate recommendations in relation to the violation of such measures (par. 3, c)); accordingly, a Monitoring Group was created, as well as a Sanctions Enforcement Support Team for states bordering Afghanistan (par. 4, a), b)).

As a consequence of the military action guided by the U.S. forces in Afghanistan, in December 2002 the Taliban regime collapsed, and this had repercussions also on the tone of the Security Council Resolutions adopted thereafter, as they were not directed against the Afghan state anymore[610]. Indeed, Resolution 1390 (2002)[611] reiterated the asset freezing measures set out by Resolutions 1267 (1999) and 1333

---

[607] S/RES/1333 (2000), adopted by the Security Council at its 4251st meeting on 19 December 2000.

[608] In this respect, it has been remarked that "*the extension of the sanctions to Al-Qaida represented a qualitative shift in Security Council sanctions policy, Al-Qaida not being in control of any defined geographical area*": I. CAMERON, "*European Union Anti-Terrorist Blacklisting*", in *Human Rights Law Review*, Vol. 3 (2), 2003, 227.

[609] S/RES/1363 (2001), adopted by the Security Council at its 4352nd meeting on 30 July 2001.

[610] C. DI STASIO, *Ibid.*, 140-141.

[611] S/RES/1390 (2002), adopted by the Security Council at its 4452nd meeting on 16 January 2002.

(2000), but stopped the travel ban put on the Afghanistan territory (par. 1), thus imposing sanctions only against designated people and individuals, regardless of their geographical location (par. 2, b), c)), in this way displaying an open-ended character and making the Taliban/Al Qaeda sanctions regime unprecedented in its scope, both in terms of number of targets and the geographical coverage and time scale[612].

Moreover, Resolution 1390 (2002) is of particular relevance because for the first time the Security Council decided to elaborate guidelines for the 1267 Committee (par. 5, d)). Indeed, while having been established in 1999, the 1267 Committee was not provided with internal guidelines until November 2002[613], which designed an internal procedure for listing and delisting, clarified the mandate of the Committee, voting procedures and the update of the lists[614]. Still, the procedure outlined by the Guidelines raised a number of criticisms, especially in relation to the protection of human rights and due process, since the persons included in the list were still not informed of the process they were involved in until the publication of their names, and the sole remedy available for the listed persons was represented by the delisting procedure[615]. In fact, a person could be included in the blacklist on the basis of a report made by a single member State to the Committee, without the person being informed or being able to verify the information at the basis of such report. After the inclusion in the list, the person could ask to be removed only via its State of residence or citizenship, which could arbitrarily decide whether proposing the

[612] L. VAN DEN HERIK, N. SCHRIJVER, *Ibid.*, 333, who underline that these features made the sanctions system different from all others and possibly less justifiable and acceptable in the long run.

[613] Guidelines of the Committee for the Conduct of its Work. The Guidelines were first adopted on 7 November 2002, and then have been periodically revised and amended, namely on 10 April 2003, 21 December 2005, 29 November 2006, 12 February 2007, 9 December 2008, 22 July 2010, 26 January 2011, 30 November 2011, 15 April 2013, 23 December 2016, and, lastly, 5 September 2018.

[614] In this regard, it is interesting to notice that in this sense 1267 Committee was no exception, since all the other UN sanctions committees in place relied on political trust as well; the need to reinforce the protection of fundamental human rights of the 1267 Committee can be explained on the particular wide and broad characteristics of the sanctions regime itself: E. ROSAND, "The Security Council's Efforts to Monitor the Implementation of Al Qaeda/Taliban Sanctions", in *The American Journal of International Law*, Vol. 98 (4), 2004, 748-749.

[615] For an analysis: C. DI STASIO, *Ibid*., 144 ss.

request to the Committee or not; the Committee, besides, decided by consensus with a close doors procedure[616].

A first attempt to limit the backlashes of asset freezing measures was made by Resolution 1452 (2002)[617], which established certain exceptions for the release of funds if necessary for basic or extraordinary expenses (par. 1); however, the Security Council action to interrupt the flow of funds for terrorist purposes did not stop: in order to ensure the effective adoption and review of the lists issued by states, Security Council Resolution 1455 (2003)[618] introduced the obligation to regularly submit the lists of targeted persons and entities and of the assets frozen, and Security Council Resolution 1526 (2004)[619] replaced the Monitoring Group with the Analytical Support and Sanctions Monitoring Team, aimed at supporting the Sanctions Committee with technical assistance.

From the point of view of the protection of individual rights, however, the sanctioning system created was causing growing concern, both with regard to the nature of the measures imposed – which significantly restricted the right to property and personal life of people targeted – and the procedure adopted. In this sense, a first step was taken by Resolution 1617 (2005)[620], which, along with reiterating the measures previously adopted, specified the meaning of being "associated with", in order to better define the scope of the sanctions[621], and decided that States should

---

[616] Therefore, the Guidelines did not bring significant improvements on the rights of the designate persons: A. MARSCHIK, "The Security Council's Role: Problems and Prospects in the Fight Against Terrorism", in "International Cooperation in Counter-Terrorism. The United Nations and Regional Organizations in the Fight Against Terrorism", edited by G. Nesi, Ashgate, 2005, 72-73, who underlines that, given the lack of effective legal remedies, States could use even this blacklisting system to designate dissidents or members of political opposition.

[617] S/RES/1452 (2002), adopted by the Security Council at its 4678th meeting on 20 December 2002.

[618] S/RES/1455 (2003), adopted by the Security Council at its 4686th meeting on 17 January 2003.

[619] S/RES/1526 (2004), adopted by the Security Council at its 4908th meeting on 30 January 2004.

[620] S/RES/1617 (2005), adopted by the Security Council at its 5244th meeting on 29 July 2005.

[621] S/RES/1617 (2005), par. 2: " (The Security Council) *Further decides that acts or activities indicating that an individual, group, undertaking, or entity is "associated with" Al-Qaida, Usama bin Laden or the Taliban include:*

– participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of;

– supplying, selling or transferring arms and related materiel to;

– recruiting for; or

– otherwise supporting acts or activities of;

provide the Committee a statement of case describing the basis of the proposal of listing (par. 4) and requested States to inform, preferably in written form, natural and legal persons included in the list of what kind of measures they are subjected to as well as listing and delisting procedures (par. 5).

Moreover, with Resolution 1730 (2006) the Security Council established a Focal Point under the UN Secretariat to receive requests of delisting from individuals. In this way, a new possible way for individuals to be removed from the blacklist was added, since they could now choose to request their removal via their state of citizenship or residency, or autonomously proposing their request of removal directly to the Focal Point. However, the powers of the Focal Point were quite limited: when addressed, indeed, it merely transmitted the request to the State that had previously proposed the admission to the blacklist, as well as to the State of citizenship or residency of the individual; after engaging in consultations, if one of the interested States opposed to the removal or if none of them expressed a position within three months, the request had to be intended as rejected[622]. Therefore, Resolution 1730 (2006) gave the individual the mere faculty to start the procedure[623]: individuals gained the status of "petitioners", but decisions were still taken by consensus, and individuals did not have the possibility to be auditioned during the procedure[624]. Moreover, instead of expanding the access to the delisting procedure, it has been remarked that, since States could decide to establish the procedure in front of the Focal Point as mandatory[625], the resolution could potentially limit even more the access to jurisdictional protection, as it would prevent the possibility for

Al-Qaida, Usama bin Laden or the Taliban, or any cell, affiliate, splinter group or derivative thereof".

[622] M. ARCARI, "Sviluppi in tema di tutela dei diritti di individui iscritti nelle liste dei comitati delle sanzioni del Consiglio di Sicurezza", in *Rivista di diritto internazionale*, Vol. 3, 2007, 661-662.

[623] In this respect, it has been remarked that it is a formal power, rather than a substantial one: M. ARCARI, *Ibid*. 662-663; C. DI STASIO, *Ibid*., 168-169.

[624] T. TREVES, "Diritto individuale di petizione e sanzioni "intelligenti", appunti", in "Diritti individuali e giustizia internazionale, Liber Fausto Pocar", edited by G. Venturini, S. Bariatti, Giuffre, Milano, 2009, 917.

[625] S/RES/1730 (2006), 2, note 1: "*a State can decide, that as a rule, its citizens or residents should address their de-listing requests directly to the focal point*".

individuals to enjoy jurisdictional protection within the State[626], and no judicial remedy was available at the international level[627].

Shortly after, the Security Council intervened again with Council Resolution 1735 (2006), which introduced the obligation for States to provide detailed information on the reasons at the basis of listing requests through a specific dossier and to specify which information could be made public; moreover, in case of listing request, the Resolution established that the Committee would notify within two weeks the state of citizenship or residence, which was charged to notify the interested person, together with the dossier with the public information, further information on the procedure, as well as the possibility to be removed and humanitarians exceptions (pars 10 and 11)[628]. Besides, Security Council Resolution 1822 (2008)[629] enriched the administrative procedure with more safeguards, as it required States to identify those parts of the statement of proposal that may be publicly released (par. 12), called the 1267 Committee to publish on its website the names added to the List, together with a narrative summary of reasons for listing (par. 13), and shortened the term to notify the name of the listed person to relevant state from two to one week (par. 15).

A more significant step, however, was marked with Security Council Resolution 1904 (2009)[630], which introduced an independent Ombudsperson appointed with the task of processing the requests of individuals and entities to be removed from the list. Charged with the task of collecting information, interacting with petitioners

---

[626] M. ARCARI, *Ibid*., 662-664.

[627] In this sense, it has been remarked the lack of competence of the International Court of Justice and the political nature of the Security council and the risk of abuse of blacklisting system by states for political reasons C. DI STASIO, *Ibid*., 144-147.

[628]The goal of Resolution 1735 (2006) was to improve the transparency of the procedure, but, once again, the efforts seem to be too little: the Resolution does not intervene on the periodical revision of the information at the bases of the signing up on the list, which has been remarked to be crucial in order to ensure the pre-emptive nature of the sanctions, and while Resolution 1730 addresses all the sanctions committees, Resolutions 1735 addresses only 1267 Committee; in this respect, it has been remarked the lack of a comprehensive vision, which hampers the efforts to reach a satisfactory standards of protection of fundamental rights and fairness and transparency of listing procedures: M. ARCARI, *Ibid*., 667-669.

[629] S/RES/1822 (2008), adopted by the Security Council at its 5928th meeting on 30 June 2008.

[630] S/RES/1904 (2009), adopted by the Security Council at its 6247th meeting on 17 December 2009.

and drafting reports to the 1267 Committee, the final decision on delisting was still up to the Committee – which was not bound by the position expressed by the Ombudsperson[631]. Two years later, however, the role of the Ombudsperson has been strengthened with Resolution 1989 (2011)[632], which established that recommendation to delist from the Ombudsperson would become effective it is not rejected by consensus in the Sanctions Committee within 60 days[633].

Besides the efforts to enrich listing and delisting procedures with more effective safeguards, over the years the scope of the 1267 has expanded in order to address the evolution of the terrorist threat. Indeed, Resolution 1989 (2011), together with Resolution 1988 (2011)[634], split the list of individuals and entities subject to sanctions in two different committees: the 1267 Committee thus became known as the "Al-Qaida Sanctions Committee" and a separate Committee was established by Resolution 1988 (2011) dedicated to monitor the implementation of sanctions against individuals and entities associated with the Taliban. Furthermore, with Resolution 2253 (2015)[635] the Security Council expanded the list to include individuals and entities linked to ISIL, thus becoming the "ISIL & Al-Qaida Sanctions Committee".

---

631 For these reasons, it has been noticed that while the creation of an Ombudsperson should be welcome favourably, was not sufficient to fully address the lack of due process and transparency surrounding the listing and delisting processes: A. ADDIS, *Ibid*., 197 ss. In the same sense: G. L. WILLIS, "Security Council Targeted Sanctions, Due Process and the 1267 Ombudsperson", in *Georgetown Journal of International Law*, Vol. 42 (3), 2011, 673-746.

632 S/RES/1989 (2011), adopted by the Security Council at its 6557th meeting on 17 June 2011.

633 It has been pointed out that the strengthened powers of the Ombudsperson are in response to the deficiencies underlined by Kadi II (*infra* § 3.3): J. KOKOTT, C. SOBOTTA, "The Kadi Case – Constitutional Core Values and International Law – Finding the Balance?", in *European Journal of International Law*, Vol. 23 (4), 1021. Still, it has been pointed out that the Office of the Ombudsperson would represent a "legal grey hole" – which paradoxically could be even more dangerous, as it would legitimise exceptional practices, making it more difficult to question them: G. SULLIVAN, M. DE GOEDE, "Between Law and the Exception: the UN 1267 Ombudsperson as Hybrid Model of Legal Expertise" in *Leiden Journal of International Law*, Vol. 26 (4), 2013, 833-854.

634 S/RES/1988 (2011), adopted by the Security Council at its 6557th meeting on 17 June 2011.

635 S/RES/2253 (2015), adopted by the Security Council at its 7587th meeting on 17 December 2015.

Besides, the Security Council continued to reiterate the travel ban, arms embargoes and asset freezing measures, and the mandate of the Ombudsperson has been constantly renovated – the current mandate expiring in June 2024[636].

1.2 And the autonomous sanctions under Security Council Resolution 1373 (2001)

As already illustrated (*supra* Chapter I), in the wake of the 9/11 attacks the Security Council adopted Resolution 1373 (2001), which, apart from requiring States to criminalise terrorism financing, established the freeze of "*funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist act*s", as well as "*of entities owned or controlled directly or indirectly by such persons and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities*" (par. 1, c)).

In this way, two different sanctions regime against terrorism were created: a first sanctions regime pursuant to Resolutions 1267 (1999), 1333 (2000), 1390 (2002) and a second sanctions regime pursuant to Resolutions 1373 (2001), which work in parallel. However, the two regimes present significant differences: while pursuant to the first sanctions regime is the United Nations – through the Sanctions Committee – which decides who to list, the rules regarding listing and delisting processes and the review of the list, the second sanctions regime allows each member state to autonomously identify its own terrorist suspects[637]., as well as the

[636] S/RES/2610 (2021), adopted by the Security Council at its 8934th meeting on 17 December 2021.
[637] C. ECKES, " EU counter-terrorist policies and fundamental rights: the case of individual sanctions", Oxford University Press, 2009, 19.

related listing and delisting procedures, and leaving states to cooperate on a bilateral basis in enforcing their respective freezing orders[638].

2. The FATF endorsement of asset freezing measures

Before focusing on the regional implementation of UN sanctions regimes against terrorism at the European level, it is interesting to briefly note as, from the outset, the FATF acknowledged the work of the United Nations regarding the sanction regimes against terrorists. Special Recommendation III, indeed – which addressed both asset freezing measures as well as confiscation – stated that "*each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts*".

Therefore, the FATF expressively endorsed the two sanctions regimes against terrorism established at the United Nations level, namely by Resolution 1267 (1999) – and its successor Resolutions – and Resolution 1373 (2001), underlying the fact that they "*differ in the persons and entities whose funds or other assets are to be frozen, the authorities responsible for making these designations, and the effect of these designations*" (Int. Note to S. Rec. III, 4)

Following the integration of the Special Recommendations within the Forty Recommendations and their 2012 update, currently targeted financial sanctions related to terrorism and terrorist financing are established by Recommendation 6[639],

[638] It is interesting to notice that this difference between the two systems has been linked to the lack of a shared definition of terrorism: while on Taliban – and then Al-Qaeda and ISIL - there was broad agreement, on terrorism overall there still were different positions: L. G. RADICATI DI BROZOLO, "Freezing the Assets of International Terrorist Organisations", in "Enforcing International Law Norms against Terrorism"; ed. By A. Bianchi, Hart Publishing, 2004, 396-397.

[639] Recommendation 6: "*Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under*

which does not present relevant differences from Special Recommendation III, except for the fact that it takes into account the development of the regime established by Resolution 1267 (1999) over the years; in particular, pursuant to Interpretive Note to Recommendation 6, the FATF clarifies that it supports both the "ISIL &Al Qaeda Sanctions Committee" – established by Resolutions 1267 (1999), 1989 (2011) and 2253 (2015) – as well as the separate Sanctions Committee established by Resolution 1988 (2011) dedicated to monitor the implementation of sanctions against individuals and entities associated with the Taliban.

Lastly, it is interesting to notice that FATF also endorses the United Nations targeted financial sanctions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing (Rec. 7).

3. The implementation of the United Nations targeted sanctions at the European Union level

As already underlined when analysing the criminalisation of terrorism financing (Chapter I), the European Union approach to terrorism shows a marked preventive nature, which not only shapes the criminal law provisions, but also informs the corresponding complex sanctions systems – which have been held as a "model of preventive justice", since they do not require a criminal conviction and are applied to individuals or entities under the mere suspicion of being associated to terrorism on the basis of an on-going risk assessment[640].

Formally, the European Union is not a member of the United Nations: according to art. 4 of the UN Charter, indeed, membership is open only to States, and, pursuant to articles 25 and 48 of the UN Charter, the Resolutions of the Security Council are

Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001)".

[640] V. MITSILEGAS, "EU criminal law after Lisbon : rights, trust and the transformation of justice in Europe", *Ibid.*, 236 ss. In particular, the Author clarifies that here preventive justice is understood as "*the exercise of state power in order to prevent future acts which are deemed to constitute security threats*".

binding only to Member States[641]. Nonetheless, from the outset the European Union showed a strong political will to implement the Resolutions of the Security Council regarding sanctions against terrorism, doing so through a creative use of the options offered by the European institutional architecture[642] and displaying a drop-down approach ("*a cascata*")[643].

In this regard, it is interesting to analyse the different legal basis the European Legislator resorted to when implementing such Resolutions, both in relation to the 1267 Committee and the sanctions system established by Resolution 1373 (2001).

Due to their different character, indeed, the European Union resorted to different legal instruments: the 1267 Committee, indeed, imposes the obligation to freeze the assets of identified persons and entities included in a list created and updated by the United Nations itself – thus leaving no discretion to States; on the contrary, Resolution 1373 (2001) leaves to States the choice of which individuals to impose sanctions on. Therefore, there are two separate anti-terrorist sanctions systems within the European Union: one deriving from the Security Council blacklisting and an autonomous one.

3.1 Before the Treaty of Lisbon

Before the entry into force of the Treaty of Lisbon, the European Union used to implement the sanctions established by the 1267 Committee via a combination of cross-pillar legal instruments, namely second pillar Common Positions combined with first pillar Regulations. However, the legal basis for the adoption of such

641 On the relationship between the European Union and the UN Security Council Resolutions: A. LANG, "Le risoluzioni del Consiglio di sicurezza delle Nazioni Unite e l'Unione Europea", Giuffré, 2002.

642 In this sense: V. MITSILEGAS, "EU criminal law after Lisbon : rights, trust and the transformation of justice in Europe", *Ibid*., 241.

643 V. MASARONE, "Politica criminale e diritto penale nel contrasto al terrorismo internazionale: tra normativa interna, europea ed internazionale", Edizioni Scientifiche Italiane, Napoli, 2013, 133 ss.

measures slightly changed over the years, according to the changes of the characteristics of the sanctions imposed.

Security Council Resolutions 1267 (1999) and 1333 (2000) were implemented respectively through Council Common Position of 15 November 1999 (1999/727/CFSP)[644] and Council Regulation 337/2000[645], and through Council Common Position 26 February 2001 (2001/154/CFSP)[646] and Council Regulation 467/2001[647]. Both the two Common Position were adopted under art. 15 TEU, which allowed member states to unanimously adopt Common Positions to establish the Union's approach to a matter of geographical or thematic nature, and both the two Regulations were adopted under art. 301 EC – which enabled the Council to take the necessary urgent measures to stop or limit economic relations with third countries – and art. 60 TEC – which served as a legal basis to extend the power of the Union to adopt financial restrictive measures[648].

However, after the fall of the Taliban regime and the corresponding removal of any reference of the Afghan territory, a different legal basis for the adoption of the Regulations was needed: indeed, since articles 60 and 301 TCE were aimed at addressing urgent measures against third countries, they could not serve as legal basis to justify the implementation of the Security Council's sanctions alone: an additional legal basis was needed. The European Legislator overcame this obstacle by adding art. 308 TEC to articles 60 and 301 TEC: art. 308 TEC, indeed, established the so-called "implicit powers" that the European Legislator could resort to in order to reach the goals of the Union, and has then been used to implement the Resolution

[644] Council Common Position of 15 November 1999 concerning restrictive measures against the Taliban (1999/727/CFSP).

[645] Council Regulation (EC) No 337/2000 of 14 February 2000 concerning a flight ban and a freeze of funds and other financial resources in respect of the Taliban of Afghanistan.

[646] Council Common Position of 26 February 2001 concerning additional restrictive measures against the Taliban and amending Common Position 96/746/CFSP (2001/154/CFSP).

[647] Council Regulation (EC) No 467/2001 of 6 March 2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan, and repealing Regulation (EC) No 337/2000.

[648] I. CAMERON, "EU Sanctions: Law and Policy issues concerning restrictive measures", ed. by I. Cameron, Intersentia, 2013, 8-9.

thereafter[649]. Therefore, Security Council Resolutions 1333 (2000) and 1452 (2002) were respectively implemented by Council Common Position 2002/402/CFSP[650], under art. 15 TEU and Council Regulation 881/2002[651], under art. 60, 301 and 308 TEC, and by Council Common Position 2003/140/CFSP[652] under 15 TEU and Council Regulation 561/2003[653] under art. 60, 301 and 308 TEC.

A different strategy was applied to implement Resolution 1373 (2001): indeed, the implementation of its provisions were split into two separate Council Common Positions, both adopted under a joint second and third pillar basis (art. 15 and 34 TEU)[654] on 27 December 2001: Council Common Position (2001/930/CFSP) on combating terrorism[655] and Council Common Position on sanctions against individuals (2001/931/CFSP)[656], which included a list of individuals and entities whose assets were to be frozen to be drawn up on the basis of "*precise information or material (…) irrespective of whether it concerns the instigation of investigations or prosecution for a terrorist act, an attempt to perpetrate, participate in or facilitate such an act based on serious and credible evidence or clues, or condemnation for such deed*" (art. 1, par. 4).

Moreover, Council Common Position (2001/931/CFSP) was accompanied by Regulation 2580/2001[657] , adopted under art. 60, 301 and 308 TEC, which ordered

---

[649] C. DI STASIO, *Ibid.*, 264-265.

[650] Council Common Position of 27 May 2002 concerning restrictive measures against Usama bin Laden, members of the Al-Qaida organisation and the Taliban and other individuals, groups, undertakings and entities associated with them and repealing Common Positions 96/746/CFSP, 1999/727/CFSP, 2001/154/CFSP and 2001/771/CFSP (2002/402/CFSP).

[651] Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan.

[652] Council Common Position 2003/140/CFSP of 27 February 2003 concerning exceptions to the restrictive measures imposed by Common Position 2002/402/CFSP.

[653] Council Regulation (EC) No 561/2003 of 27 March 2003 amending, as regards exceptions to the freezing of funds and economic resources, Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban.

[654] We remark here the hybrid nature of these sanctions, stretched between CFSP and criminal nature.

[655] Council Common Position of 27 December 2001 on combating terrorism (2001/930/CFSP).

[656] Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP).

[657] Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.

the asset freeze of listed persons pursuant to art. 2, par. 3, and explicitly excluded from that list persons and groups already listed pursuant to the implementation of Resolutions 1267 (1999) and 1333 (2000) (Recital No. 15).

3.2 After the Treaty of Lisbon

After the entry into force of the Treaty of Lisbon the distinction in different pillars ceased; therefore, the legal basis for the implementation of the United Nations sanctions had to change. Nowadays, the main legal basis for the implementation of sanctions is represented by art. 215 TFUE, which explicitly covers states, natural and legal persons, groups or non-State entities, as well as both financial and trade sanctions; moreover, pursuant to art. 275, par. 2 TFEU, individuals subject to restrictive measures (i.e., sanctions) have the right to appeal to the Court of Justice of the European Union[658].

Moreover, the Treaty of Lisbon also established a second legal basis to address sanctions directed against "EU internal" terrorist suspects, namely art. 75 TFEU, which, in order to be included in the list, have to constitute a threat to the European Union as a whole[659].

[658] I. CAMERON, "EU anti-terrorist sanctions", in "Research Handbook on EU Criminal Law", *Ibid*., 549. For instance, the most recent amendments to Regulation (EC) 2580/2001 explicitly recall art. 215 TFEU as main legal basis, namely Council Regulation (EU) 2016/1710 and Council Regulation (EU) 2017/2061. However, according to Protocol 36 to the Treaty of Lisbon, the Common Positions adopted prior its entry into force are still effective and do not enjoy the rights established by the new art. 215, par. 2 TFEU: M. A. MANNO, *Ibid*., 68.

[659] I. CAMERON, "EU anti-terrorist sanctions", in "Research Handbook on EU Criminal Law", *Ibid*., 549.

3.3 The tension between UN and EU orders: finding the right balance

As outlined in the previous paragraphs, the United Nations sanctions system presented many flaws, the main issue being the quest for the right balance between the adoption of effective tools against terrorism and the protection of individual fundamental rights.

This situation gave birth to a number of judicial cases within the EU, whose outcomes have contributed to improve the protection of fundamental human rights of the persons included in the UN sanctions list within the European Union. In this regard, it appears interesting to briefly recall what can be arguably held as the leading case in this context, namely the Kadi case. In 2001, Yassin Abdullah Kadi addressed the European Court of First Instance (CFI) to annul the Regulation (EC) 2001/467 on the grounds that the UN listing procedure and sanctions harmed its property rights, as well as the right to due process and to a judicial review[660]. With a highly debated judgement, the CFI refused to annul the EC Regulation on the basis that it merely transposed the obligations established by the Security Council: therefore, the CFI stated that it had no competence to review it, since doing so would amount to a review of the measures of the Security Council[661] - in this respect, the CFI clarified that it could review the obligations established by the Security Council only in case of breach of the *jus cogens* – that in that case the CFI established had not be infringed[662].

[660] Case T-315/01, *Kadi v. Council of the European Union and Commission of the European Communities*, 21 September 2005.

[661] In particular the CFI argued that the lack of power of the EC to review the Resolutions of the Security Council would lie on the grounds of international customary law, articles 5 and 27 of the Vienna Convention on the Law of Treaties (1969), and the rule of primacy laid down by art. 103 of the UN Charter – in accordance with art. 30 of the Vienna Convention, as well as art. 25 of the UN Charter: T-315/01, pars. 182-184. For a critical comment of the CFI position on the lack of powers of judicial review on the grounds of international law : P. EECKHOUT, "Community Terrorism Listings, Fundamental Rights, and UN Security Council Resolutions: in Search of the Right Fit", in *European Constitutional Law Review*, Vol. 3 (2), 190 ss.

[662] Case T-315/01, par. 238.

However, the appealed Court of Justice of the European Union (CJEU)[663] overturned the judgment of the CFI, declaring itself entitled to assess whether the Regulation would infringe individual fundamental rights and annulling Regulation *ratione personae*[664]. However, while some remarked the strong shift operated by the ECJ in respect to the previous position of the Court of First Instance[665], others underlined that, although abandoning the monistic approach adopted by the CFI resulting from an extreme integration between the international order and the European Community, the shift operated by the CJUE would not be as strong as it could seem at a first glance. Indeed, it has been remarked that, according to the reasoning of the CJUE, Security Council Resolutions remain "untouchable": the shift is operated only in relation to the power of assessing the acts of the European Union[666]; moreover, the ECJ judgment referred solely to the procedure adopted by the listing procedure, thus not embracing a full dualist approach[667]. Therefore, the ECJ would have shifted from almost complete monism to a sort of tempered dualism, informed by a logic of constitutional pluralism[668].

However, as early as 22 October 2008, Kadi was informed in written form that the Commission would maintain him in the terrorist sanctions, and that he could make observations and provide information to the Commission by 10 November 2008.

---

[663] Joined Cases C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, 3 September 2008.

[664] Joined Cases C-402/05 P and C-415/05 P, par. 374.

[665] In this sense, this judgment has been remarked as "rebellious", as it would question the primacy of the UN Security Council and possibly the UN system of collective security as a whole: L. VAN DEN HERIK, N. SCHRIJVER, "Eroding the Primacy of the UN System of Collective Security: The Judgment of the European Court of Justice in the Cases of Kadi and Al Barakaat", in *International Organizations Law Review*, Vol. 5 (2), 330.

[666] In this way, it has been noticed that the ECJ found a "smart way out of the dilemma" of taking position on the hierarchical relationship between EU/EC law and UN law: R. A. WESSEL, "Introduction to the Forum – The Kadi Case: Toward a More Substantive Hierarchy in International Law", in *International Organizations Law Review*, Vol. 5 (2), 326.

[667] However, it has been noted this dualist approach appears to be limited to the procedure: J. KOKOTT, C. SOBOTTA, "The Kadi Case – Constitutional Core Values and International Law – Finding the Balance?", in *European Journal of International Law*, Vol. 23 (4), 1019.

[668] Due to the constitutional maturity of the European legal order, that makes it different both from national and international law: G. MARTINICO, O. POLLICINO, V. SCIARABBA, "Hands off the Untouchable Core: A Constitutional Appraisal of the Kadi Case", in *European Journal of Law Reform*, Vol. 11 (3), 2009, 291.

Having submitted his comments, on 28 November 20018 the Commission adopted Regulation (EC) 2008/1190[669], which, stating to have took into account the comments presented by Kadi, decided nonetheless that there were grounds for his reintroduction in the sanctions list. As a consequence, Kadi appealed the General Court[670], which once again annulled the Regulation (EC) 2008/1190 on the basis of the infringement of the rights of defence, as Kadi could not effectively challenge the allegations against him[671]. The Commission appealed to the ECJ[672], which confirmed the annulment of the Regulation (EC) 2008/1190 on the basis that the reasons to re-list Kadi were not substantiated with evidence[673].

Moreover, also the European Court of Human Rights (ECtHR) has significantly contributed to the improvement of the protection of individual human rights of the listed persons. In particular, we can recall here the *Nada v. Switzerland* case[674], which stated that Switzerland should apply the *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities* judgment, that is to say granting an effective judicial review of the national legislation implementing the UN sanctions[675]. More recently, the ECHR has confirmed its position – although applying a different reasoning, based on the criterion of equivalent protection[676].

---

669 Commission Regulation (EC) No. 1190/2008 of 28 November 2008 amending for the 101st time Council Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban.

670 Case T-85/09, *Kadi v. Commission*, 30 September 2010.

671 Case T-85/09, pars. 171-181. For an overview of the case: T. ANDERSSON, "Developing Multiple EU Personalities: Ten Years of Blacklisting an Mutual Trust", in "EU Sanctions: Law and Policy Issues Concerning Restrictive Measures", ed. by I. Cameron, Intersentia, 2013, 89-92.

672 Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, *Commission and Others v. Kadi*, 18 July 2013.

673 For a comprehensive analysis of the judgment: V. SCIARABBA, "La Corte di giustizia, le misure antiterrorismo, i diritti fondamentali e la "Carta di Nizza": l'epilogo della vicenda Kadi", in *European rights Newsletter*, 2014, 17 ss.

674 ECtHR, Grand Chamber, *Nada v. Switzerland*, 12 September 2012.

675 For a deeper analysis of the Nada v. Swtizerland case: D. ALBRECHT, "*Nada v Switzerland*: United Nations Security Council Terrorist Sanctions Regime and Human Rights", in *Cyprus Human Rights Law Review*, Vol. 1, No. 2, 2012, 212-220.

676 ECtHR Grand Chambre, *Case Al-Dulimi And Montana Management Inc. v. Switzerland*, 21 June 2016, par. 83.

Finally, few considerations on the nature of targeted sanctions appear here to be necessary. As outlined in the previous paragraphs, targeted sanctions are inherently preventive measures, which do not require a criminal conviction in order to be adopted. However, at the European level they have been implemented via cross-pillar instruments, in this way acknowledging their hybrid nature, which has also been pointed out by the CJUE in the *Segi* case[677]. Besides, given the significant impact of targeted sanctions on private and daily life and reputation of the targeted persons, it has been suggested they would actually display a criminal nature, at least on the basis of the famous *Engels* principles[678] set out by the ECHR[679]. However, targeted sanctions are still largely considered to be preventive measures, and their possible criminal nature has not been fully acknowledged[680].

4. The Italian legal framework on the implementation of targeted sanctions

At the beginning, the Italian Legislator used to implement terrorist sanctions lists elaborated by the United Nations and by the European Union through the adoption of *ad hoc* Law Decrees[681]. However, this approach changed with Law Decree No.

[677] Case C-355/04 P, *Segi and Others v. Council of the European Union*, 27 February 2007. In its Opinion, the Advocate General Mengozzi remarked that while Common Position 2001/931 can be considered being part of the common foreign and security policy, "*some of the measures for which that act provides (…) are operational instruments and as such come within the scope of police and judicial cooperation in criminal matters under Title VI of the EU Treaty*": Joined Opinion of Advocate General Mengozzi, 26 October 2006, par. 55, Case C-355/04 P.

[678] Namely, i. the classification of the offence under national law, ii. the nature of the offence, iii. the nature and degree of severity of penalty: ECHR, Court (Plenary), Engel and others v. The Netherlands, 8 June 1976.

[679] In this sense: M. TEBALDI, " Le black lists nella lotta al terrorismo. Tra esigenze di sicurezza e tutele dei diritti", in *Diritto Penale Contemporaneo*, Vol. 7, 2018, 82.

[680] M. A. MANNO, *Ibid*., 69.

[681] This was the case of Regulation (EC) 467/2001, implemented by Law Decree 28 September 2001, n. 353, "Disposizioni sanzionatorie per le violazioni delle misure adottate nei confronti della fazione afghana dei Talibani», converted with amendments by Law 27 November 2001, n. 415. For a comment: E. ROSI, "Terrorismo internazionale: le nuove norme interne di prevenzione e repressione: Profili di diritto penale sostanziale", in *Diritto Penale e Processo*, Vol. 2, 2002, 150 ss.

369/2001[682], which established the Committee for the Financial Security (*Comitato per la Sicurezza Finanziaria*, CSF) within the Ministry of Economy and Finance (MEF), with powers of coordination and supervision of the implementation of supranational terrorist sanctions[683]. Few years later, Legislative Decree 109/2007[684], amended the mechanism previously set out, and enriched the protection of the individuals included in the lists by establishing the possibility to appeal against the decision of the CSF at national level (Tar del Lazio) (art. 14, par. 1)[685] .

Ten years later, Legislative Decree No. 90/2017)[686] amended Legislative Decree 109/2007 and expanded the powers of the CSF[687]. Nowadays, within the Italian legal system there are three different listing procedures in place: i. asset freezing measures adopted pursuant to United Nations Resolutions (art. 4), and ii. asset freezing measures adopted autonomously by the Italian Ministry of Economy and Finance (on the basis of a proposal of the CSF) pursuant to the United Nations list before their implementation at the European Union level (art. 4 *bis*); iii. moreover, according to art. 4 *ter*, the CSF has the faculty of proposing to the United Nations

---

[682] Law Decree 12 October 2001, No. 369 "Misure urgenti per reprimere e contrastare il finanziamento del terrorismo internazionale" converted with amendments by Law of 4 December 2001, No. 431.

[683] After the amendments made by Law 431/2001, the established Committee was chaired by the General Director of Treasury and is composed of eleven members appointed by the Ministry of Economy and Finance on the basis of designations made by the Ministry of the Interior, the Ministry of Foreign Affairs, Bank of Italy, CONSOB, and Italian Office of Exchanges; moreover, are part of the Committee also one manager of the Ministry of Economy and Finance, one Guardia di Finanza official, one official of the Direzione Investigativa Antimafia, of official of Arma dei Carabinieri and one representative of the Direzione Nazionale Antimafia.

[684] Legislative Decree 22 June 2007, No. 109 "Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attivita' dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE". We remind that through Legislative Decree 109/2007 the Italian Legislator implemented the III AML Directive.

[685] Before Legislative Decree 109/2007, indeed, the only judicial remedy available was the appeal to the European Court of Justice: C. DI STASIO, *Ibid.*, 598.

[686] Legislative Decree 25 May 2017, No. 90, "Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006". We remind here that Legislative Decree No. 90/2017 transposed the IV AML Directive and implemented the 2012 updated FATF Recommendations (*supra* Chapter III § 5).

[687] Pursuant to art. 3, nowadays the composition of the CSF includes the members appointed by the Ministry of Economic Development; moreover, pursuant to Law Decree 18 February 2015 No. 7, Direzione Nazionale Antimafia has become Direzione Nazionale Antimafia e Antiteterrorismo.

and European Union competent authorities the inclusion of individuals in their lists[688].

This new architecture, however, raised some concerns. The listing procedure laid down by art. 4 *quinquies* does not establish in favour of individuals any right to be informed of the procedure; in addition, it grants the right to a judicial review only against the administrative fines imposed in case of violation of obligations deriving from the inclusion in the list, which can be appealed to the Court of Rome (art. 14). In this way, the current framework takes a step back in terms of rights to defence respect to the previous art. 14 established in 2007[689], which established the faculty of appealing to the Administrative Court of Rome (TAR Lazio) against both the issues related to the listing procedure and the violations of the corresponding obligations[690].

Following the international approach, art. 2 of Legislative Decree 109/2007 remarks the preventive nature of the sanctions. Nonetheless, their effects would question its preventive nature, making it leaning towards the characteristics of criminal sanctions – notably, their highly afflictive effects on the life of the persons listed.

However, in the light of the Italian legal framework as a whole, asset freezing measures adopted by the CSF can still better considered to display a preventive nature[691].

---

[688] M. A. MANNO, *Ibid.,* 130-132.

[689] M. A. MANNO, *Ibid*., 133-138.

[690] However, it has been remarked that, following the general principle of jurisdiction, the competence to assess the listing procedure would rely on the Administrative Court of Roma (TAR LAZIO). Still, being the decision at the basis of listing characterised by a discretional nature, the judicial review would be quite limited: M. CERFEDA, "Le 'nuove' misure di congelamento nazionali e il traffico di capitali volti al finanziamento del terrorismo. Le liste degli interdetti, ultima frontiera di una prevenzione di cui vanno minimizzati i costi", in *Diritto Penale Contemporaneo*, Vol. 1, 2018, 24-25. In this respect, on the basis that preventive but highly afflictive measures set out by arts. 84, 91 Legislative Decree No. 159/2011 cannot be submitted to a proper judicial review, it has been suggested that, following the ECtHR judgment *De Tommaso v. Italia*, their constitutional legitimacy is questionable: G. AMARELLI, " L'onda lunga della sentenza De Tommaso: ore contate per l'interdittiva antimafia 'generica' ex art. 84, co. 4, lett. d) ed e) d.lgs. n. 159/2011?", in *Diritto Penale Contemporaneo*, Vol. 1, 2018, 290-299.

[691] In this sense: M. A. MANNO, *Ibid*., 133-137.

Section II – Stemming the flow of funds: the application of confiscation to terrorist offences

5. The expansion of confiscation: from profit-driven crimes to terrorist offences

At the supranational level, we have seen a renovated attention towards the instrument of confiscation starting from the Eighties, namely in relation to the proceeds of drug trafficking. The initial focus, indeed, was represented by tackling profit-driven crimes, with the two-fold purpose of deterring criminals – since confiscation would eliminate the main reason of their commission (i.e., financial gain) – and to disrupt the flows of illicit funds. In this sense, art. 5 of the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) required State Parties to confiscate the material object of crimes (e.g. narcotic drugs and psychotropic substances), instrumentalities, and proceeds, or property of value of such proceeds (i.e., value confiscation).

Starting from the Nineties, however, the scope of application of confiscation started to expand: with Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (1990) the Council of Europe established the application of confiscation beyond drug-related offences, and shortly after numerous Conventions introduced confiscation among their provisions – all of them showing also a strong interest cooperation-related matters[692]. Among them, we find also the 1999 UN Convention for the Suppression of the Financing of Terrorism (1999)[693], whose art. 8, par. 2 required State Parties to confiscate the funds used or allocated for the

[692] It is interesting to remark that also the United Nations Treaty Against Transnational Organized Crime (2000) (Palermo Convention) established the confiscation of proceeds or property the value of such proceeds of crimes covered by the Convention, as well as instrumentalities (art. 12, par. 1). For an overview of the evolution of supranational sources: A. M. MAUGERI, "Le moderni sanzioni patrimoniali tra funzionalità e garantismo", Giuffré, Milano, 2001, 64 ss.

[693] Art. 8, par. 2, 1999 UN Convention: "Each State Party shall take appropriate measures, in accordance with its domestic legal principles, for the forfeiture of funds used or allocated for the purpose of committing the offences set forth in article 2 and the proceeds derived from such offences".

commission of the offences included in art. 2 (*supra* Chapter I § 2.2) and the related proceeds – albeit omitting any reference to the confiscation of property of value of such proceeds. Indeed, the "War on Terror" led legislators to focus on the disruption of the flow of funds for terrorist purposes, which resulted to the extension of confiscation measures to terrorist offences – in this way thus extending instruments aimed to tackle acquisitive crimes to crimes not driven by profit, rather by ideological and/or political reasons[694].

However, the harmonisation of national legislations and the creation of an effective cross-border cooperation on confiscation matters has proven difficult, first and foremost because of the many – and sometimes significant – differences among countries' legislations in this field, which have hampered the efforts of finding a common ground. In addition, it has to be noted that to such varied approach corresponds a varied terminology, which could led to misunderstandings[695].

6. The Council of Europe Conventions on confiscation

The 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141) has been one of the first attempts at the international level to provide common rules on the recovery of the proceeds from crime. Art. 2, par. 1, indeed, required State Parties establish the confiscation of instrumentalities and proceeds, or property the value of which corresponds to such proceeds – thus including both traditional and value confiscation – and identified "proceeds" as "*any economic advantage from criminal offences*" (art. 1, a)), "property" as "*property of any description, whether corporeal or*

[694] M. FERNANDEZ-BERTIER, "The History of Confiscation Laws: From the Book of Exodus to the War on White-Collar Crime", in "Chasing Criminal Money. Challenges and Perspectives on Asset Recovery in the EU", ed. by K. Ligeti, M. Simonato, Hart, 2017, 71-72

[695] On the different concept of "asset recovery" between the United Nations and the European Union: "Asset Recovery in the EU: Towards a Comprehensive Enforcement Model beyond Confiscation? An Introduction", in "Chasing Criminal Money. Challenges and Perspectives on Asset Recovery in the EU", *Ibid.*, 3.

incorporeal, movable or immovable, and legal documents or instruments evidencing title to, or interest in such property" (art. 1, b)); "instrumentalities" as "*any property used or intended to be used, in any manner, wholly or in part, to commit a criminal offence or criminal offences*" (art. 1, c)); and "confiscation" as "*penalty or a measure, ordered by a court following proceedings in relation to a criminal offence or criminal offences resulting in the final deprivation of property*" (art. 1, d).

Besides, in response to the War on Terror and the focus on disrupting terrorists' financial flows, in 2005 the Council of Europe reinforced the provisions on provisional measures and confiscation, with a particular focus on terrorism financing. The 2005 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198), indeed, explicitly recalls in the Preamble the 1990 Convention, as well as Security Council Resolution 1373 (2001), par. 3 d), and expressively requires State Parties to "*confiscate property, of a licit or illicit origin, used or allocated to be used by any means, in whole or in part, for the financing of terrorism, or the proceeds of this offence, and to provide co-operation to this end to the widest possible extent*" (art. 2, par. 1) – in this way openly extending the application of confiscation to terrorism financing offences. With regards to confiscation measures, art. 3, par. 1 establishes the confiscation of the instrumentalities and proceeds, or of property value of such proceeds for a series of crimes (art. 3, par. 2), and specifies that State Parties may also provide for mandatory confiscation (art. 3, par. 3); moreover, art. 3, par. 4 requires countries to establish that the offender demonstrates the origin of alleged proceeds or other property liable to confiscation – as long as this is allowed by the principles of its domestic law.

Lastly, it is interesting to notice that the 2005 Convention further details the definition of proceeds, which are now defined at "*any economic advantage, derived from or obtained, directly or indirectly, from criminal offences*" (art. 1 par 1).

7. The FATF focus on cross-border asset recovery

As illustrated in the previous Chapters[696], the FATF plays a crucial role both as a *push* and *pull* factor for the international cooperation and harmonisation in the AML/CFT field. With regard to asset recovery, as early as in their first version issued in 1990, the Forty Recommendations invited members to implement provisional measures and confiscation following the path traced by the Vienna Convention (Rec. 8), and to enhance international cooperation, supporting international initiatives such as the Draft of the Council of Europe 1990 Convention – which then became an invitation to become part of it after the 1996 amendments (Rec. 35). Furthermore, with the extension of the FATF mandate to terrorism financing(*supra* Chapter I § 2.2), Special Recommendation III, required States to "*adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations*".

Nowadays, the FATF provisions on confiscation are located in Recommendation 4, and, with regard to cross-border cooperation, in Recommendation 38.

Recommendation 4 expressively endorses the measures on assets recovery set out by international conventions, including the 1999 Terrorist Financing Convention, requiring member States to "*enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of bona fide third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, or (d) property of corresponding value*" and to "*consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation*", as long as "*such a requirement is consistent with the principles of their domestic law*".

[696] *Supra* Chapter I and Chapter III.

Since non-conviction-based confiscation constitutes one of the main concern also within European Union cooperation among members (*infra* § 8), it is interesting to make a few remarks on the position of the FATF. First of all, for the purpose of the FATF Recommendations, non-conviction-based confiscation has to be intended as "*confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required*"; therefore, while there is no need for a conviction, we are still within a criminal proceeding. Moreover, according to Recommendation 38 member states are required to take immediate action in response to confiscation requests by foreign countries, and, what is of particular interest, they are specifically asked to respond also to requests made pursuant to non-conviction-based proceedings, "*unless this is inconsistent with fundamental principles of their domestic law".* Besides, Interpretive Note to Recommendation 38, par. 2 further specifies that, while countries are not requested to welcome all non-conviction-based requests, they however should be able to do so "*at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown*".

8. The development of the European Union legal framework on confiscation

The development of asset recovery measures at the European level has suffered of the varied national approaches to confiscation. The first attempt to harmonise national legislations was taken in 1998 with Joint Action 98/699/JHA[697], which recalled the I AML Directive and FATF Recommendation 4, and called State Members to apply the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (art. 1, par. 1), welcoming the definitions of 'property', 'proceeds', and 'confiscation' established by the

[697] Joint Action of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime (98/699/JHA).

Convention (art. 2, 2); moreover, art. 1, par. 2 also required States to ensure that their national legislation would also establish the confiscation of property of value of the proceeds of crime, allowing countries to exclude value confiscation only in relation to minor cases crimes.

Shortly after, the legal framework was reinforced by Council Framework Decision 2001/500/JHA[698], which repealed some of the provisions set out by the 1998 Joint Action and devoted a specific article to value confiscation (art. 3), allowing member states to exclude value confiscation when the value would be less than EUR 4 000 (art. 3, par. 1) and reiterating that 'property', 'proceeds' and 'confiscation' were to be intended as defined by 1990 Convention (art. 1, par. 2). In addition, 2001 Council Framework Decision reinforced cross-border cooperation, establishing that countries should uphold any reservation in relation to art. 2-6 of the 1990 Convention (art. 1).

Further steps were taken with Council Framework Decision 2005/212/JHA[699] – which, once again, followed the definitions of proceeds, property, instrumentalities and confiscation of the 1990 Convention. The European Legislator, indeed, took a further step by trying to harmonise the rules on extended confiscation (i.e., going beyond the direct proceeds of crime) across Member States by providing three different criteria for its application (art. 3 para 2)[700]; still, the Council Framework Decision left to Member States the choice of whether implementing all of the three

---

[698] Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA).

[699] Council Framework Decision 2005/212/JHA of 24 February 2005 on Confiscation of Crime-Related Proceeds, Instrumentalities and Property.

[700] Framework Decision 2005/212/JHA, art. 3, para. 2: "*(a) where a national court based on specific facts is fully convinced that the property in question has been derived from criminal activities of the convicted person during a period prior to conviction for the offence referred to in paragraph 1 which is deemed reasonable by the court in the circumstances of the particular case, or, alternatively, (b) where a national court based on specific facts is fully convinced that the property in question has been derived from similar criminal activities of the convicted person during a period prior to conviction for the offence referred to in paragraph 1 which is deemed reasonable by the court in the circumstances of the particular case, or, alternatively, (c) where it is established that the value of the property is disproportionate to the lawful income of the convicted person and a national court based on specific facts is fully convinced that the property in question has been derived from the criminal activity of that convicted person*".

criteria or only some of them, in this way not showing a significant improvement in terms of harmonisation[701].

Similarly, also the subsequent Framework Decision 2006/783/JHA[702] on mutual recognition did not reinforce the framework established by 2005 Council Framework Position, since it left to member states the possibility to refuse the execution of extended confiscation orders if the issuing member state had adopted a different option – out of the three available pursuant to art. 3, par. 2 of the 2005 Council Framework Decision.

In order to address the unsatisfactory framework resulting from the numerous Council Framework Decisions adopted[703], in 2014 the European Union adopted Directive 2014/42/EU[704]: repealing some of the provisions of 2001 and 2005 Council Framework Decisions (art. 14), it did not bring any amendments on the rules on mutual recognition of confiscation orders as set out by the 2006 Council Framework Decision, in this way focusing only on the approximation of national laws (Recital No. 5).

While with regard to extended confiscation, art. 5, par. 1 did not bring any significant amendment to the provision set out by 2005 Council Framework Decision[705], article 4 of the Directive called particular attention, as it tried to find a

---

[701] K. LIGETI, M. SIMONATO, "Asset Recovery in the EU: Towards a Comprehensive Enforcement Model beyond Confiscation? An Introduction", *Ibid.*, 6. This choice is linked to the different constitutional traditions on confiscation, which led the European Legislator to offer three different options to accommodate the different needs: V. MITSILEGAS, "The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU", in *Common Market Law Review*, Vol. 43, 2006, 1288, note No. 55.

[702] Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders.

[703] For an overview on confiscation framework prior to Directive (EU) 2014/42/EU: L. SALAZAR, "L'applicazione del principio del reciproco riconoscimento nel settore della confisca e del congelamento dei patrimoni criminali", in "Le sanzioni patrimoniali come moderno strumento di lotta contro il crimine: reciproco riconoscimento e prospettive di armonizzazione", ed. by A. M. Maugeri, Giuffrè, Milano, 2008, 539-555.

[704] Directive 2014/42/EU of the European Parliament and of the of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union.

[705] Art 5, par. 1, Directive (EU) 2014/42: "ember States shall adopt the necessary measures to enable the confiscation, either in whole or in part, of property belonging to a person convicted of a criminal offence which is liable to give rise, directly or indirectly, to economic benefit, where a court, on the basis of the circumstances of the case, including the specific facts and available evidence, such as

common ground for harmonisation of non-conviction-based confiscation. This is significant, since the 2014 Directive is the first binding provision at the supranational level that requires Member States to introduce the possibility to issue a confiscation order not based on a prior conviction: until that moment, the only provision that took into account the possibility of non-conviction based confiscation was represented by FATF Recommendation 4 (*supra* § 7). However, the provision laid down by art. 4, par. 2 appears to be quite limited[706], since it actually allows the application of confiscation without a conviction only under two circumstances, namely illness or absconding of the suspect[707] – therefore, the non-conviction-based established by the 2014 Directive is still related to criminal proceedings: art. 4, par. 2 refers to a traditional confiscation in a criminal proceeding that for some reasons did not achieve a final conviction[708]. Furthermore, 2014 Directive established for the first time as well the confiscation of assets of third parties - except for bona fide persons – requiring States to establish confiscation, including value confiscation, which were transferred by a suspect or convicted person (art. 6, par. 1)[709].

---

that the value of the property is disproportionate to the lawful income of the convicted person, is satisfied that the property in question is derived from criminal conduct".

[706] For a critical comment on the Directive (EU) 2014/42: M. SIMONATO, "Directive 2014/42/EU and non-conviction based confiscation. A step forward on Asset Recovery?", in *New Journal of European Criminal Law*, Vol. 6 (2), 2015, 213-228.

[707] For a deeper analysis of the requirements set out by art. 4, par. 2: J. P. RUI, U. SIEBER, "NCBC in Europe – Bringing the Picture Together", in "Non-Conviction-Based Confiscation in Europe. Possibilities and Limitations on Rules Enabling Confiscation without a Criminal Conviction", ed. by J. P. Rui, U. Sieber, Duncker & Humblot, Berlin, 2015, 277 ss.

[708] M. SIMONATO, *Ibid.*, 221-222. Moreover, it has been remarked that art. 5 of the Proposal of 2014 Directive was explicitly named "non-conviction-based confiscation"; although its content have been largely transposed into art. 4, par. 2, the European Legislator did not choose maintain that title: M. PANZAVOLTA, "Confiscation and the Concept of Punishment: Can There be a Confiscation Without a Conviction?", in "Chasing Criminal Money. Challenges and Perspectives on Asset Recovery in the EU", *Ibid.*, 26: "*yet the fact remains that the European drafters did not want to use the label 'confiscation without conviction*'".

[709] Art. 6, par. 1: "*Member States shall take the necessary measures to enable the confiscation of proceeds, or other property the value of which corresponds to proceeds, which, directly or indirectly, were transferred by a suspected or accused person to third parties, or which were acquired by third parties from a suspected or accused person, at least if those third parties knew or ought to have known that the purpose of the transfer or acquisition was to avoid confiscation, on the basis of concrete facts and circumstances, including that the transfer or acquisition was carried out free of charge or in exchange for an amount significantly lower than the market value*".

As a final remark, it is interesting to notice that the 2014 Directive provides a more detailed definition of proceeds than the 1990 and 2005 Council of Europe Conventions definitions: proceeds are defined "*any economic advantage derived directly or indirectly from a criminal offence; it may consist of any form of property and includes any subsequent reinvestment or transformation of direct proceeds and any valuable benefits*"[710] (art. 2, 1)), and it has interestingly partially amended the definition of confiscation, choosing not to mention its nature of "penalty or measure", but merely stating that it consists of a "*final deprivation of property ordered by a court in relation to a criminal offence*" (art. 1, 4)). Besides, we remark that the 2017 Directive explicitly recalls the provisions on freeze and confiscation established by Directive 2014/42/EU to apply them to "*the proceeds derived from and instrumentalities used or intended to be used in the commission or contribution to the commission of any of the offences referred to in this Directive*" (art. 20, par. 2)[711].

Despite the ambition to enhance the harmonisation of national legislation on confiscation, the 2014 Directive appears to be not bold enough and its effectiveness has been questioned on multiple grounds[712]. Recently, the European Legislator tried to reinforce the framework on mutual recognition of freezing an confiscation orders with Regulation (EU) 2018/1805[713], but still the European approach seem to be too

[710] According to Recital No. 11, indeed: " *There is a need to clarify the existing concept of proceeds of crime to include the direct proceeds from criminal activity and all indirect benefits, including subsequent reinvestment or transformation of direct proceeds. Thus proceeds can include any property including that which has been transformed or converted, fully or in part, into other property, and that which has been intermingled with property acquired from legitimate sources, up to the assessed value of the intermingled proceeds. It can also include the income or other benefits derived from proceeds of crime, or from property into or with which such proceeds have been transformed, converted or intermingled*".

[711] Similarly, also art. 9 of Directive(EU) 2018/1673 on combating money laundering by criminal law recalls the applicability of confiscation pursuant to Directive (EU) 2014/42: "*Member States shall take the necessary measures to ensure, as appropriate, that their competent authorities freeze or confiscate, in accordance with Directive 2014/42/EU, the proceeds derived from and instrumentalities used or intended to be used in the commission or contribution to the commission of the offences as referred to in this Directive*".

[712] For a critical remark on the effectiveness of the EU legal framework on confiscation: M. FAZEKAS, E. NANOPOULOS, "The Effectiveness of EU Law: Insights from the EU Legal Framework on Asset Confiscation", in *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 24 (1), 2016, 39-64.

[713] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders.

fragmented and insufficient[714]. Aware of the need to strengthen the instruments on asset recovery the European Union adopted a Proposal for a new Directive on asset recovery and confiscation[715] on May 2022. Meant to work together with Regulation (EU) 2018/1805 and replacing Council Framework Decision 2005/212/JHA and Directive 2014/42/EU (as well as Council Decision 2007/845/JHA[716]), the proposed Directive intervenes on different levels, by specifying the existing provisions and setting minimum common rules to be applied throughout asset recovery stages, enhancing the powers of Asset Recovery Offices and encouraging the adoption of a national strategy on asset recovery. In particular, with regard to confiscation the Proposal extends the range of confiscation forms within the framework of proceedings in criminal matters, in this way continuing the work started with Regulation 2018: the Proposal Directive intervenes on the extension of the scope of extended confiscation (art. 14) to all criminal offences under art. 2, including terrorism ; the expansion of the application of non-convicted-based confiscation to death, immunity, amnesty and prescription of a limited time period; and the introduction of the new "confiscation of unexplained wealth linked to criminal activities" (art. 16) on a subsidiary bases when no other previous confiscation forms can be applied[717].

[714] For a deeper analysis of the shortcomings of Regulation EU) 2018/1805: A. H. OCHNIO, "The Tangled Path From Identifying Financial Assets to Cross-Border Confiscation. Deficiencies in EU Asset Recovery Policy", in *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 29, 2021, 218-240.

[715] Proposal for a Directive of the European Parliament and of the Council on asset recovery and confiscation COM (2022) final.

[716] Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime.

[717] A. SAKELLARAKI, "EU Asset Recovery and Confiscation Regime – *Quo vadis*? A First Assessment of the Commission's Proposal to Further Harmonise the EU Asset Recovery and Confiscation Laws. A Step in the Right Direction?", in *New Journal of European Criminal Law*, Vol. 13 (4), 2022, 492-496.

9. The Italian legal framework on confiscation

The Italian legal framework on confiscation has greatly evolved over the years, thanks both to the numerous interventions of the Italian Legislator and to the active role played by the case law.

Originally, indeed, the Criminal Code laid down one form of general confiscation, (art. 240 c.p.) and two forms of confiscation related to the commission of specific crimes (arts. 722 c.p. and art. 733 c.p.); however, soon after numerous other forms of confiscation have been introduced, both within and outside the Criminal Code, and the catalogue of forms of confiscations greatly expanded, with the aim of disrupting the financial gain deriving from the commission of crimes[718].

For the purpose of this work, the analysis will be focused on the specific forms of confiscation introduced in relation to terrorist offences, namely mandatory confiscation pursuant art. 270 *bis*, par. 4 c.p. and mandatory confiscation – which covers also value confiscation – pursuant to art. 270 *septies* c.p., and the problems of interpretation and coordination with other forms of confiscation they could pose, namely with regard to the form of mandatory confiscation pursuant to art. 416 *bis*, par. 7 c.p., the form of extended confiscation pursuant to art. 240 *bis* c.p.[719] and the form of preventive confiscation pursuant to arts. 16, 24 of the Legislative Decree 159/2011 ("Antimafia Code").[720]

Overall, it is interesting to notice that the reinforcement of the instrument of confiscation in relation to terrorist offences responds to a two-fold strategy, the first line of direction being the increase of the penalties provided for the commission of

[718] For a comment on this trend, which involves both the Italian and European frameworks: V. MANES, "L'ultimo imperativo della politica criminale: nullum crimen sine confiscatione", in *Rivista Italiana di Diritto e Procedura Penale*, Vol. 3, 2015, 1259-1282.

[719] Former art. 12 *sexies* Legislative Decree 8 June 1992, converted with amendments by Law 7 August 1992 No. 356, modified by Law Decree 20 June 1994, converted with amendments by Law 8 August 1994 No. 501. Pursuant to art. 6, par. 1, Legislative Decree 1 March 2018, the provisions laid down by art. 12 *sexies* have been transposed into art. 240 *bis* c.p.

[720] Recently amended by Law 17 October 2017 No. 161.

such offences[721], and the second line being, indeed, the strengthening of confiscation[722].

9.1 Confiscation and terrorism financing

Looking specifically at the microsystem of terrorist offences established within the Criminal Code (*supra* Chapter I § 5), we can see that the Italian Legislator has introduced two specific forms of confiscation; art. 270 *bis*, par. 4 c.p., introduced by Law Decree 374/2001 at, and art. 270 *septies*, introduced by Law 153/2016.

Introduced in order to neutralise the instruments used to carry out the conducts punished by art 270 *bis* c.p.[723], par. 4 of art. 270 *bis*, c.p. establishes the mandatory confiscation of the instrumentalities, price, product, profit or benefits deriving from their use. Fifteen years later, similar motives pushed the Italian Legislator to reinforce the instrument of confiscation in relation to terrorist offences, and new article 270 *septies* c.p. was introduced in the Criminal Code, which establishes the mandatory confiscation of the instrumentalities of the crime and, also in the form of value confiscation, of the profit, price and product of the crimes committed for terrorist purposes pursuant to art. 270 *sexies* c.p. – in this way implementing the 2005 Council of Europe Convention Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (art. 3)[724] (*supra* § 6).

In particular, by referring to the offences committed for terrorist purposes pursuant to art. 270 *sexies* c.p., it has been remarked that art. 270 *septies* c.p. would apply also

---

[721] On this point: F. ROSSI, "Il contrasto al terrorismo internazionale nelle fonti penali multilivello", Jovene, Napoli, 2022, 46-47, who remarks that European states overall have increased the penalties connected with crime with terrorist purposes.

[722] M. PELISSERO, "Delitti di terrorismo", in "Reati contro la personalità dello Stato e contro l'ordine pubblico", edited by M. Pelissero, in Trattato Teorico Pratico di diritto penale, directed by F. Palazzo, C. E. Paliero, Giappichelli, Torino, 2010, 160-161.

[723] A. CORBO, "Terrorismo", in "Codice delle confische", ed. by T. Epidendio, G. Varraso, Giuffré, Milano, 2018, 879.

[724] R. BORSARI, "Articolo 270 *septies* c.p.", in "Commentario breve al codice penale", ed. by G. Forti, S. Seminara, G. Zuccalà, 6th ed., CEDAM, Padova, 2017, 928.

to art. 270 *bis*, pars. 1, 2, thus extending value confiscation to the crime of association for terrorist purposes[725]. However, value confiscation would not cover those cases were the association pursuant to art. 270 *bis* c.p. is carried out with the purpose of subversion of the democratic order[726].

Looking at the structure of these two provisions, they both appear to have been shaped on the form of confiscation established by art. 416 *bis*, par. 7 c.p[727]. However, if art. 270 *bis*, par. 4 c.p. displays, indeed, an identical structure[728], some differences in the structures of articles 270 *septies* c.p. and art. 416 *bis*, par. 7 c.p. can be remarked: unlike art. 416 bis, par. 7 c.p., art. 270 *septies* c.p. includes, in addition to conviction, the plea bargain pursuant to art. 444 c.p.p. as basis for the application of confiscation, and it explicitly excludes third party confiscation – whereas art. 416 *bis*, par. 7 c.p. merely omits any reference to it; moreover, unlike art. 416 *bis*, par. 7 c.p., art. 270 *septies* c.p. includes value confiscation[729].

Besides, the two forms of confiscation established by art. 270 *bis* c.p. and art. 270 *septies* c.p. pose similar issues in terms of coordination.

Given their identical structure, art 270 *bis*, par. 4 c.p. poses the same coordination issues of art. 416 *bis*, par. 7 c.p., namely in relation to the form of extended confiscation established by art. 240 bis c.p., which include terrorist-related offences among the list of crimes it applies to[730]. However, it has been pointed out that , while art. 270 *bis*, par. 4 c.p. refers to the instrumentalities and proceeds of crime, art. 240 *bis* c.p. refers to those to money, goods or other assets whose origin cannot be justified and appear to be disproportionate in relation to his income; therefore, their

---

[725] R. BORSARI, *Ibid*.,928.

[726] In this sense: R. BERTOLESI, *Ibid*., V. ARAGONA, *Ibid*., 103, R. BORSARI, *Ibid*., 928. *Contra*: A. CORBO, *Ibid*., 883, who suggests that the broad wording of art. 270 *sexies* c.p. could be interpreted as to include also subversive purposes.

[727] R. BORSARI, *Ibid*., 928.

[728] E. NICOSIA, "La confisca, le confische. Funzioni politico-criminali, natura giuridica e problemi ricostruttivi-applicativi", Giappichelli, Torino, 2012, 8.

[729] A. CORBO. *Ibid*., 881-882.

[730] The extension to crimes committed with terrorist purposes was established by Law 15 July 2009, No. 94, and by Legislative Decree 29 October 2016 No. 202, which specified that also offences with the purposes of "international" terrorism are included.

scope would be different[731]. Moreover, also the coordination of art. 270 *septies* c.p. and art. 240 *bis* c.p. could raise some doubts; nonetheless, the scope of art. 270 *septies* c.p. seems to be broader, as it includes also the instrumentalities of the crime – whereas art. 240 *bis* c.p. would refer only to the proceeds, product and profit of the crime[732].

Furthermore, possible coordination issues have been remarked in relation to the form of preventive confiscation established by the Anti-mafia Code: however, with regard both to art. 270 *bis*, par. 4 c.p. and art. 270 *septies* c.p., preventive confiscation[733] would show a narrower scope of application – namely, only the product or the proceeds of crime, not including the instrumentalities[734].

Section III – Virtual Assets and asset freezing and confiscation measures: key issues

10. The application of targeted sanctions and confiscation to Virtual Assets: possible challenges

As outlined in the previous chapters, international actors are intensively working on updating and adapting their legal instruments in order to address the new challenged posed by Virtual Assets. This effort is particularly intense at the regulatory level, where multiple international bodies are coordinating their efforts in order to build a comprehensive and coherent framework. However, the attention on Virtual Assets has also invested issues other than the development of an effective

[731] A. CORBO, *Ibid*., 880.

[732] A. CORBO, *Ibid*., 883.

[733] For an overview of the Italian preventive confiscation: M. PANZAVOLTA, R. FLOR, "A necessary Evil? The Italian "Non-Criminal System" of Asset Forfeiture", in "Non-Conviction-Based Confiscation in Europe. Possibilities and Limitations on Rules Enabling Confiscation Without a Criminal Conviction", *Ibid.*, 111-150.

[734] A. CORBO, *Ibid*., 880; 883.

regulatory framework – namely the application of asset freezing measures and the possible challenges in the perspective of asset recovery.

With regards to asset freezing measures, the peculiar characteristics of Virtual Assets – especially (*pseudo*) anonymity and decentralisation – could represent an effective way to avoid or mitigate the limitations on rights to property imposed by targeted sanctions: in particular, individuals could resort to the use of privacy coins and other instruments that obfuscate the trail of transactions (*supra* Chapter I § 5.5.1) and to unhosted wallets and decentralised exchanges (*supra* Chapter I § 5.5.3)– in this way possibly hampering the identification of individuals.

After the Russian invasion of Ukraine in February 2022, the public debate in this regard increased, as following the imposition of economic sanctions[735], concerns were raised on the possibility that Russia could mitigate them by resorting to Virtual Assets[736].

Looking specifically at the economic sanctions (i.e., general sanctions) imposed by the European Union, they build on Regulation (EU) No. 833/2014[737] - adopted in response to Russian annexation of Crimea – through the adoption of specific Council Decisions, commonly referred to as "sanctions packages". To this date, the European Union has adopted nine sanctions package, which targets different sectors of the Russian economy[738]; however, for the purpose of this work, the Fifth package[739] is of particular interest. Indeed, it specifically addresses Virtual Assets by forbidding to "*provide crypto-asset wallet, account or custody services to Russian*

[735] On the same day of the Russian Invasion, the European Union announce the adoption of economic sanctions against Russia: Special meeting of the European Council (24 February 2022) – Conclusions, European Council, EUCO 18/22.

[736] For instance, as early as on 7 March 2022, the U.S. FinCEN warned the possible misuse of Virtual Assets to avoid sanctions: FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts, FinCEN Alert, 7 March 2002.

[737] Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

[738] The latest package (Ninth package) has been adopted on 16 December 2022: Council Regulation (EU) 2022/2474 of 16 December 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

[739] Council Decision (CFSP) 2022/578 of 8 April 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

nationals or natural persons residing in Russia, or legal persons, entities or bodies established in Russia, if the total value of crypto-assets of the natural or legal person, entity or body per wallet, account or custody provider exceeds EUR 10 000" (art. 1, par. 4), and it requires state members to exchange information on "*detected instances of breach circumvention and attempts at breach or circumvention of the prohibitions set out in this Regulation through the use of crypto-assets*" (art. 1, par. 24).

Therefore, virtual assets service providers based in the European Union cannot hold "*crypto assets or the keys to crypto assets on behalf of Russian nationals or natural persons residing in Russia, or legal persons, entities or bodies established in Russia, with a total value exceeding EUR 10 000 per wallet, account or custody provider*", and are also requested to take the appropriate safeguards and remedies in relation to the high volatility and rapid value fluctuation of these instruments (*supra* Chapter I)[740]. Such provision appears to be particularly severe, as fluctuations are quite unpredictable – therefore, in order to be compliant service providers seems to be pushed to entirely stop their services.

Furthermore, alongside the obligations introduced with the Fifth package, the European Union clarified the application of asset freeze measures to Virtual Assets, by stating that, according to their characteristics and functions, they could fall under the classification of "funds" or "economic resources" set out by Regulation (EU) 269/2014 at art. 1, g) and art. 1, d) respectively, or under the category of "transferable securities" set out by art. 1, f) of Regulation (EU) 833/2014 – except when they act as instrument of payment[741].

While the attention on the inclusion of Virtual Assets among the reach of sanctions and asset freezing measures is increasing, the international legal framework on asset recovery is being implemented in order reinforce harmonisation and international cooperation. As outlined in the present Chapter, indeed, the current

[740] "Crypto Assets" – Frequently asked questions, Finance - European Commission, 11 April 2022: "*These safeguards and remedies should duly take into account the fact that the value of crypto-assets can fluctuate substantially over a short period of time*".

[741] "Crypto Assets" – Frequently asked questions, Finance - European Commission, 11 April 2022. On the possible functions and classifications of Virtual Assets: *supra* Chapter II.

international framework on asset recovery appears to be still fragmented and not suited to effectively address the issues arising from cross-border cooperation. For this reason, the European Union has recently issued a new Regulation on mutual recognition of confiscation orders, and it is currently working on the Proposal for a new Directive to replace the 2014 Directive on confiscation(*supra* § 8). Besides, the interest of the European Union on enhancing its reach on asset recovery is part of a larger picture shared by other supranational actors. Indeed, the Council of Europe is considering to update the 2005 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, taking into account the FATF Recommendations[742]. Besides, while Virtual Assets' (*pseudo*) anonymity and decentralisation could pose similar issues as the one identified above in relation to the enforcement of asset freezing measures, here their cross-border nature and the highly variegated national approaches on their regulation could constitute the main obstacles for the creation of an effective framework.

[742] Council Of Europe Committee on Counter-Terrorism (CDCT), 9th Plenary Meeting, Strasbourg, 30-2 December 2022, par. 8.

Conclusions

The present work aimed to offer a complete overview of the possible impact of Virtual Assets on terrorism financing schemes, as well as the possible implications on both the regulatory and criminal side.

Throughout the Chapters, some peculiarities as well as some recurring features have emerged.

First of all, we have seen how the arduous quest for a shared definition of terrorism has hampered the international efforts to build an effective preventive and repressive framework, and how these difficulties have reflected on terrorism financing. In this context, the United Nations have played a central role, both through the adoption of traditional international law instruments, namely the 1999 UN Convention, and, especially, through the adoption of binding Resolutions adopted under Chapter VII of the UN Charter, which have informed the criminalisation of terrorism financing at both regional and national levels, and have established solid sanctions regimes against terrorism. Similarly, the FATF plays a central role in the AML/CFT regulatory framework, which relies on the adoption of hard-soft laws reciprocally endorsed by international standard-setting bodies. While the drafting of a comprehensive international convention on terrorism is still undergoing, the United Nations Resolutions and FATF Recommendations have managed to create an effective framework on terrorism financing, capable to quickly respond to the current needs and legitimised both by the Council of Europe and the European Union.

The resulting legal framework appears to be characterised by a marked preventive approach informed by a pervasive emergency logic. This is evident when looking at the structure of criminal provisions on terrorism and terrorism financing, which largely punish mere preparatory acts and largely base the rationale of such criminalisation on the subjective element of the author. In this way, the Italian Legislator created a microsystem which challenges the fundamental legal principles

at the basis of criminal law and that poses significant issues in terms of coordination, since many of the criminal provisions introduced have been scarcely applied – thus risking to fall into mere symbolical legislation. Besides, the preventive approach is typical of the regulatory framework: operating outside criminal law, AML/CFT regulations aim at preventing the commission of crimes by imposing several obligations on obliged entities, namely customer due diligence and know your customer measures. Based on an ongoing risk-assessment, the regulatory architecture gives to private actors an active role on counter-terrorism financing, charging them with the concrete task to identify the situations at risk and monitoring their evolution. Shifting the focus on the measures adopted to disrupt the flow of funds, it is impossible not to remark the preventive – yet afflictive – nature of asset freezing measures imposed by the United Nations and European Union targeted sanctions: not requiring a prior conviction, such measures can be applied to suspected terrorists, on whose private life they have a significant impact, through specific listing procedures. These procedures have been at the centre of highly debated judgments, which have gradually managed to enrich the legal safeguards for the protection of individual fundamental rights. At the same time, the instrument of confiscation has been reinforced. At the supranational level, confiscation has been extended in relation to the crimes it can be applied to and new forms of confiscation have been introduced, trying to harmonise national legislations and strengthen cross-border cooperation. Their highly debated nature comes into light when looking at the Italian legal framework, which provides for multiple forms of confiscation, some of them specifically related to crimes committed for terrorist purposes, including terrorism financing.

To the complex framework on terrorism financing, which involves different actors at different levels, Virtual Assets possibly add other layers of complexity. While their inclusion among the broad definitions of assets, funds, or proceeds is not questioned, issues arise in relation to the concrete application of criminal and regulatory provisions, as well as asset freezing measures and confiscation. The higher levels of anonymity they are able to grant – especially with regard to the so-

called privacy coins and the use of specific tools as mixers and tumblers or ring signatures – can hamper the identification of terrorists' flows. Their cross-border nature can represent a significant challenge in terms of cooperation. The decentralised systems they rely to, peer-to-peer transactions, decentralised exchange platforms and the use of unhosted wallet providers could poses significant issues in terms of regulation, especially from the AML/CFT perspective. The different national approaches to the world of Virtual Assets and their regulation could offer attractive opportunities for terrorism financing purposes, in terms of forum shopping across jurisdictions with limited regulations – or no regulations at all.

In the light of these features, the supranational actors, as well as national legislators are engaging in strengthening and adapting their legal instruments to address the challenges posed by Virtual Assets; whether these measure will be effective and proportionate is too early to say.

References

ADACHI M., BENTO PEREIRA DA SILVA P., BORN A., CAPPUCCIO M., CZÁK-LUDWIG S., GSCHOSSMANN I., PAULA G., PELLICANI A., PHILIPPS S., PLOOIJ M., ROSSTEUSCHER I., ZEOLI P., "Stablecoins' role in crypto and beyond: functions, risks and policy", Macroprudential Bulletin, European Central Bank, Vol. 18, 2022, 1-15;

ADDIS A., "Targeted Sanctions as a Counterterrorism Strategy", in *Tulane Journal of International and Comparative Law*, Vol. 19 (1), 2010, 187-206;

AGAMBEN G., "State of Exception", University of Chicago Press, 2005;

ALBANESE D., "Le motivazioni della Corte d'Assise di Milano sul "caso Fatima": spunti di riflessione su terrorismo internazionale e organizzazione di trasferimenti ex art. 270-*quater*.1 c.p", in *Diritto Penale Contemporaneo*, Vol. 3, 2017, 346-355;

ALBRECHT D., "*Nada v Switzerland*: United Nations Security Council Terrorist Sanctions Regime and Human Rights", in *Cyprus Human Rights Law Review*, Vol. 1, No. 2, 2012, 212-220;

AMARELLI G., " L'onda lunga della sentenza De Tommaso: ore contate per l'interdittiva antimafia 'generica' ex art. 84, co. 4, lett. d) ed e) d.lgs. n. 159/2011?", in *Diritto Penale Contemporaneo*, Vol. 1, 2018, 290-299;

AMETRANO F. M., "Bitcoin: oro digitale per nuovi standard monetari", in "Dal sesterzio al bitcoin. Vecchie e nuove dimensioni del denaro", edited by A. Miglietta, A. Mingardi, Rubettino, 2020;

AMMOUS S., "The bitcoin standard: the decentralized alternative to central banking", Wiley, 2018, 11-72;

ANDERSSON T., "Developing Multiple EU Personalities: Ten Years of Blacklisting an Mutual Trust", in "EU Sanctions: Law and Policy Issues Concerning Restrictive Measures", ed. by I. Cameron, Intersentia, 2013;

ARAGONA V., "Il contrasto al finanziamento del terrorismo. Criticità e innovazioni della nuova disciplina italiana", in *Diritto Penale Contemporaneo*, Vol. 1, 2017, 96-106;

ARAMONTE S., HUANG W., SCHRIMPF A., "DeFi risks and the decentralisation illusion", in *BIS Quarterly Review*, December 2021, 21-36;

ARANGIO-RUIZ G., "On the Security Council's 'Law Making'", in *Rivista di Diritto Internazionale*, Vol. 2, 2000, 609-726;

ARCARI M., "Sviluppi in tema di tutela dei diritti di individui iscritti nelle liste dei comitati delle sanzioni del Consiglio di Sicurezza", in *Rivista di diritto internazionale*, Vol. 3, 2007, 657-680;

ARNER D., AUER R., FROST J., "Stablecoins: Risks, Potential and Regulation", BIS Working Papers, No. 905, Bank for International Settlements, November 2020, 1-31;

ATTICO N., "Blockchain. Guida all'ecosistema. Tecnologia, business e società, GueriniNEXT, 2018;

AUST A., "Counter-Terrorism: A New Approach. The International Convention for the Suppression of the Financing of Terrorism", in *Max Planck Yearbook of United Nations Law*, 2001, Vol. 5, 285-306;

AZANI E., LIV N., "Jihadists' Use of Virtual Currency", International Institute for Counter-Terrorism (ICT), 20 June 2018, 1-20;

BADRAN T., E. OTTOLENGHI, "Hezbollah Finance in Lebanon. A Primary-Source Review", Foundation for Defense of Democracies, 23 September 2020;

BAINS P., ISMAIL A., MELO F., SUGIMOTO N., "Regulating the crypto ecosystem. The case of unbacked crypto assets", in *Fintech Notes*, Vol. 7, September 2022, 2-47;

BALZACQ T., "A theory of securitization. Origins, core assumptions, and variants", in Securitization theory. How security problems emerge and dissolve, edited by T. Balzacq, Routledge, London, 2011;

BANTEKAS I., "The International Law of Terrorist Financing", in *The American Journal of International Law*, Vol. 97, 2003, 315-332;

BARBERIS M., "Non c'è sicurezza senza libertà. Il fallimento delle politiche antiterrorismo", il Mulino, Bologna, 2017;

BARR M. S., MILLER G. P., "Global Administrative Law: The View from Basel", in *The European Journal of International Law*, Vol. 17 (1), 2006, pp. 15-46;

BARTOLI R., "Lotta al terrorismo internazionale. Tra diritto penale del nemico *ius in bello* del criminale e annientamento del nemico assoluto", Giappichelli, Torino, 2008;

BARTOLI R., "Le nuove emergenze terroristiche", in "Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali. Atti del convegno Trento, 2 e 3 ottobre 2015", edited by R. Wenin, G. Fornasari, 2017;

BARTOLI R., "Legislazione e prassi in tema di contrasto al terrorismo internazionale: un nuovo paradigma emergenziale?", in *Diritto Penale Contemporaneo*, Vol. 3, 2017, 233-259;

BASSIOUNI M. C., "Introduzione", in "La cooperazione internazionale per la prevenzione e repressione della criminalità organizzata e del terrorismo", edited by M. C. Bassiouni, Giuffrè, Milano, 2005;

BAUER K., LEVITT M., "Funding in Place: Local Financing Trends Behind Today's Global Terrorist Threat", in *Evolutions in Counter-Terrorism*, The International Centre for Counter-Terrorism – The Hague (ICCT), Vol. 2, 2020, pp. 47-76;

BAXTER R., "A skeptical look at the concept of terrorism", in *Akron Law Review*, Vol. 7 (3), 1974, 380-387;

BENIGNO F., "Terrore e terrorismo: Saggio storico sulla violenza politica", Einaudi, Torino, 2018;

BERNARDI A., "L'europeizzazione del diritto e della scienza penale, Giappichelli, Torino, 2004;

BERNARDI A., "La sovranità penale tra Stato e Consiglio d'Europa", Jovene, 2019;

BERTOLESI R., "Ancora nuove norme in materia di terrorismo", in *Diritto Penale Contemporaneo*, 19 October 2016;

BIANCHI A., Security Council's Anti-terror Resolutions and their Implementations by Member States, in Journal of International Criminal Justice, 2006, Vol. 4 (5), 1044-1073;

BORSARI R., "Diritto punitivo sovranazionale come sistema, CEDAM, Padova, 2007;

BORSARI R., "Articolo 270 *quater*.1 c.p.", "Articolo 270 *quinquies*. 1 c.p.", Articolo 270 *septies* c.p.", "in "Commentario breve al codice penale", ed. by G. Forti, S. Seminara, G. Zuccalà, 6th ed., CEDAM, Padova, 2017;

BRYAN D., KELLY L., TEMPLER S., "The failed paradigm of 'terrorism'", in *Behavioral Sciences of Terrorism and Political Aggression*, 2011, Vol. (3)2, 80-96;

BROWN C., "After 'Caroline': NSS 2002, practical judgment, and the politics and ethics of pre-emption", in *The Ethics of Preventive War*, edited by D. K. Chatterjee, Cambridge University Press, 2013;

BULLMANN D., KLEMM J., PINNA A., "In search for stability in crypto-assets: are stablecoins the solution?", European Central Bank – Occasional Papers Series, August 2019, No. 230, 1-55;

BUZAN B., "Will the 'global war on terrorism' be the new Cold War?", in *International Affairs*, 2006, Vol. (82) 6, 1101-1118;

BYMAN D. L., "Deadly connections: states that sponsor terrorism", Cambridge University Press, 2005;

CAMERON I., "European Union Anti-Terrorist Blacklisting", in *Human Rights Law Review*, Vol. 3 (2), 2003, 225-256;

CAMERON I., "EU Sanctions: Law and Policy issues concerning restrictive measures", ed. by Cameron I., Intersentia, 2013;

CAMERON I., "EU anti-terrorist sanctions", in "Research Handbook on EU Criminal Law" ed. By V. Mitsilegas, M. Bergström, T. Konstadinides, Edward Elgar, 2016;

CASSESE A., "The Multifaceted Criminal Notion of Terrorism in International Law", in *Journal of International Criminal Justice*, 2006, Vol. (4) 5, 933–958;

CASSESE E., COSTANZO P., "La terza direttiva comunitaria in materia di antiriciclaggio e antiterrorismo", in *Giornale di Diritto Amministrativo*, Vol. 1, 2006, 5-16;

CASSESE S., "Global Administrative Law: The State of the Art,", *in International Journal of Constitutional* Law, Vol. 13 (2), 2015, 465-468;

CAVALIERE A., "Le nuove emergenze terroristiche: il difficile rapporto tra esigenze di tutela e garanzie individuali", in "Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali. Atti del convegno Trento, 2 e 3 ottobre 2015", edited by R. Wenin, G. Fornasari, 2017;

CAVALIERE A., "Considerazioni critiche intorno al D.L. Antiterrorismo, n. 7 del 18 febbraio 2015", in *Diritto penale Contemporaneo*, Vol. 2, 2015, 226-235;

CERFEDA M., "Le 'nuove' misure di congelamento nazionali e il traffico di capitali volti al finanziamento del terrorismo. Le liste degli interdetti, ultima frontiera di

una prevenzione di cui vanno minimizzati i costi", in *Diritto Penale Contemporaneo*, Vol. 1, 2018, 21-35;

Ching B., "Echoes of 9/11: Rhetorical Analysis of Presidential Statements in the "War on Terror"", in *Seton Hall Law Review*, Vol. 51 (2), 2020, 431-460;

CHINNICI C., "Il contrasto al finanziamento al terrorismo: studio comparato sull´implementazione degli strumenti dell´Unione Europea", coordinated by V. Militello, Palermo, 2018;

CHOMSKY N., "Rogue States. The Rule of Force in World Affairs", Pluto Press, London, 2000;

CIAMPI A., "Sanzioni del Consiglio di Sicurezza e diritti umani", Giuffré, 2007;

COLE D., "Enemy Aliens", in *Stanford Law Review*, 2002, Vol. (54) 5, 953-1004;

COLLINS S. D., "State-Sponsored Terrorism: In Decline, Yet Still a Potent Threat", in *Politics & Policy*, Vol. (42)1, 2014, 131-159;

CONFORTI B., FOCARELLI C., "The Law and Practice of the United Nations", 5th ed., BRILL, 2016;

COOPER K., WALKER C., "Security from terrorism financing: models of delivery applied to informal value transfer systems", in *British Journal of Criminology*, Vol. (56) 6, 2016, 1125-1145;

CORBO A., "Terrorismo", in "Codice delle confische", ed. by T. Epidendio, G. Varraso, Giuffré, Milano, 2018, 877-883;

COVOLO V., "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", in *European journal of crime, criminal law and criminal justice*, Vol. 28, 2020, 217-251;

CRAVEN M., "Humanitarianism and the Quest for Smarter Sanctions", in *European Journal of International Law*, Vol. 13 (1), 2002, 43-61;

CRISPINO S., "Finalità di terrorismo, snodi ermeneutici e ruolo dell'interpretazione conforme", in *Diritto Penale Contemporaneo*, Vol. 1, 2017, 226-238;

D'AMATO S., TERLIZZI A., "Strategic European counterterrorism? An empirical analysis", in *European Security*, Vol. 31 (4), 2022, 540-557;

DE GOEDE M., "Hawala discourses and the war on terrorist finance", in *Environment & Planning D: Society & Space*, Vol. (21) 5, 2003, 513-532;

DE GOEDE M., "Blacklisting and the ban: Contesting targeted sanctions in Europe", in *Security Dialogue*, Vol. 42 (6), 2011, 499-515;

DE VIDO S., "Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione Europea", CEDAM, Padova, 2012;

DE VIDO S., "Soft Organizations, Hard Powers: The FATF and the FSB as Standard-Setting Bodies", in *Global Jurist*, Vol. 19, November 2018, 1-12;

DE VIDO S., "All that Glitters is not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive", in *DPCE Online*, Vol. 38 (1), April 2019, 59-76;

DIDENKO N., BUCKLEY R. P., *The evolution of currency: cash to cryptos to sovereign digital currencies*, in *Fordham International Law Journal*, April 2019, 1041-1095;

DI STASIO C., "La lotta multilivello al terrorismo internazionale. Garanzia di sicurezza versus tutela dei diritti fondamentali", Giuffré, Milano, 2010;

DION-SCHWARZ C., MANHEIM D., JOHNSTON P. B., "Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats", RAND Corporation 2019;

DOBITSCH S., "Terrorism and Digital Financing: how Technology is Changing the Threat", Statement at the U.S. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security, 22 July 2021, 8-11;

DOLCINI E., GATTA G. L., "Codice penale commentato", Vol. II, Wolters Kluwer, 2021;

DONOHUE L. K., "The Cost of Counterterrorism", Cambridge University Press, 2008;

DONINI M., "Diritto penale di lotta vs. diritto penale del nemico", in "Contrasto al terrorismo interno e internazionale", edited by R. E. Kostoris, R. Orlandi, Giappichelli, Torino, 2006;

DONINI M., "Mafia e terrorismo come "parte generale" del diritto penale", in *Meridiana*, No. 97, 2020, pp. 203-228;

DREVONA J. , HAENNI P. : "Redefining Global Jihad and Its Termination: The Subjugation of al-Qaeda by Its Former Franchise in Syria", in *Studies in Conflict & Terrorism*, 2022, 1-16;

DURKIN T. A., "Permanent States of Exception: A Two-Tiered System of Criminal Justice Courtesy of the Double Government Wars on Crime, Drugs & Terror", in *Valparaiso University Law Review*, 2016, Vol. 50 (2), 419-492;

ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", European Central Bank – Occasional Papers Series, No. 223, May 2019, 1-39;

ECB CRYPTO-ASSETS TASK FORCE, "Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area", European Central Bank – Occasional Paper Series No. 247, September 2020;

EASSON J., SCHMID A. P., "250-plus Academic, Governmental and Intergovernmental Definitions of Terrorism", in "The Routledge Handbook of Terrorism Research", edited by Alex P. Schmid, Taylor & Francis Group, 2011, 99-158;

EECKHOUT P., "Community Terrorism Listings, Fundamental Rights, and the Security Council Resolutions: In Search of the Right Fit", in *European Constitutional Law Review*, Vol. 3 (2), 183-206;

EISERT J., "Terrorism and Digital Financing: how Technology is Changing the Threat", Statement at the U.S. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security, 22 July 2021, 11-16;

EIZENGA D., WILLIAMS W., "The Puzzle of JNIM and Militant Islamist Groups in the Sahel", in *Africa Security Brief*, The Africa Center for Strategic Studies, No. 38, December 2020, 1-8;

EVANGELISTA M., "Law, Ethics, and the War on Terror", Polity Press, Cambridge, 2008;

FASANI F., "Le nuove fattispecie antiterrorismo: una prima lettura", in *Diritto Penale e Processo*, Vol. 8, 2015, 926-961;

FASANI F., "Un nuovo intervento di contrasto al terrorismo internazionale", in *Diritto Penale e Processo*, Vol. 12, 2016, 1555-1572;

FASANI F., "L'impatto della direttiva antiterrorismo sulla legislazione penale sostanziale italiana", in *Diritto Penale e Processo*, Vol. 1, 2018, 12-24;

FANTACCI L., "Cryptocurrencies and the Denationalization of Money", in *International Journal of Political Economy*, Vol. (48), 2019, 105-126;

FASSBENDER B., "The Un Security Council and International Terrorism", in "Enforcing International Law Norms Against Terrorism", edited by A. Bianchi, Hart Publishing, 2004;

FAZEKAS M., NANOPOULOS E., "The Effectiveness of EU Law: Insights from the EU Legal Framework on Asset Confiscation", in *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 24 (1), 2016, 39-64;

FERNANDEZ-BERTIER M., "The History of Confiscation Laws: From the Book of Exodus to the War on White-Collar Crime", in "Chasing Criminal Money. Challenges and Perspectives on Asset Recovery in the EU", ed. by K. Ligeti, M. Simonato, Hart, 2017, 53-76;

FLETCHER G. P., "Indefinable concept of terrorism", in *Journal of International Criminal Justice*, 2006, Vol. (4) 5, pp. 894-911;

FORZATI F., "La sicurezza fra diritto penale e potere punitivo. Genesi e fenomenologia dell'illecito securitario postmoderno fra involuzioni potestative e regressioni al premoderno", Edizioni Scientifiche Italiane, Napoli, 2020;

FRANCO J., HOLTMANN P., "Pledges to Islamic State: Weak and Strong Alliances", in *RSIS Commentary*, No. 221, 12 November 2014, 1-2;

FREEMAN M., RUHESEN M., "Terrorism Financing Methods: An Overview", in *Perspectives on Terrorism*, Vol. (7) 4, 2013, 5-26;

GALLI F., "Terrorism", in "Research Handbook on EU Criminal Law", ed. By V. Mitsilegas, M. Bergström, T. Konstadinides, Edward Elgar, 2016;

GANOR B., "Defining terrorism: is one man's terrorist another man's freedom fighter?", in *Police Practice and Research*, 2002, Vol. (3) 4, 287-304;

GARDELLA A., "Fighting the Financing of Terrorism: Judicial Cooperation", in Freezing the Assets of International Terrorist Organisations", in "Enforcing International Law Norms against Terrorism", ed. By A. Bianchi, Hart, 2004;

GARTENSTEIN-ROSS D., KODUVAYUR V., HODGSON S., "Crypto-Fascists. Cryptocurrency Usage by Domestic Extremists", Foundation for Defense and Democracy, March 2022;

GATHII J., "The Financial Action Task Force and Global Administrative Law", in *Journal of the Professional Lawyer*, 2010,

GERBA E., RUBIO M., "Virtual Money: how much do Cryptocurrencies alter the fundamental functions of money?" in *Monetary Dialogue Papers* –European Parliament, December 2019, 1-33;

GERGES F. A., "ISIS: a history", Princeton University Press, 2016;

GHOSHRAY S., "Compliance Convergence in FATF Rulemaking: The Conflict between Agency Capture and Soft Law," in *New York Law School Law Review,* Vol. 59 (3), 2014-2015, 521-546;

GIOIA A., "The UN Conventions on the Prevention and Suppression of International terrorism", in "International Cooperation in Counter-terrorism. The United Nations and Regional Organizations in the Fight Against Terrorism", ed. by G. Nesi, Ashgate, 2005, 3-24;

GODINHO SILVA P., "Recent developments in EU legislation on anti-money laundering and terrorist financing", in *New Journal of European Criminal* Law, Vol. 10 (1), 2019, 57–67;

GRAY C., "International Law and the Use of Force", 4th edition, Oxford University Press, 2018;

GRONWALD M., "Is Bitcoin a Commodity? On price jumps, demand shocks, and certainty of supply", in *Journal of International Money and Finance,* Vol. 97, 2019, 86–92;

HALBERSTAM M., "The evolution of the United Nations position on terrorism: from exempting National Liberation Movements to criminalizing terrorism wherever and by whomever committed", in *Columbia Journal of Transnational Law*, 2003, Vol. 41(3), 573-584;

HAFFKE L., FROMBERGER M. & ZIMMERMANN P., "Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them", in *Journal of Banking Regulation*, Vol. 21 (2), 2020, 125-138;

HAPPOLD M., Security Council Resolution 1373 and the Constitution of the United Nations, in Leiden Journal of International Law, 2003, Vol. 16 (3), 593-610;

HARARI Y. N., "Money", Vintage, London, 2018;

HARRINGTON J., THOMPSON J., "Examining Extremism: Harakat al Shabaab al Mujahideen (al Shabaab)", Center for Strategic & International Studies, 23 September 2021;

HE D., HABERMEIER K., LECKOW R., HAKSAR V., ALMEIDA Y., KASHIMA M., KYRIAKOS-SAAD N., OURA H., SEDIK T. S., STETSENKO N., VERDUGO-YEPES C., "Virtual Currencies and Beyond: Initial Considerations", in *IMF Discussion Note*, January 2016, 1-42;

HELLMICH C., "Al-Qaeda: From Global Network to Local Franchise", Bloomsbury, 2011;

HENG Y., MCDONAGH K., "The Other War on Terror Revealed: Global Governmentality and the Financial Action Task Force's Campaign against Terrorist Financing", in *Review of International Studies*, Vol. 34 (3), 2008, pp. 553- 573;

HERNÀNDEZ DE COS P., "Computers and money: the work of the Basel Committee on cryptoassets", Keynote speech at the 36th Annual General Meeting of the International Swaps and Derivatives Association, Madrid, 12 May 2022;

HIGGINS S., "ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide", CoinDesk, 7 July 2014;

HOFFMAN B., "Inside Terrorism", 3rd ed., Columbia University Press, New York, 2017;

JAKOBI A. P., "Governing illicit finance in transnational security spaces: the FATF and anti-money laundering," in *Crime, Law and Social Change*, Vol. 69 (2), 2018, 173-190;

JAKOBS G., "Diritto penale del nemico? Una analisi sulle condizioni della giuridicità", in "Delitto politico e diritto penale del nemico", edited by A. Gamberini, R. Orlandi, Monduzzi, Bologna, 2007;

JACOBSON M., "Terrorist Financing and the Internet", in *Studies in Conflict & Terrorism*, Vol. 33 (4), 2010, pp. 353-365;

JACKSON R., "Writing the war on terrorism. Language, politics and counter-terrorism", Manchester University Press, 2005;

JACKSON B. A., "Technology Acquisition by Terrorist Groups - Threat Assessment Informed by Lessons from Private Sector Technology Adoption, RAND Corporation, 2001, 1-50;

JERVIS R., "Understanding the Bush doctrine: Preventive Wars and Regime Change", in *Political Science Quarterly*, Vol. (131), 2016, 285-311;

JONES G., VALLEE C., NEWLEE D., HARRINGTON N., SHARB C., BYRNE H., "The Evolution of the Salafi-Jihadist Threat. Current and Future Challenges from the Islamic State, Al-Qaeda, and Other Groups", Center for Strategic and International Studies, November 2018, 1-72;

JURITH E., "Acts of Terror, Illicit Drugs and Money Laundering", in *Journal of Financial Crime*, Vol. 11 (2), 2003,158-162;

KALICHARAN V. S., "An Evaluation of the Islamic State's Influence over the Abu Sayyaf", in *Perspectives on Terrorism*, Vol. (13)5, 2019, 90-101;

KEDEM S., "Central African Republic freezes the adoption of Bitcoin", African Business, 26 July 2022;

KELSEN H., "Collective Security and Collective Self-Defense Under the Charter of the United Nations", in *The American Journal of International Law*, , Vol. (42), 1948, 783-796;

KENGOR P., "Reagan's "March of Freedom in a Changing World" in "Reagan's Legacy in a World Transformed", edited by J. L. Chidester and P. Kengor, Harvard University Press, 2015;

KIRGIS JR. F. L., "The Security Council's first fifty years", in *The American Journal of International Law*, 1995, Vol. (89) 3, 506-539;

KINGSBURY B., KRISCH N., STEWART R. B., "The Emergence of Global Administrative Law", in *Law and Contemporary Problems*, Vol. 68(3& 4), pp. 15-62;

KLEIN P., "International Convention for the Suppression of the Financing of Terrorism", in *United Nation Audiovisual Library of International Law*, 2009, 1-5;

KOKOTT J., SOBOTTA C., "The Kadi Case – Constitutional Core Values and International Law – Finding the Balance?", in *European Journal of International Law*, Vol. 23 (4), 1015-1024;

KOSSE A., MATTEI I., "Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies", in *BIS Papers*, May 2022, 1-23;

LANG A., "Le risoluzioni del Consiglio di sicurezza delle Nazioni Unite e l'Unione Europea", Giuffré, 2002;

LAQUEUR W., "Terrorism", Weidenfeld and Nicolson, London, 1977;

LAUB Z., MASTERS J., "Al-Qaeda in the Islamic Maghreb", Council of Foreign Relations, 27 March 2015;

LAVALLE R., "The International Convention for the Suppression of the Financing of Terrorism", in *Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht*, 2000, 491-510;

LEVITT G., "Is terrorism worth defining?", in *Ohio Northern University Law Review*, Vol. 13 (1), 1986, 97-116;

LEVITT M., "Charitable Organizations and Terrorist Financing: A War on Terror Status-Check", The Washington Institute for Near East Policy, 19 March 2004;

LEVITT M., "Hamas : Politics, Charity, and Terrorism in the Service of Jihad", Yale University Press, 2006;

LEVY I., "How Iran Fuels Hamas Terrorism", The Washington Institute for Near East Policy, 1 June 2021;

LISTER C., "How al-Qa`ida Lost Control of its Syrian Affiliate: The Inside Story", in *CTC Sentinel*, Vol. 11 (2), 2018, 1-9;

LIV N., "Jihadists' Use of Virtual Currency 2", International Institute for Counter-Terrorism (ICT), 18 January 2018, 1-8;

LOOSVELD S., "The 5th Anti-Money Laundering Directive: virtual currencies and other novelties", in *Journal of International Banking Law and Regulation*, 2018, Vol. 33 (9), 297-304;

MALIK N., "Terror in the Dark: How terrorists use encryption, the Darknet and cryptocurrencies", The Henry Jackson Society, 2018;

MAKARENKO T., "The Crime-Terror Continuum: Tracing the Interplay between Organised Crime and Terrorism", in "Global crime today : The changing face of organised crime", edited by M. Galeotti, Routledge, 2007;

MANCINI GRIFFOLI T., MARTINEZ PERIA M. S., AGUR I., ARI A., KIFF J., POPESCU A., ROCHON C., "Casting light on Central Bank Digital Currency", IMF, 2018, 1-39;

MANES V., "L'ultimo imperativo della politica criminale: nullum crimen sine confiscatione", in *Rivista Italiana di Diritto e Procedura Penale*, Vol. 3, 2015, 1259-1282;

MANNO A. M., "Il contrasto al finanziamento del terrorismo internazionale. Tra prevenzione sanzionatoria e punizione preventiva", Giappichelli, Torino, 2020;

MANTOVANI M., "Le condotte con finalità di terrorismo, in Contrasto al terrorismo interno e internazionale", in "Contrasto al terrorismo interno e internazionale" a cura di R. E. Kostoris e R. Orlandi, Giappichelli, Torino, 2006;

MARINO G., "Il sistema antiterrorismo alla luce della L. 43/2015: un esempio di 'diritto penale del nemico'?", in *Rivista italiana di diritto e procedura penale*, Vol. 3, 2016, 1388-1426;

MARINO G., "Lo statuto del terrorista", in *Diritto Penale Contemporaneo*, Vol. 1, 2017, 44-52;

MARINO G., "Il 'filo di Arianna'. Dolo specifico e pericolo nel diritto penale della sicurezza", in *Diritto Penale Contemporaneo*, Vol. 6 (2018), 41-64;

MARSCHICK A., "The Security Council as a World Legislator? Theory, Practice & Consequences of an Expanding World Power", in *Institute for International Law and Justice New York University School of Law*, Working Paper 2005/18, 1-36;

MARSCHIK A.,"The Security Council's Role: Problems and Prospects in the Fight Against Terrorism", in "International Cooperation in Counter-Terrorism. The United Nations and Regional Organizations in the Fight Against Terrorism", edited by G. Nesi, Ashgate, 2005;

MARTINICO G., POLLICINO O., SCIARABBA V., "Hands off the Untouchable Core: A Constitutional Appraisal of the Kadi Case", in *European Journal of Law Reform*, Vol. 11 (3), 2009, 281-304;

MASARONE V., "Politica criminale e diritto penale nel contrasto al terrorismo internazionale: tra normativa interna, europea ed internazionale", Edizioni Scientifiche Italiane, Napoli, 2013;

MASARONE V., "La 'lotta' al terrorismo", in "L'incidenza di decisioni quadro, direttive e convenzioni europee sul diritto penale italiano", ed. by A. Cavaliere, V. Masarone, Edizioni Scientifiche Italiane, Napoli, 2018, 33-53;

MAUGERI A. M., "Le moderne sanzioni patrimoniali tra funzionalità e garantismo", Giuffré, Milano, 2001;

MCCALLUM B. T., "The Bitcoin Revolution", in *Cato Journal*, Vol. 35 (2), 2015, 347-356;

MILITELLO V., "Terrorismo e sistema penale: realtà, prospettive, limiti", in *Diritto Penale Contemporaneo*, Vol. 1, 2017, 3-10;

MINNEROP P., "Rogue States – State Sponsors of Terrorism?", in *German Law Journal*,Vol. 3, 2002, 1-5;

MITSILEGAS V., "Countering the chameleon threat of dirty money. 'Hard' and 'soft' law in the emergence of a global regime against money laundering and terrorist financing", in "Transnational Organised Crime", Taylor & Francis, 2003, 195-211;

MITSILEGAS V., "The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU", in *Common Market Law Review*, Vol. 43, 2006, 1277-1311;

MITSILEGAS V., GILMORE B., "The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards", in *International and Comparative Law Quarterly*, 56 (1), 2007, 119-140;

MITSILEGAS V., "EU Criminal Law", Hart, London, 2009;

MITSILEGAS V., "EU criminal law after Lisbon : rights, trust and the transformation of justice in Europe", Hart, Oxford, 2016;

MITSILEGAS V., "Transnational Criminal Law and the Global Rule of Law", in "The Global Community: Yearbook of the International Law and Jurisprudence 2016", Oxford University Press, 2017;

MOCCIA S., La perenne emergenza. Tendenze autoritarie nel sistema penale, 2nd ed., ESI, Napoli, 2000;

MORSE J. C., "Blacklists, market enforcement, and the global regime to combat terrorist financing", in *International Organization*, Vol. 73 (3), 2019, pp. 511-546;

MUDDE C., "The far right today", Polity Press, 2019;

MUGAVERO R., SABATO V., SOLDATELLI S., "Analisi degli eventi terroristici e delle tecnologie impiegate", in "Terrorismo e Nuove Tecnologie", edited by R. Mugavero, R. Razzante, Pacini Giuridica, Pisa, 2016;

MURPHY S. D., "The doctrine of preemptive self-defense", in *Villanova Law Review*, Vol. (50) 3, 2005, 703-704;

MUZTABA HASSAN A., NAWED NAFEES S., "Cryptocurrency and Terrorist Financing in Asia", The Diplomat, 4 February 2022;

NARAIN A., MORETTI M., "Regulating Crypto. The right rules could provide a safe space for innovation", in *Finance and Development*, International Monetary Fund, September 2022, 18-19;

NAKAMOTO S., " Bitcoin: A Peer-to-Peer Electronic Cash System";

NICOSIA E., "La confisca, le confische. Funzioni politico-criminali, natura giuridica e problemi ricostruttivi-applicativi", Giappichelli, Torino, 2012;

OCHNIO A. H., "The Tangled Path From Identifying Financial Assets to Cross-Border Confiscation. Deficiencies in EU Asset Recovery Policy", in *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 29, 2021, 218-240;

O'DONNELL L., "Pakistan Sponsored Terror Next Door. Now, It's Back to Roost", Foreign Policy, 31 May 2022;

OROSZ A., "Violent extremism in the Sahel is strengthening its grip in West Africa", London School of Economics Blog, 15 February 2022;

OTTOLENGHI E., "State sponsors of terrorism: an examination of Iran's Global Terrorism Network", Congressional Testimony: Foundation for Defense of Democracy, 17 April 2018;

QASSEM N., "Hizbullah. The story from witihin", SAQI, London, 2010;

PALMISANO M., "Prevenzione del finanziamento al terrorismo e congelamento dei capitali", in "Mobilità, sicurezza e nuove frontiere tecnologiche", edited by V. Militello, A. Spena, Giappichelli, Torino, 2018;

PANETTA F., "Cash still king in times of COVID-19" – Keynote speech at the Deutsche Bundesbank's 5th International Cash Conference – "Cash in times of turmoil", European Central Bank, 15 June 2021;

PANETTA F., "The present and future of money in the digital age", European Central Bank, 10 December 2021;

PANETTA F., "For a few cryptos more: the Wild West of crypto finance", Speech at Columbia University, 25 April 2022;

PANZAVOLTA M., FLOR R., "A necessary Evil? The Italian "Non-Criminal System" of Asset Forfeiture", in "Non-Conviction-Based Confiscation in Europe. Possibilities and Limitations on Rules Enabling Confiscation Without a Criminal Conviction", *Ibid*., 111-150;

M. PANZAVOLTA, "Confiscation and the Concept of Punishment: Can There be a Confiscation Without a Conviction?", in "Chasing Criminal Money. Challenges and Perspectives on Asset Recovery in the EU", ed. by K. Ligeti, M. Simonato, Hart, 2017, 25-52;

PASCULLI L., "Le misure di prevenzione del terrorismo e dei traffici criminosi internazionali", Padova University Press, 2012;

PASSAS N., "Informal Value Transfer Systems and Criminal Organizations; a study into so-called underground banking networks", 1999, 1-86;

PATRONE I. J., "La legislazione dell'Unione Europea tra esigenze di armonizzazione e logiche emergenziali", in *Speciale Questione Giustizia*, 2016, 283-290;

PAVLIDIS G., "Learning From Failure: Cross-Border Confiscation in the EU", in *Journal of Financial Crime*, Vol. 26 (3), 2019, 683-691;

PELISSERO M., "Delitti di terrorismo", in "Reati contro la personalità dello Stato e contro l'ordine pubblico", edited by M. Pelissero, in Trattato Teorico Pratico di diritto penale, directed by F. Palazzo, C. E. Paliero, Giappichelli, Torino, 2010, 159-212;

PELISSERO M., "Contrasto al terrorismo internazionale e il diritto penale al limite", in *Speciale Questione Giustizia*, 2016, 99-112;

PERKEL W., "Money Laundering and Terrorism: Informal Value Transfer Systems", in *American Criminal Law Review*, Vol. 41 (1), 2004, 183-214;

PETRICH K., "Cows, Charcoal, and Cocaine: Al-Shabaab's Criminal Activities in the Horn of Africa", in *Studies in Conflict & Terrorism*, 2019, 1-22;

PICOTTI L., "Terrorismo e sistema penale: realtà, prospettive, limiti", in Diritto Penale Contemporaneo, Vol. 1, 2017, p. 249-263;

PICOTTI L., "Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali", Giuffrè, Milano, 1993;

PIETH M., "Criminalizing the financing of terrorism", in *Journal of International Criminal Justice*, 2006, Vol. (4) 5, 1074-1086;

PIETH M., AIOLFI G., "Anti-Money Laundering: Levelling the Playing Field", in *Basel Institute on Governance Working Paper Series – Working Paper 1*, 2003, 1-47;

PRENTIS M., "Digital Metal: Regulating Bitcoin as a Commodity", Case Western Reserve Law Review, 66 (2), 2015, 609-638;

PRESOTTO A., "Le modifiche agli artt. 270-*quater* e *quinquies* del codice penale per il contrasto al terrorismo", in *Diritto penale contemporaneo,* Vol. 1, 2017, p. 107-114;

RADICATI DI BROZOLO L. G., "Freezing the Assets of International Terrorist Organisations", in "Enforcing International Law Norms against Terrorism"; ed. By A. Bianchi, Hart Publishing, 2004, 377-413;

RAPHAELI N., "Financing of terrorism: sources, methods, and channels", in *Terrorism and Political Violence*, Vol. 15 (4), 2003, 59-82;

RAPOPORT D. C., "The four waves of modern terror. International dimensions and consequences", in *An international history of terrorism: Western and non-Western experiences*, edited by J. Hanhimäki and B. Blumenau, Routledge, 2013;

RISICATO L., "Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?", Giappichelli, Torino, 2019;

ROSAND E., "Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight against Terrorism", in *American Journal of International Law*, 2003, Vol. 97 (2), 333-341;

ROSAND E., "The Security Council's Efforts to Monitor the Implementation of Al Qaeda/Taliban Sanctions", in *The American Journal of International Law*, Vol. 98 (4), 2004, 745-763;

ROSAND E., "Resolution 1373 and the CTC: The Security Council's Capacity-building", in "International Cooperation in Counter-terrorism. The United Nations and Regional Organizations in the Fight Against Terrorism", ed. by G. Nesi, Ashgate, 2005, 81-88;

ROSI E., "Terrorismo internazionale: le nuove norme interne di prevenzione e repressione: Profili di diritto penale sostanziale", in *Diritto Penale e Processo*, Vol. 2, 2002, 148-163;

ROSSI F., "La circolarità dei modelli nazionali nel processo di armonizzazione europea delle legislazioni penali antiterrorismo", in *Diritto Penale Contemporaneo*, Vol. 1, 2017, pp. 176-190;

ROSSI F., "Il contrasto al terrorismo internazionale nelle fonti penali multilivello", Jovene, Napoli, 2022;

ROSTOW N., "Before and after: the changed UN response to terrorism since September 11th", in *Cornell International Law Journal*, 2002 Vol. (35) 3, 475-490;

RUDNER M., "'Electronic Jihad': the Internet as Al Qaeda's Catalyst for Global Terror", in *Studies in Conflict & Terrorism*, Vol. 40 (1), 2017, 10-23;

RUI J. P., SIEBER U., "NCBC in Europe – Bringing the Picture Together", in "Non-Conviction-Based Confiscation in Europe. Possibilities and Limitations on Rules Enabling Confiscation without a Criminal Conviction", ed. by J. P. Rui, U. Sieber, Duncker & Humblot, Berlin, 2015, 245-304;

SABIA R., "Delitti di terrorismo e responsabilità da reato degli enti tra legalità e esigenze di effettività", in *Diritto Penale Contemporaneo*, Vol. 1 (2017), 208-225;

SAKELLARAKI A., "EU Asset Recovery and Confiscation Regime – *Quo vadis*? A First Assessment of the Commission's Proposal to Further Harmonise the EU Asset Recovery and Confiscation Laws. A Step in the Right Direction?", in *New Journal of European Criminal Law*, Vol. 13 (4), 2022, 478-501;

SALAZAR L., "L'applicazione del principio del reciproco riconoscimento nel settore della confisca e del congelamento dei patrimoni criminali", in "Le sanzioni patrimoniali come moderno strumento di lotta contro il crimine: reciproco riconoscimento e prospettive di armonizzazione", ed. by A. M. Maugeri, Giuffrè, Milano, 2008, 539-555;

SANTINI S., "L'Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della Direttiva 2017/541", in *Diritto Penale Contemporaneo*, Vol. 7-8, 2017, 13-48;

SAUL B., "Defining Terrorism in International Law", Oxford University Press, 2006;

SAVAGE R., "Central African Republic launches 'Sango Coin' cryptocurrency amid industry rout", Reuters, 15 July 2022;

SCHMID A. P., "Terrorism. The Definitional Problem", in *Case Western Reserve Journal of International Law*, 2004, Vol. 36 (3), 375-420;

SCHWARZ N., CHEN K., POH K., JACKSON G., KAO K., FERNANDO F., MARKEVYCH M., "Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1). Some Legal and Practical Considerations", in *Fintech Notes*, International Monetary Fund, No. 2, October 2021, 1-15;

SCHWARZ N., CHEN K., POH K., JACKSON G., KAO K., FERNANDO F., MARKEVYCH M., "Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2). Some Legal and Practical Considerations", in *Fintech Notes*, International Monetary Fund, No. 2, October 2021, 1-11;

SCIARABBA V., "La Corte di giustizia, le misure antiterrorismo, i diritti fondamentali e la "Carta di Nizza": l'epilogo della vicenda Kadi", in *European rights Newsletter*, 2014, 1-31;

SIENA F. A., "The European anti-money laundering framework – At a turning point? The role of financial intelligence units", in *New Journal of European Criminal Law*, Vol. 13 (2), 2022, 216-146;

SIMONATO M., "Directive 2014/42/EU and non-conviction based confiscation. A step forward on Asset Recovery?", in *New Journal of European Criminal Law*, Vol. 6 (2), 2015, 213-228;

SINGH B., "The Talibanization of Sutheast Asia. Losing the war on terror to Islamist extremists", Praeger Security International, Westport, 2007;

SINGH B., "Crime-Terror Nexus in Southeast Asia: Case Study of the Abu Sayyaf Group", in *Counter Terrorist Trends and Analyses* - International Centre for Political Violence and Terrorism Research, Vol. (10) 9, 2018;

SKINNER K. K., "The Beginning of a New U.S. Grand Strategy. Policy on Terror during the Reagan Era", in "Reagan's Legacy in a World Transformed", edited by J. L. Chidester and P. Kengor, Harvard University Press, 2015;

SLAUGHTER A., "Sovereignty and power in networked world order", in *Stanford Journal of International Law*, Vol. 40 (2), 2004, 283-328;

SOANA G., "Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?", in *Economic Notes*, Wiley Online, 2021, 1-14;

STAMPNITZKY L., "Disciplining terror: how experts invented "terrorism"", Cambridge University Press, 2013;

STANISLAWSKI B. H., PEŁCZYŃSKA-NAŁĘCZ K., STRACHOTA K., FALKOWSKI M., CRANE D. M., LEVITSKY M., "Para-States, Quasi-States, and Black Spots: Perhaps Not States, but Not "Ungoverned Territories," Either", in *International Studies Review* , Vol.(10) 2, 2008, 366-396;

SUTTON G. W., "The new FATF Standards", in *George Mason Journal of International Commercial Law*, Vol. 4 (1), 2012, 68-136;

SWARTZ N. D., "Bursting the Bitcoin Bubble: The Case to Regulate Digital Currency as Security or Commodity", in *Tulane Journal of Technology and Intellectual Property*, 2014, Vol. 17, 319-336;

SZABO N., "Smart Contracts", 1994;

SZASZ C., "The security council starts legislating", in *American Journal of International Law*, 2002, Vol. 96 (4), 901-904;

TEBALDI M., " Le black lists nella lotta al terrorismo. Tra esigenze di sicurezza e tutele dei diritti", in *Diritto Penale Contemporaneo*, Vol. 7, 2018, 77-92;

THOMPSON E. A., "Misplaced Blame: Islam, Terrorism and the Origins of Hawala", in *Max Planck Yearbook of United Nations Law*, Vol. 11, 2007, 279-305;

THOMPSON J., "Examining Extremism: Jama'at Nasr al-Islam wal Muslimin", Center for Strategic & International Studies, 15 July 2021;

THOMPSON J., "Examining Extremism: Islamic State in the Greater Sahara", Center for Strategic & International Studies, 22 July 2021;

THURSTON A., "Boko Haram: The History of an African Jihadist Movement", Princeton University Press, 2018;

THURSTON A., "Why Jihadists are collecting Zakat in the Sahel", in *Political Violence at a Glance*, 12 July 2021;

TURNER N. W., "The financial action task force: international regulatory convergence through soft law" in *New York Law School Law Review*, Vol. 59 (3), 2014,

VACCANI M., "Alternative remittance systems and terrorism financing: issues in risk mitigation", World Bank Working Papers, 2010;

VALLEE C., "Jemaah Islamiyah: Another Manifestation of al Qaeda Core's Global Strategy", in *New Perspectives in Foreign Policy*, Issue 15, 2018, pp. 63-68;

VALSECCHI A., "Le modifiche alle norme incriminatrici in materia di terrorismo", in "Il nuovo 'pacchetto antiterrorismo", edited by R. E. Kostoris, F. Viganò, Giappichelli, Torino, 2015;

VALSECCHI A., "Per la prova della partecipazione all'Isis sono necessari e sufficienti contatti anche indiretti fra adepto e membri dell'organizzazione (accompagnati dall'adesione ideologica al programma terroristico)", in *Sistema Penale*, 15 March 2021;

VAN DEN HERIK L., SCHRIJVER N., "Eroding the Primacy of the UN System of Collective Security: The Judgment of the European Court of Justice in the Cases of Kadi and Al Barakaat", in *International Organizations Law Review*, Vol. 5 (2), 329-338;

VIDINO L., LEWIS J., MINES A., "Dollars for Daesh. Analyzing the Finances of American ISIS Supporters", The Georgetown Washington University, 2020, 1-48;

VIGANÒ F., "Il contrasto al terrorismo di matrice islamico-fondamentalistica: il diritto penale sostanziale", in "Terrorismo internazionale e diritto penale", edited by C. De Maglie, S. Seminara, CEDAM, Padova, 2007;

VIGANÒ F., "Sul contrasto al terrorismo di matrice islamica tramite il sistema penale, tra 'diritto penale del nemico' e legittimi bilanciamenti", in *Studi Urbinati, A - Scienze Giuridiche, Politiche Ed Economiche*, Vol. 58 (4), pp. 334-336;

WALZER M., "Just and Unjust Wars", 5th edition, Basic Books, New York, 2015;

WARDLAW G., "Political Terrorism: theory, tactics, and counter-measures", Cambridge University Press, 1982;

WAEVER O., "Securitization and Desecuritization", in "On Security", by R. D. LIPSCHUTZ, Columbia University Press, 1995;

WAEVER O., BUZAN B., DE WILDE J., "Security: a new framework for analysis", Lynne Rienne Publishers, 1998;

WEIGEND T., "Universal Terrorist", in *Journal of International Criminal Justice*, Vol. 4 (5), 2006, 912-932;

WENIN R., "Una riflessione comparata sulle norme in materia di addestramento per finalità di terrorismo", in *Diritto Penale Contemporaneo*, Vol. 4, 2016, p. 108-140;

WESSEL J., "The Financial Action Task Force: study in balancing sovereignty with equality in global administrative law", in *Widener Law Review*, Vol. 13 (1),2006, 169-198;

WESSEL R. A., " Introduction to the Forum – The Kadi Case: Toward a More Substantive Hierarchy in International Law", in *International Organizations Law Review*, Vol. 5 (2), 2008, 323-328;

WILLIAMSON M., "Terrorism, War and International Law. The Legality of the Use of Force Against Afghanistan in 2001", Ashgate, 2009;

WILLIS G. L., "Security Council Targeted Sanctions, Due Process and the 1267 Ombudsperson", in *Georgetown Journal of International Law*, Vol. 42 (3), 2011, 673-746;

YERMACK D., "Is Bitcoin a real currency? An economic appraisal", National Bureau of Economic Research – Working Paper 19747, December 2013, 1-22;

ZETZSCHE D. A., ANNUNZIATA F., ARNER D. W., BUCKLEY R. P., "The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy", in *Capital Markets Law Journal*, Vol. 16 (2), 2021, 203-225.

Acts and Documents

LEAGUE OF NATIONS

Convention for the Prevention and Punishment of Terrorism, League of Nations, Geneva, 1937.

UNITED NATIONS

CONVENTIONS

Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo, 1963); Convention for the Suppression of Unlawful Seizure of Aircraft (the Hague, 1970);

Convention on Psychotropic Substances (Vienna, 1971);

Single Convention on Narcotic Drugs, 1961 as amended by Protocol of 25 March 1972 (New York, 1975);

Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal, 1971) and its supplementary Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (Montreal, 1988);

Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973);

International Convention against the Taking of Hostages (1979);

Convention on the Physical Protection of Nuclear Material (Vienna, 1980);

Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (Rome, 1988);

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna, 1988);

Convention on the Marking of Plastic Explosives for the Purpose of Detection (Montreal, 1991); International Convention for the Suppression of Terrorist Bombings (1997);

International Convention for the Suppression of Terrorism Financing (New York, 1999);

United Nations Convention against Transnational Organized Crime and the Protocols Thereto (Palermo, 2000);

United Nations Convention against Corruption (New York, 2003);

International Convention for the Suppression of Acts of Nuclear Terrorism (New York, 2005).

RESOLUTIONS ADOPTED BY THE GENERAL ASSEMBLY

A/RES/27/3034 (1972), adopted at its 2114th plenary meeting on 18 December 1972;

A/RES/32/147 (1977), adopted at its 105th plenary meeting on 16 December 1977;

A/RES/34/145 (1979), adopted at its 105th plenary meeting on 17 December 1977;

A/RES/36/109 (1981), adopted at its 92nd plenary meeting on 10 December 1981;

A/RES/38/130 (1983), adopted at its 101st plenary meeting on 19 December 1983;

A/RES/48/122 (1993), adopted at its 85th plenary meeting on 20 December 1993;

A/RES/49/60 (1994), adopted at its 84th plenary meeting on 9 December 1994;

A/RES/49/185 (1994), adopted at its 94th plenary meeting on 23 December 1994;

A/RES/51/210 (1996), adopted at its 88th plenary meeting on 17 December 1996;

A/RES/53/108 (1998), adopted at its 83rd plenary meeting on 8 December 1998;

A/RES/60/288 (2006), adopted at its 99th plenary meeting on 8 September 2006;

A/RES/62/272 (2008), adopted at its 120th plenary meeting on 5 September 2008;

A/RES/64/235 (2009), adopted at its 68th plenary meeting on 24 December 2009;

A/RES/64/297 (2010), adopted at its 117th plenary meeting on 8 September 2010;

A/RES/62/71 (2007), adopted at its 62nd plenary meeting on 6 December 2007;

A/RES/66/282 (2012), adopted at its 120th plenary meeting on 29 June 2012;

A/RES/68/276 (2014), adopted at its 97th plenary meeting on 13 June 2014;

A/RES/70/291 (2016), adopted at its 110th plenary meeting on 1 July 2016;

A/RES/71/291 (2017), adopted at its 87th plenary meeting on 15 June 2017;

A/RES/72/284 (2018), adopted at its 101st plenary meeting on 26 June 2018;

A/RES/75/291 (2021), adopted at its 88th plenary meeting on 30 June 2021;

A/RES/76/121 (2021), adopted at its 49th plenary meeting on 9 December 2021.

RESOLUTIONS ADOPTED BY THE SECURITY COUNCIL

S/RES/232 (1966), adopted at the 1340th meeting on 16 December 1966;

S/RES/579 (1985), adopted by the Security Council at its 2637th meeting on 18 December 1985;

S/RES/661 (1990), adopted by the Security Council at its e 2933rd meeting on 6 August 1990;

S/RES/748 (1992), adopted by the Security Council at its 3063rd meeting on 31 March 1992;

S/RES/1044 (1996) adopted by the Security Council at its 3627th meeting on 31 January 1996;

S/RES/1127 (1997), adopted by the Security Council at its 3814th meeting on 28 August 1997;

S/RES/1173 (1998), adopted by the Security Council at its 3891st meeting on 12 June 1998;

S/RES/1176 (1998), adopted by the Security Council at its 3894th meeting on 24 June 1998;

S/RES/1189 (1998), adopted by the Security Council at its 3915th meeting, on 13 August 1998;

S/RES/1267 (1999), adopted by the Security Council at its 4051st meeting on 15 October 1999;

S/RES/1269 (1999), adopted by the Security Council at its 4053rd meeting on 19 October 1999;

S/RES/1333 (2000), adopted by the Security Council at its 4251st meeting on 19 December 2000.

S/RES/1363 (2001), adopted by the Security Council at its 4352nd meeting on 30 July 2001.

S/RES/1368 (2001), adopted by the Security Council at its 4370th meeting on 12 September 2001;

S/RES/1373 (2001) adopted by the Security Council at its 4385th meeting on 28 September 2001;

S/RES/1390 (2002), adopted by the Security Council at its 4452nd meeting on 16 January 2002;

S/RES/1452 (2002), adopted by the Security Council at its 4678th meeting on 20 December 2002;

S/RES/1455 (2003), adopted by the Security Council at its 4686th meeting on 17 January 2003;

S/RES/1483(2003), adopted by the Security Council at its 4761st meeting on 22 May 2003;

S/RES/1518 (2003), adopted by the Security Council at its 4872nd meeting on 24 November 2003;

S/RES/1526 (2004), adopted by the Security Council at its 4908th meeting on 30 January 2004;

S/RES/1535 (2004) adopted by the Security Council at its 4936th meeting, on 26 March 2004;

S/RES/1540 (2004), adopted by the Security Council at its 4956th meeting on 28 April 2004;

S/RES/1617 (2005) adopted by the Security Council at its 5244th meeting on 29 July 2005;

S/RES/1822 (2008), adopted by the Security Council at its 5928th meeting on 30 June 2008;

S/RES/1904 (2009), adopted by the Security Council at its 6247th meeting on 17 December 2009;

S/RES/1988 (2011), adopted by the Security Council at its 6557th meeting on 17 June 2011;

S/RES/1989 (2011) adopted by the Security Council at its 6557th meeting on 17 June 2011;

S/RES/2178 (2014) adopted by the Security Council at its 7272nd meeting on 24 September 2014;

S/RES/2195 (2014), adopted by the Security Council at its 7351st meeting, on 19 December 2014;

S/RES/2253 (2015) adopted by the Security Council at its 7587th meeting on 17 December 2015;

S/RES/2199 (2015) adopted by the Security Council at its 7379th meeting on 12 February 2015;

S/RES/2322 (2016), adopted by the Security Council at its 7831st meeting on 12 December 2016;

S/RES/2331 (2016), dopted by the Security Council at its 7847th meeting on 20 December 2016;

S/RES/2368 (2017) adopted by the Security Council at its 8007th meeting on 20 July 2017;

S/RES/2370 (2017), adopted by the Security Council at its 8017th meeting on 2 August 2017;

S/RES/2388 (2017), adopted by the Security Council at its 8111t meeting on 21 November 2017;

S/RES/2396 (2017), adopted by the Security Council at its 8148th meeting on 21 December 2017;

S/RES/2462 (2019), adopted by the Security Council at its 8496th meeting on 28 March 2019;

S67 2021.

REPORTS AND DOCUMENTS

Letter dated 3 November 1998 from the Permanent Representative of France to the United Nations addressed to the Secretary-General - Draft international convention for the suppression of terrorist financing, adopted by Sixth Committee of the General Assembly on 4 November 1998 (A/C.6/53/9);

S/2015/939, Special meeting of the Counter-Terrorism Committee on stemming the flow of foreign terrorist fighters adopted by the Security Council on 23 December 2015;

S/2018/1177, Addendum to the guiding principles on foreign terrorist fighters (2018) adopted by the Security Council on 28 December 2018;

"Responding to terrorist threats against soft targets", UN CTED Analytical Brief, United Nations Security Council Counter-Terrorism Committee Executive Directorate, 2019;

"Member States concerned by the growing and increasingly transnational threat of extreme right-wing terrorism", UN CTED Trends Alert, United Nations Security Council Counter-Terrorism Committee Executive Directorate, April 2020;

Joint Report of the Counter Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team on actions taken by Member States to disrupt terrorism financing, adopted by the Security Council on 3 June 2020 (S/2020/493);

Final Report of the Panel of Experts on Somalia, adopted by the Security Council on 28 September 2020 (S/2020/949);

Report on Civil Society Perspectives: ISIL in Africa – Key Trends and Developments, United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), April 2022, 10;

Fourteenth Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat, 28 January 2022 (S/2022/63);

Twenty-nineth Report of the Analytical Support and Sanctions Monitoring Team pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities, 3 February 2022 (S/2022/83);

"Concern over the use of proceeds from the exploitation, trade, and trafficking of natural resources for the purposes of terrorism financing", UN CTED Trends Alert, United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), June 2022.

FINANCIAL ACTION TASK FORCE (FATF)

"The FATF Recommendations", FATF (1990, 1996, 2003, 2004, 2012, 2018, 2022);

Report on "Terrorist Financing Typologies", FATF, 2008;

Report on "The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing", FATF, October 2013;

Report on "Risk of Terrorist Abuse in Non-Profit Organisations", FATF, June 2014;

Report on "Virtual Currencies Key Definitions and Potential AML/CFT Risk", FATF, June 2014;

Report on "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", FATF, February 2015;

Guidance for a risk-based approach on "Virtual Currencies", FATF, June 2015;

Report on “Emerging Terrorist Financing Risks”, FATF, October 2015;

Guidance for a risk-based approach on “Money or value transfer systems”, FATF, February 2016;

Report on “Terrorist Financing in West and Central Africa”, FATF-GIABA-GABAC, October 2016;

Report on “Financing of Recruitment for Terrorist Purposes”, FATF, January 2018;

Report on “Financial Flows from Human Trafficking”, FATF, July 2018;

Report to G20 Finance Ministers and Central Bank Governors, FATF, July 2018;

Mandate – Approved by the Ministers and the Representatives of the Financial Action Task Force, FATF, 12 April, 2019, Washington D.C.

Guidance for a risk-based approach on “Virtual Assets and Virtual Assets Service Providers”, FATF, June 2019;

Report on “Terrorist Financing Risk Assessment Guidance”, FATF, July 2019;

Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, FATF, June 2020;

Report on “Ethnic or Racially Motivated Terrorism”, FATF, June 2021;

Public Statement on the Financing of ISIL, Al Qaeda and Affiliates, FATF, 21 October 2021;

Report on “Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling”, FATF, March 2022;

FATF has added a specific Recommendation on cash couriers in 2004 (Special Recommendation IX),

FATF, “Virtual Currencies – Key Definitions and Potential AML/CFT Risks”, 2014,

Report on “Virtual Currencies – Key Definitions and Potential AML/CFT Risks”, FATF, June 2014

Guidance on “Proliferation financing risk assessment and mitigation”, FATF, June 2021;

Updated Guidance for a risk-based approach on "Virtual Assets and Virtual Assets Service Providers", FATF, October 2021;

"Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems", FATF, October 2021;

Report on "Targeted update on implementation of the FATF Standards on Virtual Assets and Virtual Assets Service Providers", FATF, June 2022.

INTERNATIONAL MONETARY FUND (IMF)

IMF Executive Board Concludes 2021 Article IV Consultation with El Salvador, Press Release, No. 22/13, International Monetary Fund, 25 January 2022.

WORLD BANK

Bitcoin Versus Electronic Money, World Bank, 2014;

Guidance Manual on "Virtual Assets and Virtual Assets Service Providers. ML/TF Risk Assessment Tool", World Bank Group, June 2022.

FINANCIAL STABILITY BOARD (FSB)

Crypto-asset markets Potential channels for future financial stability implications, FSB, 10 October 2018;

Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements Final Report and High-Level Recommendations, FSB, 13 October 2020;

Regulation, Supervision and Oversight of "Global Stablecoin Arrangements Progress Report on the implementation of the FSB High-Level Recommendations", FSB, 7 October 2021;

Assessment of Risks to Financial Stability from Crypto-assets, FSB, 16 February 2022;

Statement on International Regulation and Supervision of Crypto-asset Activities, FSB, 11 July 2022;

Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements - Consultative report, FSB, 11 October 2022;

Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets Consultative document, FSB, 11 October 2022;

International Regulation of Crypto-asset Activities A proposed framework – questions for consultation, FSB, 11 October 2022.

INTERNATIONAL ORGANISATION OF SECURITIES COMMISSION (IOSCO)

Research Report on Financial Technologies (Fintech), IOSCO, February 2017;

Communication on Concerns related to Initial Coin Offerings (ICOs), IOSCO Board, Madrid, 18 January 2018 (IOSCO/MR/01/2018);

Consultation Report on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms, IOSCO Board, CR02/2019, May 2019;

Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms Final Report, IOSCO, February 2020;

Public Report on Stablecoins Initiatives, IOSCO, March 2020 (OR01/2020);

Crypto-Asset Roadmap for 2022-2023, IOSCO, 7 July 2022.

BASEL COMMITTEE ON BANKING SUPERVISION (BCBS)

Statement on crypto assets, BCBS, 13 March 2019;

Guidelines on sound management of risks related to money laundering and financing of terrorism, BCBS, January 2014 (rev. July 2020);

Prudential treatment of cryptoasset exposure – Consultative document, BCBS, June 2021;

Second consultation on the prudential treatment of cryptoasset exposures, BCBS, June 2022.

COUNCIL OF EUROPE

European Convention on the Suppression of Terrorism (ETS No. 090), Strasbourg 27 January 1977;

Declaration of the Committee of Ministers on the fight against international terrorism, Council of Europe – Committee of Ministers, 12 September 2001;

Decision on the fight against international terrorism (Committee of Ministers' Declaration of 12 September 2001), Council of Europe – Committee of Ministers, 21 September 2001;

Protocol amending the European Convention on the Suppression of Terrorism" (ETS 190), Strasbourg, 15 May 2003;

Convention on the Prevention of Terrorism (CETS 196), Warsaw, 16 May 2005;

Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198) , Warsaw16 May 2005;

Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (CETS 217), Riga, 22 October 2015.

Council Of Europe Committee on Counter-Terrorism (CDCT), 9th Plenary Meeting, Strasbourg, 30-2 December 2022.

EUROPEAN UNION

ACTS

Council Directive of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (91 /308/EEC);

Joint Action of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime (98/699/JHA);

Joint Action of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union (98/733/JHA);

Council Recommendation of 9 December 1999 on cooperation in combating the financing of terrorist groups, (1999/C 373/01);

Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA);

Proposal for a Council Framework Decision on combating terrorism, 19 September 2001 (COM(2001)521 final);

Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001, (SN 140/01);

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering;

Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/930/CFSP);

Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP);

Council Framework Decision of 13 June 2002 on combating terrorism (2002/4 Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism;

Council Common Position 2003/140/CFSP of 27 February 2003 concerning exceptions to the restrictive measures imposed by Common Position 2002/402/CFSP;

Council Regulation (EC) No 561/2003 of 27 March 2003 amending, as regards exceptions to the freezing of funds and economic resources, Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban;

European Security Strategy – A secure Europe in a better world, Council of the European Union, 8 December 2003 (15895/03);

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;

Declaration on Combating Terrorism, European Council, Brussels, 25 March 2004;

Council Framework Decision 2005/212/JHA of 24 February 2005 on Confiscation of Crime-Related Proceeds, Instrumentalities and Property;

Communication from the Commission to the Council and the European Parliament, "The Hague Programme: Ten priorities for the next five years The Partnership for European renewal in the field of Freedom, Security and Justice", Brussels, 10.5.2005, COM(2005) 184 final;

The European Union Counter-Terrorism Strategy, Council of the European Union, 14469/4/05 REV 4, 30 November 2005;

Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders;

Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime;

Commission Regulation (EC) No. 1190/2008 of 28 November 2008 amending for the 101st time Council Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban;

Council Framework Decision of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (2008/919/JHA);

Directive 2009/110/EC of the European Union and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC;

"The Stockholm Programme - An open and secure Europe serving and protecting the citizen", European Council, 4 May 2010 (2010/C 115/01);

Directive 2014/42/EU of the European Parliament and of the of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union;

Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine;

"The European Agenda on Security", Communication form the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 28 April 2015 (COM(2015) 185 final);

Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC;

Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing, 2 February 2016, (COM(2016) 50 final);

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA;

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

Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders;

Regulation (EU)2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods;

Communication from the Commission to the European Parliament and the Council "Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework" 24.7.2019 (COM(2019) 360 final);

Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the

internal market and relating to cross-border activities, 24.7.2019 (COM(2019) 370 final);

Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, 13.5.2020 (2020/C 164/06).

European Parliament Resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission's Action Plan and other recent developments (2020/2686(RSP)).

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of Regions on the EU Security Union Strategy, 24.7.2020 (COM (2020) 605);

Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937, 24.9.2020 (COM/2020/593 final);

Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937;

Council Conclusions on anti-money laundering and countering the financing of terrorism, 5.11.2020 (12608/20);

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee of the Regions: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 9.12.2020 (COM (2020) 795 final);

Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, 20.7.2021 (COM (2021) 420 final);

Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, 20.7.2021 (COM (2021) 421 final);

Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets, 20.7.2021 (COM(2021) 422 final);

Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use

of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, 20.7.2021, (COM (2021) 423 final).

Special meeting of the European Council (24 February 2022) – Conclusions, European Council, EUCO 18/22.

Council Decision (CFSP) 2022/578 of 8 April 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine;

Council Regulation (EU) 2022/2474 of 16 December 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

DOCUMENTS

"Virtual Currency Schemes", European Central Bank, October 2012;

"Opinion on 'virtual currencies'", European Banking Authority, 4 July 2014 (EBA/Op/2014/08);

Study on "Virtual Currencies and Terrorism financing: assessing the risks and evaluating responses", European Parliament, 2018;

"Study on the payment attitudes of consumers in the euro area (SPACE)", European Central Bank, December 2020;

Internet Organised Crime Threat Assessment (IOCTA), EUROPOL, 2021;

Spotlight on "Cryptocurrencies: tracing the evolution of criminal finances", EUROPOL, 26 January 2022;

European Union Terrorism Situation & Trend Report (TESAT), EUROPOL, 14 July 2022;

"Crypto Assets" – Frequently asked questions, Finance - European Commission, 11 April 2022.

NATIONAL REPORTS

BUSH G. W., Address to the Joint Session of the 107th Congress, 20 September 2001, in *Selected Speeches of President George W. Bush 2001 – 2008*, White House Archives, 65-75;

"The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Report)", U.S. Government, 22 July 2004;

"Country Reports on Terrorism 2020", U.S. Department of State, December 2021;

"Annual Threat Assessment of the U.S. Intelligence Community", Office of the Director of National Intelligence, 7 February 2022;

"2022 National Terrorist Financing Risk Assessment", U.S. Treasury Department, February 2022, 6.

"Progress of Research & Development Development of E-CNY in China", People's Bank of China, July 2021.

Regulation of Cryptocurrency Around the World: November 2021 Update", U.S. Library of the Congress, November 2021.

CASE LAW

EUROPEAN UNION

Case T-315/01, *Kadi v. Council of the European Union and Commission of the European Communities*, 21 September 2005;

Joined Opinion of Advocate General Mengozzi, 26 October 2006, par. 55, Case C-355/04 P;

Case C-355/04 P, *Segi and Others v. Council of the European Union*, 27 February 2007;

Joined Cases C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, 3 September 2008;

Case T-85/09, *Kadi v. Commission*, 30 September 2010;

Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, *Commission and Others v. Kadi*, 18 July 2013.

EUROPEAN COURT OF HUMAN RIGHTS

ECtHR, Grand Chamber, *Nada v. Switzerland*, 12 September 2012;

ECtHR Grand Chambre, *Case Al-Dulimi And Montana Management Inc. v. Switzerland*, 21 June 2016.

ITALY

Cass. pen., sez. I, 15 June 2006 (dep. 19 September 2006), No. 30824;

Cass. pen., sez. I, 11 October 2006, (dep. 17 January 2007), No. 1072;

Court of Assise of Milan, 19 December 2016 (dep. 24 February 2017), No. 8;

Cass., Sez. V, 18 December 2020 (dep. 4 March 2021), n. 8891.